IJACSA
WHERE WISDOM SHARES
International Journal of Advanced Computer Science and Applications

Special Issue

Wireless & Mobile Networks

ISSN 2156-5570(Online)
ISSN 2158-107X(Print)

www.ijacsa.thesai.org

INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS

A Publication of
The Science and Information Organization

International Journal of Advanced Computer Science and Applications

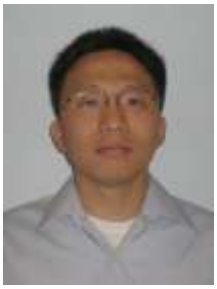
Special Issue on Wireless and Mobile Networks

Scope of this Issue:

The range of topics covered by Special Issue on Wireless & Mobile Networks includes the following areas:

- ***Architectures, protocols, and algorithms to cope with mobile & wireless Networks***
- ***Distributed algorithms of mobile computing***
- ***OS and middle ware support for mobile computing and networking***
- ***Routing and communication primitives in ad-hoc and sensor networks***
- ***Synchronization and scheduling issues in mobile and ad hoc networks***
- ***Data management on mobile and wireless computing***
- ***Integration of wired and wireless networks***
- ***Broadband access networks***
- ***Complexity analysis of algorithms for mobile environments***
- ***Information access in wireless networks***
- ***Cryptography, security and privacy of mobile & wireless networks***
- ***Performance of mobile and wireless networks and systems***
- ***Wireless multimedia systems***
- ***Recent trends in mobile and wireless applications***

IJACSA Special Issue Guest Editors



Dr. Zuqing Zhu
Associate Professor
University of Science and Technology of China, China

Dr. Zuqing Zhu received his PhD degrees from the Department of Electrical and Computer Engineering, University of California, Davis. After that, Dr. Zhu joined the Service Provider Technology Group of Cisco Systems, San Jose.

In Jan. 2011, Dr. Zhu joined the School of Information Science and Technology in the University of Science and Technology of China, as an Associate Professor. Dr. Zhu has published more than 40 peer-reviewed technical papers in the journals and conferences. Dr .Zhu also serves as an Editor for Elsevier Journal of Optical Switching and Networking (OSN), Springer Telecommunication Systems Journal (TSMJ), Springer Networking and Electronic Commerce Journal (NAEC) and 10 other well-known journals.

Dr.Ka Lok Man
Senior Lecturer
Xi'an Jiaotong-Liverpool University (XJTLU), China

Dr. Ka Lok Man is a Senior Lecturer in the Department of Computer Science and Software Engineering at the Xi'an Jiaotong-Liverpool University, China; and a Visiting Professor at the Myongji university, Korea.

His research interests include design, analysis and tools for integrated circuits and systems; formal methods; process algebras; real-time, hybrid systems and physical cyber systems; communication and wireless sensor networks.
On the above-mentioned topics, he has authored or co-authored about 120 refereed publications including books, edited books, journal articles, book chapters and conference proceedings.

Mr.Mohd Helmy Abd Wahab
Lecturer
Universiti Tun Hussein Onn Malaysia, Malaysia

Mohd Helmy Abd Wahab is a lecturer at the Department of Computer Engineering, Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia (UTHM). He received a Bachelor of Information Technology with Honours from Universiti Utara Malaysia and Master of Science (Intelligent System) from the same university in 2002 and 2004 respectively.

His research interests are in data mining, artificial intelligence, mobile and wireless computing and web-based applications. He has published more than 100 papers in various journals and conferences at national and international level. He is a member of IEEE, IEEE Computer Society, IAEng, and IACSIT

IJACSA Editorial

From the Desk of Managing Editor…

It is a pleasure to present our readers with the Special Issue on Wireless and Mobile Networks of International Journal of Advanced Computer Science and Applications (IJACSA). What is particularly attractive and significant in the present issue is the range of applications that is covered. It is a timely and refreshing addition to the knowledge base in the practical application of wireless and mobile networks.

This special issue is devoted to the topic of the latest research and development on wireless and mobile networks. We do not wish to repeat here the significance and the challenges of developing a special issue of this nature on a subject of such complexity and variety. The coverage is quite broad while the treatment is in depth where needed. Our focus is squarely on experimental research, rather than on work that is largely descriptive.

The wireless communication revolution is bringing fundamental changes to data networking, telecommunication, and is making integrated networks a reality. By freeing the user from the cord, personal communications networks, wireless LAN's, mobile radio networks and cellular systems, harbour the promise of fully distributed mobile computing and communications, anytime, anywhere.

Wireless technology is a truly revolutionary paradigm shift, enabling multimedia communications between people and devices from any location. It also underpins exciting applications such as sensor networks, smart homes, telemedicine, and automated highways. This book provides a comprehensive introduction to the underlying theory, design techniques and analytical tools of wireless communications, focusing primarily on the core principles of wireless system design.

Focusing on the networking and user aspects of the field, Wireless Networks provides a global forum for archival value contributions documenting these fast growing areas of interest. The journal has published this special issue consisting of refereed articles dealing with research, experience and management issues of wireless and mobile networks. Its aim is to allow the reader to benefit from experience, problems and solutions described.

On behalf of the Journal we wish to extend our sincere thanks to all our Guest Editors for their precious time and hard work.

We hope to continue exploring the always diverse and often astonishing fields in Advanced Computer Science and Applications.

Thank You for Sharing Wisdom!

Managing Editor
IJACSA
Special Issue on Wireless and Mobile Networks
25 August 2011
editorijacsa@thesai.org
ISSN 2156-5570 (Online)
ISSN 2158-107X (Print)

CONTENTS

Simulation and Evaluation of a Simple Adaptive Antenna Array for a WCDMA Mobile Communication

Idigo V.E, Ifeagwu E.N,Azubogu A.C.O, Akpado K.A., Oguejiofor O.S
Department of Electronics and Computer Engineering, Nnamdi Azikiwe University Awka

***Abstract*— This paper presents a uniform Linear Array model of a simple adaptive antenna array based on signal-to-interference and noise ratio (SINR) maximization. The SINR using the adaptive antenna array was investigated for a conventional narrowband beam former by varying the number of antenna array elements and number of interfering signals or users. The results obtained were compared with that of omni-directional antenna. The graph obtained from the results showed significant improvement in SINR as the number of antenna elements increases in the presence of large interferers for odd numbered array.**

Keywords-Smartantenna; bandwidth; SINR; adaptive beam forming.

I. INTRODUCTION

The Smart antennas technology is one of the leading innovations for achieving highly efficient networks that maximize network capacity and improve quality of service and coverage. Smart Antennas are arrays of antenna elements that change their antenna pattern dynamically to adjust to the noise, interference in the channel and mitigate multipath fading effects on the signal of interest[1]. In other words, smart antenna has a pattern that is not fixed but adapts to current radio conditions ,and nulls out the interferers. Smart antenna systems are classified into three levels of intelligence on the basis of their transmit strategy [2,3].

Smart antennas provide greater capacity and performance benefits than omni-directional antennas because they can be used to customize and fine-tune antenna coverage pattern to the changing traffic or radio frequency (RF) conditions in a wireless communication system like the WCDMA network.

Beam forming (BF) in smart antenna technology is a process in which each user's signals is multiplied by complex weight vectors that adjust the magnitude and phase of the signal from each antenna element [4]. The beam forming appropriately combines the signals received by different elements of an antenna array to form a single output[5]. Many adaptive algorithms have been developed to determine the optimal weight vectors of antenna array elements dynamically, based on different performance criteria.

The weight vectors produce the desired radiation pattern that can be changed dynamically.

II. BLOCK DIAGRAM AND IMPLEMENTATION.

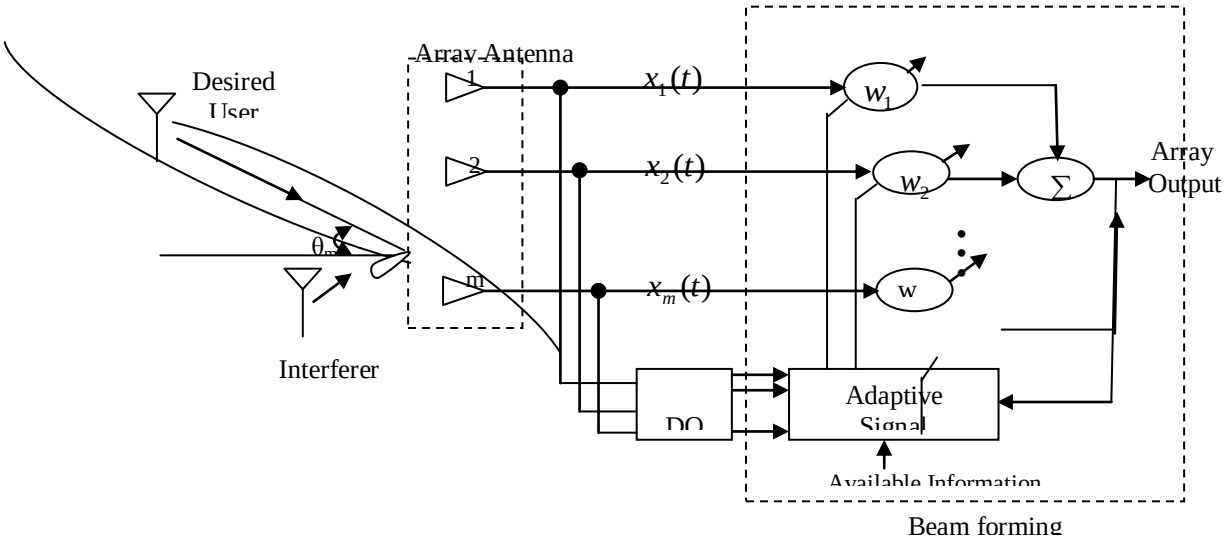


Figure 1: Functional Block Diagram of an Adaptive Antenna System [6]

The block diagram of a simple adaptive antenna array is shown in Fig.1.The signals induced on an antenna array are multiplied by the adjustable complex weights

(w_1, w_2……..w_m) and then combined to form the system output using adaptive beam forming algorithm[7].

A. Mean path loss

The path loss is used to describe the attenuation of radio signal as it travels in space[8]. The path loss model to be considered here is that of an outdoor environment.

When there are no obstacles between the BS and MS, the propagation characteristics are subject to free space propagation.

In this case, the path loss is given by :

$$LP_f\,(dB) = 32.44 + 20\log_{10}f_c + 20\log_{10}d \quad (1)$$

Where LP_f is the free space path loss, fc is the carriers' frequency in (MHz), d is the distance between the BS and MS in (Km).

In the presence of obstacles the path loss model for urban and suburban environment are as follows [9]

$LP(dB)= 69.55 + 26.16\log_{10}f_c + (44.9\text{-}6.55\log_{10}h_b)+\log d\text{-}13.82\log h_b$ - □(hm) (2)

Where □(hm) is the correlation factor for MS antenna height, h_b is the height of BS (km).

The correlation factor □(h_m) for MS antenna height is evaluated as

1) for large cities.

□ (h_m) = $8.29[\log_{10}(1.54hm)]^2 - 1.1$,

$f_c \leq 200$ MHz

$=3.2\,[\log10(11.57hm)]2 - 4.97$,

$f_c \geq 400$MHz (3)

Where h_m is the height of MS.

2) For small and medium size cities

□(hm) = $[1.1\log_{10}f_c - 0.7]h_m - [1.56\log fc - 0.8]$ (4)

For suburban area:

$Lp_s = Lp - 2[\log_{10}(fc/28)]^2 - 5.4$ (5)

For rural area:

$Lp0 = Lp - 4.78(\log_{10}f_c)^2 + 18.33\log_{10}f_c - 40.94$ [dB] (6)

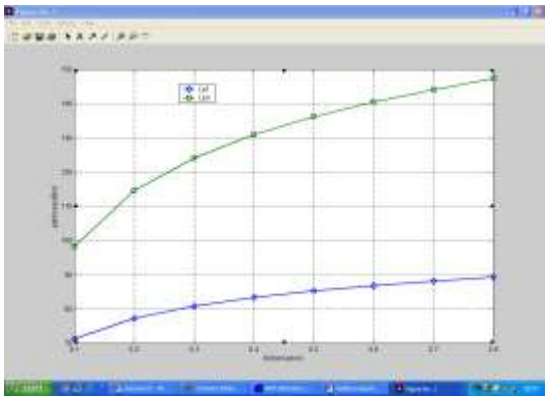


Figure 2. Path loss vs distance for a typical suburban area (with BS opposite B-division police station, awka).

The path loss in figure 2. is obtained for a suburban environment with the BS at B-division Police station opposite new state secretariat, Awka. The CDMA operator is Visafone Nigeria and the carrier frequency, f_c was set at 878.1325MHz and reference power level is -30dBm. The height of the base station, h_b is 120ft (0.03658km) and that of mobile station, h_{ms} is taken to be 6ft (0.00183km).

To compute the path loss and the graph of figure 2 Matlab was used. The graph shows that path loss increases with distance. This path loss would be minimized or completely eliminated if adaptive antenna array is deployed at the BS.

III. RESULTS AND ANALYSIS.

A cell model deploying adaptive antenna array at BS is presented and received signal at the antenna elements is simulated and modeled by considering uniform linear array model. A real time measurement of signal strength, distance of MS from BS, and AOA of arriving signal from uplink is carried out at a test bed belonging to Visafone Nigeria which is a CDMA carrier situated at B-division police station, Awka.

To evaluate the path loss of a typical WCDMA environment we deployed sectorized antenna at the BS. The results obtained are helpful in the simulation and performance analysis of adaptive antenna array. All simulations are done in Matlab

A. Strength and AOA measurement.

The measurements were carried out using mobile monitoring system (MMS) equipment belonging to Nigerian Communication Commission, NCC. The signal strength is measured using spectrum analyzer and the AOA is seen on the visualizer.

TABLE 1: SIGNAL STRENGTH (DBM) AND AOA (^{0}) MEASUREMENTS.

Distance (m)	Signal strength (dBm)	AOA (^{0})
100	-35.50	15
200	-46.29	20
300	-38.24	28
400	-30.03	30
500	33.59	118
600	42.67	105
700	-40.00	89
800	-40.17	74

The measured results were obtained using base height (120ft),power level

(-30dBm),central frequency(878.1325Hz).

TABLE 2: SINR WHEN THE NUMBER OF INTERFERERS IS TWO.

M	SINR (d=0.5λ)	SINR (d=0.75λ)
1	0.50	0.50
2	0.10	0.45
3	159.89	177.05
4	9.97	838.13
5	526.11	1899.80
6	43.81	2310.70
7	1103.30	1293.50
8	102.54	160.06
9	1549.70	1012.30
10	125.66	1167.40
11	1421.30	764.61
12	63.86	100.57

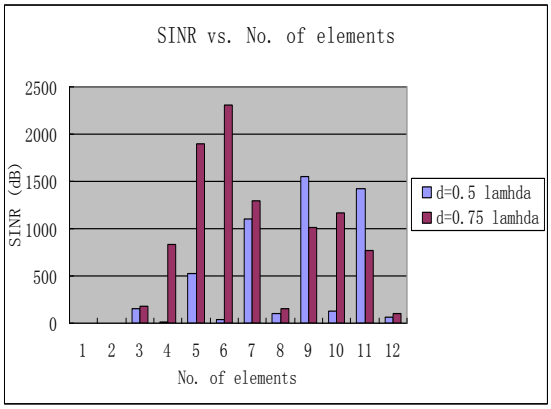


Figure 2. SINR vs. No. of antenna elements in the presence of two interferers.

Figure 2. shows that there is significant improvement in the SINR as the inter-element spacing increases between 1-element and 6-element array. Better performance is achieved in real time with inter-element spacing of 0.5λ as seen in figure 2 when M = 5, 7, 9 or 11.

TABLE 3: SINR OF OMNI-DIRECTIONAL ANTENNA AND 2-ELEMENT ARRAY.

No. of interferers	SINR for Omni-directional	SINR for 2-array
2	0.50	0.10
4	0.25	0.60
6	0.17	0.81
8	0.13	0.88
10	0.10	0.92
12	0.08	0.94

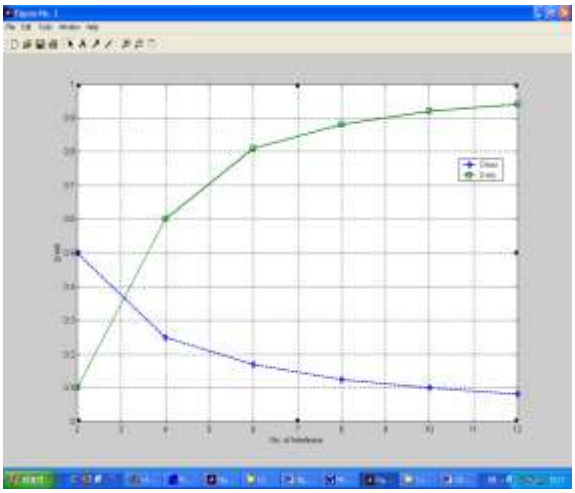


Fig. 3: SINR of Omni-directional antenna and 2-element array.

Figure 3. shows that adaptive antenna array increases the SINR as the number of interferers increases, while the omni-directional decreases the SINR as the number of interferers increases..

IV. SUMMARY OF RESULTS.

The graphs obtained for SINR vs. No. of antenna elements showed that better performance is achieved as the number of antenna elements and interferers increase with inter-element spacing of 0.5λ. The graphs for SINR against the number of interferers reveals that odd numbered arrays give significant performance improvement compared to their even numbered counterpart for our model.

Therefore, from the analysis, 9-ary or 11-ary would be the best choice for designers . Since our interest is in deploying a simple adaptive antenna at BS, 5-element and 7-element arrays are ideal for the proposed system as they also showed significant improvement in SINR over standard antennas. The graphs also reveal over 9 folds SINR for 2-ary against omni-directional antenna system while higher arrays showed over 1500 folds in the presence of large interferers

V. CONCLUSION

From the charts, it was observed that the signal-to-interference and noise ratio depends on the number of antenna element, the inter-element spacing between the arrays and the number of interferers.

There was great improvement in the SINR when odd numbered elements were used with inter-element spacing of $d=0.5\lambda$ in the presence of large interferers. Adaptive antenna as observed from our analysis showed greater improvement in the SINR over omni-directional antenna in the presence of large interferers.

Finally, improving the interference suppression and noise reduction capabilities of any antenna system in the presence of large interferers, increases the capacity of that system deploying such an antenna. Therefore, adaptive antenna proposed here will increase capacity of a WCDMA network.

REFERENCES

[1] A.Boukalov "Introduction to smart Antenna Technologies and Algorithms'', 2009, workshop on smart Antenna Technology and Application, RAWCON.

[2] A.F. Naguib "Adaptive Antenna for CDMA wireless Networks", 2008, Department of Electrical Engineering, Stanford University.

[3] S. R. Saunders, "Antennas and propagation for wireless communication systems", 2009, John Wiley and son.

[4] Bernard Widrow and Samuel D. Stearns, "Adaptive Signal Processing," 2008, Prentice Hall, New Jersey.

[5] J. Fuhl, A. Kuchar, and E. Bonek, "Capacity increase in cellular PCS by smart antennas", 2007, IEEE Transactions on Vehicular Technology, vol.3, pp. 1962 – 1966.0

[6] R. Kawitkar, "Issues in deploying smart Antennas in Moblie Radio Networks," 2008, Proceeding World Academy of Science, Engineering And Technology, vol 31.

[7] Applebaum S. "Adaptive Arrays," 2008, IEEE Transactions on Antenna and propagation, vol 24, No 5, pp 585-598.

[8] Chris Loadman, Zhizhang chen, and Dylan Jorgensen, "An Overview of Adaptive Antenna Technologies for wireless communication", 2009, Communication Networks and service Research conference, New Brunwick, Canada.

[9] J.H Winters, "Smart Antenna Techniques and their application to wireless Ad-hoc networks", 2006, IEEE Trans. On Wireless communication, vol.13, pp 77-83.

Video Transmission over Cognitive Radio TDMA Networks under Collision Errors

Abdelaali CHAOUB
Laboratory of Electronic and Communication
Mohammadia School of Engineers,
Mohammed V-Agdal University
Rabat, Morocco

Elhassane IBN ELHAJ
Department of Telecommunication
National Institute of Posts and Telecommunications
Rabat, Morocco
IEEE Member

Jamal EL ABBADI
Laboratory of Electronic and Communication
Mohammadia School of Engineers,
Mohammed V-Agdal University
Rabat, Morocco

***Abstract*—Cognitive Radio (CR) networks are emerging as new paradigm of communication and channels sharing in multimedia and wireless networks. In this paper, we address the problem of video transmission over shared CR networks using progressive compression source coding associated to fountain codes. We consider a TDMA-based transmission where many subscribers share the same infrastructure. Each Secondary User (SU) is assigned one time slot where he transmits with a certain probability. The given model allows each SU to transmit opportunistically in the remaining slots. Therefore, packets are not only corrupted by reason of Primary traffic interruptions, but also we consider losses caused by collisions between several SUs due to the Opportunistic Spectrum Sharing. We use a redundancy-based model for link maintenance to compensate for the loss of spectrum resources caused by the primary traffic reclaims. Moreover, we setup up many Secondary User Links to mitigate the collision effects. Numerical simulations are performed to evaluate the proposed approaches in view of the average Goodput. We conduct a stability and performance analysis of the system and we highlight the achieved gains when using our transmission model.**

Keywords-component; Cognitive Radio network; video transmission; TDMA; progressive compression source coding, LT codes; Collision; Goodput.

I. INTRODUCTION

Mobile and multimedia communications services have experienced a great evolution over the last decades. Increasing demand for the frequency spectrum resource makes the radio spectrum more precious. This finding is reinforced by the frequency allocation charts around the world [1]. On the other hand, actual observations of the spectrum occupancy taken on some bands reveal the low and discontinuous usage of the licensed spectrum in time and space [2, 3]. Hence the emergence of the Cognitive Radio [4] as a new paradigm to find strategies for enhancing and sustaining the growth of multimedia and wireless networks with limited spectrum.

The CR concept has been proposed in the objective of improving the spectral resources utilization and management. Cognitive devices are allowed to occupy the spectrum that has been left vacant by licensed users. Therefore, every telecommunication system will be divided into two networks: a primary network called Primary Users (PUs), which owns the spectrum license and has full rights on it, and a secondary network called Secondary Users (SUs), which is allowed to use the primary network's bandwidth in case of PU absence. In order to enable the coexistence of both primary and secondary networks within the same architecture, regulatory authorities [5] aim at exploiting the notions of Negotiated and Opportunistic Spectrum Sharing (OSA) for CR networks.

The OSA [6] is a core technique in Cognitive Radio networks to exploit the temporarily unused spectral resources. Licensed spectrum bands are continuously sensed to detect the unoccupied spectrum hole. From that sensing-derived information, Secondary User Links (SULs) are formed from a composition of multiple subchannels (SCs) currently not in use by licensed users. Subchannels selected to create a SUL should be scattered over multiple PU frequencies. The advantages of this principle are two fold: (1) it limits performance degradation due to the interference caused by primary reappearance; (2) it reduces the number of jammed subchannels once the primary user appears during the lifetime of a SUL.

In summary, the Cognitive Radio solution is introduced as an enabling technology for managing and controlling the frequency spectrum allocation. It has gained considerable maturity during the last years. This emerging approach not only promises great future technological advances and seems to meet many needs of today, but also could be exploited for enhancing a wide range of legacy technologies in particular those frequency-spectrum-based like wireless networks [7].

A wireless network refers to, as its name suggests, a network in which at least two devices could communicate without a wire connection, it is among the largest communication technology worldwide. The explosive growth of wireless services, as internet and multimedia, has increased the need for more quality of service and bandwidth. This standard is completely based on the radio frequency resource and in fact influenced by the scarcity of radio spectrum. That's way, in many works [8, 9, 10], the Cognitive Radio generates a big interest as a key cost-effective solution for the underutilization of frequency spectrum in wireless communication networks. Cognitive Radio based wireless networks promote the objective of supporting large volumes of customers, very important for operators and industrials. The tricky part is tailoring the legacy wireless services to suit the specificities of the CR context, which makes the problem of

studying the scalable video transmission over CR networks challenging.

Furthermore, there exist many research efforts on the problem of secondary traffic transmission over Cognitive Radio networks (Fig. 1). In [11], Kushwaha, Xing, Chandramouli and Heffes have studied the transmission of multimedia traffic over CR networks, the primary traffic arrival was modelled as a Poisson process and Luby Transform (LT) code (Fig. 2) [12] has been used as channel correcting code and also for some coordination reasons. They have proposed a QoS metric to order the available subchannels in the decreasing order of their quality to establish the transmission link efficiently. They investigate the spectral efficiency of the selected SUL in terms of successful transmission probability of the required number of packets needed for recovering the original multimedia stream. Unfortunately, this study has not considered the opportunistic aspect of the network (Fig. 5) where many SUs transmit in the same CR network and consequently there is an additional packets loss average due to collision effects which degrades considerably the spectral efficiency of the system. In [13], Cuiran and Chengshu have investigated the successful transmission over Cognitive Radio networks shared by several SUs (Fig. 1) using the TDMA technique. They have assumed a slotted transmission; each SU transmits in his assigned slot and can transmit in the other slots with certain probability. The results have been presented in terms of throughput and energy efficiency. They have considered that the only reception failure reason would be packet collisions due to time sharing. This study has not taken into account the interference effects caused by the primary user appearance. The reception failure depends also on the Primary traffic type and arrival model which affects the reception of the whole transmitted message. In addition, it may happen that the SU does not transmit data in his own slot because there may be no data to transfer, hence the probability that the secondary device transmits in his assigned slot should be, in practice, less than one.

In previous work [14], we have done some contribution on the problem of image transmission over lossy networks using progressive source coding associated to fountain codes where the stream delivery is reinforced by the use of Unequal Error Protection based on the block duplication technique. Currently, our work is addressing the video transmission problem through shared Cognitive Radio networks (Fig. 1). That is, our aim is to develop a compression scheme that allows us to generate multiple levels of quality using multiple layers simultaneously with a network delivery protection model that allows us to deliver subsets of layers to a given population of receivers over unreliable subchannels. So, the same issue has been already treated in [15] by using fountain codes under different subchannel selection policies in a fading environment with the assumption that the primary traffic arrival follows a Poisson process. Herein, we consider the binomial traffics used instead of Poisson where there are a finite number of sources. The given distribution is associated to the general model for link maintenance introduced in [16] (Fig. 3). Some redundancy is added to the secondary applications to combat the interruptions caused by the primary traffic arrival. After sending the message, the used spectrum bands are sensed and the SULs will be restructured in case some packets got lost as a consequence of the PU appearance. We assume a slotted transmission (Fig. 3) and we adopt the TDMA method as a network sharing technique. TDMA allows sharing the same CR infrastructure among multiple subscribers (SUs). The secondary traffic is divided into different time slots (Fig. 5). We consider a centralized scheduler that allocates to each subscriber SU_i the time slot i with some probability q. Nevertheless, the scheduler tries to maximize the achieved secondary Goodput by using the OSA feature of CR networks, so SU_i is allowed to use opportunistically the other slots, let p be the probability that this SU transmits in the remaining slots $j \neq i$ (Fig. 5). The transmission performance on the proposed network model, as the realistic case, is mainly affected by two crucial aspects: (1) interferences caused by the primary traffic arrival leading to more corrupted secondary packets, and (2) packets may collide with one another regarding the fact that each SU attempts to transmit in other slots reserved for other SUs. In our Cognitive Radio network model, collision is defined as the fact that two or more SUs attempt to transmit a packet or many packets across the same Secondary User Link at the same time. Throughout the paper, we develop a system for video transmission based on Joint Source Channel Coding approach. More precisely, we propose to combine a progressive source coder like Set Partitioning in Hierarchical Trees (SPIHT) [17] as the source coding with a fountain code [18] like LT (Luby Transform) codes [12] as the channel coder. The proposed scheme has already shown his benefits and effectiveness in [19]. SPIHT is a high quality source coder based on wavelets, it produces a fully progressive code which means that if the transmission is stopped at any point, a lower bit rate video can still be decompressed and reconstructed. LT code [12] (Fig. 2) is used to cope with packet losses caused by Primary User interference and other channel conditions. Generally, we can also use other fountain codes [18] like raptor codes [20]. It has been shown in [11] that the use of fountain codes kills two birds with one stone. First of all, it avoids the coordination problems between different SCs belonging to the same SUL. Second, it acts as an erasure correcting code. Luby

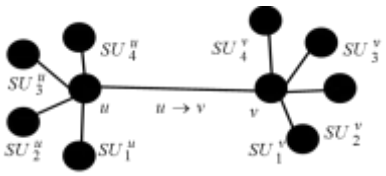


Figure 1. Cognitive Radio network

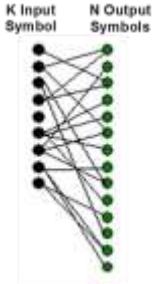


Figure 2. Tanner Graph of LT codes

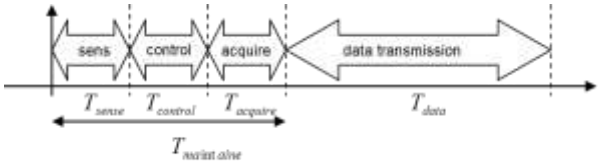


Figure 3. Time frame structure

has used a particularly designed degree distribution for the construction of LT codes called the Robust Soliton Distribution, it has two parameters: $c \succ 0$ and $\delta \in [0,1]$. To reduce the collision effects, we propose to set up many Secondary User Links during the sensing phase (Fig. 3). In [15], we have developed a simple algorithm to establish several SULs having the same efficiency. The formed SULs are pairwise disjoint, which implies that any subchannel belonging to a given SUL can't be reused for constructing other SULs. The existence of many available SULs enables many SUs to transmit in the same time slot without perturbing each other; each SU would be able to transmit in the same time slot and through a specific SUL different from the other subscribers' paths. We assume that collision result in the total communication failure on the chosen SUL, so the occurrence of collisions impedes the performance of the CR network. Moreover, we assume that there is no algorithm to assign to each new secondary user a new secondary user link currently not in use, the existence of such algorithms will reduce the collision probability to the detriment of increasing costs and time delay. We investigate the trade-offs between different system parameter settings and the average Goodput of the developed model. We conclude that, under some parameter settings, the system continue to achieve good performance despite of the presence of primary interferences and secondary collisions. The proposed SULs redundancy-based approach exhibit good results in compensating the performance degradation caused by collisions. We emphasize also the importance of finding a balance that meets quality and Goodput, which means that there is optimal transmission parameters to ensure the expected quality with a given over all Goodput.

The remainder of this paper is organized as follows: In Section 2 we give a brief summary about the Spectrum Pooling concept. We recall the link maintenance model reused in our study. In Section 3 we make use of joint Source Compression and Channel Coding techniques to combine the advantages of both methods. Then, we compute the analytic expression of the achieved Goodput which considers both Primary traffic interruptions and TDMA collisions. In Section 4 we present the numerical results and we show the resulting gains in terms of system Goodput, and finally Section 5 draws our conclusions.

II. System Descriptions

Here we introduce some concepts that will be used in our study.

A. Spectrum Pooling Concept

The Spectrum Pooling Concept [21] basically consists of selecting several spectral ranges from the primary frequency bands to constitute a common pool. The so called COgnitive Radio for Virtual Unlicensed Spectrum (CORVUS) [22] is based on this approach. The whole frequency spectrum covered by the system is divided into N subchannels each of bandwidth $W = B/N$ where the total available system bandwidth is B. The dashed frequency bands in Fig. 4 indicate that de PU is currently active, consequently this frequency band can not be used by any secondary user. The gradient grey color in Fig. 4 shows the vacant subchannels that are selected to construct a Secondary User Link.

Under the single uniform subchannel selection, an SUL should consist of only one subchannel per primary frequency band to ensure a low effect of the PU arrival on a SUL, only one subchannel need to be vacated in case a PU arrives. However, practically, it is expected that in one SUL, more than one subchannel per primary frequency band can be allocated (Fig. 4). Thus, the subchannels within the same frequency band are more likely to be jammed at the same time once the primary user appears, this subchannel selection policy is recommended for cases with available priori knowledge on subchannels state information.

B. Link maintenance model review for primary traffic interruptions

For the proposed link maintenance model introduced in [16] and as shown in Fig. 3, the frame consists of four parts: a sensing block T_{sens}, a reporting block $T_{control}$, an acquire block $T_{acquire}$ and a data transmission block T_{data}.

In the sensing block, all users conduct local spectrum sensing simultaneously. The local sensing results are reported and disseminated between different peers through the Group Control Channel sequentially in the reporting block. Then during the acquire block, new subchannels need to be acquired to compensate for the lost ones. Finally, the next stream is ready to transmission over the cognitive radio network in a delay of T_{data}.

The PU appearance is considered the only reason for a subchannel to be excluded from the SUL. Consequently, the subchannel exclusion probability p_x is restricted to the Primary User appearance probability p_a :

$$p_x = p_a . \quad (1)$$

In the secondary usage scenario, the SU selects a set of subchannels from the PU bands. The SU is required to vacate the subchannel as soon as the corresponding PU becomes active and claims his spectral resource. Therefore, the secondary user loses some packets on that subchannel. To compensate for that loss, the source packets are encoded with LT codes. Let the secondary user has a message m of K packets to transmit. The LT decoder needs at least N packets in order to

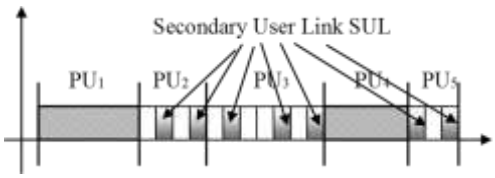


Figure 4. Spectrum Pooling Concept

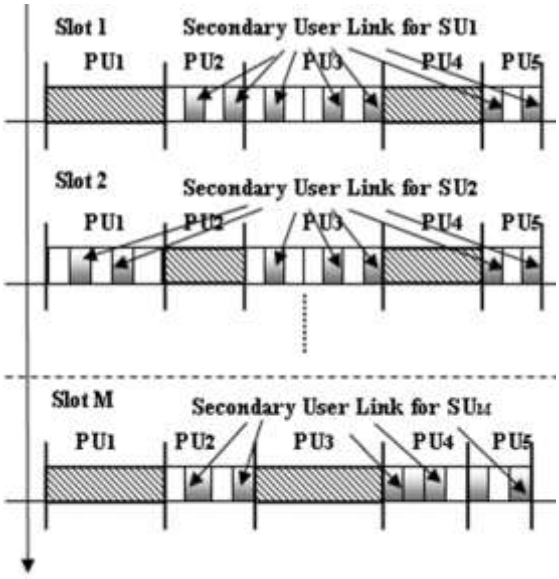


Figure 5. Shared Cognitive Radio network based on TDMA technique.

recover the original K packets with probability $1-DEP$. Then in order to compensate for the loss due to PU appearance, we add some redundancy, denoted X, which depends on the PU arrival probability p_a. If the PU arrival is frequent then we need to use high value of X. If the PU arrives occasionally then even a small X value will be sufficient. The considered link maintenance model assumes that one packet is transmitted per subchannel. Then, the total number of subchannels used by SU is $S = N + X$. This communication will succeed only if at most X of the subchannels are claimed by their associated licensed users. Hence, the message error probability for secondary users, which take into consideration only the Primary traffic interruptions, is given by:

$$P_{err} = \sum_{i=1}^{N} \binom{N+X}{X+i} {p_a}^{X+i} (1-p_a)^{N-i} . \quad (2)$$

Then the total Goodput can be computed as:

$$G = \frac{(1-P_{err}) \times N \times b_{sc} \times T_{data}}{T_{sens} + T_{control} + P_m \times T_{acquire} + T_{data}} . \quad (3)$$

Where P_m is the probability that the SUL has to be restructured and is given by:

$$P_m = 1-(1-p_a)^{N+X} . \quad (4)$$

b_{sc} is the bit rate per subchannel.

III. Proposed Network Model

In this section, we propose a solution to video communication services in cognitive radio context. For this purpose, we give an analytic expression of the Goodput metric which quantifies the QoS requirements of the secondary transmission.

A. General Analysis

Consider a cognitive radio network where a cognitive source is sending data to a cognitive destination over a spectrum hole unoccupied by licensed users.

In our study, we focus our attention on delay video transmission applications over wireless networks. One or many participants are providing access to video application directly available to a given population of clients with heterogeneous reception bandwidths and quality of service requirements. That is, high quality of service is required and higher data rates must be supported [23, 24, 25, 26].

The video data consists of a group of pictures (GOP). The GOP consists of K packets. We assume that the TDMA frame consists of M slots each of the same time duration T.

We introduce the following practical model of TDMA scheduling: Each Secondary user SU_i always transmits in his assigned slot i with probability q and transmits with probability p in the remaining time slots ($M-1$ slots).

At the start of every slot i, a Secondary User Link is formed by selecting a set of S subchannels from different PU bands of the spectrum pool. Then, SU_i starts transmitting his GOP packets over this link during the data duration T_{data}. That is, the sensing part is decoupled from the transmission part. So, we have $T = T_{setup} + T_{data}$, where $T_{setup} = T_{sens} + T_{control} + T_{acquire}$. The probability of PU appearance for any subchannel is given by p_a. For simplicity of analysis, p_a is assumed to be the same for different subchannels.

Despite of the presence of PUs reclaims and SUs concurrency, reliable schemes are required to enable the continuous provision of service for the communication among the secondary network to some satisfying extent. Hence, sophisticated signal processing and coding techniques remains the cornerstone of a successful secondary transmission.

More precisely, in this work we adopt a Joint Source Channel Coding method which is among the most appropriate ways to communicate multimedia content over a lossy packets network. We make use of a progressive encoding system which allows transmitting the coded video as a sequence of layers over CR networks. The use of progressive amounts of redundancy will guarantees a high protection level to the most important data i.e. the base layer of the stream.

In deed, we first form a scalable bit stream $(R_f)_{0 \le f \le F}$ by applying SPIHT [17] or any compression scheme on the video [27]. We partition the bit stream source into F layers $(L_f)_{1 \le f \le F}$ indexed in order of decreasing importance; we use the fact that a progressive source coder produces an output in which information important to video quality is emitted first. We denote the boundaries of layer f by bits R_{f-1} and R_f such that $0 = R_0 \le R_1 \le ... \le R_F$. Each layer L_f is blocked into K_f source blocks. The use of source coding permits to recover the content up to a certain quality commensurate with the number of layers received.

Let Q_f where $1 \le f \le F$ be the achieved quality corresponding to the layer L_f. Regarding the fact that we use a progressing source coding, the reception of the layer L_{f+1} implies the reception of all the subordinate layers $(L_j)_{1 \le j \le f}$. Stream L_1 is the first stream (most important data), and stream L_F is the last stream (least important data).

We make use of the LT codes (Fig. 2) to protect the video traffic against PU interferences. We propose to create one fountain code per layer, LT codes is applied on every layer L_f where $f \in \{1, \cdots, F\}$. Note N_f as the number of LT encoded packets needed to recover the original K_f transmitted packets corresponding to the layer L_f with probability $1 - DEP$. An overhead of 5% is sufficient in order to reconstruct the data at the receiver, so: $N_f = 1.05 \times K_f$.

Regarding the fact that N_f is the minimal amount of encoded packets needed to recover the original video up to the quality Q_f, any PU interruptions will immediately cause the loss of the layer f and consequently the data of the respective enhancement layers are rendered useless. That is, we add some amount of redundancy, noted X_f, to overcome the corruption of data packets du to PU arrival.

At a specific time slot, several SUs could be actives and using this slot for transmission or reception at the same time and on the same Secondary User Link. Hence, collisions could occur on the network. Collision errors indicate a serious performance problem on the CR network. We propose a simple way to prevent CR networks from packet collisions [15]. During the sensing phase, many Secondary User Links will be established, such that each active cognitive user will be assigned an SUL different from the others. Therefore, if many SUs' communications coincide at the same time slot, each SU has more chance to take a different SUL and consequently the risk of collision decreases.

As a matter of fact, under a targeted level of quality Q_f there are mainly two events that affect the traffic distribution on the selected SUL. A secondary user succeeds his transmission if (1) for the secondary receiver, at least N_f packets are received successfully from the set of selected subchannels S, and (2) if there is no packet collisions due to the fact that every SU_i could transmit opportunistically on other slots not assigned to him. We notice that the last factor is quality independent.

Let u and v be two active secondary users (Fig. 1), the objective is to study the Goodput of the communicatio $u \to v$ with the sought quality Q_f. We remember that this transmission is perturbed by the PU reclaims and the collision risks.

Define $P'_{err,f}$ as the message error probability of the transmission $u \to v$ with the sought quality Q_f (Fig. 1).

In our scheme for secondary use, we define the message error probability as the probability that the active cognitive user v could not reconstruct the GOP sent by u up to the quality Q_f. In other words, if (1) X_f or more subchannels got jammed due to the arrival of PUs, or (2) the transmission $u \to v$ is subject to collision, the GOP cannot be successfully reconstructed at the receiver with the desired quality Q_f.

Then, we compute $P'_{err,f}$ as:

$$P'_{err,f} = P_{err,f} + P_{collision}. \quad (5)$$

$P_{err,f}$ is the probability that the active cognitive user v fails to receive N_f packets over the selected SUL.

$P_{collision}$ is the probability that there is other SUs trying to access the same SUL as the cognitive user u.

B. An Analytical Expression for $P_{err,f}$

Using the expression (2):

$$P_{err,f} = \sum_{i=1}^{N_f} \binom{N_f + X_f}{X_f + i} p_a^{X_f + i} (1 - p_a)^{N_f - i}. \quad (6)$$

C. An Analytical Expression for $P_{collision}$

Let i be the time slot assigned to the active cognitive user u and Deg_v defined as the number of neighbors of the active cognitive user v ($(SU_i^v)_{1 \le i \le 4}$ in Fig. 1). We remember that q is the probability that u transmits in his assigned time slot i and p the probability that he transmits in the remaining time slots $j \ne i$ (Fig. 5).

Let $P_{no\,collision}$ be the probability that there is no collisions perturbing the transmission $u \to v$.

$P_{no\,collision}$ should be derived in the following manner :

For the time slot i :

$$P_{i,\,no\,collision} = q(1 - p)^{Deg_V}. \quad (7)$$

For the remaining time slots $j \ne i$, there are two cases: (1) the time slot j coincides with the specific time slot of one of the v neighbors, or (2) there is no user belonging to the v neighbors which owns the time slot j.

Hence,

$$P_{j,\,no\,collision} = p(1 - p)^{Deg_V} + p(1 - q)(1 - p)^{Deg_V - 1}. \quad (8)$$

We should note that when $q = 1$, we obtain the given results in [13].

Using (7) and (8), the average probability of no collisions over the frame and for one Secondary User Link is:

$$P_{no\,collision} = \frac{q(1 - p) + (M - 1)p(2 - p - q)}{M}(1 - p)^{Deg_V - 1}. \quad (9)$$

Because the two events are complementary, we have,

$$P_{collision} = 1 - P_{no\,collision}. \quad (10)$$

Then, from (9) and (10) we obtain,

$$P_{collision} = 1 - \frac{q(1-p) + (M-1)p(2-p-q)}{M}(1-p)^{Deg_V - 1}. \quad (11)$$

If we consider several structured SULs which are pairwise disjoin as defined in [15], the total average probability of collisions over the available Secondary User Links N_{SUL} is:

$$P_{collision} = \left(1 - \frac{q(1-p) + (M-1)p(2-p-q)}{M}(1-p)^{Deg_V - 1}\right)^{N_{sul}} \quad (12)$$

From (5), (6) and (12) $P'_{err,f}$ is completely defined.

We extend the general model of link maintenance introduced in [16] to take the collision aspect caused by the opportunistic transmission into consideration. The total achieved Goodput will be given by:

$$G'_f = \frac{(1 - P'_{err,f}) \times N_f \times b_{sc} \times T_{data}}{T_{sens} + T_{control} + P_m^f \times T_{acquire} + T_{data}}. \quad (13)$$

We recall that $P_m^f = 1 - (1 - p_a)^{N_f + X_f}$. P_m^f is the probability that the SUL has to be maintained.

IV. Numerical Results

In this section, we present some numerical results to reinforce the theoretical aspect previously addressed and to outline the achieved gains when using Join Source Channel Coding in Cognitive Radio based wireless networks.

A. General Simulations

For real video transmission, we consider an MPEG-4 [27] LT encoded video stream with a resolution of 720x576 pixels and a frame rate of 25 frames/s (DVD quality for example). Our purpose is to study the Goodput average of this transmission on a Cognitive Radio TDMA-based network shared by several Secondary Users.

For the time frame, we suppose that:

$$T_{sens} = T_{control} = T_{acquire} = T_{data} = 1ms$$

The Robust Soliton distribution used for the LT coding has as parameters $c = 0.1$ and $\delta = 0.5$, we consider a decoding error probability of $DEP = 0.1\%$. We assume a BPSK modulation with a code rate of 1/2 which means a bit rate of $b_{sc} = 125kbit/s$ per subchannel.

For the given video transmission, we take a data rate of 1.66Mbit/s, LT codes overhead included. The given data rate represents the maximum achieved Goodput of this transmission. We evaluate the expression (13) by replacing variables with the given values to find the minimal number of packets N needed to ensure this multimedia transmission (we must take $P'_{err,f} = P_m^f = 0$). Thus, $N_f = 40$.

Fig. 6 depicts the impact of the number of available Secondary User Links N_{SUL} on the total achieved Goodput plotted against the amount of redundant subchannels X . Deg_V and M values has been fixed respectively at 3 and 5. The estimated traffic average on the assigned slot is $q = 90\%$ and in the remaining slots is about $p = 30\%$. As it is seen and according to what was expected, the Goodput performs good results where increasing the number of available SULs. Indeed, at a specific time slot, if there are many available SULs, it is very unlikely that two Secondary Users transmits over the same SUL and consequently more chance to avoid collisions. It is also interesting to note that there is some X value that maximizes the achieved Goodput. Adding other SCs to the Secondary User Link over this value doesn't give any amelioration; on the contrary, degrades the transmission performance.

For all the following numerical result, the number of available Secondary User Links has been fixed to 20 .

Fig. 7 illustrates the achieved Goodput over Cognitive Radio network shared by several SUs using TDMA techniques plotted against the number of additional subchannels X . Here, we study the impact of the probability q on the traffic transmission performance for a fixed value of $p = 30\%$. We have fixed the following settings $Deg_V = 3$ and $M = 5$. Thus, while decreasing the q value, the proposed network model provides better results in terms of Goodput. This is due to the fact that when the SU is increasing the traffic transmission on his assigned slot, eventual collisions on this slot are more likely to happen for a fixed p value.

In Fig. 8, the computed Goodput is given versus the redundancy X ; simulations were run for several p values for a fixed value of $q = 90\%$. It can be observed that for low p values, the Goodput increases. High traffic performance is attained where approaching $p \approx 0.1$ and the Goodput approaches his maximum value $G_f^{\max} = 1.66$Mbit/s. It is obvious that where decreasing the traffic among the other slots assigned to the other SUs, we reduce the chance that our SU interferes with the other active cognitive users. There is always an optimal value

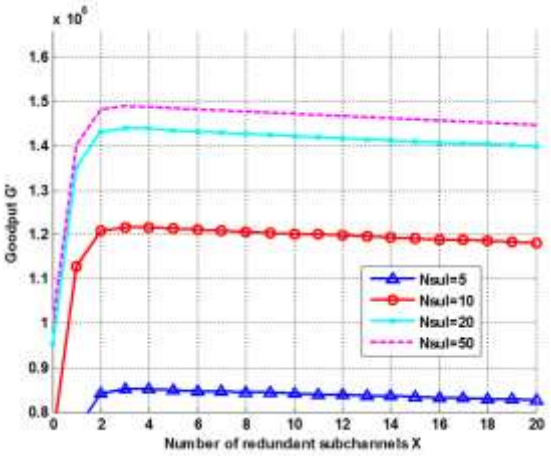


Figure 6. Computed Goodput for different N_{sul} values

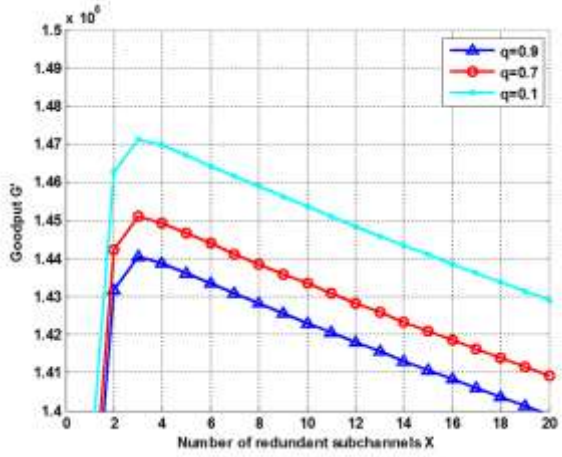


Figure 7. Goodput comparison for different values of the probability q $(p = 0.3)$

of the added redundancy that realize a trade-off between the computed Goodput of the system and the added redundancy. On the other hand we notice that there exists an optimal value of the probability p which maximizes the system Goodput $(p \approx 0.1)$.

Fig. 9 represents the Goodput against the redundancy X for several values of Deg_v. The slots number has been fixed at 5 and the probabilities p and q has been fixed respectively to 0.1 and 0.9. The Goodput is improved by decreasing the number of neighbors of the active cognitive user v. The reason is obvious, more neighbors mean more active SUs which will arouse more collisions. For different values of Deg_v there is a local maximum of the graph. For low values of Deg_v, the Goodput comes close to his maximum value.

Fig. 10 shows the achieved Goodput metric in terms of redundancy X for different number of slots M. The Deg_v value has been fixed at 3 and the probabilities p and q has been fixed respectively to 0.1 and 0.9. The proposed model exhibits good performance in terms of Goodput while decreasing the number of slots M since fewer slots can be subject to eventual

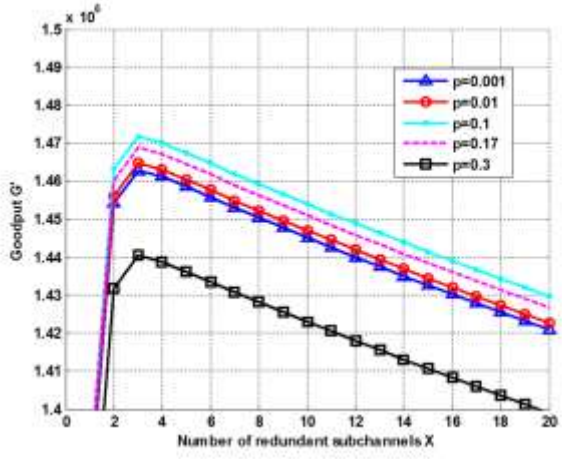


Figure 8. Goodput comparison for different values of the probability p $(q = 0.9)$

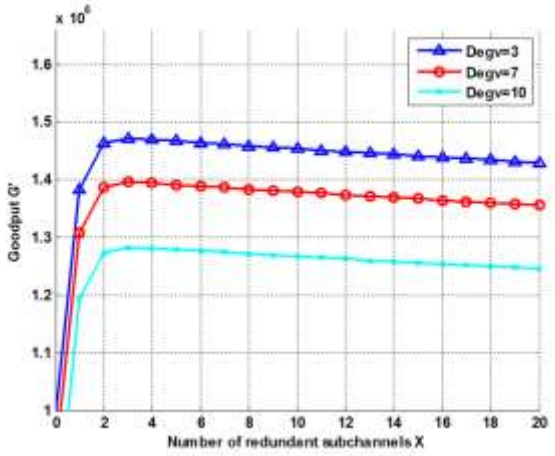


Figure 9. Achieved Goodput comparaison for different Deg_v values

collisions. Increasing the number of slots M enlarge the portions of time where different SUs could be active and collide with one another.

Fig. 11 illustrates the obtained Goodput in view of redundancy X for several sought qualities. The Deg_v value has been fixed at 3 and the probabilities p and q has been fixed respectively to 0.1 and 0.9. Where increasing the number of transmitted packets, the achieved Goodput increases. Nevertheless, we notice that where increasing the packets number, the Goodput get away from his local maximum (see Fig. 11 and Tab. 1) which outlines the real need for reaching a good compromise between the computed Goodput and the expected quality.

B. *Analysis and discussions*

The proposed model has many parameters that influence the stability of the system such as, inter alia, the average traffic on the assigned slot, the average traffic on the remaining slots, frame size, neighbors' number, redundancy and number of available Secondary User Links. This is due to the fact that our model considers two critical features of the Cognitive Radio networks: Primary interruptions and Secondary Opportunistic Spectrum Sharing. The last factor was not taken into

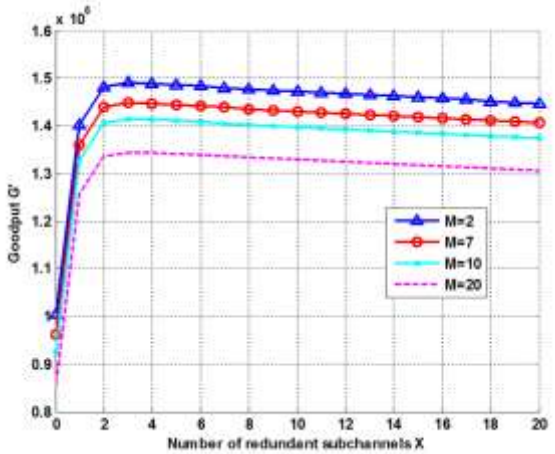


Figure 10. Achieved Goodput comparaison for different M values

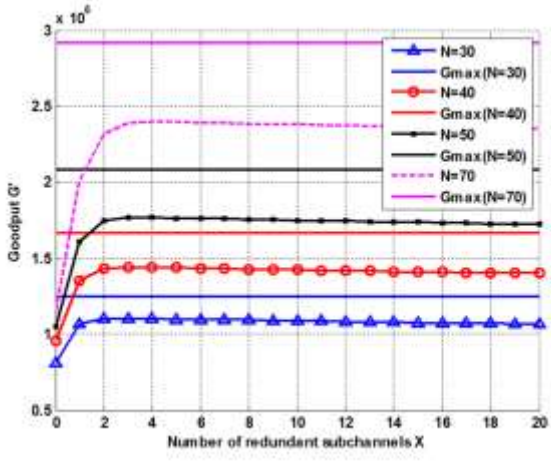


Figure 11. Achieved Goodput comparaison for different expected qualities

consideration in [16] where the system is only sensitive to the amount of added redundancy. It is apparent that studying other Cognitive Radio factors will render the system stability more complex but also challenging. The system parameters need to be accordingly well adjusted.

The centralized scheduler set the value of slots number M , and the network architecture imposes the number of neighbors of each SU Deg_{su} . During the sensing phase, the CR system determines the vacant subchannels ready for secondary use; hence the Secondary Users Links N_{SUL} could be established using the technique introduced in [15]. The average traffics p and q and the additional redundancy X values could be analytically derived by addressing the Goodput maximization problem explored in the previous paragraph.

It is also shown that depending on the quality that we seek, we need to ensure a specific video data rate. Where our video transmission is "quality hungry", we must support higher bit rates and then our video transmission parameter settings have to be chosen adaptively depending on our system limitation. As a matter of fact, where increasing the transmission rate, we ameliorate the quality of the received video but more

TABLE I. QUALITIES AND MAXIMUM GOODPUTS

Packets number (sought quality)	Maximum Goodput (Mbit)
30	1.25
40	1.66
50	2.08
70	3

subchannels are needed to successfully achieve this communication, however if we use less spectral resources, we optimize the use of the cognitive resources but the quality of the video stream at the consumer is degraded. We stat that when increasing the transmitted quality, it does not necessarily result in a more reliable transmission.

V. CONCLUSION

In this paper, we consider scalable video transmission over Cognitive Radio networks. The primary network has a binomial-modeled traffic. We have suggested making use of a progressive source coding associated to a fountain code. Then, we have evaluated the impact of the primary traffic interruptions on the secondary traffic and used a general model for collisions to modelize the opportunistic access of secondary users to CR network. Further, we have exploited a simple duplication-based mechanism for SULs to ameliorate the Goodput of the video transmission and make the SUs concurrency more infrequent. Our numerical results have been presented in terms of computed Goodput of the system. The achieved gain, while increasing the SULs number, proves the effectiveness of the given solution in terms of QoS requirements for video communication in secondary use. The paper concludes by emphasizing the importance of finding a balance that meets expected quality and achieved Goodput of the system. Hence, our video transmission parameters should be carefully chosen.

REFERENCES

[1] http://www.fcc.gov/oet/info/database/spectrum/

[2] Shared Spectrum Compagny. Spectrum occupancy measurement. site internet, http://www.sharedspectrum.com/measurements/.

[3] NTIA, "U.S. frequency allocations." [Online]. Available: http://www.ntia.doc.gov/osmhome/allochrt.pdf

[4] J. Mitola III, "Cognitive radio: an integrated agent architecture for software defined radio," Ph.D Thesis, KTH Royal Institute of Technology, 2000.

[5] FCC, ET Docket no. 03-322. Notice of Proposed Rule Making and Order, December 2003

[6] D. Cabric, S. M. Mishra, D. Willkomm, R. W. Broderson, and A. Wolisz, "A cognitive radio approach for usage of virtual unlicensed spectrum," in 14th IST Mobile Wireless Communications Summit 2005, Dresden, Germany, June 2005.

[7] I. Akyildiz, Y. Altunbasak, F. Fekri, and R. Sivakumar, "AdaptNet: an adaptive protocol suite for the next-generation wireless Internet," Communications Magazine, IEEE , vol.42, no.3, pp. 128- 136, Mar 2004.

[8] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," Computer Networks Journal, vol. 50, Sept. 2006.

[9] C. Cordeiro, K. Challapali, D. Birru, and N. Sai Shankar, "IEEE 802.22: the first worldwide wireless standard based on cognitive radios," IEEE DySPAN, pp.328-337, Nov. 2005.

[10] B. Ishibashi, N. Bouabdallah, and R. Boutaba, "QoS performance analysis of cognitive radio-based virtual wireless networks," INFOCOM 2008. The 27th Conference on Computer Communications. IEEE , vol., no., pp.2423-2431, 13-18 April 2008.

[11] H. Kushwaha, Y. Xing, R. Chandramouli, and H. Heffes, "Reliable multimedia transmission over cognitive radio networks using fountain codes," Proc. IEEE, vol. 96, no. 1, pp. 155-165, Jan. 2008.

[12] M. Luby, "LT codes," Proc. 43rd Ann. IEEE Symp. on Foundations of Computer Science, 2002, pp. 271–282.

[13] L. Cuiran and L. Chengshu, "Opportunistic spectrum access in cognitive radio networks," Neural Networks, 2008. IJCNN 2008. (IEEE World Congress on Computational Intelligence). IEEE International Joint Conference on , vol., no., pp.3412-3415, 1-8 June 2008.

[14] A. Chaoub, E. Ibn Elhaj, and J. El Abbadi, "Unequal protected fountain code for progressive image source coding using block duplication," Seventh JFMMA & TELECOM 2011, Tangier, Morocco, March 2011.

[15] A. Chaoub, E. Ibn Elhaj, and J. El Abbadi, "Multimedia traffic transmission over TDMA shared cognitive radio networks with poissonian primary traffic," Multimedia Computing and Systems, 2011. ICMCS '11. International Conference on , vol., no., pp.1-6, 7-9 April 2011.

[16] D. Willkomm, J. Gross, and A. Wolisz, "Reliable link maintenance in cognitive radio systems," in Proc. IEEE Symp. New Frontiers Dyn. Spectrum Access Netw. (DySPAN 2005), Baltimore, MD, Nov. 2005.

[17] A. Said and W. A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," IEEE Trans. Circuits Syst. Video Technol., vol. 6, pp. 243–250, June 1996.

[18] D.J.C. MacKay, "Fountain codes," IEE Proc.-Commun., vol. 152(6), 2005, pp.1062-1068.

[19] A. Chaoub, E. Ibn Elhaj, and J. El Abbadi, "Multimedia traffic transmission over cognitive radio networks using multiple description coding," ACC 2011, Part I, CCIS 190, pp. 529–543, 2011, Springer-Verlag Berlin Heidelberg 2011.

[20] A. Shokrollahi, "Raptor codes," IEEE Trans. Inform. Theory, vol. 52, pp. 2551–2567, June 2006.

[21] T. Weiss and F. Jondral, "Spectrum pooling: an innovative strategy for the enhancement of spectrum efficiency," IEEE Communications Magazine, Vol. 42, no. 3, March 2004, pp. 8-14.

[22] R. W. Broderson, A. Wolisz, D. Cabric, S. M. Mishra, and D. Willkomm, "Corvus: a cognitive radio approach for usage of virtual unlicensed spectrum," White Paper, Univ. California Berkeley, Tech. Rep., Jul. 2004.

[23] H. Su and X. Zhang, "Cross-Layer Based Opportunistic MAC Protocols for QoS Provisionings Over Cognitive Radio Wireless Networks," IEEE Journal on Selected Areas in Communications (J-SAC), Vol. 26, No. 1, pp. 118–129, January 2008.

[24] J. Tang and X. Zhang, "Quality-of-service driven power and rate adaptation over wireless links," IEEE Transactions on Wireless Communications, Vol. 6, No. 8, pp. 3058–3068, August 2007.

[25] X. Zhang, J. Tang, H. H. Chen, S. Ci, and M. Guizani, "Cross-layer based modeling for quality of service guarantees in mobile wireless networks," IEEE Communications Magazine, Vol. 44, No. 1, pp. 100 106, January, 2006.

[26] J. Tang and X. Zhang, "Cross-layer-model based adaptive resource allocation for statistical QoS guarantees in mobile wireless networks," IEEE Transactions on Wireless Communications, Vol. 7, No. 6, pp. 2318–2328, June 2008.

[27] R. Koenen, "MPEG-4 multimedia for our time," IEEE Spectrum, vol. 36, no. 2, Feb. 1999, pp. 26-33.

Scalable TCP: Better Throughput in TCP Congestion Control Algorithms on MANETs

M.Jehan
Associate Professor, Department of Computer Science,
D.J.Academy for Managerial Excellence,
Coimbatore, India

Dr. G.Radhamani
Professor & Director, Department of Computer Science,
Dr.G.R.Damodaran College of Science,
Coimbatore, India

***Abstract*—In the modern mobile communication world the congestion control algorithms role is vital to data transmission between mobile devices. It provides better and reliable communication capabilities in all kinds of networking environment. The wireless networking technology and the new kind of requirements in communication systems needs some extensions to the original design of TCP for on coming technology development. This work aims to analyze some TCP congestion control algorithms and their performance on Mobile Ad-hoc Networks (MANET). More specifically, we describe performance behavior of BIC, Vegas and Scalable TCP congestion control algorithms. The evaluation is simulated through Network Simulator (NS2) and the performance of these algorithms is analyzed in the term of efficient data transmission in wireless and mobile environment.**

Keywords- TCP Congestion Control Algorithms; MANET; BIC; Vegas; Scalable TCP.

I. INTRODUCTION

Ad hoc network is a temporary network connection for a specific purpose (such as transferring data from one computer to another) in wireless networks. It is self organizing networks, which all end nodes are act as routers or data user. It improves the efficiency of fixed and mobile internet access and enables new applications for public. A Mobile Ad hoc Networks (MANET) consists of a set of mobile hosts within the communication range and exchange data among themselves without using any pre-existing infrastructure. MANET nodes are typically distinguished by their limited power, processing and memory resources as well as high degree of mobility. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information to other node.

MANETs uses in the disparate situations such as moving battlefield communications to disposable sensors which are dropped from high altitude and dispersed on the ground for hazardous materials detection. The civilian applications include simple scenarios such as people at a conference in a hotel their laptops comprise a temporary Ad hoc Networks to more complicated scenarios such as highly mobile vehicles on the highway which form an Mobile Ad hoc Networks in order to provide traffic monitoring system.

This paper is entirely devoted to evaluating the Control Window (cwnd), Round Trip Delay Time (rtt) and Throughput using the TCP BIC, Vegas and Scalable TCP congestion control algorithms in the wireless networks.

II. BACKGROUND WORK

A. *Congestion Control in Transmission Control Protocol Algorithms*

TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. It operates at a higher level, concerned only with the two end systems. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. Among its other management tasks, TCP controls segment size, flow control, the rate at which data is exchanged, and network traffic congestion.

TCP can support the mechanisms of flow and congestion control for reliable data transmission. Due to the unconstrained movement of the mobile nodes, TCP is unable to notice network congestion or link down to activate related controls on the MANET [3]. The standard congestion control mechanism of the TCP is not able to handle the special properties of a shared wireless multi-hop channel well. In particular, the frequent changes of the network topology and the shared nature of the wireless channel create some critical issues [7].

It provides consistent end-to-end delivery of data over wired networks, several recent studies have indicated that TCP performance degrades significantly in MANET [10] [11]. In [16], TCP-F is proposed to overcome the TCP false reaction towards route failures in MANETs. In [17] the simulation shows that the route change results in link disconnections, which reduces TCP throughput.

TCP Vegas was the first attempt to depart from the loss-driven paradigm of the TCP by introducing a mechanism of congestion detection before packet losses [12].

Using TCP more computers are interconnected to increase data transaction between users rapidly. The MIMD and PIPD protocols developed and provides better throughput for the wireless networks [15], [19] and [20].

So, this experiment on the existing TCP congestion control algorithms and its performance on MANET will be very useful to design new algorithms and create innovative approach for mobile wireless communication in the point of reducing data loss during transmission.

B. Congestion Control Algorithms For Evaluationons

Congestion is characterized by delay and loss of packets in delivery. In TCP, congestion is said to have occurred when the sender receives three duplicate acknowledgments (dupacks) or when a timeout (packet loss) occurs, resulting in wastage of resources. Congestion Control and Congestion Avoidance are two known solutions which address the above problem. In congestion control [2], system controls the network parameters after realizing congestion (reactive); whereas, in congestion avoidance, system controls the network parameters before congestion (proactive). After the invention of TCP, there is numerous congestion control algorithms discovered for different purposes. Each of them has unique characteristics [4]. In [5][6] the simulation result shows the TCP BIC giving good throughput for long distance wireless networks, but the TCP Vegas giving better result in the overall performance..

1) Binary Increase Congestion Control (BIC)

BIC-TCP (Binary Increase Control-TCP) incorporated binary search increase in the protocol. Binary search increase provides reliable feedback on any network congestion and lost packets, allowing BIC-TCP to aggressively increase its transmission speed toward the maximum allowed by the high-speed network. Binary Increase congestion Control for TCP v2.0 is called as CUBIC and it is a default TCP algorithm in Linux.

2) TCP VEGAS

Until the mid 1990s, all TCPs set timeouts and measured round-trip delays were based upon only the last transmitted packet in the transmit buffer. In TCP Vegas, timeouts were set and round-trip delays were measured for every packet in the transmit buffer. In addition, TCP Vegas uses additive increases in the congestion window.

3) SCALABLE TCP

Scalable TCP (STCP) involves a simple sender-side alteration to the standard TCP congestion window update algorithm. It robustly improves performance in high-speed, wide-area networks using traditional TCP receivers. Scalable TCP updates its congestion window using fixed increase and decrease parameters.

The Scalable TCP window update algorithm, as defined in [7], is divided into two phases.

Slow-start phase: in which the congestion window is increased by one packet for each acknowledgment received:

$$W = W + 1 \quad Ack;$$

Congestion avoidance phase: If congestion has not been detected in at least one round trip time, the window responds to each acknowledgment received with the update

$$W=W+ \alpha,$$

Where $\alpha \in (0, 1)$ is a constant parameter. In the event of congestion, the congestion window is multiplicatively decreased as follows:

$$W= \beta \cdot W,$$

Where $\beta \in (0, 1)$ is also constant. Typical values of these parameters are $\alpha= 0.01$ and $\beta = 0.875$. Further details on the Scalable TCP algorithm are available in [9].

III. THE SIMULATION

In this paper, these algorithms has been successfully implemented and evaluated using NS-2 simulator on a computer with Intel Core 2 Duo CPU (T6400 processor @ 2.00 GHz) 2 GB of RAM.

A random wireless mobile ad hoc network topology was used for these experiments.

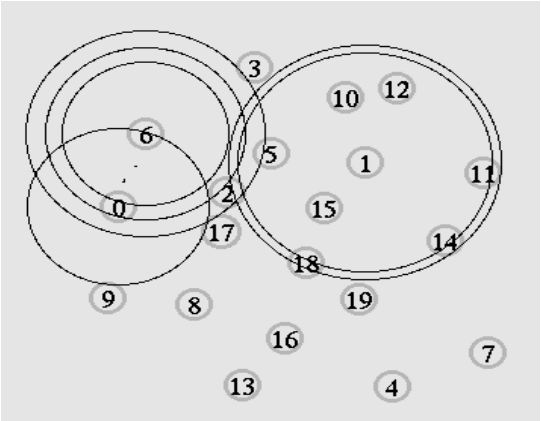


Figure 1. The MANET Scenario

Some of the important parameters of the Ad hoc Network simulation are:

Number of Nodes	20
Number of Sending Nodes	1
Topography	x=500 y=500
Mobility	0 or 20m/s
Mobility Start Time	20th Sec
Routing Protocol	AODV
Mac Type	802.11
Queue	DropTail / PriQueue
Queue Size	50
The Traffic Application	FTP
TCP Packet Size	1448
TCP Initial Window Size	30000

As far as the different parameters of congestion algorithm are concerned, all default parameters of TCP-Linux have been used in all our simulations. For simplicity and clarity of outputs, we used only one TCP flow during evaluating the algorithms.

IV. Result And Discussion

A. Simulation Results in MANETs

In this section, we carried out the simulation results of congestion control window, Round Trip Delay Time and the Throughput in the Wireless Ad hoc Network without nodes movement and the nodes movement after 20 m/s. This simulation has been run for 200 seconds.

1) Control Window in MANETs

In the experimental network that we have used to perform experiments for congestion control window comparison between the three algorithms as shown in Figure 2 and Figure 3.

Figure 2 shows the congestion control window increasing and decreasing in all algorithms without any similarities except TCP Vegas.

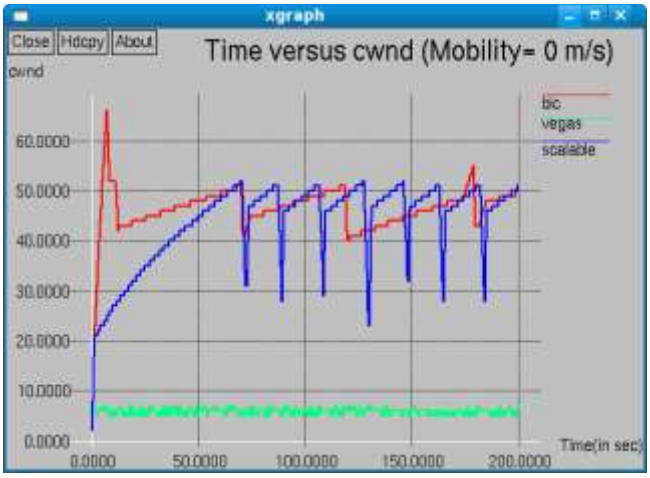


Figure 2. The cwnd on Ad hoc Network without nodes movement

Figure 3. The cwnd on Ad hoc Network nodes movement after 20 ms

In the above Figure 3, the exponential window size increase, linear increase and drop-off occurs irregularly during the simulation. In this Mobile Ad hoc Networks the TCP Vegas giving good result than other algorithms from this group of algorithms. The algorithm Scalable TCP giving second level good performance result in the simulation.

2) Round Trip Delay Time in MANETs

The Round Trip Delay Time estimation of congestion control algorithms on wireless ad hoc network as shown in the Figure 4 and Figure 5. This simulation result shows the TCP Vegas performance is better than other algorithms. But, the algorithm Scalable TCP is the second highest in this simulation result.

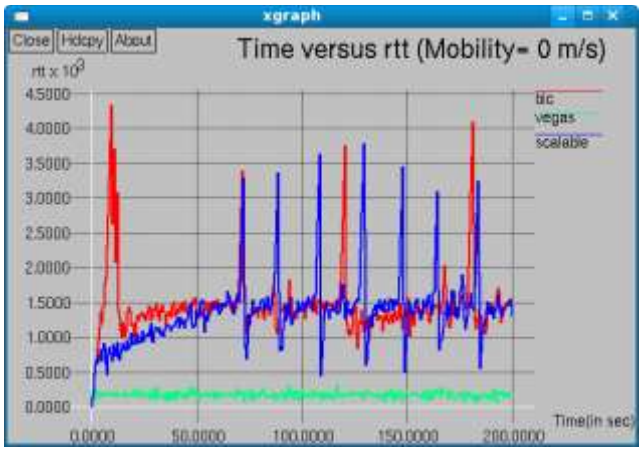


Figure 4. The rtt on Ad hoc Network without mobility

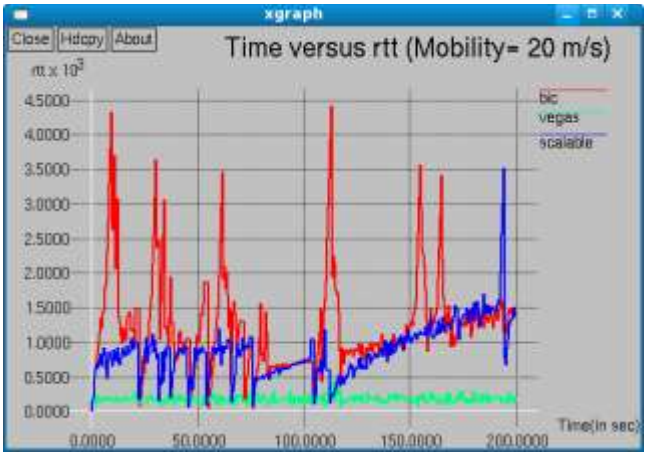


Figure 5. The rtt on Ad hoc Network, the nodes mobility after 20 m/s

3) Throughput Over Time in MANETs

Throughput is the average rate of successful message delivery over a communication channel to the destination node. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

In this simulation, the throughput is the number of packets reaching to the destination node per ms/second. Here we find out the instant throughput over time.

Figure 6 shows the throughput over time in the non movement (0 ms or no mobility) duration. As per the simulation setup after 50 seconds, all algorithms provided equal performance. During the initial stage, TCP BIC given very low throughput; but over time, all algorithms performed well.

The Figure 7 shows the throughput over time in the case of nodes movement environment. In this network scenario, all nodes started to move after the time period of 20 seconds in the simulation. As per the simulation result the algorithm Scalable TCP performance was better than other algorithms.

If we carefully observe the two sections (up to 50 seconds and 100 to 200 seconds) of Figure 7, we can say that Scalable TCP throughput performance is better than other algorithms. The algorithm Vegas tried to give better result in the time duration of 20 to 50 seconds. But in the overall time duration Scalable TCP performance was better than other algorithms. So as a final outcome, we selected Scalable TCP is the best performer in mobile ad hoc network scenario to long distance networks. As per the results, we can say the Vegas can be used for short distance communication applications in the less time duration of TCP communication applications.

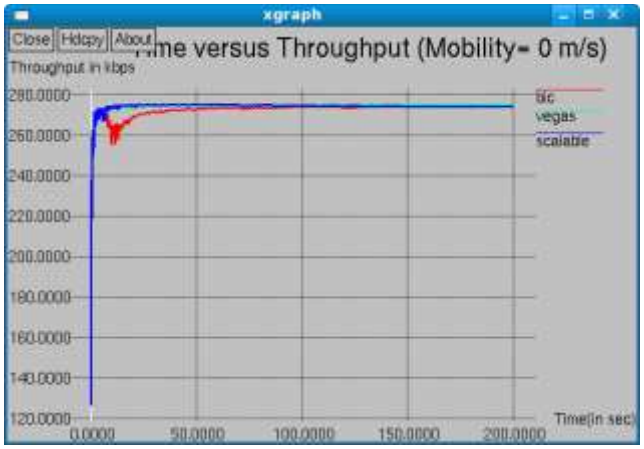


Figure 6. Throughput without Mobility

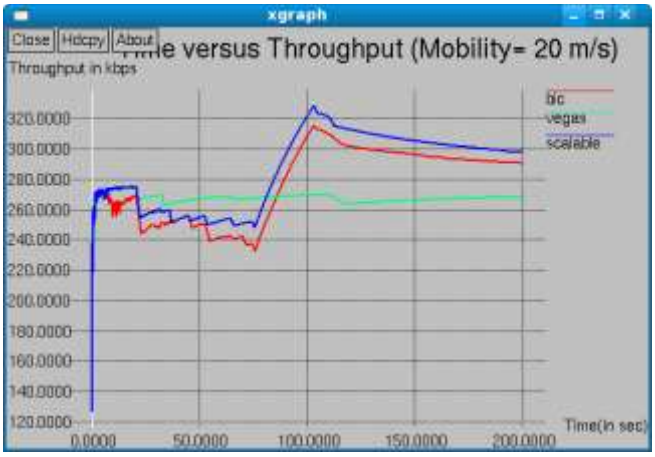


Figure 7. Throughput with Mobility

V. Conclusion

In this paper we have outlined our implementation and deployment experiences with BIC, Vegas and Scalable TCP in ad hoc network environment. Our experiments have provided the performance of these congestion algorithms in very ideal condition without any cross traffic and any additional flows. In this small MANET scenario, the algorithm Scalable TCP provided good throughput than other algorithms. Algorithm Vegas performance is better in the control window and RTT. But in the throughput measurement point of view TCP Vegas performance is not good for long distance networks.

Except Scalable TCP, all other assessed algorithms provided low throughput in this simulation. So we conclude Scalable TCP will be the better algorithm for high throughput to long distance data transmission in MANETs.

VI. Future Work

As a further work, we have considered to do the improvement on throughput and few more extension in Scalable TCP for better performance. Based on the results, we would extend the future enhancement towards specific application on MANETs.

Acknowledgment

The authors thank the authorities of the Dr.G.R. Damodharan College of Science, Coimbatore, India, who provided opportunities and resources for carrying out this research work and for the research activities in the Department of Computer Science at the College. The first author further thanks the Management and the Principal of the D.J. Academy for Managerial Excellence, Coimbatore, India for their support and encouragement extended to him to pursue research in the chosen field of study.

References

[1] D. X. Wei and P. Cao, "NS-2 TCP- Linux: An NS-2 TCP Implementation with Congestion Control Algorithms from Linux", proceedings of ValueTool'06 -- Workshop of NS-2, Oct, 2006.

[2] S. Ryu, C. Rump, and C. Qiao, "Advances in Internet congestion control," IEEE Communications Surveys and Tutorials, vol. 3, pp. 28–39, 2003.

[3] Shin-Jer Yang , Yung-Chieh Lin, Soochow University, Taipei, Taiwan , "Tuning Rules in TCP Congestion Control on the Mobile Ad Hoc Networks", Proceedings of the 20th International Conference on Advanced Information Networking and Applications, Volume 01 , 2006.

[4] M.Jehan, G.Radhamani, T.Kalakumari, "A survey on congestion control algorithms in wired and wireless networks", *Proceedings of the International conference on mathematical computing and management (ICMCM 2010)*, Kerala, India, June 2010.

[5] M.Jehan, G.Radhamani, T.Kalakumari, "Experimental Evaluation of TCP BIC and Vegas in MANETs", International Journal of Computer Applications (0975-8887), Volume 16-No.1, pp.34-38, February 2011.

[6] M.Jehan, G.Radhamani, T.Kalakumari, " VEGAS: Better Performance Than Other TCP Congestion Control Algorithms on MANETs", International Journal of Computer Networks (IJCN), Volume 3, Issue 2, pp.151-158, May 2011.

[7] Christian Lochert, Björn Scheuermann, Martin Mauve, "A survey on congestion control for mobile ad hoc networks", Wireless Communications & Mobile Computing, Volume 7 , Issue 5, pp. 655 – 676, June 2007, ISSN:1530-8669.

[8] M.Allman, V.Paxson, and W.Stevens. TCP Congestion Control. RFC2581 (Proposed Standard), Apr.1999. Updated by RFC3390.

[9] Kelly T, Scalable TCP: Improving Performance in Highspeed Wide Area Networks, 2002, available at http://www-lce.eng.cam.ac.uk/~ctk21/scalable/.

[10] I. Chlamtac, M. Conti, and J. Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks Journal, vol.1, no. 1, pp. 13-64, Jul. 2003.

[11] A. Al Hanbali, E. Altman, P. Nain, "A Survey of TCP over Mobile Ad Hoc Networks", Research Report no. 5182, INRIA Sophia Antipolis research unit, May 2004.

[12] Brakmo, L. S., O'Malley, S.W., and Peterson, L.,"TCP Vegas: End-to end congestion avoidance on a global Internet", IEEE Journal on Selected Areas in Communications (JSAC), 13(8), (1995), pp. 1465-1480.

[13] Mascolo, S. "Congestion control in high-speed communication networks", Automatica, Special Issue on Control Methods for Communication Networks, Vol. 35, no. 12, Dec. 1999, pp. 1921-1935.

[14] Sally Floyd and Kevin Fall, "Promoting the use of end-to end Congestion control in the Internet," IEEE/ACM Transactions on Networking, vol. 7(4), pp. 458–472, August 1999.

[15] Chandrasekaran M. and Wahida Banu R.S.D., "Interaction Between Polynomial Congestion Control algorithms Queue Management schemes in wired TCP Networks," International Journal of Soft Computing, Vol. 1, No. 2, pp.83-90, 2006.

[16] K. Chandran, S. Raghunathan, S. Venkatesan, and R. Prakash,, "A feedback based scheme for improving TCP performance in Ad-Hoc wireless networks", Proceedings of the International Conference on Distributed Computing Systems (ICDCS 98), Amsterdam, Netherlands, May 1998.

[17] Foez ahmed, Sateesh Kumar Pradhan, Nayeema Islam , and Sumon Kumar Debnath, " Performance Evaluation of TCP over Mobile Ad-hoc Networks" in (IJCSIS) International Journal of Computer Science and Information Security ,Vol. 7, No. 1, 2010.

[18] Mascolo, S., Casetti, C., Gerla, M., Sanadidi, M., Wang. R. "TCP Westwood: End-to-End Bandwidth Estimation for Efficient Transport over Wired and Wireless Networks", In the Proceedings of ACM Mobicom 2001, (Rome, Italy, July 2001).

[19] Chandrasekaran M, Kalpana M and Wahida Banu R.S.D., "Congestion Control using Polynomial Window size adjustment Algorithms for wired and wireless networks", In the Proceedings of International Conference on Network –ICN06 conducted at Mauritius, April 2006.

[20] Chandrasekaran M, , Kalpana M and Wahida Banu R.S.D., "Interaction between MIMD-Poly & PIPD-Poly Algorithms and other TCP Variants in Multiple Bottleneck TCP Networks", In the Proceedings of IEEE Conference WOCN2006, Bangalore, April 2006.

[21] Tomoya Hatano, Hiroshi Shigeno, Ken-ichi Okada, "TCP-friendly Congestion Control for High Speed Network", International Symposium on Applications and the Internet- SAINT'07, pp.10, 2007.

[22] David X. Wei, Cheng Jin, Steven H. Low, and Sanjay Hedge., "Fast TCP: Motivation, Architecture, Algorithms, Performance", IEEE/ACM transactions on networking, 2006.

[23] K. Satyanarayan Reddy and Lokanatha C. Reddy., "A survey on congestion control mechanisms in high speed networks", IJCSNS-International Journal of Computer Science and Network Security, vol. 8, no. 1, 2008, pp. 187 – 195.

[24] Colin Perkins and Ladan Gharal., "Rtp and the datagram congestion control protocol", In Proceedings of .IEEE International Conference on Multimedia and Expo, Toronto, Canada, July 2006.

[25] Van Jacobson., "Congestion Avoidance and Control", Computer Communications Review, Volume 18 number 4, pp. 314-329, August 1988.

[26] Van Jacobson., "Modified TCP Congestion Control Avoidance Algorithm", end-2-end-interest mailing list,pp.1-14 April 30, 1990.

[27] A Linux TCP implementation for NS-2. URL: http://www.cs.caltech.edu/weixl/ns2.html

[28] A mini – tutorial for NS-2 TCP-Linux. URL: http://www.cs.caltech.edu/weixl/ns2.html

AUTHORS PROFILE

M.Jehan is an Associate Professor of Computer Science Department at D. J. Academy for Managerial Excellence, Coimbatore, India. He received his B.Sc degree in Computer Science from Manonmaniam Sundaranar University in 1998 and the M.Sc degree in Computer Science from Bharathidasan University, Tiruchirappalli, India in 2000. He completed him M.Phil degree under Manonmaniam Sundaranar University, Tirunelveli, India in 2003. He is doing him Ph.D in Mobile Computing at Dr.G.R.Damodaran College of Science, Coimbatore under Bharathiar University, India. He has published more number of papers in International Journals and Conferences. His research interests are Wireless Networks, Congestion Control and Ad hoc Networks.

Dr.G.Radhamani has over 20 years of experience in teaching and research, working as Professor and Director, Department of Computer Science, Dr. G.R.Damodaran College of Science, India. She did her PDF (Post Doctoral Fellow) in the Department of Computer Science and Engineering from IIT Chennai. She received her PhD (Computer Engineering) from Multimedia University, Malaysia and M.Sc., M.Phil (Computer Science) degrees from PSG College of Technology, India. She served in Multimedia University, Malaysia from August 2001 to May 2006. She has published more number of papers in International Journals and Conferences. She is a Senior Member of IEEE and CSI. Her research interests are Databases, Computer Security and Mobile Computing.

Performance Comparison of different hybrid amplifiers for different numbers of channels

Sameksha Bhaskar[1] , M.L.Sharma[2]
Department of Electronics and Communication,
BGIET, Sangrur, India

Ramandeep Kaur[2]
Department of Electronics and Communication
THAPAR, Patiala, India

***Abstract*—We have investigated the performance comparison of different hybrid optical amplifiers (RAMAN-EDFA,RAMAN-SOA,SOA-EDFA,EDFA-RAMAN-EDFA).The proposed configuration consists of 16, 32 and 64 Gbps channels at speed of 10 Gbps. We have realized the different hybrid amplifiers and their parameters like quality factor, ber, eye opening and jitter at different number of channels. The different combinations can provide a better result and better feasibility for long distance transmission. It is observed that SOA-EDFA showed good performance as it can travel max distance of 220,240,260 km at 16, 32 and 64 channels respectively. Also, RAMAN-EDFA showed a good performance as it has a high QUALITY FACTOR (24.27) and BER (1 X 10^{-40}) at 16 channels.**

Keywords-RAMAN-EDFA; RAMAN-SOA; SOA-EDFA; EDFA-RAMAN-EDFA; QUALITY FACTOR; BER; EYE OPENING; JITTER.

I. INTRODUCTION

Technology developments have described that optical is fantastic for the transmission. In fiber optic communications, WDM is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths at speed in Gbps [1-3].WDM of optical signals is a promising way to increase transmission capacity of a fiber. The development of WDM has allowed us to exploit large amount of bandwidth available in optical fiber as low capacity channels [4]

An optical network is optical but switching could be optical, electrical or hybrid as well [5] whereas optical amplifiers are used which directly amplify the transmitter optical signal without conversion to electric forms and also can be used for long distance transmission which can be pre or post amplifier. An optical amplifier is a laser without a feedback [6]. It uses the principle of stimulated emission same as used in laser.

Dense wavelength division multiplexing (DWDM) uses the same transmission window but with denser channel spacing. Channel plans vary, but a typical system would use 40 channels at 100 GHZ spacing or 80 channels with 50 GHZ spacing. The cascading a semiconductor optical amplifier (SOA) and a fiber Raman amplifier (FRA or RA) is called hybrid amplifier. There are two kinds of hybrid amplifiers (HA): seamless and wideband hybrid amplifiers (SWB-HA) and narrowband amplifier (NA). Hybrid amplifier increases the transmitter power by placing it just after the transmitter and before the receiver without any splitters, boosters in between as it increases the noises and distortion.

A Carena et al. [7] investigated on the optimal configuration of hybrid Raman/Edfa yielding a closed form analysis. In order to compare different system configurations, impact of fiber non linearities has been introduced. The maximum reachable distance has been evaluated with a target signal to noise ratio. Also he demonstrated that Raman amplification, combined with EDFAs, allow the increase of the maximum reachable distance and/or the span length. Raman amplification can also be used to substantially reduce the impact of fiber nonlinearity.

Chieng Hung Yeh et al. [8] demonstrated a new hybrid three stage L-band fiber amplifier module composed of a semiconductor optical amplifier and two Edfa over gain bandwidth of 1540 to 1600 nm. This proposed amplifier also provides a broadband amplified spontaneous emission light source. Also he experimentally demonstrated a new hybrid L-band fiber amplifier utilizing a semiconductor optical amplifier and two erbium-doped fiber amplifiers over the gain bandwidth of 1540 to 1600 nm. This proposed amplifier also provides broadband ASE light source. Therefore, this amplifier is useful in application to WDM networks.

Ju Han Lee et al. [9]demonstrated on the performance of three different schemes of single pump dispersion compensating fiber based Raman/Edfa hybrid amplifier together with a DCF based Raman only amplifier in terms of static properties, dynamic and system impact. With respect to overall gain and system impact, based on BER hybrid amplifier was found to have the best performance among other types. On the contrary, a much higher transient tolerance was observed in the Raman-only amplifier than the hybrid amplifiers since the EDF section in the three types of hybrid amplifiers is highly sensitive to transient environments.

Seung Kwan Kim et al. [10] proposed the design of hybrid amplifier composed of a distributed Raman amplifier and Edfa. They characterize the distributed Raman amplifier by numerical simulation based on measured Raman gain coefficient of single mode fiber. They estimated the performance of the hybrid amplifier for long haul optical transmission. In single channel amplification, the crosstalk caused by double Rayleigh scattering was independent of signal input power and simply given as a function of the Raman gain. Compared with erbium-doped fiber amplifiers, the

optical signal-to-noise ratio was calculated to be higher by more than 3 dB in the optical link using the designed hybrid amplifier

T. Sakamoto et al. [11] designed the gain characteristics of the hybrid fiber amplifier that consists of cascaded thulium doped fiber amplifiers and Edfa are reported. The results showed that the hybrid amplifier have a gain of over 20 dB with bandwidth of 20Db and wavelength range of about 1460 and 1560nm. The low noise figure (NF) below 7 dB was obtained in 1460–1540 nm when placing a TDFA in the first stage followed by an EDFA and in 1480–1560 nm when placing amplifiers in a reversed order. The gain-equalization technique was applied, and the hybrid amplifier that had an average gain of 20 dB, a gain excursion of less than 2 dB, an output power of 14.5 dbm, and an NF of less than 7 dB in the 77-nm gain band was achieved.

We pursue and extend the same work which includes comparison of only 16 channel whereas we have compared the performances of different hybrid amplifiers on various number of channels of 16, 32 and 64.

This paper is organized into four sections. We focus on the comparison and performance of hybrid amplifiers. In section 2, simulation setup for comparison of different hybrid amplifiers. The performance of amplifiers is analyzed here. Section 3 gives the discussions of results observed after simulation. Section 4 gives the conclusion of Quality Factor, Ber, Eye Opening, Jitter, and Power at different channels.

II. Simulation Setup

To investigate the performance of the hybrid amplifiers, at sixteen, thirty two or sixty four user transmitters are used at a speed of 10 Gbps speed as shown in fig 1. The signals from data source and laser are fed to the external Mach-Zehnder modulator, where the input signals from data source are modulated through a carrier optical output signal is transmitted. These signals are transmitted over spliter to which the optical power meter and optical spectrum analyser is attached. The optical splitter splits the optical signals into two or more outputs. Further a compound component is placed which consists of Raman-Edfa, Raman-Soa, Soa-Edfa, and Edfa-Raman-Edfa. We can also choose any other hybrid amplifiers according to the requirements. Again then optical splitter is attached to which optical power meter and optical spectrum analyser are attached. Later, the receiver is attached which is used to detect all signals and converted into electrical signal. Different types of optical amplifiers are applied at different channels. The optical signal is transmitted and measured over different distance using different number of channels. The different parameters like quality factor, Ber, eye opening, jitter are calculated at different channels and best of it is calculated at various channels. Optical signals are amplified using EDFA amplifier. The signal power is measured by power meter and optical probe. The modulated signal is converted into original signal with the help of PIN photodiode and filters. A compound receiver is used to detect all the signals and converts these into electrical signals. Also a power meter can be attached to achieve the power at the receiver end which is needed for the project.

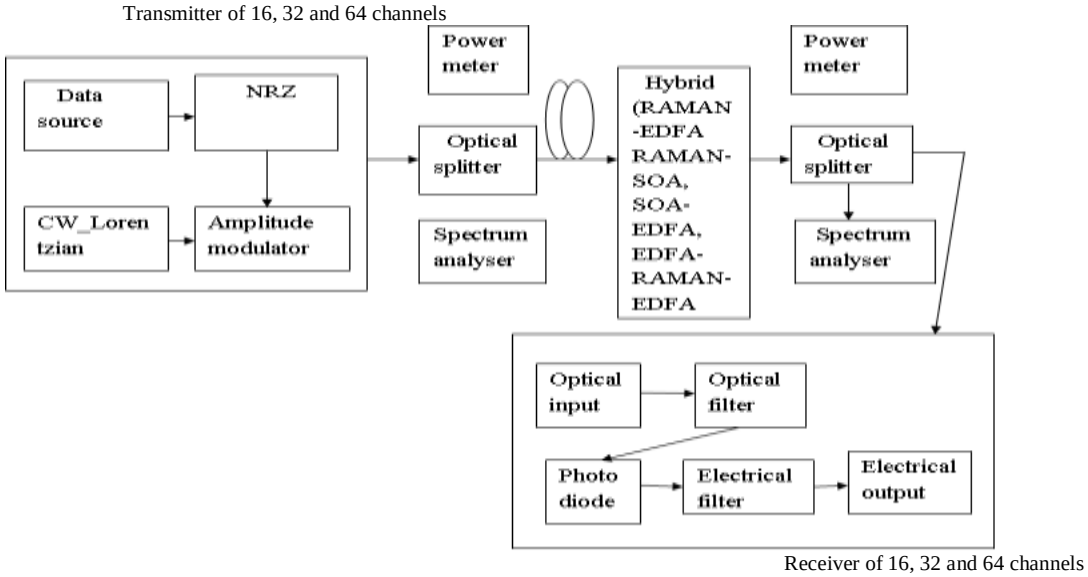


Fig 1: block diagram of simulation setup

III. Results and Discussions

The performance of different hybrid amplifiers is compared at different distances. As we increase the distance, the output power decreases simultaneously. Different components have different operational parameters. The comparison of different hybrid amplifiers at different channels is discussed.

In order to observe the performance of different amplifiers (Raman-Edfa, Raman-Soa, Soa-Edfa, Raman-Edfa-Raman), the quality factor versus transmission distance graph is plotted.

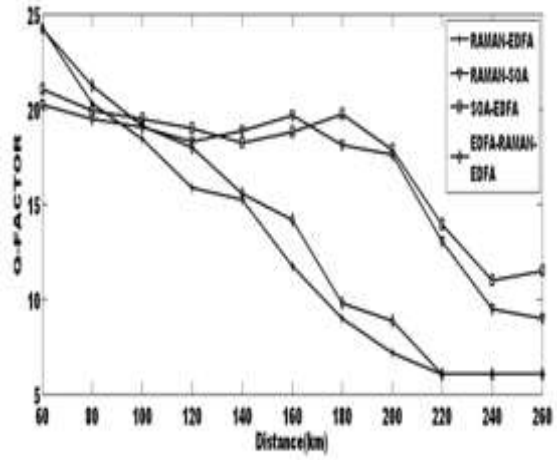


Fig 2 Distances vs. Quality Factor for 16 channels

As we increase the transmission distance from 60 km to 260, the quality factor decreases because of the crosstalk and carrier density fluctuation in SOA. The variation in different optical amplifier at distance 60 km is 24.273 for Raman-Edfa, 20.206 for Raman-Soa, 21.019 for Soa-Edfa, and 24.249 for Raman-Edfa-Raman. The variation in Quality Factor for different optical amplifier at distance 220 km is 6.020 for Raman-Edfa, 13.020 km for Raman-Soa, 13.904 for Soa-Edfa, 6.020 for Raman-Edfa-Raman.

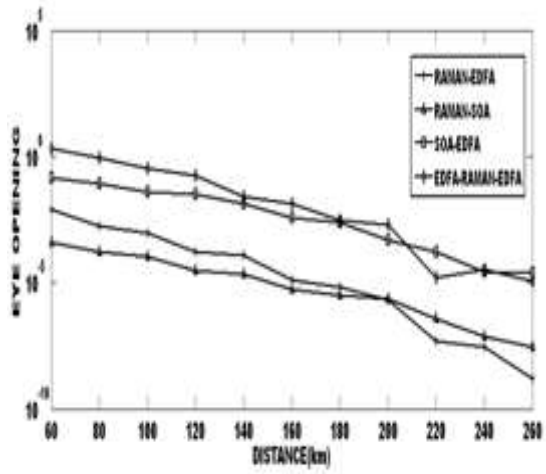


Fig 3 Distances vs. Eye Opening for 16 channels

In order to observe the performance of different hybrid amplifiers, the eye opening versus transmission distance are shown in figure 3.This graph shows that as we increase the transmission distance from 60 to 260 km, the eye opening increases simultaneously from .007676 to $1.61481X10^{-09}$. The eye opening from different amplifiers verses transmission distance is shown in figure 3.Large eye opening means less BER and good communication

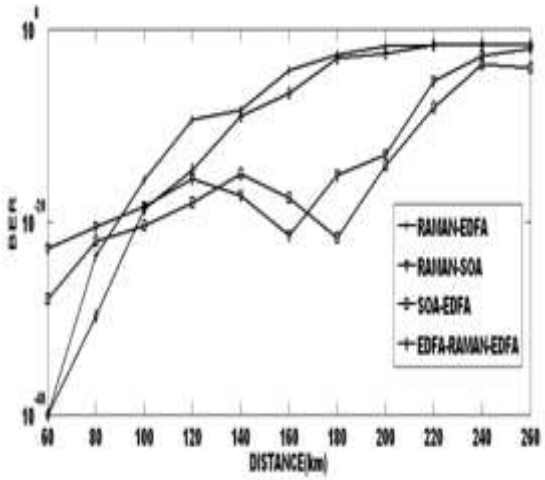


Fig 4 Distances vs. Ber for 16 channels

As shown in figure 3.BER increases with distance from 10^{-40} to .0227501 for Raman-Edfa and 10^{-23} to 10^{-06} for Raman-Soa. Further for Soa-Edfa, BER increases from $10^{-29\ to}$ 10^{-05}. The acceptable bit error rate (BER) for optical transmission is 1×10^{-10}. Means there is more distortion in the detected signal. The BER versus transmission distance is shown in figure. It is observed that by increasing the transmission distance from 60 to 260 km, BER is also increasing.

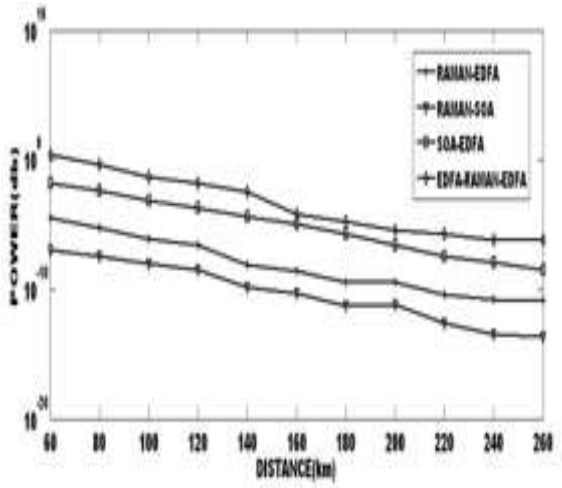


Fig 5 Distances vs. Power for 16 channels

As shown in fig 5 the power versus distance, power decreases with distance from .112 X 10^{-06} to .231 X 10^{-13} db for Raman-Edfa,.314 X 10^{-04} to .128 X 10^{-10} for Raman-Soa,.143 X 10^{-01} to .361X 10^{-08} for Soa-Edfa and .240 X 10^{01} to .712 X 10^{-06} for Raman-Edfa-Raman for 16 channel The acceptable power for optical transmission is 10 db. It is observed that by increasing distance from 60 to 260 km, power is also decreasing.

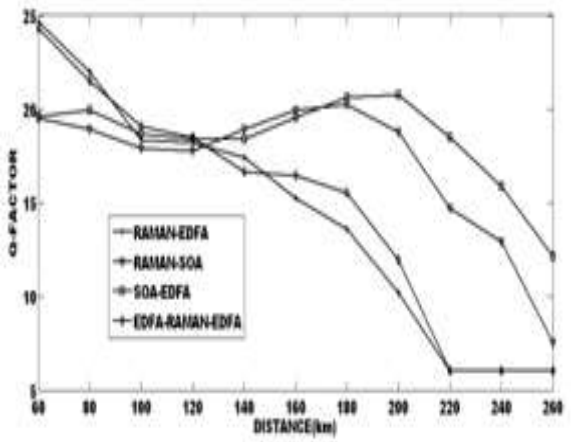


Fig 6 Distance vs. Quality factor for 32 channels

In order to observe the performance of different hybrid amplifiers, the quality factor versus transmission distance are shown in figure 6.This graph shows that as we increase the transmission distance from 60 to 260 km, the quality factor decreases simultaneously. The quality factor decreases from 24.645 to 6.020 dB for Raman-Edfa,19.495 to7.52 db for Raman-Soa,19.58 to12.157 for Soa-Edfa and 24.32 to 6.020 for Raman-Edfa-Raman.

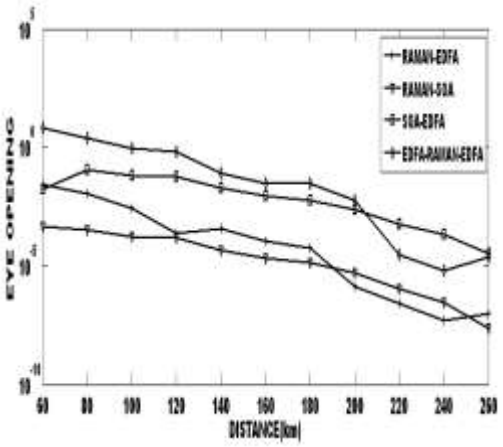


Fig 7 Distances vs. Eye Opening for 32 channels

In order to observe the performance of different hybrid amplifiers, the eye opening versus transmission distance are shown in figure 7. Large eye opening means less BER and good communication. This graph shows that as we increase the transmission distance from 60 to 260 km, the eye opening increases simultaneously

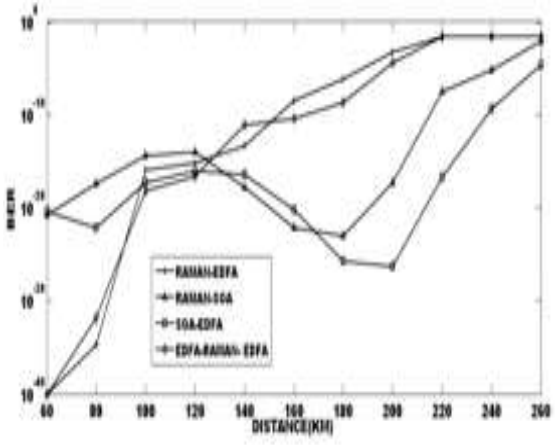


Fig 8 Distances vs. Ber for 32 channels

The BER versus transmission distance for different dispersion is shown in figure. It is observed that by increasing the transmission distance from 60 to 260 km, BER is also increasing. The acceptable bit error rate (BER) for optical transmission is 1×10^{-10}.

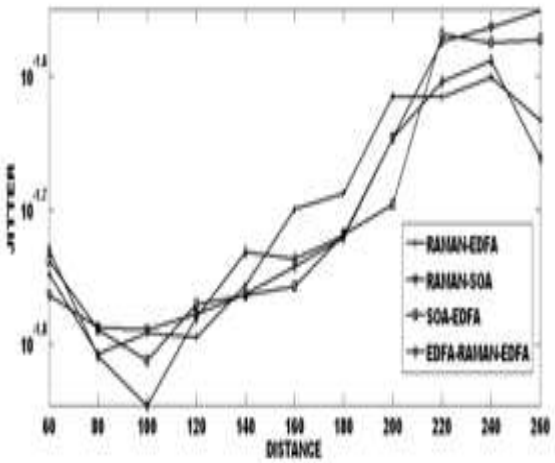


Fig 9 Distances vs. Jitter for 32 channels

In order to observe the performance of different hybrid amplifiers, the jitter versus transmission distance are shown in figure 3.This graph shows that as we increase the transmission distance from 60 to 260 km, the jitter decreases and then increases simultaneously.

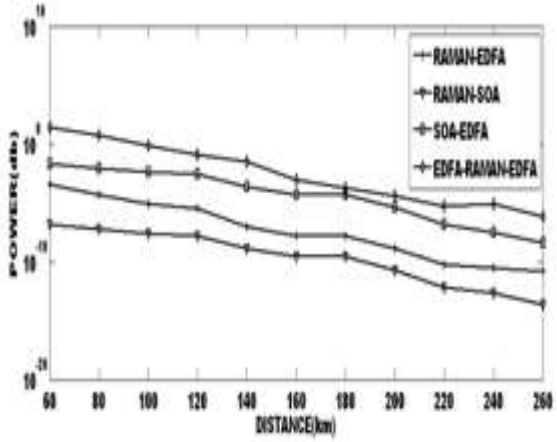


Fig 10 Distances vs. Power for 32 channels

The power versus distance is shown in figure 4.Power decreases with distance from .350 X 10^{-03} db to .163 X 10^{-10} for 32 channels for Raman-Edfa. It is because of non linearities and losses in the channel. The acceptable power for optical transmission is 10 db. It is observed that by increasing distance from 60 to 260 km, power is also decreasing.

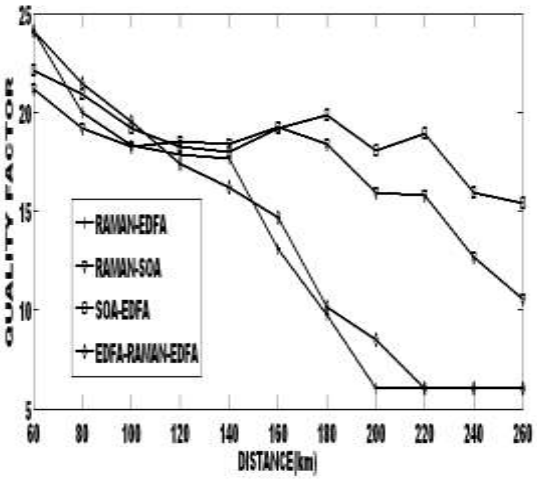


Fig 10 Distances vs. Quality Factor for 64 channels

This graph shows that as we increase the transmission distance from 60 to 260 km, the quality factor decreases simultaneously because of the carrier density fluctuation and crosstalk in SOA. The quality factor decreases from 24.117 to 6.020 db for Raman-Edfa, 21.184 to10.521 db for Raman-Soa, 22.105 to 15.321 for Soa-Edfa and 24.125 to 6.020 for Raman-Edfa-Raman.

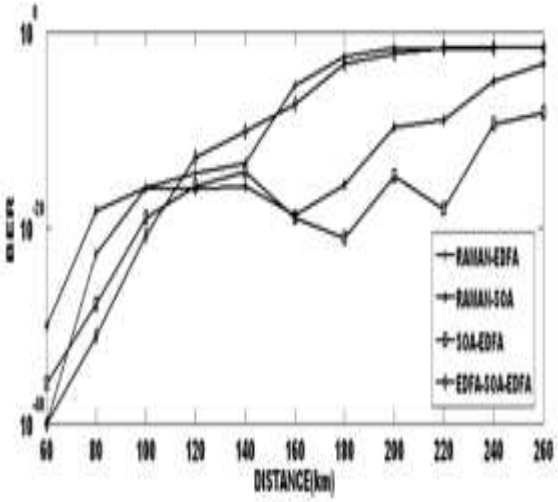


Fig 11 Distances vs. Ber for 64 channels

The BER versus transmission distance for different dispersion is shown in figure. It is observed that by increasing the transmission distance from 60 to 260 km, BER is also increasing. As shown in figure 11, BER increases with distance from 10^{-40} to .0227501 for Raman-Edfa and 10^{-31} to .000488 for Raman-Soa. Further for Soa-Edfa, BER increases from 10^{-37} to 10^{-09}

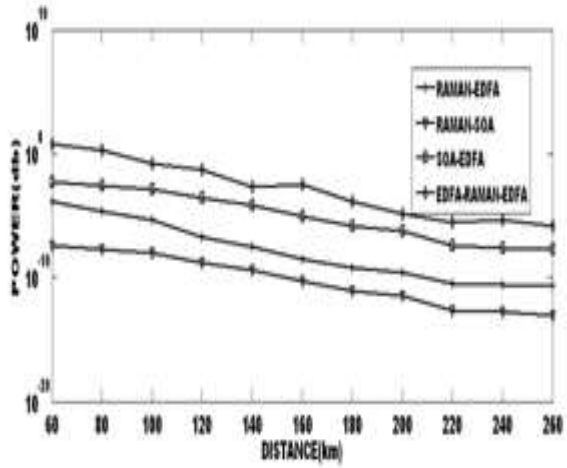


Fig 12 Distances vs. Power for 64 channels

The power versus distance is shown in figure 12.Power increases with distance from .57 X 10^{01} to .134 X 10^{-05}db for 64 channels. The acceptable power for optical transmission is 10 db. It is observed that by increasing distance from 60 to 260 km, power is also decreasing.

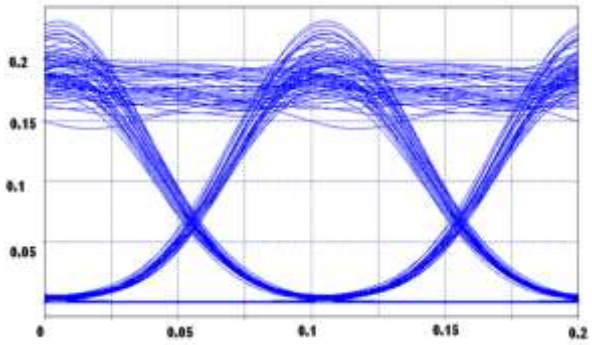


Figure 13(a) SOA-EDFA, 16 channels for Distance = 60

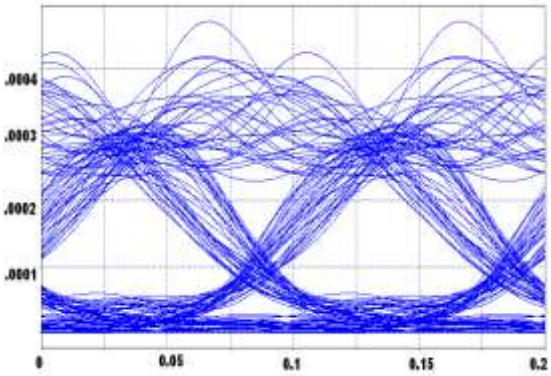


Figure 13(b) SOA-EDFA, 16 channels for Distance = 220 kms

It is observed from the simulation result that maximum eye opening is obtained from SOA-EDFA is 1.37×10^{-1}, 4.6×10^{-4} for D=60km and D=220kms respectively.

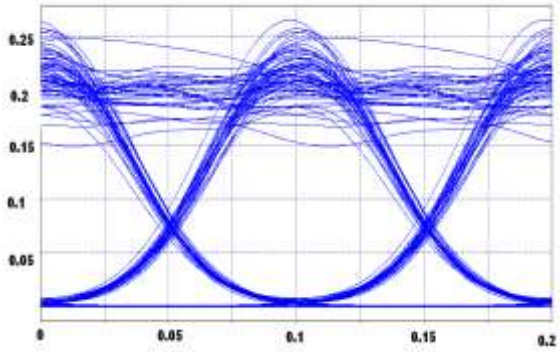


Figure 14(a) SOA-EDFA, 32 channels for Distance = 60kms

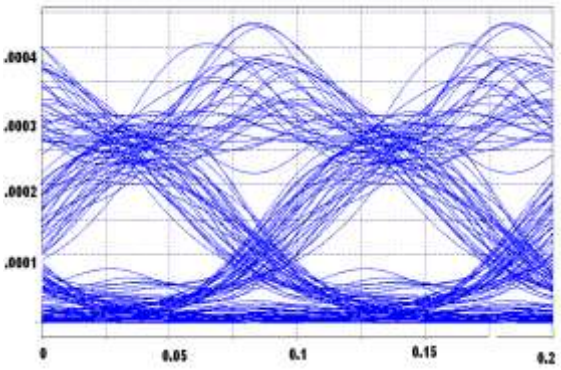


Figure 14(b) SOA-EDFA, 32 channels for Distance = 240kms

Eye diagram of signal for 32 channel of SOA- EDFA at 60 kms and 240 kms distance shown in figure. The eye opening for distance 60 km is 1.7×10^{-1} and for 240 km is 2.1×10^{-4} respectively.

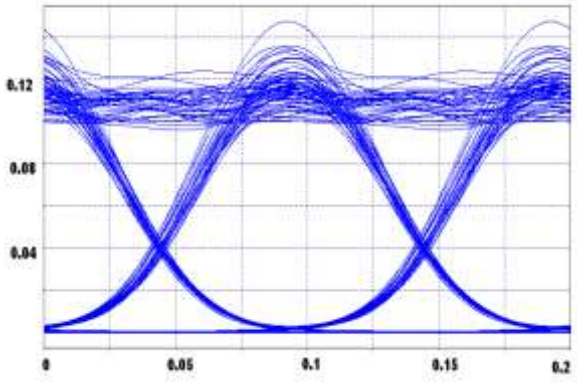


Figure 15(a) SOA-EDFA, 64 channels for Distance = 60 kms

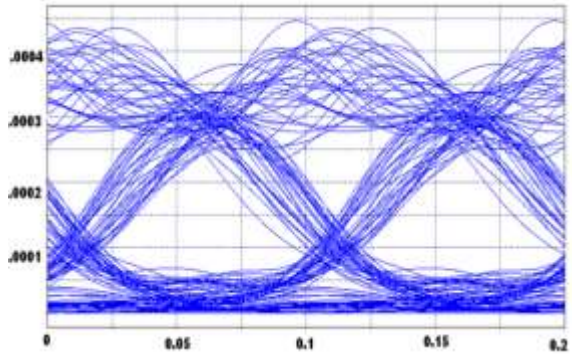


Figure 15(b) SOA-EDFA, 64 channels for Distance = 260 kms

Eye diagram of signal for SOA-EDFA at 60 km and 260 distances for 64 channels is shown in figure 3.13. The eye opening for distance 60 km is 9.3×10^{-2} and 1.7×10^{-4} respectively.

IV. Conclusion

The performance of different hybrid amplifiers is compared at different distances. The result shows that SOA combined with EDFA allows the increase of maximum reachable distance and span length. In this SOA-EDFA showed good performance at all the channels as it can travel max distance. The proposed configuration consists of 16, 32 and 64 channels. Hybrid SOA-EDFA are enabling and promising for future as it can travel the maximum distance. It is observed through simulation that RAMAN-EDFA provides the best performance in terms of quality factor, ber, eye opening and jitter. But as the distance increases, the quality factor and power degrades whereas ber increases. In case of SOA-EDFA, covers maximum distance i.e. 220, 240 and 260 kms with variations in channel.

References

[1] Manjit Singh, Ajay K. Sharma, R.S.Kaler 'Investigations on order and width of RZ super Gaussian pulse in pre-, post- and symmetrical-dispersion compensated 10Gb/s optical communication system using standard and dispersion compensating fibers', Optik -International Journal for Light and Electron Optics, Vol 121, Issue 7, Apr 2010, Pg 609-616.

[2] Manjit Singh, Ajay K. Sharma, R.S.Kaler 'Optimizing 10 Gbps optical communication system with duty cycle selection of return to zero pulse', Optik - International Journal for Light and Electron Optics, Vol 119, Issue 8, 16 Jun 2008, Pg 359-364.

[3] D.P, Mitchel J.E, 'A 10-Gb/s 1024-Way-Split 100-km Long-Reach Optical-Access Network', journal of lightwave technology, Vol 25,Issue 3, 2007, Pg 685-695.

[4] A. Jourdan, F. Masetti, M. Garnot, G. Soulage, M. Sontom, Design and implementation of a fully reconfigurable all-optical cross connect for high capacity multi wavelength transport networks, J. Lightwave. Tech. 14 (6) (1996) 1198–1206

[5] Biswanath Mukherjee, 'Optical WDM Networks', University of California, pg 15-18

[6] G.P.Aggarwal, ' Fibre Optic Comm.', John Wiley and Sons, New York, pg 226

[7] A.Carena,V.Curri and P.Poggiolini, 'On the Optimization of Hybrid Raman/Erbium-Doped Fiber Amplifiers', Vol. 13, NO. 11, Nov 2001, pg 1170-1172

[8] Chien-Hung Yeh, Kuo Hsiang Lai, Ying Jie HUANG Chien-Chung LEE and Sien CHI. ' Hybrid L-Band Optical Fiber Amplifier Module with Erbium-Doped Fiber Amplifiers and Semiconductor Optical Amplifier', Vol. 43, No. 8A, 2004, pg 5357–5358

[9] Ju Han Lee, You Min Chang, Young Geun Han, Haeyang Chung, Sang Hyuck Kim, and Sang Bae Lee. A Detailed Experimental Study on Single-Pump Raman/EDFA Hybrid Amplifiers: Static, Dynamic and System Performance Comparison, Vol 23, I11, 2005, pg 3484-3493

[10] Seung Kwan Kim, Sun Hyok Chang, Jin Soo Han, and Moo Jung Chu. Design of Hybrid Optical Amplifiers for High Capacity Optical Transmission, Vol 24, No2, 2002, pg-81-96

[11] Tadashi Sakamoto, Shin-ichi-Aozasa, Makoto Yamada, and Makoto Shimizu. Hybrid Fiber Amplifiers Consisting of Cascaded TDFA and EDFA for WDM Signals, 2006, Vol 24, I6, pg-2287-2295

Fidelity Based On Demand Secure(FBOD) Routing in Mobile Adhoc Network

Himadri Nath Saha
Assistant Professor
Department of Computer Science and Engineering,
Institute of Engineering and Management
West Bengal, India.

Dr. Debika Bhattacharyya
Professor
Department of Computer Science and Engineering.
Institute of Engineering and Management, West Bengal, India.

Dr. P. K.Banerjee
Professor
Department of Electronics and Communication Engineering.
Jadavpur University, West Bengal, India.

***Abstract*—: In mobile ad-hoc network (MANET), secure routing is a challenging issue due to its open nature, infrastructure less property and mobility of nodes. Many mobile ad-hoc network routing schemes have been proposed, but none of them have been designed with security as a goal. We propose security goals for routing in mobile ad-hoc networks, an approach significantly different from the existing ones where data packets are routed, based on a specific criterion of the nodes called "fidelity" The approach will reduce the computational overhead to a lot extent. Our simulation results show how we have reduced the amount of network activity for each node required to route a data packet and how this scheme prevents various attacks which may jeopardize any MANET.**

Keywords- fidelity; sequence number; hop destination; flooding attack; black hole attack; co-operative black hole attac,routing.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network [20] infrastructure and centralized administration (Figure-1). Communication in MANET [8] is done via multi-hop paths. MANET contains diverse resources and nodes operate in shared wireless medium. [21] Network topology changes unpredictably and very dynamically. Radio link [31] reliability is necessary as connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET [28] acts a router that forwards data packets to other nodes. Therefore selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

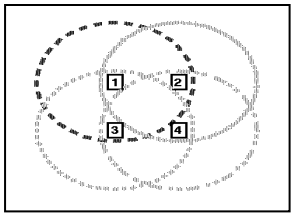


Figure 1: An ad-hoc mobile network with four nodes.

Rest of the paper is organized as follows. We have discussed related work in section 2 and describe the Fidelity in section 3,description of the scheme in section 4,algorithm of proposed scheme in section 5,simulation results in section 6 ,security aspects in section 7, the simulation analysis and performance metrics in section 8 and finally present our conclusions in section 9.

II. RELATED WORK

S. Matri [33] proposed to trace malicious nodes by using watchdog/pathrater. In watchdog when a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet by promiscuously listening to the next node's transmissions. If the watchdog finds the next node does not forward the packet during a predefined threshold time, the watchdog will accuse the next node as a malicious node to the source node; The proposal has two shortcomings: 1) to monitor the behavior of nodes two or more hops away, one node has to trust the information from other nodes, which introduces the vulnerability that good nodes may be bypassed by malicious accusation; 2) The *watchdog* cannot differentiate the misbehavior from the ambiguous collisions, receiver collisions, controlled transmission power, collusion, false misbehavior and partial dropping. In pathrater algorithm each node uses the watchdog's monitored results to rate its one-hop neighbors. Further the nodes exchange their ratings, so that the pathrater can rate the paths and choose a path with highest rating for routing. Shortcoming of this algorithm is that the idea of exchanging ratings genuinely opens door for blackmail attack.

SCAN [11] exploits two ideas to protect the mobile Ad Hoc networks [17]: 1) local collaboration: the neighboring nodes collectively monitor each other and sustain each other; and 2) information cross-validation: each node monitors its neighbors by cross-checking the overheard transmissions, and the monitoring results from different nodes are further cross validated. As a result, the security solution is self-organized, distributed, and fully localized. In SCAN once a malicious node is convicted by its neighbors, the network reacts by depriving its right to access the network by revoking its token. A powerful collusion among the attackers will break SCAN as it violates the assumption of the polynomial secret sharing scheme.

Gonzalez [24] presents a methodology, for detecting packet forwarding misbehavior, which is based on the principle of flow conservation in a network. It states that if all neighbors of a node v_j are queried for i) the amount of packets sent to v_j for forwarding and ii) the amount of packets forwarded by v_j to them, then the total amount of packets sent to and received from v_j must be equal. They assume a threshold value for non

malicious packet drop. A node v_i maintains a table with two metrics T_{ij} and R_{ij}, which contains an entry for each node v_j to which v_i has respectively transmitted packets to or received packets from. Node v_i increments T_{ij} on successful transmission of a packet to v_j for v_j to forward to another node, and increments R_{ij} on successful receipt of a packet forwarded by v_j that did not originate at v_j. All nodes in the network continuously monitor their neighbors and update the list of those they have heard recently. This algorithm does not require many nodes to overhear each others' received and transmitted packets, but instead it uses statistics accumulated by each node as it transmits to and receives data from its neighbors. Since there is no collaborative consensus mechanism, such an algorithm may lead to false accusations against correctly behaving nodes.

Himadri [34, 35, 36], in their literatures have shown ways to mitigate attacks on different MANET networks. We have extended their works n this field.

III. FIDELITY

Fidelity is the most important concept of this routing protocol. Fidelity is an integer number that is associated with each node. This fidelity of a node denotes many things about the node itself and also deciphers other information regarding the topology of the entire network. It also helps to maintain security [29] to some extent.

To make it understandable in one sentence, "fidelity is a counter that is associated with a node, which is increased whenever it forwards a data packet successfully." Whenever a node comes in a network its fidelity is zero and whenever it goes permanently off from the network its value is again refreshed to zero. Otherwise whenever a node will forward any data packet it will always increase a counter value and that counter value is its fidelity. Note whenever a source node sends a data packet to a destination node, all the intermediate nodes helping to transmit its data packet will increase their counter but the source and the destination node do not increase their fidelity value.

Fidelity is a measure of these two factors:-

A. How reliable a node is for forwarding a data packet

Whenever we observe that the fidelity value of a particular node is greater that of another node then we can conclude that the one having the greater value is a more durable node than the other from who's its value is greater. It is quite logical because a node with greater value indicates that it is an experienced node in the network and it has transmitted packets most dutifully than other nodes.

B. Network topology

If we can find some nodes with higher fidelity in a region of the network, we conclude that the network activity is higher in that region. More precisely we can also infer that the node density is also higher in that region for it is impossible to have one node having very high fidelity [19] surrounded by nodes with low fidelity because a high fidelity [18] node must send packets to someone in its vicinity which will make that other node's fidelity value also high. Thus a high fidelity value accounts for high network activity as well as high density of nodes in its surroundings.

IV. DESCRIPTION OF THE SCHEME

The term "friends of a node" used in this paper, indicates actually the nodes that fall in the physical range of a particular node. When nodes are having messages to send, all the nodes will check which nodes are in its neighborhood and they will broadcast a request. After getting reply they will make their friend list. More precisely the friend list consists of a table that contains two attributes. The first one is the address [14] of the nodes which are within its range and other is the fidelity value of that particular node. When each node is updated then they will sort that table according to the decreasing order of the fidelity value. Before we enter into the detailed discussion of our protocol there are some concepts that need to be understood. These are as follows-

There will be a sequence counter in every node. If a message is generated in a node then it will be increased by one. This sequence no. will be forwarded as a part of the message. Every node will maintain a buffer where (source, sequence no.) will be stored for last n no. of received messages. After getting a message a node will verify the tuple [24] (source, sequence no) of that message with those tuples in its buffer [13]. If anyone of them matches with that message then that node will reject that message silently. It will prevent flooding attack.

The timeout period of every node through which message is traversed, will be gradually decreased by a critical factor [15] i.e. if timeout period of sender node is x then timeout period of receiver node will be x/m, where m will be critical factor. This factor [23] signifies maximum no of failure a node can endure without causing congestion in the network.

Now the protocol is as follows-

A node can do either of three activities - message generate, message forward, message receive. If it is not doing any of the three then it is idle. Now if a message is generated in a node and it needs to be sent then the node will remain busy until an acknowledgement is received for this message. It is to be noted that a busy node can accept & process an acknowledgement and can send a fail message.

Now if destination is directly reachable from generator node then it will send message to destination node and will wait for acknowledgement, and remain busy until acknowledgement is received. If the destination node is busy it will send a fail message to generator node. After getting fail message or if timeout period exceeds, generator node will keep on sending the message after a certain time periodically until acknowledgement is received.

If destination is not directly reachable then generator node will send message to the node in its range that has highest fidelity value. If generator node get a fail message from that node or if timeout period exceeds then it will send the message to the node having second highest fidelity value and it will continue like this. If the whole list is exhausted in this way then the process will again continue from the node having highest fidelity value. Only generator node will follow this process.

Other nodes will send a fail message to its predecessor if the whole list is exhausted.

When a node receives a message, if it is busy then it will send a fail message to sender, otherwise it will check whether it itself a destination or not. If it is destination, it will accept the message and send acknowledgement to sender otherwise this node will send message to the node in its range that have highest fidelity value and that process will continue. In that acknowledgement message the sequence no. will be same as received message but source will be substituted by destination.

V. ALGORITHMS

Update friend list

STEP 1: Send broadcast request for friends to reply
STEP 2: Receive replies from neighbours
STEP 3: Update my friend list
STEP 4: Sort friend list

Generated data

STEP 1: Set my status=busy
STEP 2: If destination directly reachable from here
- Send packet to destination
- Wait for ACK
- If ACK received consider success
- Else if timeout occurs or FAIL received, arrange for resending
  Else
- Send data packet to the friend having highest fidelity value
- Wait for ACK
- If ACK received consider success and go to last step
- Else if timeout occurs or FAIL received, arrange for resending to the friend with next highest fidelity value
- Continue above three steps until ACK received
- If list is exhausted without getting an ACK then again start from the friend with the highest fidelity value and try each node in friend list in the manner told above.
- While trying to send if the list is exhausted thrice abort

STEP 3: Set my status=free

Received data

STEP 1: If my status=busy send FAIL to sender

STEP 2: Else
- Make my status=busy
- Process received data
- Make my status=free

Process received data

STEP 1: If message destination=my address
- Accept data
- Generate ACK
- Send the ACK to the node from which it directly received the message

STEP 2: Else
- Forward data packet
- Check if forward operation is successful
- If successful increase my fidelity value by 1 and send ACK to the node from which it directly received the message
- Else send FAIL to the node from which it directly received the message

Forward data packet

STEP 1: If message destination is directly reachable from here
- Send packet to destination
- Wait for ACK
- If ACK received consider success
- Else if timeout occurs or FAIL received, arrange for resending to destination.
- If resending fails 3 times consider failure.

STEP 2: Else
- Send data packet to the friend having highest fidelity value
- Wait for ACK
- If ACK received consider success
- Else if timeout occurs or FAIL received, arrange for resending to the friend with next highest fidelity value
- Continue above three steps until ACK received
- If list is exhausted without getting an ACK then consider failure.

VI. SIMULATION RESULT

We have simulated this protocol with JAVA. We need to know something to make out these simulations. These are-

1. Small circle signifies node in the network.
2. Blue circle around node signifies range of that node.
3. Red color indicates that the node is free.
4. Black color indicates that the node is busy.
5. Yellow line indicates probing for neighbors.
6. Pink line indicates reply of probing.
7. Red line between two nodes indicates sending of message.
8. Green line between two nodes indicates sending of acknowledgement.
9. Blue line between two nodes indicates sending of fail message.
10. Any node inside the range of a node is its neighbor node.

Now we will describe one test case simulation.

This is a network having four nodes. Their corresponding fidelity values are written beside the nodes. Here we are trying to send a message from node 0 to node 3. This is basically a worst case scenario according to our protocol. We will see after sending the message a no of times how our protocol makes this worst case scenario to a best case one.

The design of network is

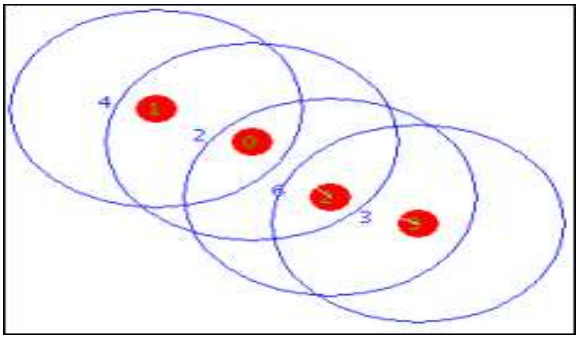


Figure 2: Design of network.

The result we get after net designing is given below-

4 <no of nodes>
2 4 2 3
-1 0 0 -1
0 -1 -1 -1
0 -1 -1 0
-1 -1 0 -1

we edit the adjacency list.txt as:-
4
2 4 2 3
-1 0 0 -1
0 -1 -1 -1
0 -1 -1 0
-1 -1 0 -1
0 <time interval>
0 3 hello <source> <destination> <msg>
10 <time interval>
0 3 hello1 <source> <destination> <msg>
10 <time interval>
0 3 hello2 <source> <destination> <msg>
10 <time interval>
0 3 hello3 <source> <destination> <msg>

then we run the simulation and see the results.

The steps of the visual simulation are given below-

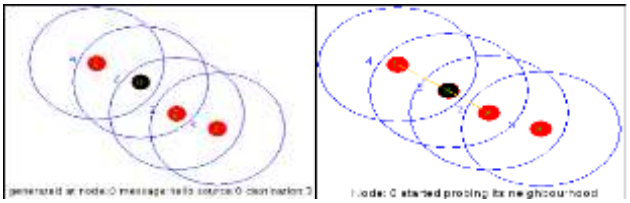


Figure 3: Message generated at node 0. . (left fig.)
Figure 4: Node 0 started probing. (right fig.)

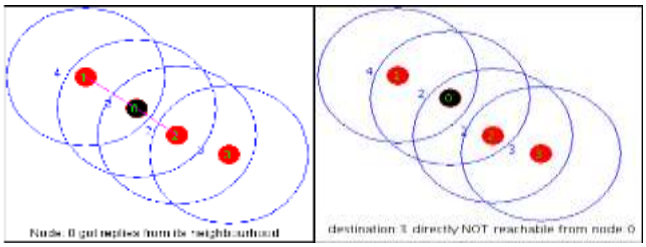


Figure 5: Node 0 got replies from neighbour nodes. . (left fig.)
Figure 6: Destination is not directly reachable from source node. (right fig.)

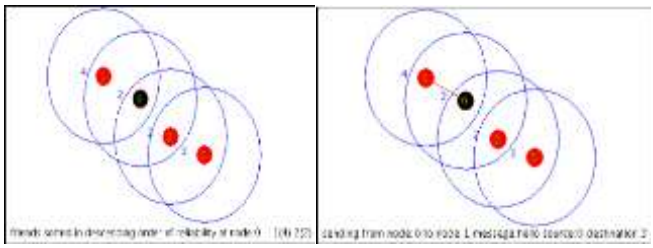


Figure 7: Friend nodes are sorted in descending order. . (left fig.)
Figure 8: Node 0 is sending message to node 1(right fig.)

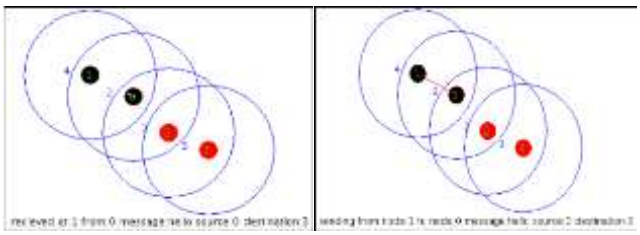


Fig 9: Message is received by node 1 (left fig.)
Fig 10: Node 1 is trying to send message to node 0. (right fig.)

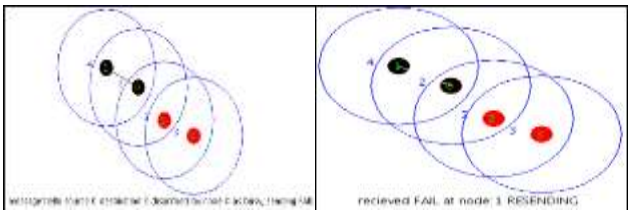


Fig 11: Node 0 discarded the message. . (left fig.)
Fig 12: Node 1 is resending the message. (right fig.)

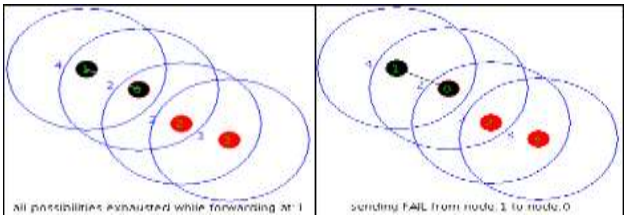


Fig 13: No possible ways to send the message. (left fig.)
Fig 14: Message sending fail from node 1 to node 0. (right fig.)

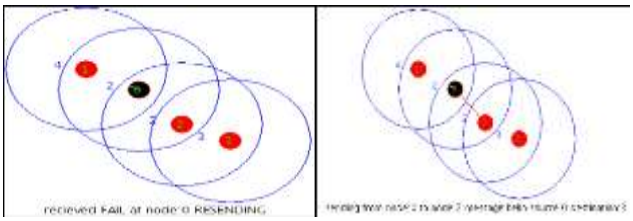


Fig 15: Node 0 resending the message via another path. . (left fig.)
Fig 16: Node 0 sending message to node 2 (right fig.)

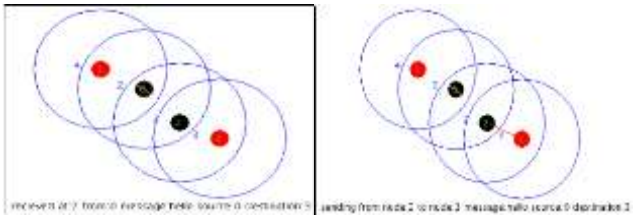


Figure 17: Message received by node 2. . (left fig.)
Figure 18: Node 2 is sending message to node 3. (right fig.)

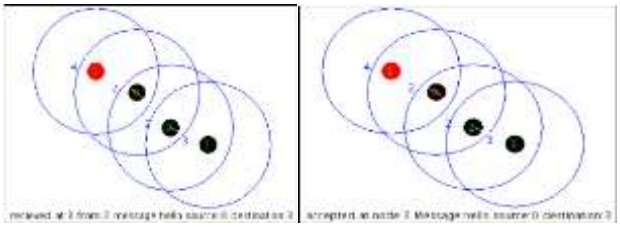


Figure 19: Message received by node 3. (left fig.)
Figure 20: Node 3 accepts the message. . (right fig.)

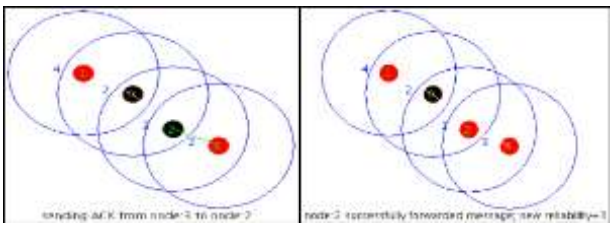


Figure 21: Node 3 is sending ACK to node 2. (left fig.)
Figure 22: Fidelity value of node 2 increases. (right fig.)

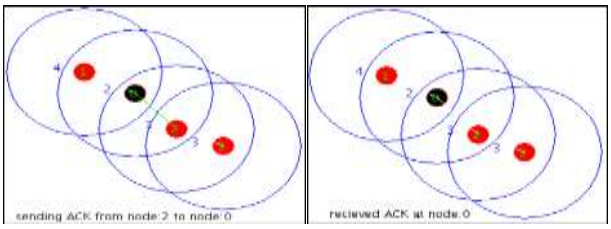


Figure 23: Node 2 is sending ACK to node 0. (left fig.)
Figure 24: Node 0 receives ACK. (right fig.)

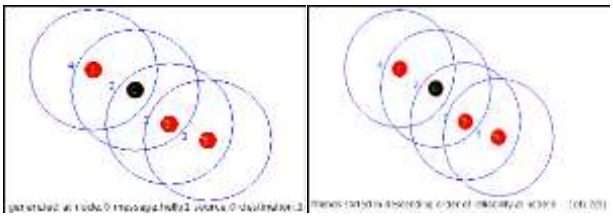


Figure 25: Node 0 wants to send another message to node 3. . (left fig.)
Figure 26: Friend are sorted by node 0 according reliability. (right fig.)

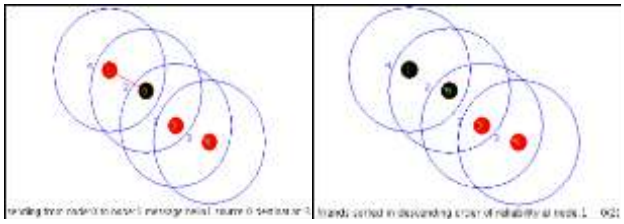


Figure 27: Node 0 is sending message to node 1. . (left fig.)
Figure 28: Friends are sorted by Node 1. (right fig.)

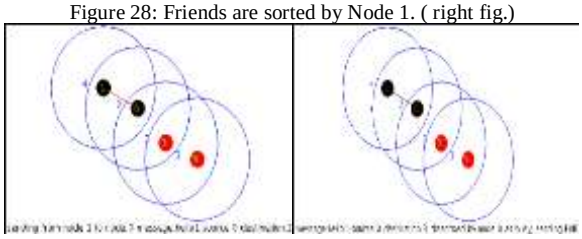


Figure 29: Node 1 is sending message to node 0. . (left fig.)
Figure 30: Node 0 discards the message. (right fig.)

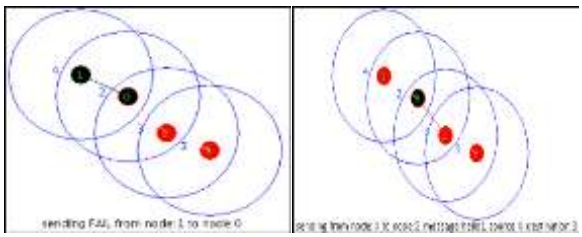


Figure 31: Node 1 fails to send the message. . (left fig.)
Figure 32: Node 0 sends the message to node 2. (right fig.)

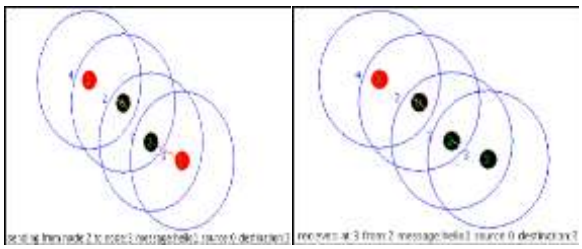


Figure 33: Node 2 sends the messages to node 3. . (left fig.)
Figure 34: Message received by node 3. (right fig.)

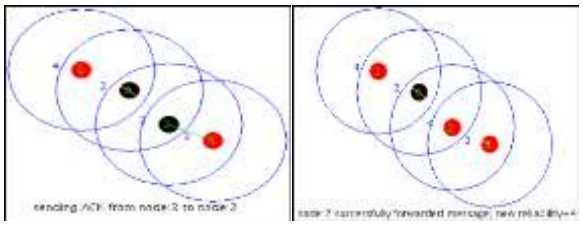


Figure 35: Node 3 is sending ACK to node 2. . (left fig.)
Figure 36: The fidelity value of node 2 increases to 4. (right fig.)

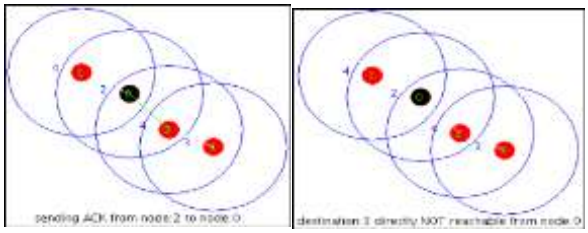


Figure 37: Node 2 sends ACK to node 0. . (left fig.)
Figure 38: Destination unreachable from source (right fig.)

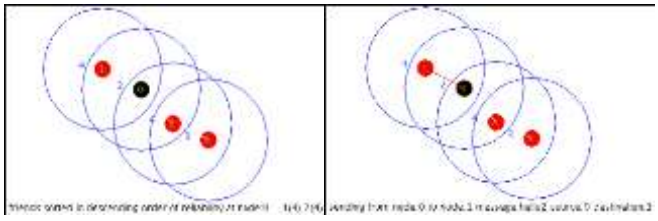


Figure 39: Node 0 sorts its friends to send another message. . (left fig.)
Figure 40: Node 0 is sending message to node 1. (right fig.)

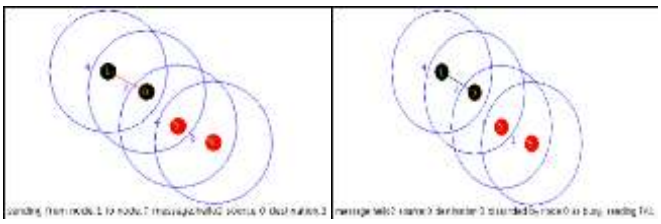


Figure 41: Node 1 is sending message to node 0. . (left fig.)
Figure 42: Node 0 discards the message. (right fig.)

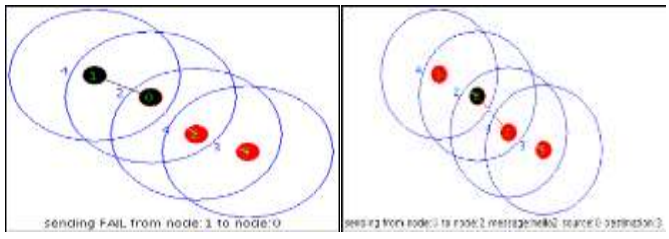


Figure 43: Node 1 couldn't send the message. . (left fig.)
Figure 44: Node 0 sends the message to node 2. (right fig.)

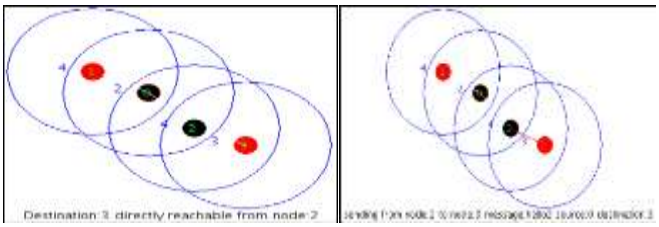


Figure 45: Node to can send the message to destination node. . (left fig.)
Figure 46: Node 2 sending message to node 3. (right fig.)

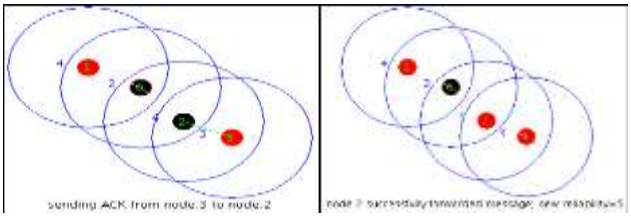


Figure 47: Node 3 sends ACK to node 2. . (left fig.)
Figure 48: Reliability of node 2 increased. (right fig.)

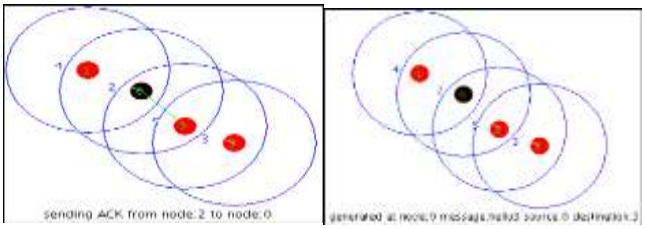


Figure 49: Node 2 sends ACK to node 0. . (left fig.)
Figure 50: New message is generated at node 0. (right fig.)

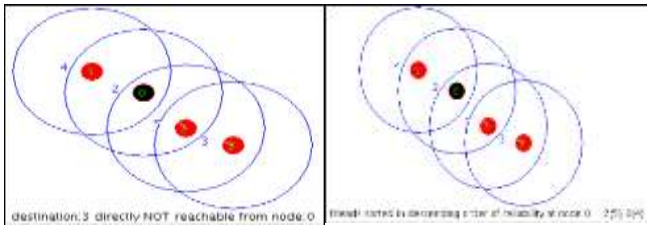


Figure 51: Source and destination node is not directly connected. . (left fig.)
Figure 52: Friends are sorted in descending order at node 0. (right fig.)

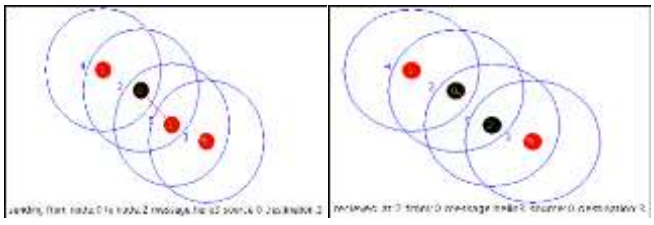


Figure 53: Node 0 sending message to node 2. . (left fig.)
Figure 54: Message received by node 2. (right fig.)

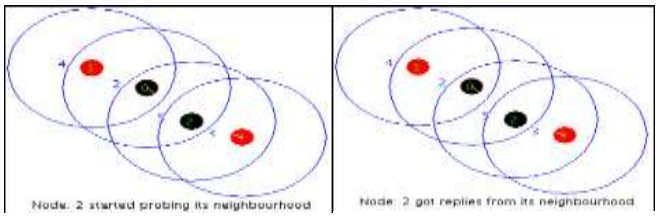


Figure 55: Node 2 started probing its neighbour nodes. . (left fig.)
Figure 56: Node 2 receives reply from neighbours. (right fig.)

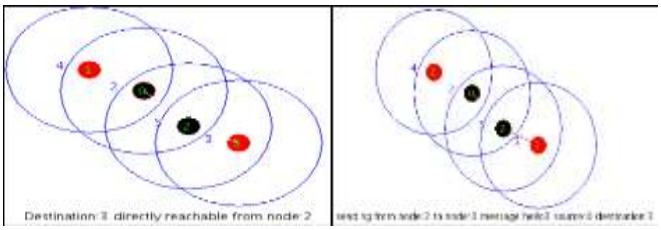


Figure 57: Destination node directly reachable from node 2. . (left fig.)
Figure 58: Node 2 sends message to node 3. (right fig.)

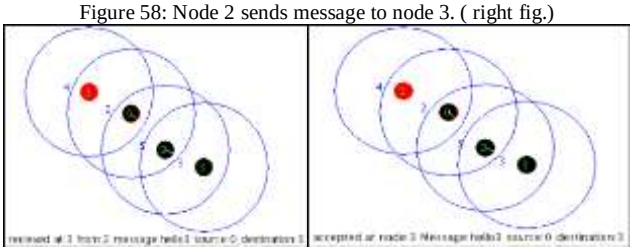


Figure 59: Message reached to node 3. . (left fig.)
Figure 60: Node 3 accepts the message. (right fig.)

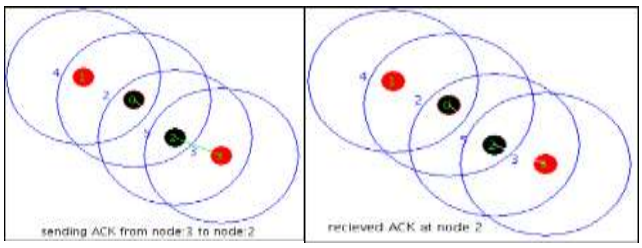


Figure 61: Node 3 sending ACK to node 2. . (left fig.)
Figure 62: Node 2 receives ACK. (right fig.)

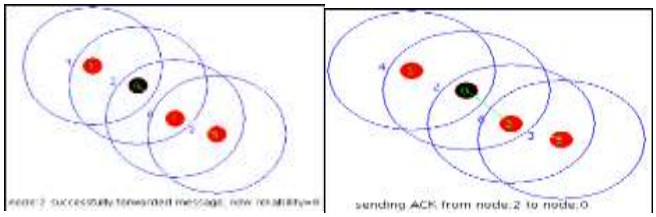


Figure 63: Message successfully forwarded by node 2. . (left fig.)
Figure 64: Node 2 sending ACK to node 0. (right fig.)

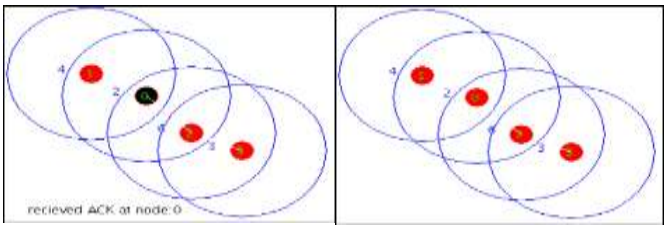


Figure 65: ACK received by node 0. . (left fig.)
Figure 66: All messages transferred successfully. (right fig.)

Message transfer is completed.

VII. Security Aspects

This scheme can efficiently mitigate Flooding attack [3], Black Holes [04] [30], Co-operative Black hole [04], Grey hole [03], Black mail attack [03], Rushing attack [01] and Wormhole Attack [03]. Our simulation has effectively depicted its immunity towards these attacks. This scheme is also safe from attacks to which AODV [08] [30], DSDV [1] is commonly subjected.

VIII. Simulation Analysis And Performance Metrics

In order to evaluate the performance of Ad Hoc network routing protocols, the following matrices were considered:

A. Packet Delivery Fraction

PDF is defined as the ratio between no. of packets originated by application layer [26] in the source node to the no of packets received by the destination node. It will describe the loss rate that will be seen by the transport protocols, which in turn affect the maximum throughput that the network supports. In terms of packet delivery fraction, our protocol FBRP performs well. As the no of nodes getting increased the no packets generated is higher so it may not transfer some of the packets, but the no of these packets are very small. When the no. of nodes is small then in ideal case PDF value is 1. But in case of DSR [10] the PDF is very fluctuating it is lesser in some of the points with respect to the other protocols but it is very higher in some of the points which are not tolerable. DSDV [12] is better in more no. of nodes but AODV [7] [2] is better in smaller no. of nodes region.

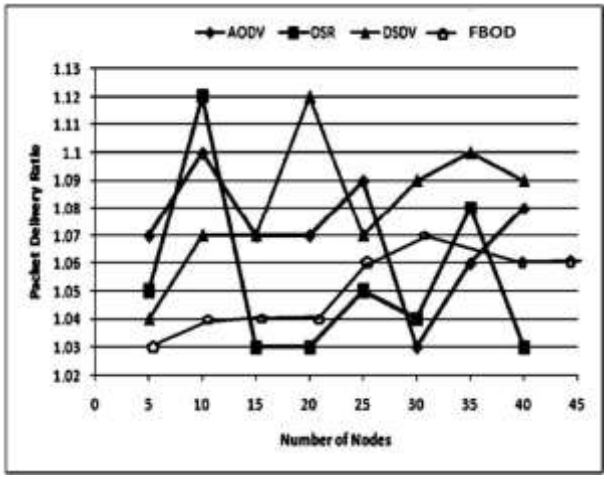


Figure 68.1: Packet Delivery Ratio for AODV, DSR, DSDV, FBOD

B. End to End Delay

The delay is affected by high rate of CBR Packets as well as the buffers become full much quicker, so packets have to stay in the buffer for a longer period of time before they are sent. This can be seen in DSR [8] when it reaches around 2300 packets in 0 mobility. For average end to end delay, the performance of DSR [9] decreases and varies with the number of nodes. In our protocol that is in FBRP the delay is getting increased with the increased no of nodes as the congestion is getting increased. But the rate of this increment id lesser as we don't maintain any kind of buffer. The performance of DSDV [9] id degrading due to increase in the number of nodes the load of exchange of routing tables becomes high and the frequency of exchange also increased. Due to the mobility of nodes the performance of AODV [6] decreases and remains constant as the no of nodes increases.

C. Number of Packets Dropped

The number of data packets that are not successfully sent to the destination is the no of packets being dropped. In terms of dropped packets AODV's [8] performance is the worst. The performance decreases with the increase in the number of packets.

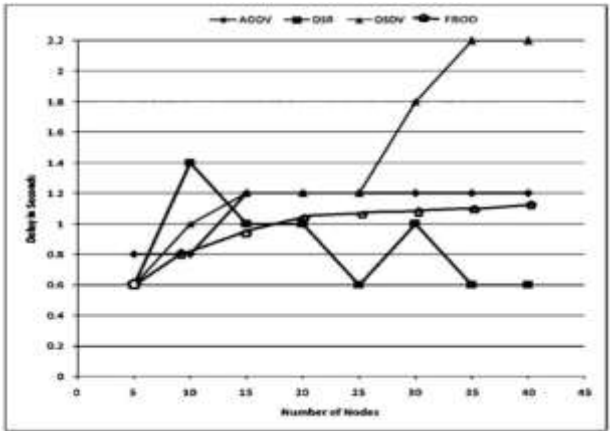


Figure 68.2: Average End to End Delay Ratio for AODV, DSR, DSDV, FBOD

DSDV [8] [9] performs consistently well with increase in the no. of nodes. DSR [10] [9] performs well when no of nodes is less but fails slightly when no of nodes is increased. In our protocol also in ideal case there is no drop of packets with the increase in no of nodes. It performs consistently well.

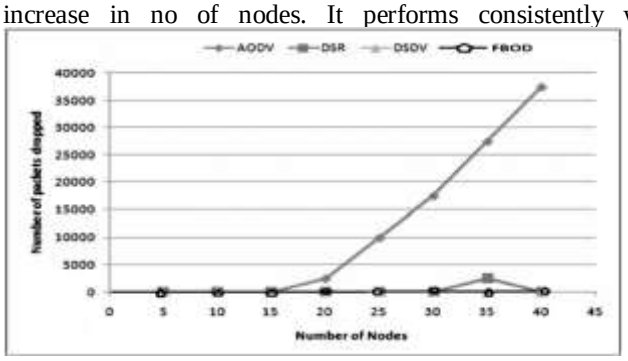


Figure 68.3: Dropped Packets for AODV, DSR, DSDV, FBOD

IX. Conclusion

This is a very light weight protocol with minimum computational overheads. In DSDV, we need to maintain a routing table. AODV has a lot of overhead while discovering routes, which clogs the network for sending data packets to desired destination. Not only does no such complicacy exist in our protocol, but it also has some of their benefits. Like AODV it is an on-demand routing protocol and the physical hardware support needed to implement it is substantially low which increases its scalability. This protocol also has added features so as to nullify some of the security threats which cause faults in the MANET networks.

References

[1] [Perkins94] C.E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" , Comp. Comm. Rev., Oct.1994, pp.234-244.

[2] Luke Klein-Berndt, "A Quick Guide to AODV Routing"

[3] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3

[4] "Avoiding Black Hole and Cooperative Black Hole Attacks in Wireless Ad hoc Networks" http://www.scribd.com/doc/26788447/Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks .

[5] Komala CR, Srinivas Shetty, Padmashree S., Elevarasi E., "Wireless Ad hoc Mobile Networks", National Conference on Computing Communication and Technology, pp. 168-174, 2010

[6] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", 2003.

[7] Sapna S. Kaushik & P. R. Deshmukh. "Comparison of effectiveness of AODV, DSDV and DSR routing protocols is mobile Ad hoc networks", International Journal of Information Technology and Knowledge Management, July – December 2009, volume 2, No. 2, pp. 499-502.

[8] V. Ramesh, Dr. P. Subbaiah, N. Koteswar Rao, M. Janardhana Raju, "Performance Comparison and Analysis of DSDV and AODV for MANET", V. Ramesh et al. / (IJCSE) International Journal on Computer Science and Engineering, Vol. 02, No. 02, 2010, 183-188.

[9] Nor Surayati Mohamad Usop, Azizol Abdullah, Ahmad Faisal Amri Abidin, "Performance Evaluation of AODV, DSDV & DSR Routing Protocol in Grid Environment", IJCSNS International Journal of Computer Science and Netwprk Security, Vol. 9, No. 7, July 2009.

[10] Anuj K. Gupta, Dr. Harsh Sadawarti, Dr. Anil K. Verma, "Performance Analysius of AODV, DSR & TORA Routing Protocols", IACSIT International Journal of Engineering & Technology, Vol. 2, No. 2, April 2010, ISSN: 1793 - 8236.

[11] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 24, issue 2, pp. 261-273, February 2006.

[12] R. Balakrishan, S. Jayabalan, Dr. U. Rajeswar Rao, Dr. T. K. Basak. Dr. V. Cyrilraj, "Performance Issues on AODV and DSDV for MNAETS", Jounnal Theoritical and Applied Information Technoilogy.

[13] Angel R. Otero, Carlos E. Otero and Abrar Qureshi, "A Multi-Criteria Evaluation of Information Security Controls Using Boolean Features", International Journal of etwprk Security & its application (IJNSA), Vol. 2, No. 4, October 2010.

[14] Anand Patwardhan, Jim Parker, Michaela Iorga. Anupam Joshi, "Tom Karygiannis, Secure Routing and Intrusion Detection in Ad Hoc Networks" 3rd International Conference on Perv asive Computing and Communications (PerCom 2005), Kauai Island, Hawaii.

[15] Bing Wua, Jie Wua, Eduardo B. Fernandeza, Mohammad Ilyasa, Spyros Magliveras, "Secure and efficient key management in mobile ad hoc networks" Journal of Network and Computer Applications 30 (2007) 937–954.

[16] C. E. Perkins, E. M. Royer, and S. R. Das, "Ad Hoc On Demand Distance Vector (AODV) Routing," IETF Mobile Ad Hoc Networks Working Group, Internet Draft, work in progress, 17 February 2003.

[17] F. Anjum, Anup K. Ghosh, Nada Golmie, Paul Kolodzy, Radha Poovendran, Rajeev Shorey, D. Lee, J-Sac, "Security in Wireless Ad hoc Networks", IEEE journal on selected areas in communications, vol. 24, no. 2, February 2006.

[18] H. A. Wen, C. L. Lin, and T. Hwang, "Provably Secure Authenticated Key Exchange Protocols for Low Power Computing Clients," Computers and Security, vol. 25, pp. 106-113, 2006.

[19] Haiyun Luo, Petros Zerfos, Jiejun Kong, Songwu Lu, Lixia Zhang, "Self-securing Ad Hoc Wireless Networks", 7th IEEE Symp. on Comp. and Communications (ISCC), Taormina, 2002.

[20] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine October 2002.

[21] Huaizhi Li Zhenliu Chen Xiangyang Qin, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks" IEEE, 2004.

[22] Huaizhi Li, Mukesh Singha, "Trust Management in Distributed Systems" IEEE Computer Society February 2007.

[23] J. Nam, S. Cho, S. Kim, and D. Won, "Simple and Efficient Group Key Agreement Based on Factoring" Proc. Int'l Conf. Computational Science and Its Applications (ICCSA '04), pp. 645-654, 2004.

[24] Oscar F. Gonzalez, Michael Howarth, and George Pavlou, Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. Center for Communications Systems Research, University of Surrey, Guildford, UK. Integrated Network Management, 2007. IM '07. 10th IFIP/IEEE International Symposium on May 21, 2007.

[25] J. Parker, J. L. Undercoffer, J. Pinkston, and A. Joshi., "On Intrusion Detection in Mobile Ad Hoc Network s". In 23rd IEEE International Performance Computing and Communications Conference Workshop on Information Ass urance. IEEE, April 2004.

[26] Jeremy J. Blum, Member, IEEE, and Azim Es kandarian, Member, IEEE, "A Reliable Link-Layer Protocol for Robust and Scalable Intervehicle Communications" IEEE Transactions On Intelligent Transportation Systems, vol. 8, no. 1, March 2007.

[27] Jung-San Lee, Chin-Chen Chang, "Secure communications for cluster-based ad hoc networks using node identities" Journal of Network and Computer Applications 22 October 2006 International Journal of Computer Science and Security, Volume (1): Issue (1) 67.

[28] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" IEEE Transaction on Mobile Computing, VOL. 6, NO. 5, May 2007.

[29] Nik os Komninos, Dimitris Vergados, Christos Douligeris, "Layered security design for mobile ad hoc networks" journal computers & security 25, 2006 , pp. 121 – 130.

[30] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks" Proc . IEEE Workshop on Security and Assurance in Ad Hoc Networks, IEEE Press, 2003, pp. 27–31.

[31] Panagiotis Papadimitratos , Zygmunt J. Haas , "Secure message transmission in mobile ad hoc networks, Ad Hoc Networks" IEEE 2003, 193–209 .

[32] S. Holeman, G. Manimaran, J. Dav, and A. Chakrabarti, "Differentially secure multicasting and its implementation methods", Computers & Security, Vol 21, No. 8, pp 736-749, 2002.

[33] S. Matri, T. J. Giuli, K. Lai and M. Baker , Mittigating Routing misbehaviour in Mobile Ad Hoc Networks. *Proceedings of the 6th annual internaional conference on Mobile Computing and Networking (MOBICOM), Boston, Massachusetts, United States, 2000, 255-265.*

[34] Himadri Nath Saha, Dr Debika Bhattacharyya, Dr.P.K.Banerjee,"A Priority Based Protocol for Mitigating Different Attacks in MANET",International Journal for Computer Science and Communication,Volume I,Number2,pp-299-302,Sept.2010

[35] Himadri Nath Saha, Dr Debika Bhattacharyya, Dr.P.K.Banerjee,"A Distributed Administration Based Approach for Detecting and Preventing Attacks in MANET",International Journal for Scientific and Engineering Reasearch,Volume-2,Issue-3,pp-1-11,Mar-2011

[36] Himadri Nath Saha, Dr Debika Bhattacharyya, Dr.P.K.Banerjee,"Semi-Centralized Multi-Authenticated RSSI Based `Solution to Sybil Attack",International Journal of Computer Science and Emerging Technologies",Volume I,Issue-4,pp-338-341,Dec 2010.

Controlling Home Appliances Remotely Through Voice Command

Marriam Butt [#1], Mamoona Khanam[#2], Aihab Khan[#3], Malik Sikandar Hayat Khiyal[#4]
[#]Department of software engineering Fatima Jinnah women university, FJWU, Rawalpindi, Pakistan
[1]marriambutt.fjwu @gmail.com, [3]aihabkhan@yahoo.com,[4]m.sikandarhayat@yahoo.com,

***Abstract*— the main concern in systems development is the integration of technologies to increase customer satisfaction. Research presented in this paper focuses mainly in three things first to understand the speech or voice of user second is to control the home appliances through voice call and third is to finds intrusion in the house. The user can make a voice call in order to perform certain actions such as switching lights on/off, getting the status of any appliance etc. And when system finds intrusion it sends an alert voice message to preconfigured cell when the user is away from the place. The proposed system is implemented using voice Global System for Mobile Communications (GSM) and wireless technology based on .NET framework and Attention (AT) commands. Microsoft speech reorganization engine, speech SDK 5.1 is used to understand the voice command of user. As it is wireless so more cost effective and easy to use. The GSM technology used in system provide the everywhere access of the system for security. Experimental results show that the system is more secure and cost effective as compared to existing systems. We conclude that this system provides solution for the problems faced by home owner in daily life and make their life easy and comfortable by proposing cost effective and reliable solution.**

Keywords-component; Voice GSM; Voice message; radio friquencey (RF); AT commands.

I. INTRODUCTION

Home automation control system (HACS) is not a new concept a lot of work has done in this field and many solutions has proposed. Some of them have used internet and wireless technology to communicate and control the appliances [1, 2]. Others have used the Bluetooth or GSM technology to send the command for controlling the home appliances [3, 4].

Problem domain related to proposed technique is telecommunication remote automation of home appliances thorough telecom technology. The proposed research provides the cost effective system that helps to satisfy their security concerns of home related to daily life such as controlling the home appliances and intrusion detection through voice message. This system can be used in any environment. It is free from the geographical limitations and can be used every where being the GSM network available.

It is affordable to everyone as no expansive hardware is used in it. Cell phones are very common these days and almost everyone can make a call very easily. That's why cell phone is used in this system that makes it real world application. It is free from the geographical boundaries and can be used from anywhere where GSM is available. The proposed solution is to implement the HACS through voice command that controls the home appliances by making a call from the preconfigured number to system and receive the voice message from the system to preconfigured number about the status of appliances over the GSM network.

AT commands are used to automatically receive the call on system from the preconfigured number and system also sends the voice message to preconfigured number about the status of appliances and intrusion through AT commands. Microsoft speech SDK 5.1 is used to reorganization of speech. Hence it is a research based real world project and is useful for working people and for those who live alone or stay out of their homes most of the time.

The system is implemented using .NET framework. AT commands set supporting voice as:

AT+FCLASS=8	for Voice Mode
ATD03004108768;	for making a call
ATA	for receiving a call
AT+VSM=128,8000	for Compression Mode
AT+ VTX	for Voice Transmition

The paper is organized in such a way that: section 2 discusses related work to proposed schemes, section 3 committed to proposed framework, section 4 discuss proposed technique along with algorithm ,section 5 discuss results and finally concluding remarks are given in section 6.

II. RELATED WORK

Nguyen et al. [1] proposed a Home appliance control system. Infrared ray and power line communication are used to control the home appliances system. This system helps user to checks the status of appliances and controls them remotely from everywhere. And this is done through their cellular phone or Internet. The simple approach to control the home appliances is given in this paper.

Haque et al. [2] proposed a system that controls the home appliances using the personal computer. This system is developed by using the Visual Basic 6.0 as programming language and Microsoft voice engine tools for speech recognition purpose. Appliances can be either controlled by timer or by voice command.

Khiyal et al. [3] proposed a system for controlling home appliances remotely that is useful for the people who are not at home mostly. The main objective of the system is to provide

security and control the home appliances such as AC, lights and alarms. The system is implemented by SMS technology that is used to transfer data from sender to receiver over GSM network. One or more computers can be used to control the home appliances. System send an alert SMS to authorized user when any intrusion is detected and user can in turn respond in order to overcome the situation. Moreover user can send SMS to system to get the status of home appliances and controlling them.

Jawarkar et al. [5] proposed the software system for communication between mobile and computer. UART 16550A chip is programmed using appropriate control format to support AT command. The mobile in this system is used for receiving and executing commands from preconfigured users and informing status about change in input to the user through SMS. The system can also send SMS to specified mobile user if there is a change in the status of the input ports. This system is not for time critical systems.

III. PROPOSED FRAMEWORK

The proposed model is the two way communication system user can send the voice command to change the state of home appliances and system sends the voice message to inform the user about intrusion.

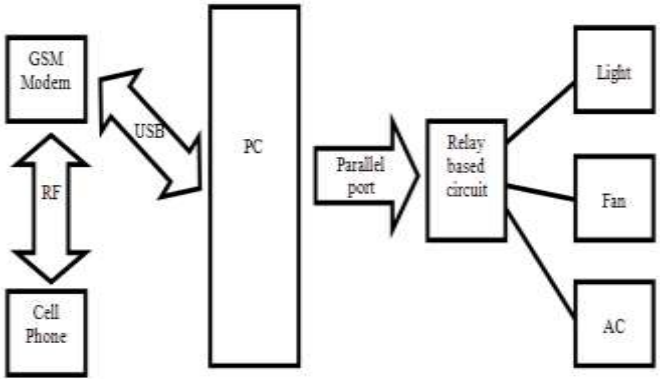


Figure 1: Block diagram of controlling home appliances through voice commands

The block diagram of proposed model is shown in fig. 1. It works in a way that the user with a specific cell number can make a call through GSM technology. System receives the call and performs the respective action as instructed by the user such as controlling the light through relay based circuit. System also sends the voice message to the preconfigured cell number to tell the status of appliances or if it finds any kind of intrusion at home.

A. hardware design

USB voice GSM modem is used to send the return voice message to preconfigured number. Voice GSM is used to send the wav file to preconfigured number through AT commands.

A relay based circuit is used to control the appliances this circuit is attached with system through DB-23 male parallel port [9]. The circuit diagram is shown in fig. 2

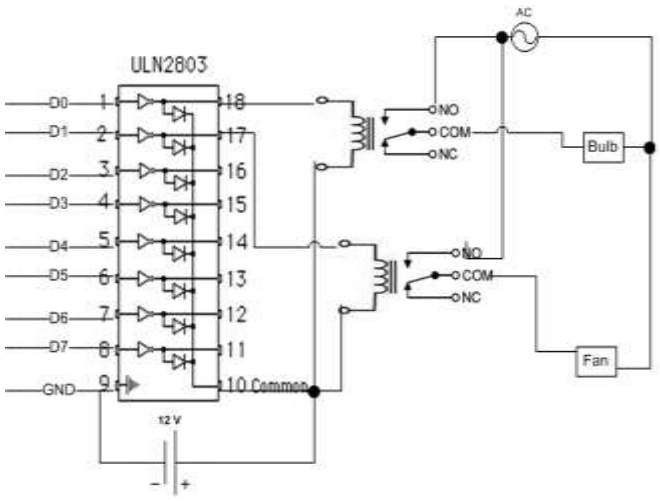


Figure 2: circuit diagram

Two relays are used to control two appliances but as there are eight data pins of parallel port so relays can be increased to control up to eight appliances. 12 volt adapter is used to give voltage to relay. An IC ULN2803 is used to interface the relay with parallel port. It is 18 pin IC whose 1 to 8 pins are data pins and 18 to 11 are corresponding output pins, pin 9 in ground and 10 is supplied with required voltage here it is supplied with 12 volts.

B. software design

This application is develop in .Net framework using the language C#. Microsoft speech SDK 5.0 is used for speech reorganization purpose.

This application has three main parts. One is to understand the speech or the voice of user. This is done through speech reorganization engine. There are many speech reorganization engines available but here Microsoft speech SDK5.1 is used. Second is to control the appliances according to the user demand. This can be done through relay based circuit that is attached with computer through parallel port. And third is to sense the intrusion in the home and sends voice message to preconfigured number. This can be done through sensors attach to the system with parallel port and AT commands respectively.

C. System overview

User from anywhere being GSM available can make a call to system to check the status of appliances or control them as describe in fig 3(a). System in return checks the authenticity of the number and if it is from the preconfigured number then it follows the instruction otherwise it discard the call. As computer receives a call timer starts and it automatically discard the call after few seconds. The voice is understood by the Microsoft speech reorganization engine that is installed in the system. If the command is about changing the status of appliances it passes the signal to parallel port to follow the instruction like turn the appliances on or off. This can be done through relay based circuit. If command is to check the status of appliances the system returns the voice message to preconfigured number using AT Commands telling the status of appliances.

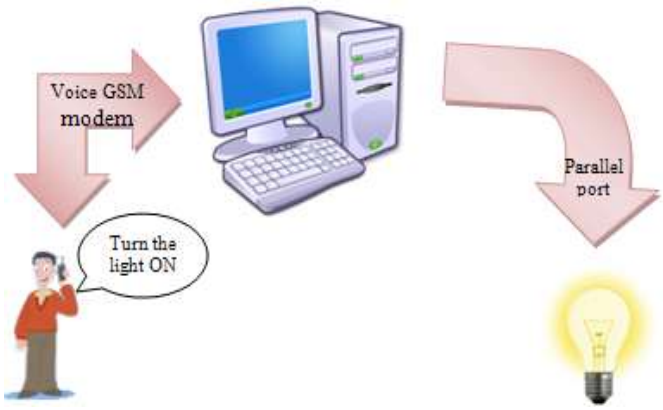


Figure 3(a): System overview

On the other hand if system finds any kind of intrusion like opening of entrance door etc in the home it sends the voice message to user telling him about the intrusion as describe in fig 3(b).

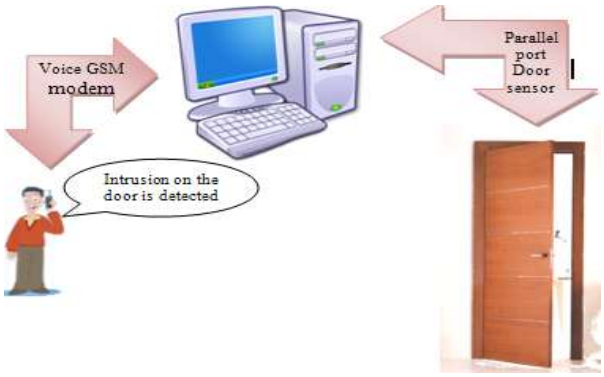


Figure 3(b): system overview

IV. PROPOSED TECHNIQUE

The proposed technique is simple and cost effective and is available to almost every one. The proposed system is given in Fig. 1 shows that GSM technology and voice messages and calls are used in the system and a relay based circuit is attach to the pc through parallel port. It enables the user to control home appliances such as turning the light on or off remotely. It detects the intrusion also.

Algorithm:

Pseudo code of proposed model is given in fig.4

Begin
If hardware test fails
Return
End
Else if hardware tests succeed then
Successful communication
If system gets a call
Check the authenticity
If call not from the preconfigured number
Aboad the call
Else
Receive the call and listen the command
If command is about controlling the appliances
Send the signal to parallel port and control them sends the respective voice message
If command is about knowing the status of appliances
Check the parallel port status of appliances and sends the status to that number
If system sense some intrusion in the home
Return the voice message to preconfigured number
End

Figure 4: Algorithm of controlling home appliances through voice commands

Test Case 2

Title: Check the authenticity of number.

System: Home Appliance Control System (HACS).

Input Instructions: make a call from any number.

Output: the system did not receive the call and discard it.

Result: Test Succeeded.

Test Case 3

Title: Check for Light Control.

System: Home Appliance Control System (HACS).

Input Instructions: make a call from preconfigured number and ask to turn the light on.

Output: the light turns on and a confirmation voice message is received on the number

Result: Test Succeeded.

Test Case 4

Title: Check for fan Control.

System: Home Appliance Control System (HACS).

Input Instructions: make a call from preconfigured number and ask to turn the fan on.

Output: the fan turns on and a confirmation voice message is received on the number.

Result: Test Succeeded.

Test Case 5

Title: Check for fan Control.

System: Home Appliance Control System (HACS).

Input Instructions: make a call from preconfigured number and ask to turn the fan off.

Output: the fan turns off and a confirmation voice message is received on the number.

Result: Test Succeeded.

Test Case 6

Title: Test for Security Check.

System: Home Appliance Control System (HACS).

Input Instructions: sensors sense the light.

Output: the light sensor turns red and a voice command is received alerting about intrusion at home on user cell phone.

Result: Test Succeeded

A. Graph of exparimental results:

As user makes a call to the system the timer starts and when user says a command regarding the appliances the system match the command with its vocabulary if it finds match it follows the instruction. If the timer exceeds from certain limit the system discard the call or if system does not find the match it sends the message to preconfigured number "sorry could not understand your message".

B. Comparison of proposed system with other systems:

The graphs of average response time of appliances and intrusion are given. These have been taken from the test cases given above.

As soon as the system receives the voice command from the preconfigured cell phone number regarding any appliances like light, AC or Fan to change the status of them or to know the current status of them the system response in 4, 6 and 3.5 seconds respectively. This is the average response time of appliances. Graph of response time of appliances like light, AC and fan are shown in the fig 3.

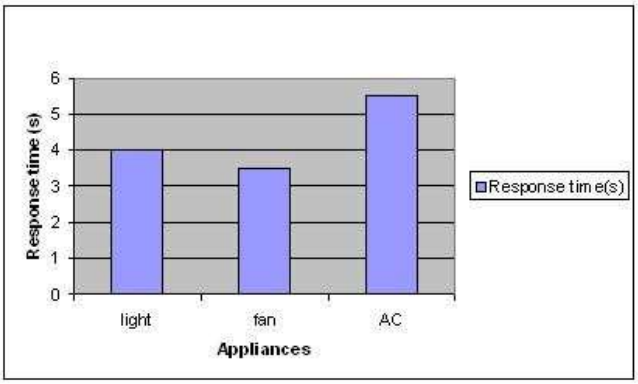


Figure 5: average response time of appliances

As soon as the system senses the intrusion through sensors attach with it, on the Main gate, Living room window or Entrance door it sends the signal to computer and computer then sends a voice message to the preconfigured cell phone number in 3.6, 4 and 3.9 seconds respectively. This is the average intrusion detection time in the home.

Graph of response time of intrusion deduction in the home is shown in the fig 4.

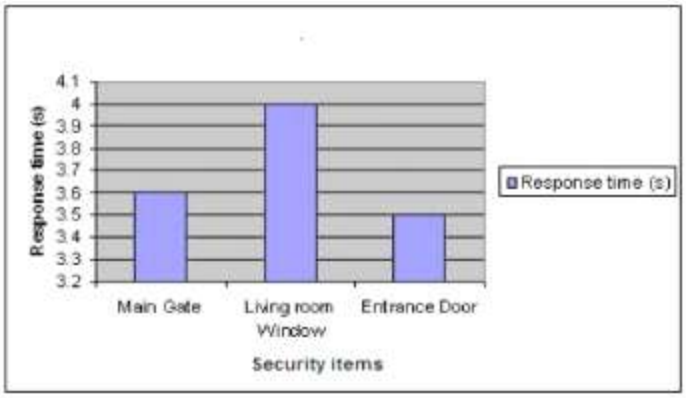


Figure 6: Average intrusion deduction time

TABLE 1: COMPARISON OF SYSTEMS

No.	System	Technique	characteristics		
			Cost effective	highly Accessible	security
1.	Ubiquitous Access to Home Appliance Control System using Infrared Ray and Power Line Communication [1]	Power Line Communication (PLC),IR	No	Yes	available
2.	Remote Control using Mobile through Spoken Commands [5]	GSM technology	Yes	No	Not available
3.	Friendly Home Automation System Using Cell Phone and J2ME with Feedback Instant Voice Messages[6]	GSM technology	Yes	Yes	available
4.	Homes Appliances Controlled Using Speech Recognition in Wireless Network Environment[7]	wireless technology	No	No	Not available
5.	Proposed System	Voice GSM technology, AT command	Yes	Yes	available

The comparison of different systems with proposed system is given in table 1. Proposed system is using voice GSM technology and AT commands for sending and receiving the voice command to control the home appliances. This is cost effective and provides security and is highly accessible. While the other system [1] is not cost effective and [5] does not provide security and every where access. In [6] the system is proposed that controls the home appliances remotely. Two cell phones are used for communication. This system is developed by using the J2ME language. The system [7] is not cost effective since it uses the internet for communication.

V. CONCLUSION

Controlling home appliances with wireless technology has revolutionized our way of living. Home owners can come to an ideal environment coming from their daily activities. Technique used in this system is not complex. It is the location independent system being GSM available for the ease of user. In future many more features can be added in it like home appliances can be controlled by using voice call by implementing more secure and efficient techniques.

REFERENCES

[1] Tam Van Nguyen, Dong Gun Lee, Yong Ho Seol, Myung Hwan Yu, Deokjai Choi, "Ubiquitous Access to Home Appliance Control System using Infrared Ray and Power Line Communication", ICI 2007, 3rd IEEE/IFIP International Conference in Central Asia, Tashkent, Uzbekistan, vol 1, pp1-4,26-28 Sept.2007

[2] S. M. Anamul Haque, S. M. Kamruzzaman and Md. Ashraful Islam1 "A System for Smart-Home Control of Appliances Based on Timer and Speech Interaction" Proceedings of the 4th International Conference on Electrical Engineering & 2nd Annual Paper Meet 26-28 , pp. 128-131,January, 2006

[3] Malik Sikandar Hayat Khiyal, Aihab Khan, and Erum Shehzadi "SMS Based Wireless Home Appliance Control System (HACS) for Automating Appliances and Security". Issue in Information Science and Information Technology Vol 6,, Pp 887-894, 2009.

[4] Jia-Ren Chang Chien, Cheng-Chi Tai "The Information Home Appliance Control System—A Bluetooth Universal Type Remote Controller" Proceedings of the 2004 IEEE. International Conference on Networking, Sensing & Control. Taipei, Taiwan, vol. 1,pp. 399-400, March 21-23. 2004

[5] N.P.Jawarkar, Vasif Ahmed and R.D. Thakare. "Remote Control using Mobile through Spoken Commands". IEEE - International Consortium of Stem Cell Networks (ICSCN) 2007. 22-24,Pp.622-625, 2007

[6] Mahmoud shaker Nasr, Fahtha H. A.salem Azwai, "Friendly home automation system using cell phone and J2ME with feedback instant voice messages," aiccsa, 2009 IEEE/ACS International Conference on Computer Systems and Applications, pp.531-538,2009

[7] Mardiana B., Hazura H., Fauziyah S., Zahariah M., Hanim A.R., Noor Shahida M.K., "Homes Appliances Controlled Using Speech Recognition in Wireless Network Environment," ICCTD, vol. 2, pp.285-288, 2009 International Conference on Computer Technology and Development, 2009

[8] Yoshiro Imai, Yukio Hori, Shin'ichi Masuda, "A Mobile Phone-Enhanced Remote Surveillance System with Electric Power Appliance Control and Network Camera Homing," ICAS, pp.51, Third International Conference on Autonomic and Autonomous Systems (ICAS'07), 2007

[9] http://jaspreetscodezone.blogspot.com/2008/01/interfacing-relays-using-parallel-port.html

AUTHOR'S PROFILE

Marriam butt is a graduate from Dept. of Software Engineering, Fatima Jinnah Women University, Pakistan.

Mr.Aihab Khan works in Dept. of Computer Sciences at Fatima Jinnah Women University, Pakistan. His research interests are in the field of Data Mining, Data Warehousing as well as Information security.

Dr. M. Sikandar H. Khiyal born at Khushab, Pakistan. He is Chairperson Dept. Computer Sciences and Software Engineering in Fatima Jinnah Women University Pakistan. He served in Pakistan Atomic Energy Commission for 24 years and involved in different research and development program of the PAEC. He developed software of underground flow and advanced fluid dynamic techniques. He was also involved at teaching in Computer Training Center, PAEC and International Islamic University. His area of interest is Numerical Analysis of Algorithm, Theory of Automata and Theory of Computation. He has more than one hundred research publications published in National and International Journals and Conference proceedings. He has supervised more than one hundred and thirty research projects at graduate and postgraduate level. He is member of SIAM, ACM, Informing Science Institute, IACSIT. He is Co editor of the journals JATIT and International Journal of Reviews in Computing and associate editor of IJCTE. He is reviewer of the journals, IJCSIT, JIISIT, IJCTE, IJCEE, JCIE and CEE of Elsevier.

Efficient Traducer Tracing System Using Traffic Volume Information

K.V.Ramana Ph.D.,
Department of Computer Science
Jawaharlal Nehru Technological University
Kakinada, 533003,India

Raghu.B.Korrapati Ph.D.,
Walden University

N. Praveen Kumar
Department of Computer Science
Jawaharlal Nehru Technological University
Kakinada, 533003,India.

D. Prakash
Department of Computer Science
Jawaharlal Nehru Technological University
Kakinada, 533003,India

***Abstract*--- Many leading Broadband access technologies and their accessing abilities have the capability to meet the future requirements of the Broadband consumer. With the enormous growth in the broadband technologies, there is a need of applying simmering technology in many applications like video conference systems and content transmission systems. Streaming content enables users to get access the files quickly and not have to wait until the file is done downloading. Security remains one of the main challenges for Content Streaming. Digital Rights Management (DRM) system must be implemented to avoid content spreading and un-intentional content usage. Water marking technology can also be used to implement the DRM system but it has its own limitations and attacks. A control method for the steaming content delivery is required to prevent abuse of the content. For this reason, authors have proposed a contended methodology that uses traffic volume information obtained from routers. Traducer tracing is one of the essential technologies that designs DRM systems, and empowers content distributors to notice and control content acquisition. This technology utilizes the main concept of traffic contours that helps to determine who is watching the streaming content and whether or not a secondary content delivery exists i.e., mainly used to determine whether the network is being traced out by the intruder or not.**

Keywords- Content Streaming; Traffic Contours; Traducer Tracing; Digital Rights Management.

I. INTRODUCTION

There are many new technologies that use Local Area Networks and Internet to replace previous systems which use leased lines [1], [2]. Streaming technology can also be implemented to content delivery systems [3]. For example, Internet TV came into existence for telecasting content streaming [4] using broadband technology plays a major role in the evolution of streaming network infrastructure. The most important feature of this kind of system is that a person can obtain the information very efficiently and not to have to wait for the complete download of the required information. However, these systems need to be securely implemented. For this reason, an efficient DRM (Digital Rights Management) system has to be implemented [5], [6]. DRM incorporated system can efficiently manage the problem of content spreading and un-intended content usage. DRM technology is necessitated to avoid some threatened problems like possibility of existence of authenticity issues i.e., using content without the knowledge of Content holder and Content provider. DRM strategy incorporated system can efficiently manage the content transmission and users operations on the content in particular phenomena [7]. Watermarking [8] [9] and Traffic patterns are the two efficient techniques that can effectively drive the DRM system. However, watermarking has its own limitations.

In regards of protection towards the content, an effective DRM technology has to be implemented. For this, the content is encrypted and decryption keys are securely transmitted to users and they can use these keys to avoid data interception [10]. This type of protection [8] is unable to control secondary distributions of decrypted data [11]. An efficient management technology is implemented by the content providers to manage and monitor the use of content [12], [13]. This technology is called Traducer-tracing technology which provides flexibility for the content providers to manage the data.

Traducer tracing system stands for incorporating unique identity to the propagating contents by embedding watermarks into them [14], [15]. Use of watermarking concept for unique content identification involves much complexity in terms of computations. Major drawbacks in using water marking concept are:

1. System that incorporates water-marking embedded techniques need surplus amount of computations to encode complex contents. This result in difficulty for evaluating the computational cost related to real-time streaming.

2. The major lapse of watermarking, content conversion, and the known Removal attacks [10], [16] has become a serious issue.

Thence, an efficient system must be introduced so that it enhances the content distribution to explore the process of finding the narrow list of users who may be traducers. In order to avoid the user's intervention in the normal functioning of the system, an effective monitoring process should be implemented based on the information obtained at the routers in the middle of streaming path. Process includes gathering information about traffic amounts and using this information to track user's contents reception. This content is helpful for the content providers to lessen the list of traducers and by using this concept, content provider can efficiently trace out whether the desired content is received by the user or not i.e., he can be able to know whether the user is watching the content or not and also can be able to determine whether the secondary content distribution exists or not [17], [18]. Since, the proposed concept is not using the packet information, privacy issues of the application is least bothered [19].

The Content is streamed with the Variable Bit Rate. Bit rate of this streaming content varies in accordance with the variations in the content. During the process of content delivery to the users from the servers, routers present in the middle of the streaming path are configured in such a way that they are capable to observe the streaming content and can generate unique contours associated with the traffic amount. It is possible to determine whether the targeted content is being watched out by the user or not, during the process of content distribution, only by comparing the user-side contours to the server side contours.

The following is a concise procedure to determine whether the user is watching the targeted content or not. Server side traffic contours are generated with the help of traffic volume information, traffic amount, obtained at the router near the content server. User-side contours are generated using traffic amount obtained at the routers near the user. These two obtained contours are compared by the management server, to decide whether the user is watching the content or not. This process does not require any operations on the user's computer. On a theoretical basis, this mechanism makes impossible for a user to tamper with the tracing process. The major benefit of the proposed mechanism is that, it can be implemented with the lower computational cost since it uses only traffic volume information but not using mechanisms, like water marking which consumes higher computational costs.

A Traducer tracing technique is said to be Network Based Traducer Tracing Technique, when it is applied in the network comprising of Servers and Users. In this paper, the details of the proposed method, and evaluating it by creating an effective environment, using an efficient Simulator called Network Simulator (NS2) is shown.

The rest of this paper is organized as follows. In Section II, Overview of DRM Technology, and the research works on these technologies are discussed. In Section III, details on technologies that construct the proposed Traducer tracing system is presented. In Section IV, the results of simulations with Network Simulator 2(NS2) are shown. Finally, Section V concludes the paper.

II. Related Work

There have been many tremendous works done in exploring DRM technology [4] and techniques that come under DRM technology. Traditional systems make use of classical technologies like Encryption [20], [21] and Access-conditioning [22] for driving DRM incorporated systems. There are many crucial technologies that construct DRM system. Traducer tracing system is one among them. With this technique, content provider is able to monitor content usage and also able to know whether the network is being traced out by the intruder or not i.e., whether the user is appropriately using the content or not.

A Simple Traducer tracing system is depicted in fig.1

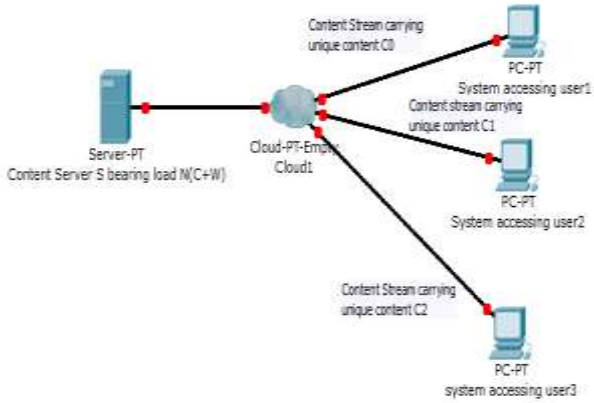


Figure 1: Example of Simple Traducer tracing.

Figure 1 represents the clear elementary traducer tracing system.

The working procedure of the mentioned system is described as below:

- Unique information is embedded into the Content using Digital watermarking, by the content provider and generates copies of the content.
- The generated copies are propagated to different users.
- Application running at user analyses the content data and re-assembles the embedded information.
- According to the analyzed and extracted information, user's application notifies that he or she is watching the content.

The following figure shows a scenario of a network comprises of a Content Server, Users and the two contents, which are made unique by using the concept of Digital Watermarking, and depicts a mechanism to find out whether secondary distribution of content exists or not and to trace out the originator or run-off source of the secondary content.

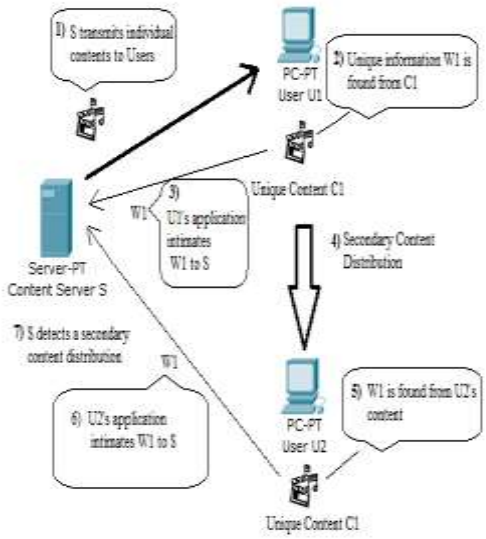


Figure 2: Technique to verify the existence of secondary content distribution and to find the runoff source of it.

The following is the mechanism to find out whether the secondary content distribution exists or not.

- Content server S delivers a unique content C1 to U1 and the user application at U1 analyzes the Watermarked information, W1, and notifies it to S.
- In case of existence of un-authorized content distribution between user1 and user2, W1 also found from U2's content and application running at U2 notifies W1 to S.
- Finally, S finds duplicated W1 and concludes that there is an existence of secondary content distribution says C1 in detail W1, in between U1 and U2.

There are two main issues that are associated with the above mechanism. They are

1. It includes lot of computational costs in encoding the content and also in embedding the watermarks, since an individual content has to be propagated to each user. Let '**C**' and '**W**' be the costs involved in encoding the content and embedding watermarks into it. Then, there will be at-least **N(C+W)** total cost involved in propagating the content, which has the traceability of traducers. '**N**' is the number of content users. This does not suite better for the real-time streaming contents. That is why an efficient method is needed to track the traducers with minimum cost.
2. Second issue is the use of Watermarking concepts for tracing traducers and for embedding information into the host signal has its own limitations. There are known attacks against Watermarks such as Copy attack, Collusion attack, Removal attack and Sensitivity attack [23], [24].

Watermarking concept does not go forward or does not suite in the field of complex networks. Since, it shows problems because of unclear network environment and users.

Hence, Traducer tracing systems with Watermarking need additional mechanisms to tighten the scope of application by shortening down the possible list of traducers. A convenient and the most efficient method to track the content stream without using the Watermarking technology is by the use of Traffic Volume Information obtained at the routers present in the middle of the streaming path. This method avoids the need of decrypting and decoding the streaming content.

In Section III, an efficient system is proposed to trace a multimedia streaming content.

III. METHODOLOGY

A. Modules

The proposed work has been segmented into three phases. The first phase deals with building network environment. The second phase establishes communication among the hosts and servers. This phase also deals with the re-configuration or re-construction of new paths in case of path failures. The third phase will explain about the mechanism to detect the flow of streaming content in variety of networks i.e., to find out whether the user is watching the streaming content or not. This is an effective mechanism find out whether the network is being traced out by the intruder or not.

Figure 3 represents the flow chart of the modules and their description was in below sections.

1) Build network:

In the first phase, a system is proposed by considering a network comprises of Servers, Clients (Users), Intermediate Routers [24]. Servers are configured to run two types of applications. One server is configured to implement effective content delivery. Content Server and the other, is configured to perform vital functionalities in detecting the traducer in the network, Management Server. There are intermediate routers at the side of each communicating party that have a capability to observe the traffic amount and propagate the obtained information to the Server that manages the built network.

2)Establish Communication:

In the second phase, a communication among the network entities has been established. The content has to be streamed from the Content Server to different Clients say Users, via intermediate routers. Content Servers make use of DRM technology in generating unique content and propagating it to different users.

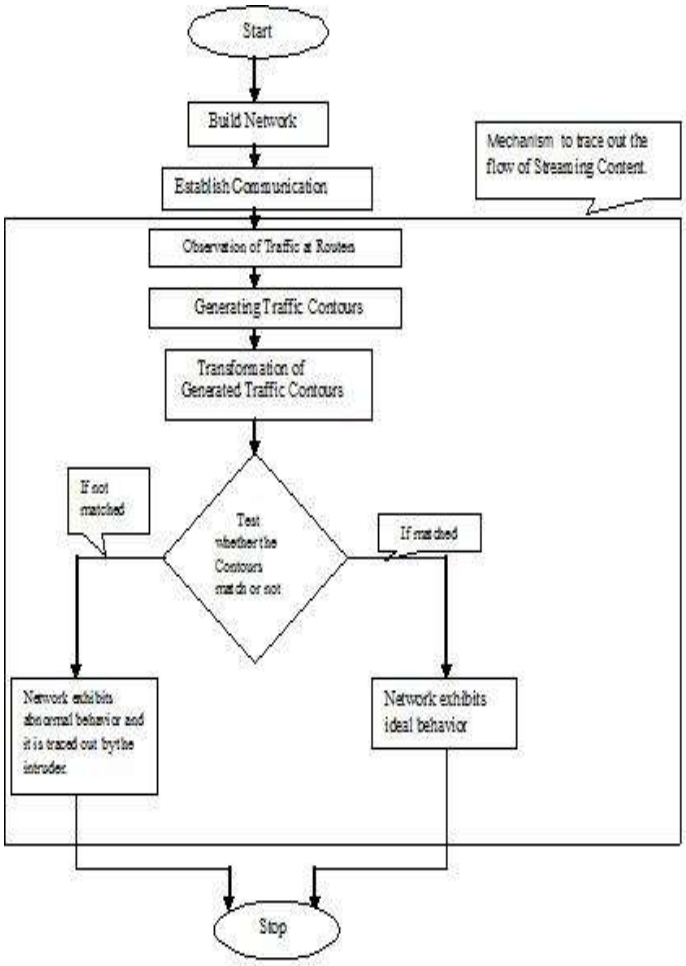


Figure 3: Flow chart to implement traducer tracing system using Traffic volume information.

3)Core Module of the Application:

In the third phase, a concise review of the proposed system is introduced. The framework of the proposed strategy is shown below.

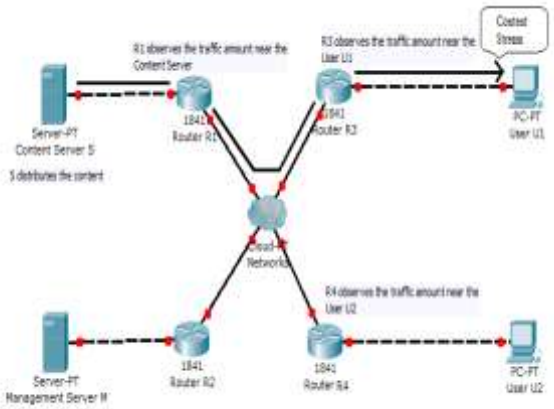


Figure 4: Framework of the proposed strategy.

Figure 4 represents a Network of Servers, Users and Routers which has the capability to drive the proposed mechanism.

The mechanism of the contended methodology is as follows:

Content Server spreads the content C and the users U1 and U2 receives the content. Routers in the middle of the streaming path say R1, R3 and R4 observe the traffic amount. For instance, Router R1 supervises the flow of content server S and mass up the sizes of the packets. Information obtained at the routers is sent to the Management Server using protocols such as ICMP and SNMP.

Management Server constructs the traffic contour from the traffic amount information obtained by the routers. Router R1 observes the content at the content server S during its propagation and transmits the observed data to the Management Server M, which generates the Server side traffic contour. Similarly, the routers at user side say R3 and R4 observes the traffic amount for few minutes and transmits the observed data to Management server that generates User side traffic contour. Transformations are performed on the obtained traffic contours to avoid breach errors. Management Server then performs comparison to find out the degree of similarity between the User-side and Server-side traffic contours. Based on the results obtained from the similarity matching, Content provider can able to know who is watching the streaming content. If the contours match, all the network behaviors are normal. If they don't, the user is not watching the content i.e., some additional noise has been added to the streaming content which can be done by the interception of the participated communicating party. Thence, there is a possibility to say that there is a traducer in the network and by the mentioned mechanism; it is possible to decide that the network is being traced out by the intruder.

The suggested system has a capability to ascertain the flow of gushing content in different breeds of networks. The contended methodology is befitting for bountiful kinds of applications. Appliances include QuickTime servers administered by Apple. The recommended procedure is suitable for streaming content and is not applicable for the downloaded content, since monitoring of the network can be done on the propagating content. The proposed system is brought to bear for a precise degree of confined networks. For instance, this totally suits for the video streaming systems using corporate LANS. With the contended mechanism, the executives of the streaming systems can effectively administer the propagating content and know who is watching them. This diminishes not only the aegis hazard on caper by the third party but also by the administrator.

B. Elucidation of Traffic Contours and Congruity

In this thesis, Variable bit rate simmering content is spotlighted and embrace of traffic contours to boast the streaming content continuance.

The traffic contour is elucidated as the heap of traffic for a certain period of time Δt [sec] and expressed as an N-dimensional vector in the following expression.

$$C = (c_{1,}\, c_{2,\ldots,}c_N)^T, \quad T = N\,\Delta t \qquad (1)$$

Where 'T' in seconds is the length of the traffic contour and 'N' is the number of slots. c_1 is the traffic contour observed in first time slot and c_2 is the traffic contour observed in second time slot.

In the proposed strategy, while the network is in running state, router present at the server observes the traffic amount throughout the content transmission and transmits this information to obtain the Server side traffic contour which is expressed as

$$C_S = (c_1, c_2, \ldots, c_s)^t, \quad \text{according to (1)}$$

User side traffic contour is expressed as

$$C_U = (c_1, c_2, \ldots, c_u)^t$$

In the above expressions, S and U are the number of time slots. The length of the Server side traffic contour or observation is greater than User side observation i.e., S>U.

To find out the similarity of these contours, a partial pattern P_U of finite length say U (length of the User side contour) of the contour C_S, is snipped off and is compared with the contour C_U.

Before computing the congruity of two contours, P_U and C_U are normalized as,

$$P'_U = \begin{pmatrix} \frac{p1-\bar{p}}{Sp} \\ \frac{p2-\bar{p}}{Sp} \\ \cdot \\ \cdot \\ \cdot \\ \frac{pU-\bar{p}}{Sp} \end{pmatrix}, \; C'_U = \begin{pmatrix} \frac{c1-\bar{c}}{Cp} \\ \frac{c2-\bar{c}}{Cp} \\ \cdot \\ \cdot \\ \cdot \\ \frac{cU-\bar{c}}{Cp} \end{pmatrix} \qquad (2)$$

In the above expression, $\bar{p}$ and $\bar{c}$ are the means of each vector, S_p and C_p are the standard deviations. After normalizing, the means of P'_U and C'_U are zero and variances are 1. Finally, by obtaining the computed values, these values are used in the below equation to find out the similarity between the user side contour and the part of server side contour.

$$R_{PC} = \frac{P'_U\, C'_U}{\sqrt{\|P'_U\|^2 \cdot \|C'_U\|^2}} \qquad (3)$$

When the two contours are in congruence, R_{PC} approximates to 1.

By using the above process, the similarity between the contours can be obtained only if there are of same length. As mentioned earlier, the length of the server side contour C_S is greater than the length of the user side contour C_U. In this contented methodology, similarity between the contours of different length has to be computed. For this reason, a concept of "window" is used. Here, a part of window of length equals to the length of the user side contour is considered and is used to snip off the partial part P_U, of the server side traffic contour. By using the partial contour P_U, of the server side traffic contour, the contended strategy computes the similarity R_{PC} by moving the window from left to right on the server side traffic contour C_S.

C. Confrontation of Traffic Contours using Similarity

The framework of comparison of traffic contours is explained in systematic way using the following three steps. In the first step, a window is considered that snips-off the partial contour P_U from the Server side contour C_S. In the second step, similarity between the partial contour P_U and User side traffic contour C_U. In this step, transformations are applied on the contour to avert from the consequences of burst errors. In the final step, window is advanced from left to right by one slot. After advanced to next slot, the mentioned three step process repeats and then applied to next slot, this process continues till the window arrives the rightmost component of the Server side contour. In total, S-U+1 values of similarity are obtained from the above computation. The following figure depicts the above mentioned process.

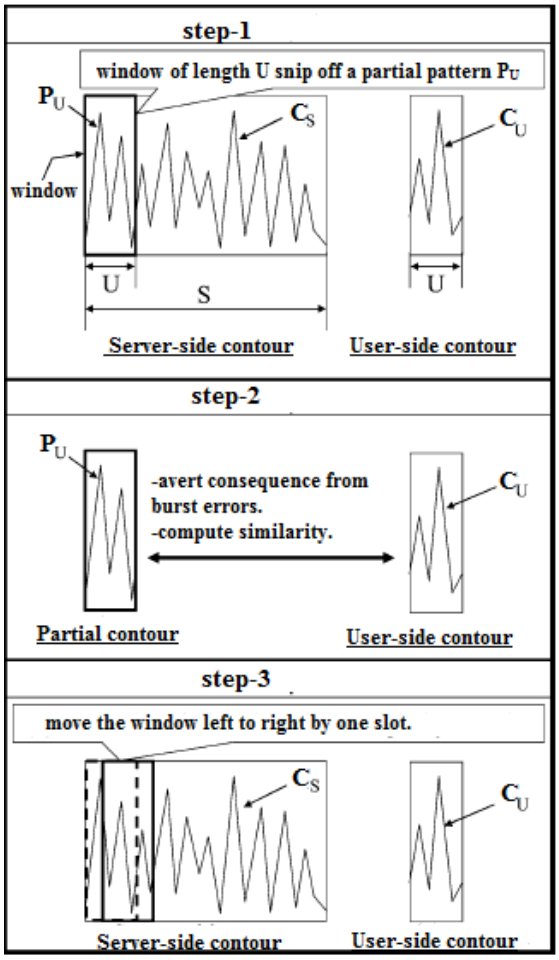


Figure 5: Framework for comparison of Traffic contours.

Figure 5 shows the systematic steps to perform the comparison of traffic contours.

1) Alleviation against Burst Errors

It becomes arduous to compute the similarity as burst errors vitiates the User side traffic contour. Transformations on the considered contours (partial contour and the user side contour) are performed to avert from the consequences of the burst errors. Due to the presence of the burst errors, the user

side traffic contour moderately drops. The following is the sequential procedure to transform the contours. A precise value is computed which is referred to a threshold value and is used as a reference to apply transformations. In the first step, user side traffic contour is speculated and the values less than or equal to the threshold are considered and are removed from the contour. In the second step, partial contour is considered and amputate its elements conferred to user side removal routine. Characteristically, in the partial contour, the components that are at the same position where the elements of user side contour are removed, are taken out. In the third step, the outlived components are consociated.

The above mentioned routine has to be implemented before the similarity comparison mechanism invokes. The traffic contours do not modify by this procedure, when there is no burst errors. The accuracy and performance of the contended mechanism depends on the appropriateness of the Threshold value. To compute the threshold value, a charismatic and dynamic procedure is used.

2) Active resolution of Threshold value

It is trivial to discover the apex value in the similarity graph using static threshold determination procedure. Packet loss compels the contended methodology. If packets drop during the process of content propagation, then the user side traffic contour gets decayed i.e., the larger value of similarity becomes smaller ones. In order to overcome this problem, a dynamic strategy is introduced to find out the threshold value, which can be easily adapted to the altering network environment. The similarity data that is obtained by this contended methodology is small and it is normally distributed around zero since, the cross-correlation values of the two distinguished random waveforms are approximated to be distributed normally. More similar patterns yield greater value of similarity. That value can be termed as an "Outlier". The following equation is used to determine the threshold value that helps in finding out the outlier among some values.

$$T_C = \min (\mu_C + 4\sigma_C , 1.0)$$

In the above equation, μ_C and σ_C are the mean and variance of the obtained similarity values. They are estimated based on the analysis. Each and every user side contour has its own μ_C, σ_C values. The coefficient of variance can be adjusted to balance the trade-off between the detection ratio and false-positives. Greater value of variance coefficient results in low false positive ratio at low detection ratio cost. Accordingly, the similarity value which is greater than T_C is considered as an outlier, which is numerically distant from the outlived values on the profile.

The computational cost needed to deploy the contended methodology is less when compared with the traditional mechanisms which include water marking and encoding techniques. In the proposed technique, Management Server is configured to compute the similarity of traffic signifiers. The total number of multiplications computed in the proposed system can better be explored in terms of three parameters. They are length of the user side contour (U), length of the server side contour (S) and the number of multiplications performed to compute the measure of similarity (M). The total number of multiplications are (S-U+1) M.

IV. Results and Discussions

The network components are configured in such a way that, they can perform their respective functionalities with minimum computation costs. This result in the less computational cost incurred in implementation of contended methodology.

Below figure depicts the network model of ten components and their connections.

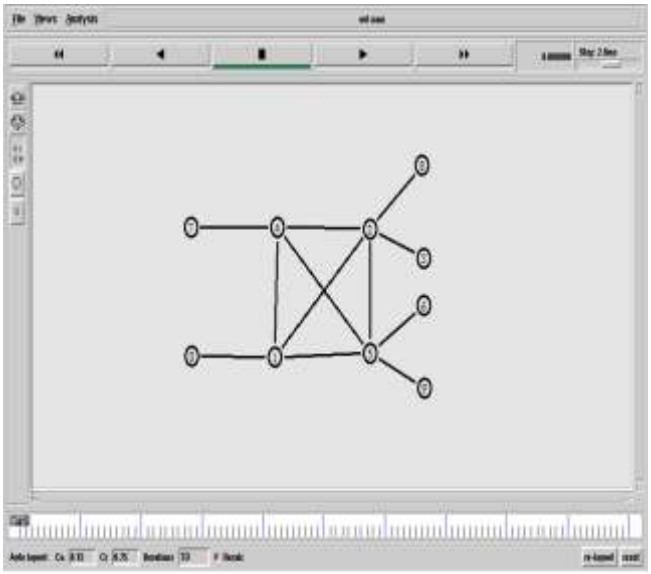


Figure 6: Network of ten components and their connections.

Figure 6 shows the organization of network and their connections.

The network components in figure 6 has to be configured at a particular time instant to perform their functionalities and is shown is in Figure 7.

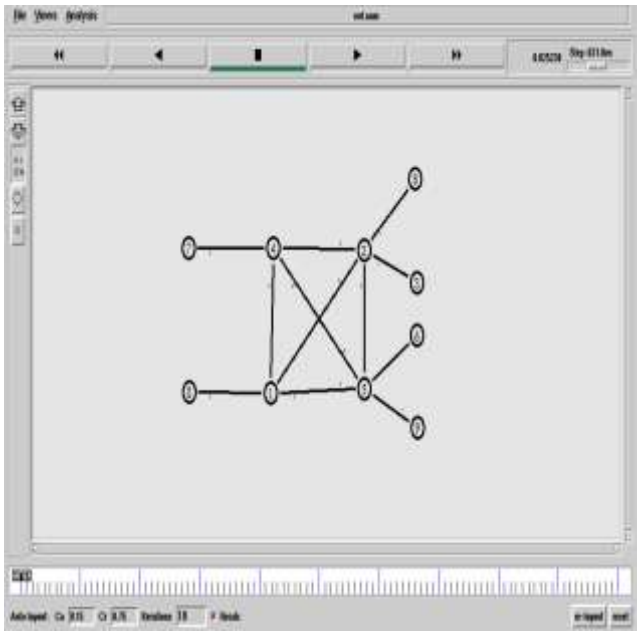


Figure 7: Configuration of network components.

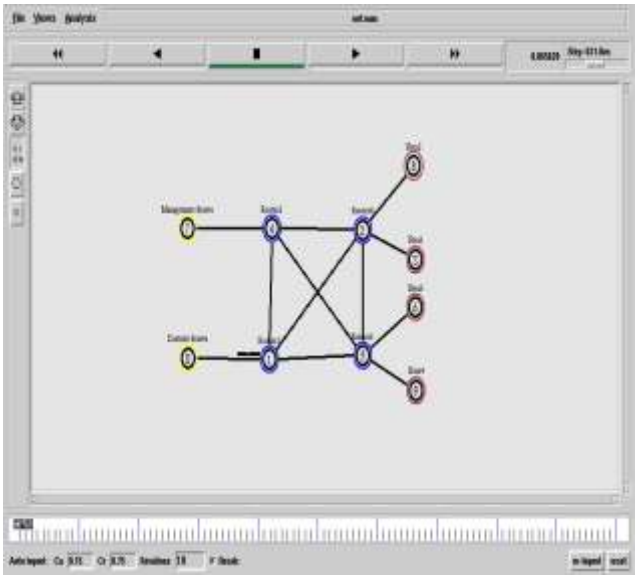


Figure 8: Labeling of network components.

Figure 8 shows the scenario of labeling the network participants involved to implement the contended methodology.

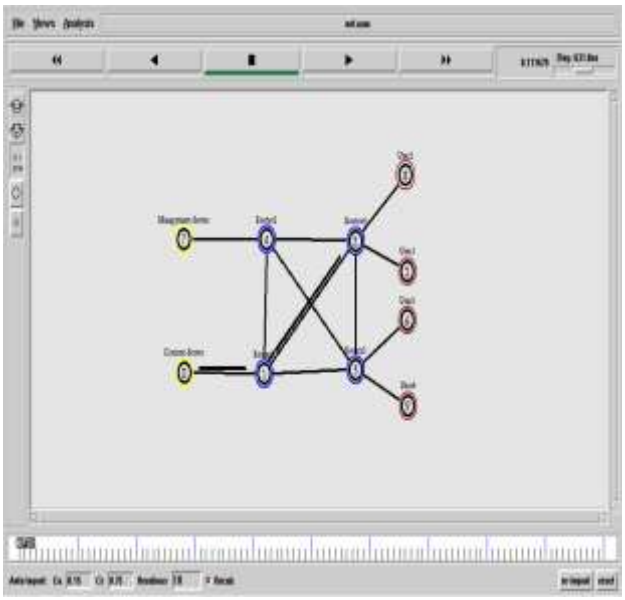


Figure 9: Content propagation from content server to intermediate router at user.

Figure 9 depicts a scenario of content simmering from content server to intermediate router at user (Router4) through intermediate router at server (Router1).

Below figure shows the immediate instance of the previous scenario.

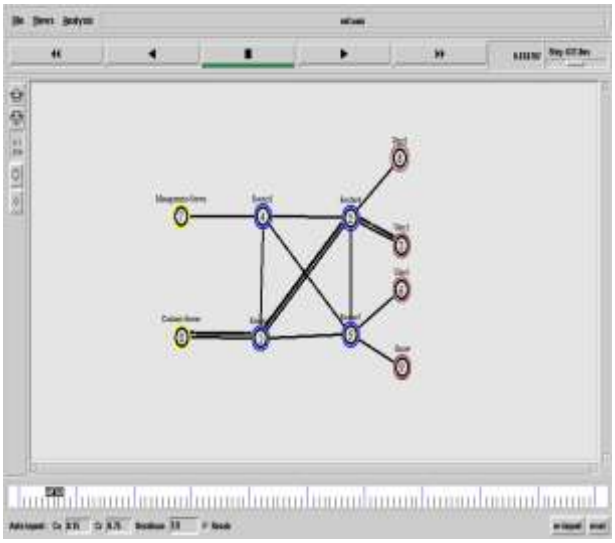


Figure 10: Content streaming from server to destined user.

Figure 10 represents streaming of contents from content server to destined user via routers in the middle of the streaming path.

The contended methodology employed in the simulation makes the network acquiring the property of self-healing. Self Healing means system can automatically recover to stable state without external interference. In this aspect, even there is a link failure in the network, the system has a capability to re-establish the path. In the meanwhile, the proposed strategy finds the alternate path to the destined user.

Below figure shows the scenario of link breakage between the routers present in the middle of the streaming path.

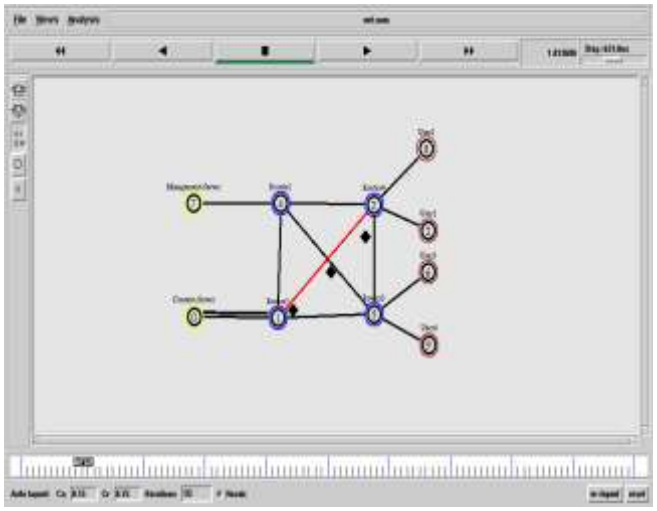


Figure 11: Link failure between the routers Router1 and Router4.

Figure 11 shows the instance describing about the link failure between the routers in the middle of the streaming path.

Below figure shows the adaptation of alternate path by the contended methodology to avoid data loss to the destined user.

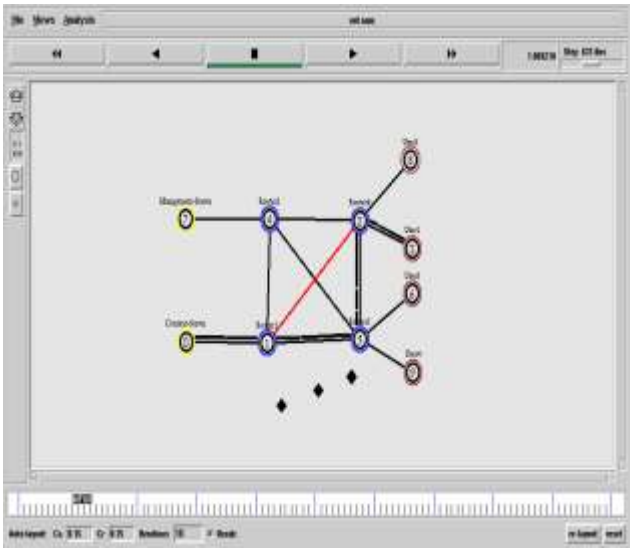


Figure 12: Adaptation of alternate path.

Below figure show the re-establishment of original path.

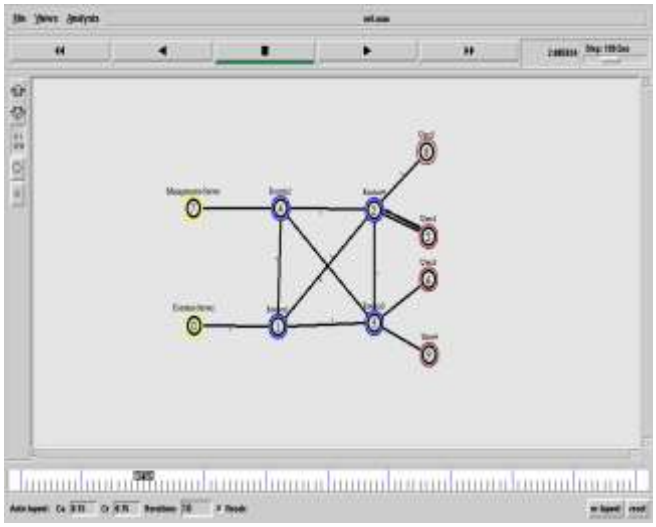


Figure 13: Re-Construction of original path.

Figure 13 shows the scenario of re-establishment of original path in order to avoid the situation of content loss at the destined user.

Below figure shows the traffic contour generated by the Management server using the traffic volume information obtained from the router at the server.

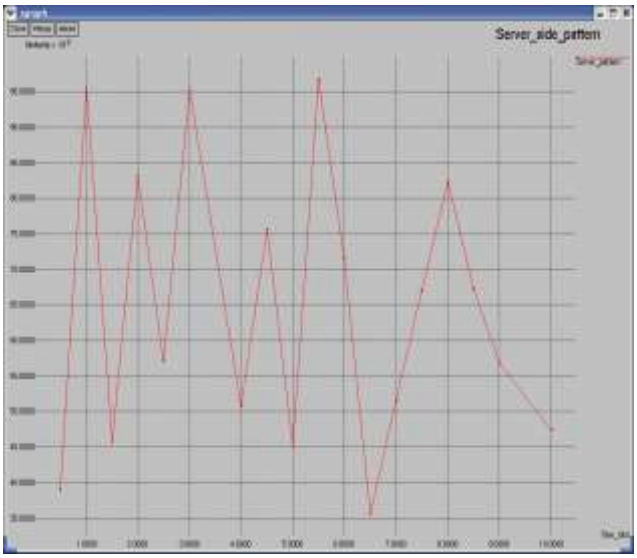


Figure 14: Server-side traffic contour.

Below figure shows the User side traffic contour generated at an instance by the management server using the traffic volume information obtained from the router at the destined user.

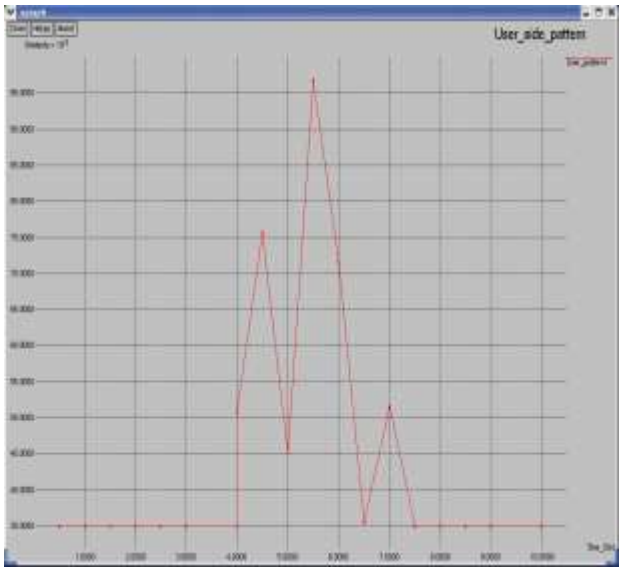


Figure 15: User-side traffic contour.

Figure 15 depicts an instance that describes about the traffic contour of the user generated using the traffic volume information.

Below figure shows the degree of similarity between the generated traffic contours of Server and User.

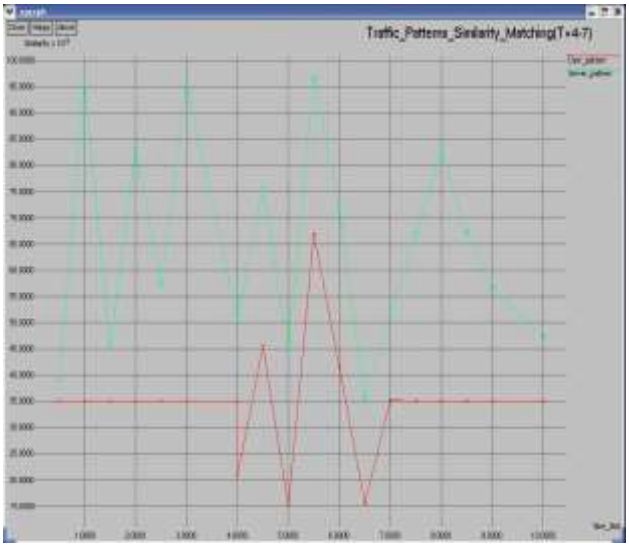


Figure 16: Traffic Contours Similarity matching.

From figure 16, the traffic contours in the time slot between 4 to 7 exhibits maximum similarity. This concludes that the destined user is receiving the content and the network exhibits ideal behavior.

V. CONCLUSION

To prevent exploitation of the content, a subjugate approach for simmering content delivery is required. For this purpose, traducer tracing technology is introduced. Conventional techniques to trace out the traducers involve high load and complex computations to produce multiple contents and watermarking has its own known limitations. To enable betterment in the security of the content delivery, an efficient mechanism is introduced which is based on traffic contours. To assess the accomplishment of the contended methodology, simulations were administered.

The contended methodology can also be incorporated with the previous DRM technology however, the computational cost involved in implementing the proposed strategy is less when compared with the costs involved in implementing watermarking and encoding techniques used in general traducer tracing techniques. The network components are configured in such a way that, they can perform their respective functionalities with minimum computation costs. This result in the less computational cost incurred in implementation of contended methodology. The proposed concept is not using the packet information, privacy issues of the application is least bothered.

REFERENCES

[1] Z. Yang, H. Ma, and J. Zhang, "A dynamic scalable service model for sip-based video conference," in Proc. Ninth Int. Conf. Computer Supported Cooperative Work in Design, May 2005, vol. 1, pp. 24–26.

[2] M. Shimakawa, D. P. Holed, and F. A. Tobagi, "Video-conferencing and data traffic over an ieee 802.11g wlan using dcf and edca," in *Proc.Int. Conf. Communications (ICC)*, May 2005, vol. 2, pp. 16–20.

[3] Niklas Carlsson, Derek L. Eager "Content Delivery using Replicated Digital Fountains", 2010 18th Annual IEEE/ACM International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems

[4] "A Secured Video Streaming System," 2010 International Conference on System Science and Engineering

[5] F. Hartung and F. Ramme, "Digital rights management and watermarking of multimedia content for m-commerce applications," *IEEE Commun. Mag.*, vol. 38, no. 11, pp. 78–84, Nov. 2000.

[6] A. Seki, and W. Kameyama, "A proposal on open drm system coping with both benefits of rights-holders and users," Proc. of the IEEE Globcom, vol.22, no.1, pp. 4111–4115, Dec. 2003.

[7] T. Liu, and C. Choudary, "Content-aware streaming of lecture videos over wireless networks," Proc. of the IEEE Multimedia Software Engineering, pp. 458–465, Dec. 2004.

[8] Jiaming He, Hongbin Zhang, "Digital Right ManagementModel Based on Cryptography and Digital Watermarking," 2008 International Conference on Computer Science and Software Engineering.

[9] Tony Thomas, Sabu Emmanuel, A. V. Subramanyam, and Mohan S. Kankanhalli, "JointWatermarking Scheme for Multiparty Multilevel DRM Architecture,"

Proc. IEEE, vol. 4, no. 4, December 2009

[10] E. I. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, "Advances in digital video content protection," *Proc. IEEE*, vol. 93, no. 1, pp. 171–183, Jan. 2005.

[11] S. Voloshynovskiy, S. Pereira, T. Pun, J. Eggers, and J. Su, "Attacks on digital watermarks: classification, estimation based attacks, and benchmarks," IEEE Comm. Magazine, vol.39, no.8, pp. 118–126, Aug. 2001.

[12] W. Luh and D. Kundur, "New paradigms for effective multicasting and fingerprinting of entertainment media," *IEEE Commun. Mag.*, vol. 43, no. 6, pp. 77–84, Jun. 2005.

[13] W. Luh and D. Kundur, "New paradigms for effective multicasting and fingerprinting of entertainment media," IEEE Commun. Mag., vol. 43, no. 6, pp. 77–84, Jun. 2005.

[14] D. Kundur and K. Karthik, "Video fingerprinting and encryption principles for digital rights management," *Proc. IEEE*, vol. 92, no. 6, pp. 918–932, Jun. 2004.

[15] B. Turnbull, "Important legal developments regarding protection of copyrighted content against unauthorized copying," IEEE Comm. Magazine, vol.39, no.8, pp. 92–100, Aug. 2001.

[16] M. Barni and F. Bartolini, "Data hiding for fighting piracy," *IEEE Signal Process. Mag.*, vol. 21, no. 2, pp. 28–39, Mar. 2004.

[17] A. Fiat, and T. Tassa, "Dynamic traitor tracing," Journal of CRYPTOLOGY, vol.14, no.3, pp. 211–223, 2001.

[18] R.S. Naini, and Y. Wang, "Sequential traitor tracing," IEEE Trans. On Information Theory, vol.49, no.5, pp. 1319–1326, 2003.

[19] B. N. Park, W. Lee, and J. W. kim, "A license management protocol for protecting user privacy and digital contents in digital rights management systems," *IEICE Trans. Inf. Syst.*, vol. E88-D, no. 8, pp. 1958–1965, Aug. 2005.

[20] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Process.*, vol. 48, no. 8, pp. 2439–2451, Aug. 2000.

[21] A. Pommer and A. Uhl, "Selective encryption of wavelet-packet encoded image data: Efficiency and security," *Multimedia Syst.*, vol. 9,no. 3, pp. 279–287, 2003.

[22] X. Wang, "Mpeg-21 rights expression language: Enabling interoperable digital rights management," *IEEE Multimedia*, vol. 11, no. 4, pp. 84–87, Oct./Dec. 2004.

[23] K. Su, D. Kundur, and D. Hatzinakos, "Statisticalinvisibility for collusion- resistant digital video watermarking," *IEEE Trans. Multimedia*, vol. 7, no. 1, pp. 43–51, Feb. 2005.

[24] M. Kutter, S. Voloshynovskiy, and A. Herrigel, "The watermark copy attack," in *Proc. Electronic Imaging '99, Security and Watermarking of Multimedia Contents II*, San Jose, Jan. 2000, vol. 3971, pp. 371–380.

Big Brother: A Road Map for Building Ubiquitous Surveillance System in Nigeria

Simon Enoch Yusuf[1] and Oluwakayode Osagbemi[2]
Department of Computer Science,
University of Ibadan,
Ibadan, Nigeria.
[1]simmypukuma@yahoo.co.uk
[2]kayodeosagbemi@yahoo.com

***Abstract*—In this paper, we propose a method to improve the security challenges in Nigeria by embedding literally hundreds of invisible computers into the environment with each computer performing its tasks without requiring human awareness or a large amount of human intervention to monitor human behaviour, natural disasters and search for stolen or lost items. Ubiquitous Dynamic Surveillance cameras embedded with Radio frequency identification (RFID) is proposed for this security system.**

Keywords-component; Ubiquitous; Surveillance; RFID; Security; Computing.

I. INTRODUCTION

The issue of security of life and property in Nigeria has taken a frightening dimension and an issue of great concern to citizens and the government.

The need to tap from the power of Information and Communication Technology (ICT) to enhance national security operations is paramount. For some time, the issue of security of life and property in Nigeria has taken a frightening dimension and an issue of great concern to citizens and the government. The problem of security spans from kidnapping in the eastern region and traverses the religious disturbances in the north, political gansterism in the west and bomb-blast becoming issues of the moment [1]. Terrorism and atrocious crimes are increasing on a world-wide scale. Moreover, natural disasters, such as earthquakes and tsunamis, have also occurred frequently in many parts of the world. Figure 1 shows the death toll reported from 2003 to 2008 in various types of natural disasters. During this five-year period, the death toll reached over 482,000 as a result of such disasters. Death toll reported in various disaster types from 2003 to 2010 is shown in the Figure 2. Several earthquakes around the world proved to be the most deadly disasters which caused 406,866 deaths in the last five years [2]. The number of people reported to be affected by these disasters (142 million) dropped by 10 per cent, while the number of people reported killed is 23833 [3]. The 2008 death toll of 235,816 was more than three times the annual average of the previous eight years [4]. In 2009 there were only 25 geophysical disasters reported compared to the 2000-2008 annual average of 37. Of these, 18 were earthquakes, four tsunamis, two volcanic eruptions and one a landslide [5]. The year 2010 was characterized by a large number of natural disasters that have claimed four times more victims than in the past thirty years for a total of 295,000 victims [6]

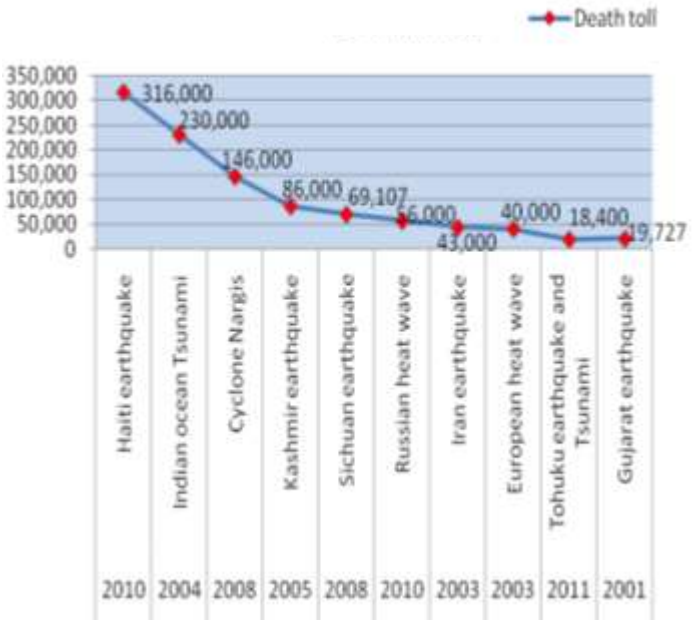


Figure 1. ten worst disaster of 21st century

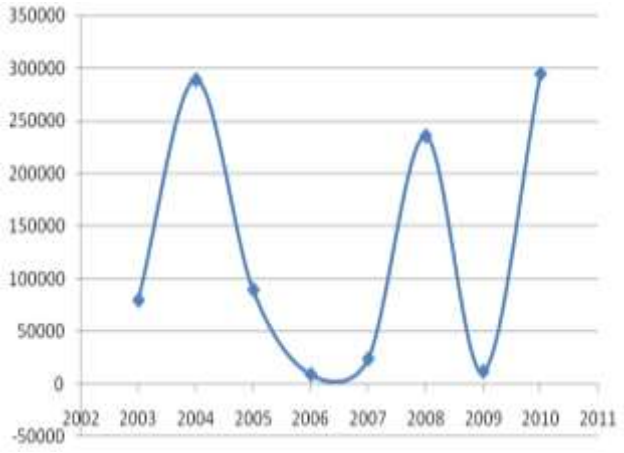


Figure 2. Average Death toll 2003 - 2010

The safety of human life is threatened by disasters caused by man and natural disasters.

In the fields of security, law enforcement, crime detection, inventory and industrial process monitoring, there is often a need to effectively identify individual subjects whether they be humans, goods or pieces of infrastructure.

II. UBIQUITOUS COMPUTING

Ubiquitous computing network is an emerging concept in computing, which integrates computation capabilities into the physical environment rather than being perceived as a visible object, so that it can provide widespread access to shared services through a variety of diverse devices irrespective of whether individuals are mobile or not.

Ubiquitous computing refers to methods of enhancing computer use by making networks of sensors and computers available and embedded in the physical environment [7]. The technologies on which ubiquitous computing applications are based span automatic identification (Auto-ID), such as Radio Frequency Identification (RFID); (wireless) communication systems, such as Global Standard for Mobile Communication (GSM); positioning services, such as Global Positioning System (GPS); and sensor networks. Together, these technologies are making new or improved security.

The term "ubiquitous computing" is a very broad term that is often overloaded to mean diverse things to different research projects. In many cases, researchers define ubiquitous computing by example, with respect to their own research. Ubiquitous computing allows us to realize additional abstractions that did not exist in traditional computing paradigms. The salient features of ubiquitous computing include the following according to [8].

- Extending Computing Boundaries. While traditional computing encompassed hardware and software entities, ubiquitous computing extends the boundaries of computing to include physical spaces, building infrastructures, and the devices contained within. This aims to transform dull, passive spaces into interactive, dynamic, and programmable spaces that are coordinated through a software infrastructure and populated with a large number of mobile users and devices.
- Invisibility and non-intrusiveness. In current computing models, computers are still the main focus of attention. In effect, people have to change some of their behaviour and the way they perform tasks so that these tasks can be computerized. To boost productivity, it is important that computing machinery disappears from the spotlight. Computers should blend in the background allowing people to perform their duties without having machines at the centre of their focus.
- Creating smart and sentient spaces. A dust of invisible embedded devices and sensors are incorporated to turn physical spaces into active, smart surroundings that can sense, "see," and "hear," effectively, making the space sentient and personalized. Ultimately, the space should become intelligent enough to understand users' intentions and become an integral part of users' everyday life.
- Context awareness. A ubiquitous computing model should be able to capture the different contexts and situational information and integrate them with users and devices. This allows the active space to take on the responsibility of locating and serving users and automatically tailoring itself to meet their expectations and preferences.
- Mobility and adaptability. To be truly omnipresent, the ubiquitous computing environment should be as mobile as its users. It should be able to adapt itself to environments with scarce resources, while being able to evolve and extend once more resources become available.

III. RADIO FREQUENCY IDENTIFICATION (RFID)

RFID is an area of automatic identification that is gaining momentum and is considered by some to emerge as one of the most pervasive computing technologies in history [9]. RFID or Radio Frequency Identification Tag Reader has revolutionized the way we live. RFID tag reader has made it possible to track any type of object by using radio frequency technology. Today RFID is a generic term for technologies that use radio waves to automatically identify people or objects (RFID Journal). There are several methods of identification, the most common of which is to associate the RFID tag unique identifier with an object or person. In most commonly touted applications of RFID, the microchip contains Electronic Product Code (EPC) with sufficient capacity to provide unique identifiers for all items produced worldwide. When an RFID reader emits a radio signal, tags in the vicinity respond by transmitting their stored data to the reader [10].

The principal advantages of RFID system are the non-contact, non-line-of-sight characteristics of the technology. Tags can be read through a variety of visually and environmentally challenging conditions such as snow, ice, fog, paint, grime, inside containers and vehicles and while in storage [11].

An RFID system consists of three main components, namely, tag, antenna, and reader. An RFID tag consists of a microchip attached to an antenna. Tags are either active or passive. Passive tags derive the power from the field generated by the reader. An RFID antenna is connected to the RFID reader. The antenna activates the RFID tag and transfers data by emitting wireless pulses.

The RFID reader handles the communication between the information system and the RFID tag. The signals transfer to the host computer and pass through to the electronic product code (EPC) network. After that, the data is stored in the database server or other business application systems. There is an important tool called RFID middleware which consists of a set of software components that act as a bridge between the RFID system components (i.e., tags and readers) and the host application software. In other words, middleware tools are used to manage RFID data by routing it between tag/readers and the systems within the businesses. Middleware solutions filter duplicate, incomplete, and erroneous data that it receives. After

digesting all data from the various sources, middleware forwards only the meaningful events to the enterprise systems. The tasks of the RFID middleware include data filtering, classification, data normalization, and aggregation of data transmitted between tags and readers for integration with the host application [12]-[21]-[28].

RFID is a type of Auto-ID technology sometimes referred to as dedicated short-range communication (DSRC), RFID is "a wireless link to identify people or objects" [13]. RFID is, in reality, a subset of the larger radio frequency (RF) market, which encompasses an array of RF technologies, including the following:

- Cellular phones
- Digital radio
- The Global Positioning System (GPS)
- High-definition television (HDTV)
- Wireless networks [14]

A. *Element of RFID*

RFID systems consist of four elements: the RFID tags, the RFID readers, the antennas and choice of radio characteristics, and the computer network that is used to connect the readers.

B. *RFID Tags*

RFID tagging is the use of very small electronic devices (called 'RFID tags') which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves.

The tag is the basic building block of RFID. Each tag consists of an antenna and a small silicon chip that contains a radio receiver, a radio modulator for sending a response back to the reader, control logic, some amount of memory, and a power system. An active tag will be used to build this system. The reasons for the choice of this tag are because of their reading range and reliability. With the proper antenna on the reader and the tag, a 915MHz tag can be read from a distance of 100 feet or more [18]. The tags also tend to be more reliable because they do not need a continuous radio signal to power their electronics as in passive tags.

IV. RELATED WORK

One of the first applications of a radio frequency identification system was in "Identify Friend or Foe" (IFF) systems deployed by the British Royal Air Force during World War II 0. IFF allowed radar operators and pilots to automatically distinguish friendly aircraft from enemies via RF signals. IFF systems helped prevent "friendly fire" incidents and aided in intercepting enemy aircraft. Advanced IFF systems are used today in aircraft and munitions, although much of the technology remains classified [31].

Identification of people, objects and locations is an obvious application of RFID technology. Security systems that use RFID proximity cards to control access to restricted areas are perhaps the most common RFID application in use today [32].

Even in developing countries, such as Bangladesh, hospitals are using RFID-enabled staff ID cards [33]-[32]. Other hospitals have extended the use of staff ID cards to control access to computers and applications [34] - [32].

At the Georgia Veteran's Medical Centre RFID has been used for location identification [35]-[32]. Patients with visual impairments can navigate around the hospital by reading these location tags with using a cane containing an RFID reader.

RFID technology is being used to track thousands of wheelchairs, beds, IV pumps and other pieces of expensive medical equipment at several hospitals, including Bielefeld City Clinic in Germany [38], Lagos de Moreno General Hospital in Mexico [36], and the Walter Reed Army Medical Centre in the US [37]. Each item is tagged and can be located in real time via a network of RFID readers throughout the hospital. Some such systems, often referred to as Real Time Location Systems (RTLSs), also keep track of whether the equipment is available, in use, awaiting cleaning, or undergoing maintenance [32].

A. *Proposed System*

In this section we describe a framework of a surveillance system that ensures that many computers are available throughout the physical environment, but making them effectively invisible. More precisely, a proliferation of hundreds or thousands of computing devices, sensors and embedded processors that will provide new functionality, offer specialized services with the surrounding environment and available resources.

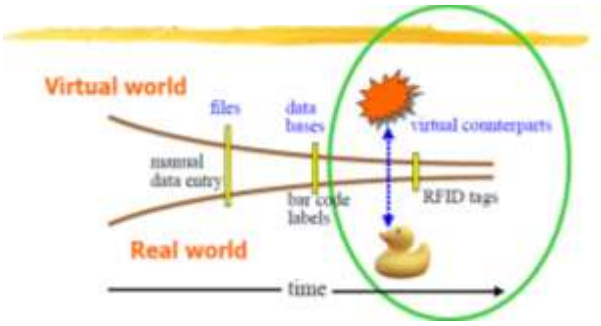


Figure 3. Tagging object from real world to the visual in a database [16]

After vigilantly studying the Camera Based Surveillance Architecture, and judged on the basis of the following parameters as provided by [17]:

i. Automation
ii. Time efficiency
iii. Ease of monitoring and administration of its operations by naive hands
iv. Impenetrable
v. Efficient for mobile and immobile objects and regions
vi. Installation cost of system

It is found that it doesn't overall fulfil the demands for ubiquitous due to technological limitations. We have come up with a roadmap using ubiquitous computing to overcome the limitations of Camera Surveillance Mechanism. The objectives of the proposed system include

- To enhance national security
- To enhance the recovery of missed and stolen items.
- To identify object and their respective location.
- To enhance policies on identifying the rightful owners of an object.

Surveillance cameras with video camera embedded with RFID is proposed in this paper to enhance national security. These surveillance cameras are connected to a recording device, IP network, and is been watched by a law enforcement officer.

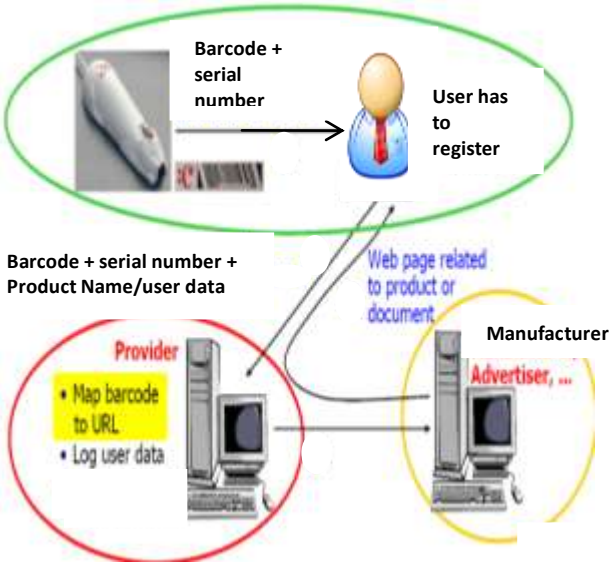


Figure 4. Mapping of barcode to Internet pages adapted from [29]

The cameras sense motion and footage. Analysis of footage is made by automated software that organizes digital video footage into a searchable database, and by automated video analysis software which can be VIRAT, HumanID [30]. The amount of footage is also drastically reduced by motion sensors which only record when motion is detected.

The surveillance cameras are embedded with RFID data server which will be communicating with both the RFID tag and RFID main data server. It is used for capturing images whether still or frames and records activities in a particular location over time. The purpose for combining both RFID and surveillance cameras is for Dynamic Surveillance which focuses over motion, location, identification and gives visual support to the system when needed. Big Brother provides a Surveillance Technique which can't be mistuned technically, manually or by any other means [17] because of RFID tag embedded with it.

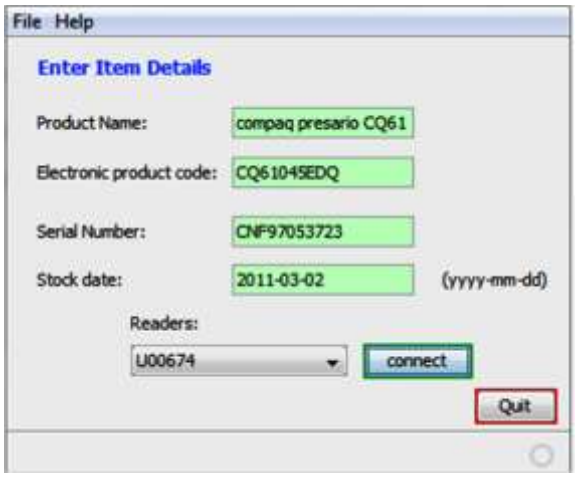


Figure 5. Taking stock of RFID tag objects

The Database consists of Product name, model number, electronic product code and readers IDs. Tags information are stored in the database and linked to the tags. The readers and tag identify objects and information about the objects, the objects are embedded with the RFID tag while in the case of humans an attachment is made to the individual cloths or in the form of any wearable device. Prototype object tag information database is shown above which provides information about the object.

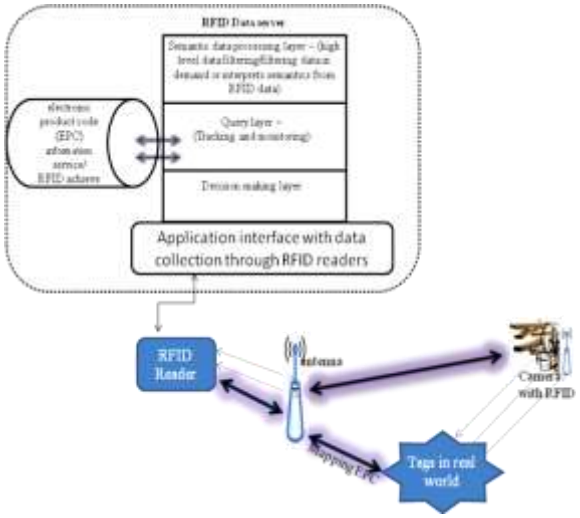


Figure 6. RFID framework

The RFID tag reader then sends an electronic signal to the embedded tag. The RFID tag responds to this signal by sending back a radio frequency signal. This signal can give the location of the object along with the product information. [15].

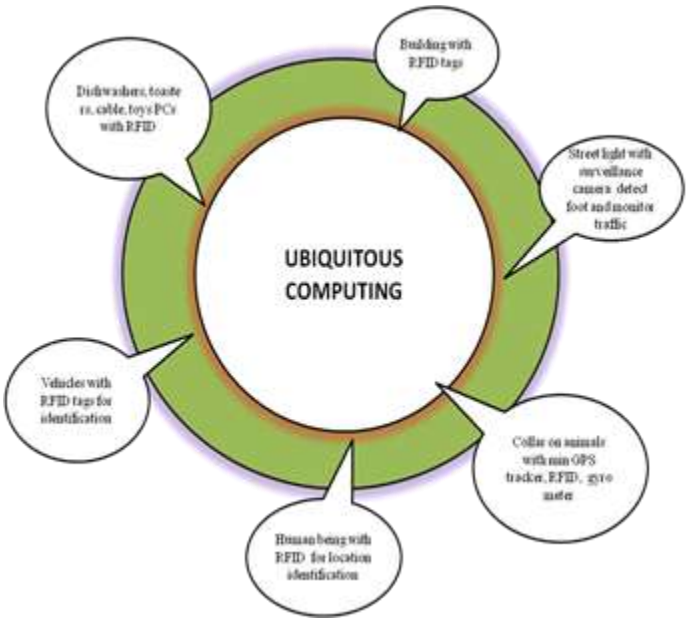


Figure 7. Ubiquitous computing Scenerio

B. RFID tags for earthquake detection

According to new research conducted by International Journal of Innovation and sustainable development, Radio frequency identification, RFID, could be used in the immediate aftermath of a major earthquake to save lives [19]. In addition, in earthquakes or tsunami, animals were the first to detect these natural disasters days before it happens and run for safety [20]. Big Brother is used to track unnatural motion in animals by combining mini GPS tracker, RFID and gyrometer chip. RFID tags are attached to a couple of hundred animals in the earthquake prone area. When these animals start to flee, the RFIDs would transmit the co-ordinates of the fleeing motion to a central computer. The GPS tracker would provide the co-ordinates where animal behaviour is abnormal to pinpoint the location of a potential earthquake. RFIDs would provide wireless transmission of the data and the gyrometer can detect uneasy motions in the animal and send warning to the connected central computer with an alarm.

C. RFID Tags for Human Identification

Big Brother can be used to identify patients in hospitals, prevent theft, and track shipments. This system provides a rapid way to read data about an individual. It can reliably identify human being and can also be used for animal identification. However, at present the most prevalent use for RFID tags is tracking merchandise. Retailers are using RFID tags to check on their merchandise to see whether they are in the premises or being transported. Big Brother (RFID) can also be incorporated into National passport just like countries like Malaysia, UK and the US now using RFID tags in passports [21].

Big Brother monitors and acts as a tracer for easy location identification. For Pupils going to school, trigger areas are set at some point in the school zone which provides alert to parent and school authority about passage of their children.

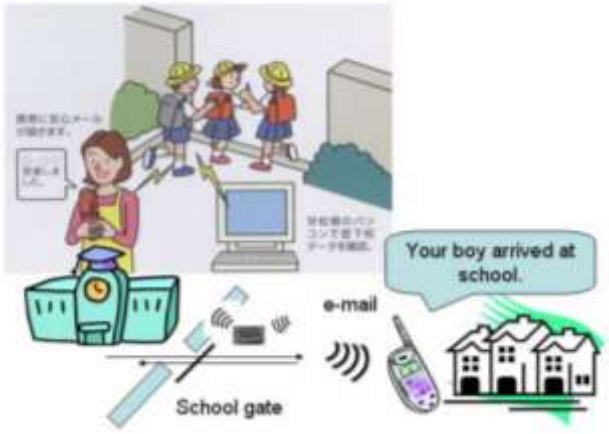


Figure 8. Checking system for prevention of kidnapping [22]

V. RECOMMNEDATIONS

Several technical problems should be considered beforehand in line with the security of the RFID system. Some of the security requirement includes [23]:

Availability: When constructing the RFID system, failure in hardware or software may occur due to deliberate action or not. Therefore, if the RFID tag cannot provide service due to attacks or physical failure during the construction of the system, the availability of the RFID system should be provided to restore the service promptly.

Forward channel security: Forward security is required to generate and provide the service through secure communication between the RFID tag and the RF reader. This is because the attacker can prey on the various information transmitted or received from the RFID tag [23].

Secure status acquisition technology: When constructing the RFID-based network, a safe service acquisition process is required to know the status of all RFID tags. This must be performed by checking the current status of all tags in the RFID system in order to ensure the availability of the service against potential physical failure that may happen during denial-of-service (DoS) attacks or during the construction of the RFID system [23].

Finally, This cost of implementation can be reduced by employing existing wireless networks.

VI. CONCLUSION

Most Surveillance agencies like National Association for the Criminal Rehabilitation of Offenders (NACRO), Home Office USA etc [27]-[17] accept the failure of Camera Surveillance due to technical, manual or any other discrepancies in the system. Thus there arises a need for better technology for Surveillance. RFID provides a Surveillance Technique which can't be mistuned technically, manually or by any other means [17]. In our work, we proposed a surveillance camera system embedded with RFID reader.

Some of the Challenges of the system include:

- Forgery: forgery is a major problem in RFID, user with illegitimate identification would devise various means to imitate legitimate tags.
- Cost: obviously, the cost of implementation is a major hurdle to consider before embarking on it. The cost of implementation can be significant, depending on the area to be covered, the number of items to be tracked, and the accuracy required.
- Denial of service attack: attackers unable to conduct forgery attack will leave the system communication channels jam preventing RFID readers from identify tags. An attacker could also seed a physical space with "chaff " tags intended to confuse legitimate readers or poison databases. Locating and removing chaff tags might be very difficult in a warehouse environment [30].
- Security and Privacy: many people consider this as in invasion of privacy because it tracks their movement and visually their activities and therefore will not allow such systems be installed around them.

REFERENCES

[1] O. E., Osuagwu, G. Nworuh, B. Asiegbu , A. Uwaleke, F. Olanapo & U. Eze, "Enhancing security of the Nigerian State through electronic roadside vehicle indentification system" 23rd National conference, Nigeria Computer Society, Conference Proceedings Volume 21, pp. 299-304, July, 2010.

[2] A. Ahmed, L. Sugianto, "RFID in Emergency Management",chap VIII Auto-Identification and Ubiquitous computing applications , RFID and smart Technologies for information converage. Infromation Science Reference. Hershey, New York 2009, pp. 39-53.

[3] Canadian Red cross articial retrieved on 2 June, 2011 from http://www.redcross.ca/article.asp?id=25285&tid=001.

[4] CBC News on World Natural disasters retrieved on 15 May, 2011 from http://www.cbc.ca/news/world/story/2009/01/23/natural-disasters.html.

[5] Alert Net News on Natural disasters in 2009 retrieved on 2nd June, 2011 from http://www.trust.org/alertnet/news/fewer-natural-disasters-in-2009-but-no-clear-trend-seen-research-group.

[6] World life Union retrieved on 23rd May, 2011 from http://www.thelivingtrees.org/forumtlt/viewtopic.php?f=12&t=6.

[7] M. Weiser "*Hot Topics: Ubiquitous Computing*", IEEE Computer, Vol. 26, No. 3, October 1993.

[8] J. F. Al-muhtadi, "An intelligent authentication infrastructure for ubiquitous computing environments". Phd dissertation, Graduate colleege of the university of illonois at urbana-champaign, 2005.

[9] R. T. Davis. "*U.S. Foreign Policy and National Security:Chronology and Index for the 20th Century"*. Praeger Security International Series (Illustrated ed.). ABC-CLIO. p. xiii=xiv. ISBN 9780313383854.

[10] "Position Statement on the use of RFID on consumer products" (2003, November). Retrieved on 23 May, 2011 from http://www.spychips.org/jointrfid_position_paper.html.

[11] C. Robert, "Radio Frequency Identification (RFID)". *Journal of Computers and Security*. Infromation Science Reference. Hershey, New York 2009.

[12] M. Bhuptani, & S. Moradpour, "RFID field guide: Deploying radio frequency identification systems". New York: Prentice Hall 2005.

[13] S. d'Hont. "*The cutting edge of RFID technology and applications for manufacturing and distribution"* Retrieved on July 10, 2003, from http://www.ti.com/tiris/docs/manuals/whtPapers/manuf_dist.pdf

[14] R. Malone, "Reconsidering the role of RFID. *Inbound Logistics"* Retrieved on September 11, 2004, from http://www.inboundlogistics.com/articles/supplychain/sct0804.shtml

[15] Horizon world wide componets co. Ltd. http://www.horizon-components.com/tag-reader-rfid-uhf-sdio.html retrived 20 june, 2011

[16] F. Mattern "Ubiquitous Computing. ETH Zurich Institute for Pervasive Computing" Copyright F. Mattern, Porquerolles, May 2003. http://www.vs.inf.ethz.ch/publ/slides/MatternPorquerolles.pdf

[17] I. Singh, H. Patil "RFID: Dynamic Surveillance Approach" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.

[18] G. Simson and H. Henry, "Understanding RFID Technology" chap II, garfinkel.book Page 15 Thursday, June 2, 2005.

[19] "The use of RFID technology in earthquakes" in Int. J. Innovation and Sustainable Development, Vol 4, 253-275. Published: May 6, 2010. Inderscience Publishers. Retreved on 23 May, 2011 from http://www.sciencenewsline.com/nature/2010050612000022.html

[20] "Quora article on Technology that should be build for earthquake detection", Retrieved on 20 june, 2011 from http://www.quora.com/Earthquakes/Which-technology-should-be-built-to-predict-Earthquakes-and-warn-related-people-to-be-on-a-safety-place.

[21] S. Shah, "Semantics and Internet of things", RFID Journal White Paper.

[22] *N. Ashida, Y. Ashida, S. Sagawa, S. Suto, T. Higash., Makimoto K.and Kawahara T.* "Safety Management and Crime Prevention by IC Tags – Cases of practical use of IC tag in medical and welfare fields", 5rd APT TELEMEDICINE Workshop, Proceedings 2007.

[23] D. Seo and I. Lee, "A Study on RFID System with Secure Service Availability for Ubiquitous Computing", *International Journal of Information Processing Systems Vol.1, No.1, 2005*.

[24] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, "Next Century Challenges Scalable Coordination in Sensor Networks.", Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking. Seattle, Washington, USA, 263-270.

[25] National Research Council, "Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers", *National Academy Press2001, Washington DC, USA.*

[26] RFID Journal (n.d.). *RFID Journal frequency asked questions*. Retrieved from http://www.rfidjournal.com.

[27] Surveillance Camera Players "ineffectiveness of surveillance cameras" updated on 17th June 2009.

[28] K. Goyal & D. Krishna, "RFID middleware integration to the entire supply chain" RFID Journal White Paper 2005.

[29] Ubiquitous Computing retrived on 2 June, 2011 from http://www.vs.inf.ethz.ch/publ/slides/MatternPorquerolles.pdf

[30] Wikipedia, retrieved June 20, 2011 from http://en.wikipedia.org/wiki/Surveillance

[31] S. A. Weis S. A. "RFID (Radio Frequency Identification): Principles and Applications" Retrived from www.eecs.harvard.edu/rfid-article.pdf on 01 August, 2011.

[32] J. Symonds, J. Ayoade, D. Parry, "Auto-Identification and ubiquitous computing applications: RFID and Smart Technologies for Information Convergence" . Chap VI . information Science reference. Hershey. New York 2009.

[33] B. Bacheldor, "RFID Take Root in Bangladesh. Retrieved February 12, 2008, from www.rfidjournal.com

[34] B. Bacheldor, "N.J. Medical Center Uses LF Tags to Protect Patient Records", Retrieved February 12, 2008, from www.rfidjournal.com

[35] D. A. Ross & B. B. Blasch, "Development of a Wearable Computer Orientation System", ACM Personal and Ubiquitous Computing 2002, 6(1), 49-63.

[36] B. Bacheldor, "Local Hospital Spearheads Mexico's Digital-Hospital Initiative", Retrieved February 12, 2008, from www.rfidjournal.com

[37] C. Broder, Hospitals Wade into Asset- Tracking Technology. Retrieved October 30, 2004, from www.ihealthbeat.com

[38] R. Wessel, "German Hospital Expands Bed-Tagging Project" 2007. Retrieved February 12, 2008, from www.rfidjournal.com

AUTHORS PROFILE

Simon Enoch Yusuf received his BSc (Hons) degree in Computer Science in 2007 from University of Adamawa State and MSc in Computer Science from University of Ibadan, Nigeria. His research Interest Includes Network security, Ubiquitous computing and ICT Diffusion in developing countries. He is a member of Nigeria Computer Society (NCS), and has published quite a number of papers in reputable Journals and conference proceedings.

Oluwakayode Osagbemi holds a BSc (Hons) degree in Computer Science (2008) and a MSc in Computer Science both from the University of Ibadan. His research interests include computer vision, content based image retrieval, and ubiquitous computing. He has published in several conference proceedings.

NIDS For Unsupervised Authentication Records of KDD Dataset in MATLAB

Mis. Bhawana Pillai
M-Tech
LNCT Bhopal
Bhopal, (M.P.) India
bhawanapillai@gmail.com

Mr. Uday Pratap Singh
Asst Prof (CSE) Lnct
Bhopal, (M.P.) India
usinghiitg@gmail.com

***Abstract*- Most anomaly based NIDS employ supervised algorithms, whose performances highly depend on attack-free training data. Moreover, with changing network environment or services, patterns of normal traffic will be changed. In this paper, we developed intrusion detection system is to analyses the authentication records and separate UNFEIGNED and fraudulent authentication attempts for each user account in the system. Intrusions are detected by determining outliers related to the built patterns. We present the modification on the outlier detection algorithm. It is important problems to increase the detection rates and reduce false positive rates in Intrusion Detection System. Although preventative techniques such as access control and authentication attempt to prevent intruders, these can fail, and as a second line of defense, intrusion detection has been introduced. Rare events are events that occur very infrequently, detection of rare events is a common problem in many domains. Support Vector Machines (SVM) as a classical pattern recognition tool have been widely used for intrusion detection. However, conventional SVM methods do not concern different characteristics of features in building an intrusion detection system. Also evaluate the performance of K-Means algorithm by the detection rate and the false positive rate. All result evaluate with the new model of KDD dataset. Result generates in ROC Curves and compared both result of K-Means and SVM in Matlab.**

Keywords- Anomaly detection; Intrusion Detection; Expectation Maximization; MATLAB; UNSOUND authentication; UNFEIGNED; reduce false.

I. INTRODUCTION

ECURITY techniques such as authentication and access control have been developed to achieve the objective of computer security namely to prevent unauthorized intruders from accessing and manipulating information. The security administrator is now faced with the problem of selecting suitable IDS for his/her particular computer system. Rapid expansion of computer network throughout the world has made security a crucial issue in a computing environment. Anomalies pattern sometimes exist within tiny or rare classes of similar anomalies. Anomaly-based network intrusion detection is a complex process. The challenge is thus important to identify "rare events" records in data set. As defined in, intrusion detection is "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions. It is also defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network". Anomaly Intrusion Detection Systems (IDS) aim at distinguishing an abnormal activity from an ordinary one.

Intrusion detection is a critical component of secure information systems. Many approaches have been proposed which include statistical, machine learning, data mining and immunological inspired techniques. Events that may not be actual security violations but those that do not fit in the normal usage profile of a user may be termed as suspicious events. Monitoring suspicious activities may help in finding a possible intrusion.

There are two main intrusion detection systems. *Anomaly intrusion detection system* is based on the profiles of normal behaviors of users or applications and checks whether the system is being used in a different manner.

The second one is called *misuse intrusion detection system* which collects attack signatures, compares a behavior with these attack signatures, and signals intrusion when there is a match. It is often impossible to analyze the vast amount of whole data, but one has to focus the analysis on an important portion of the data such as using some criteria, only the classes of interest can be selected for analysis or processing while the rest is rejected. This paper suggests the use rough set as a dimensionality reduction technique to avoid this information loss.

The theory of rough sets has been specially designed to handle data imperfections same as in fuzzy logic. Rough sets remove superfluous information by examining attribute dependencies. It deals with inconsistencies, uncertainty and incompleteness by imposing an upper and a lower approximation to set membership. Rough sets estimates the relevance of an attribute by using attribute dependencies regarding a given decision class. It achieves attribute set covering by imposing a discernibility relation With the tremendous growth of network-based services and sensitive information on networks, the number and the severity of network-based computer attacks have significantly increased. Although a wide range of security technologies such as information encryption, access control, and intrusion prevention can protect network-based systems, there are still many undetected intrusions. Thus, Intrusion Detection Systems (IDS) play a vital role in network security. Network Intrusion Detection Systems (NIDS) detect attacks by

observing various network activities, while Host-based Intrusion Detection Systems (HIDS) detect intrusions in an individual host.

To overcome the limitations of supervised anomaly based systems, a number of IDS employ unsupervised approaches. Unsupervised anomaly detection does not need attack-free training data. It detects attacks by determining unusual activities from data under two assumptions: The majority of activities are normal. Attacks statistically deviate from normal activities. The unusual activities are outliers that are inconsistent with the remainder of data set. Thus, outlier detection techniques can be applied in unsupervised anomaly detection. Actually, outlier detection has been used in a number of practical applications such as credit card fraud detection, voting irregularity analysis, and severe weather prediction.

II. Proposed Technique

Data presented to algorithm is generated by picking one of two Gaussians at random and then sampling from the selected distribution. If each Gaussian describes on of two users – UNFEIGNED and fraudulent, trying to authenticate, knowing from which Gaussian each sample of our data originated would completely solve our ID problem. Gaussian type distributions are assumed here for both UNFEIGNED and fraudulent user, So what are the hidden variables in this problem? Well, if we knew which sample in our set is generated by which distribution we could easily solve the problem. It would then be easy to calculate sample mean and variance for each distribution. All that would be left in this situation would be to somehow classify the new samples (i.e. new authentication attempts) as members of one or the other Gaussian.

The *k*-Means clustering is a classical clustering algorithm. After an initial random assignment of example to *k* clusters, the centers of clusters are computed and the examples are assigned to the clusters with the closest centers. The process is repeated until the cluster centers do not significantly change. Once the cluster assignment is fixed, the mean distance of an example to cluster centers is used as the score. Using the *k*means clustering algorithm, different clusters were specified and generated for each output class. There are two problems that are inherent to *k*-Means clustering algorithms. The first is determining the initial partition and the second is determining the optimal number of clusters.

Algorithm 1. k-means

Step 1: Choose *k* cluster centers to coincide with *k* randomly-chosen patterns or *k* randomly defined points inside the hyper volumn containing the pattern set.

Step 2: Assign each pattern to the closest cluster center.

Step 3: Recomputed the cluster centers using the current luster memberships.

Step 4: If a convergence criterion is not met, go to step 2. Typical convergence criteria are: no (or minimal) reassignment of patterns to new luster centers, or minimal decrease in squared error

In this experiment, we use a standard dataset the raw data used by the KDD Cup 1999 intrusion detection contest. This database includes a wide variety of intrusions simulated in a military network environment that is a common benchmark for evaluation of intrusion detection techniques. Test data use filename "corrected.gz" contains a total of 38 training attack types. It consists of approximately 300,000 data instances, each of which is a vector of extracted feature values from a connection record obtained from the raw network data gathered during the simulated intrusion and is labeled normal or a certain attack type. The 41 features can be divided into three groups; the first group is the basic feature of individual TCP connections, the second group is the content feature within a connection suggested by domain knowledge, and the third group is the traffic feature computed using a two-second time window. The distribution of attacks in the KDD Cup dataset is extremely unbalanced. Some attacks are represented with only a few examples, e.g. the phf and ftp_write attacks, whereas the smurf and neptune attacks cover millions of records. In general, the distribution of attacks is dominated by probes and denial-of-service attacks; the most interesting and dangerous attacks, such as compromises, are grossly under represented.

The data set has 41 attributes for each connection record plus one class label. There are 24 attack types, but we treat all of them as an attack group. A data set of size N is processed. The nominal attributes are converted into linear discrete values (integers). After eliminating labels, the data set is described as a matrix X, which has N rows and m=14 columns (attributes).

III. Test Results and Analysis

In This thesis we are take 1000 sample data and two algorithms K-Means, and SVM and there result are given below

First we taken SVM algorithm and sample data 1000 so we get result in following:-

a) False Positive rates. b) True Positive Rates

Receiver operating characteristic curve

We summarize our experimental results to detect intrusions using the unsupervised outlier detection technique over the KDD'99 dataset. We first describe the datasets used in the experiments. Then we evaluate our approach and discuss the results.

Under the sponsorship of Defense Advanced Research Projects Agency (DARPA) and Air Force Research Laboratory (AFRL), MIT Lincoln Laboratory has collected and distributed the datasets for the evaluation of computer network intrusion detection systems [20, 21]. The DARPA dataset is the most popular dataset used to test and evaluate a large number of IDSs. The KDD'99 dataset is a subset of the DARPA dataset prepared by Sal Stofo and Wenke Lee [25]. The data was preprocessed by extracting 41 features (e.g., protocol type, service, and flag) from the tcpdump data in the 1998 DARPA dataset. The KDD'99 dataset can be used without further time-consuming preprocessing and different IDSs can compare with each other by working on the same dataset. Therefore, we carry out our experiments on the

KDD'99 dataset. The full training set, one of the KDD'99 datasets, has 4,898,431 connections, which contains attacks. The attacks in the dataset fall into four categories [26]: DoS (Denial of Service), R2L (unauthorized access from a remote machine), U2R (unauthorized access to root privileges), and probing. The dataset is labeled by type of attacks. Since our approach is unsupervised, the dataset does not satisfy the needs of our experiments. We must remove the labels that indicate types of attacks from the dataset.

To generate new datasets for our experiments, we first separate the dataset into two pools according to the labels. One includes normal connections. Another includes attacks. Then, we remove all the labels from the pools. However, we need the data labeled by service to build patterns of services,

So we use service feature in the dataset as label. As a result, all the data contains 40 features and is labeled by service. For our experiments, we choose five most popular network services: ftp, http, pop, smtp, and telnet.

Five different types of data were chosen with 40 attributes each [27]. The data contain 24 attack types which are classified into four categories. They are Denial of Service (DOS), unauthorized access from a Remote Machine (URM), unauthorized access to Local Super user (ULS) and Probing and Surveillance (PAS). Denial of service (DOS) is a class of attack where an attacker makes a resource too busy to handle authorized request and in turn deny access to the authorized users. URM is a class of attack where an attacker exploits the vulnerability of the machine by sending packets to the machine, to gain illegal access as a user. In the case of ULS an attacker starts with gaining access to the account of a normal user and then exploits the systems vulnerability. PAS is a class of attack where an attacker scans a network to know the vulnerabilities and exploits them. The 40 variables are given in Table 5.1 the variables from 24 to 40 are modeled using normal distribution. The variables 8 and 9 are modeled using they are numerically viable. All the data are normalized between 0 and 1. A clustering algorithm is used for classifying them into five classes namely, NORMAL, PAS, DOS, URM and ULS. The true positive rates and false positive rates for are obtained using the formula

a) True positive rate = (positives correctly classified)/ (total positives)
b) False positive rate = (total negatives – negatives incorrectly classified)/ (Total negatives).

TABLE1. VARIABLE

Variable Name	Variable Name
Duration	Is-guest _login
Protocol Type	Count
Service	Srv_count
Flag	Serror_rate
Src_bytes	Srv_serror_rate
Dst_bytes	Rerror_rate
Wrong fragment	Srvr_rerror_rate
Urgent	Same_srv_rate
Hot	Diff_srv_rate
Num_failed _logins	Srv_diff_host_rate
Logged_ in	Dst_host_count
Num_compromized	Dst_host_srv_count
Root_shell	Dst_host_same_srv_rate
Su_attempted	Dst_host_diff_srv_rate
Num_root	Dst_host_same_src_port_rate
Num_file_creations	Dst_host_srv_diff_host_Rate
Num_shells	Dst_host_serror_rate
Num_access_files	Dst_host_srv_serror_rate
Num_outbound_cmds	Dst_host_rerror_rate
Is_host_login	Dst_host_srv_rerror_rate

A. Evaluation and discussion from K-Means

We carry out the first experiment over the attack dataset. We first optimize the parameters of K-Means algorithm by feeding the dataset into the NIDS. The NIDS builds patterns of the network services with different values of the parameters.

With the optimized parameters, we build the patterns of the network services. Over the built patterns, the NIDS calculates the Iteration of each connection. Since the attacks are injected at the beginning of the dataset, the figure shows the Iteration of the attacks is much higher than most of normal activities. Some normal activities also have high Iteration. That leads to false positives. The NIDS will raise an alert if an Iteration of a connection exceeds a specified threshold.

We evaluate the performance of K-Means algorithm by the detection rate and the false positive rate. The detection rate is the number of attacks detected by the system divided by the number of attacks in the dataset. The false positive rate is the number of normal connections that are misclassified as attacks divided by the number of normal connections in the dataset. We can evaluate the performance by varying the threshold of outlier-ness.

TABLE 2 THE PERFORMANCE OF EACH ALGORITHM OVER THE KDD'99 DATASET [1]

Algorithm	Detection rate	False positive rate
Cluster	66%	2%
Cluster	28%	0.5%
K-NN	11%	4%
K-NN	5%	2%
SVM	67%	4%
SVM	5%	3%

In intrusion detection, ROC (Receiver Operating Characteristic) curve is often used to measure performance of IDSs. The ROC curve is a plot of the detection rate against the false positive rate. Fig. 1 plots ROC curve to show the relationship between the detection rates and the false positive rates over the dataset. The result indicates that K-Means algorithm can achieve a high detection rate with a low false positive rate. Compared to other unsupervised anomaly based systems [2, 10], our system provides better performance over the KDD'99 dataset while the false positive rate is low.

A. Evaluation and discussion from K-Means Vs SVM

We carry out the first experiment over the attack dataset. We first optimize the parameters of K-Means and SVM algorithm by feeding the dataset into the NIDS. The NIDS builds patterns of the network services with different values of the parameters.

In intrusion detection, ROC (Receiver Operating Characteristic) curve is often used to measure performance of IDSs. The ROC curve is a plot of the detection rate against the false positive rate. Fig. 1 plots ROC curve to show the relationship between the detection rates and the false positive rates over the dataset.

The result indicates that K-Means algorithm can achieve a high detection rate with a low false positive rate. Compared to other unsupervised anomaly based systems [2, 10], our system provides better performance over the KDD'99 dataset while the false positive rate is low.

TABLE 3 COMPARISON OF ROC CURVES SVM ~ K-MEAN

	AUC	SE [a]	95% CI [b]
Test_Data_In_SVM	0.718	0.0739	0.689 to 0.746
Test_Data_K_mean	0.766	0.0512	0.738 to 0.791

Show that the detection rate is reduced significantly when the false positive rate is low. Although our experiments are carried out under different conditions, Fig. 1 shows that our K-Means algorithm still provides relatively higher detection rates when the false positive rates are low. For example, the detection rate is 97.9%

TABLE 4 PAIR WISE COMPARISON OF ROC CURVES

Test_Data_In_SVM ~ Test_Data_K_mean	
Difference between areas	0.0470
Standard Error [c]	0.0631
95% Confidence Interval	-0.0766 to 0.171
z statistic	0.745
Significance level	P = 0.4560

To evaluate our system under different number of attacks, we carry out the experiments over attack dataset. Fig. 1 plots the ROCs for each dataset using comparison of ROC curves. The result shows that the performance tends to be reduced while increasing number of attacks.

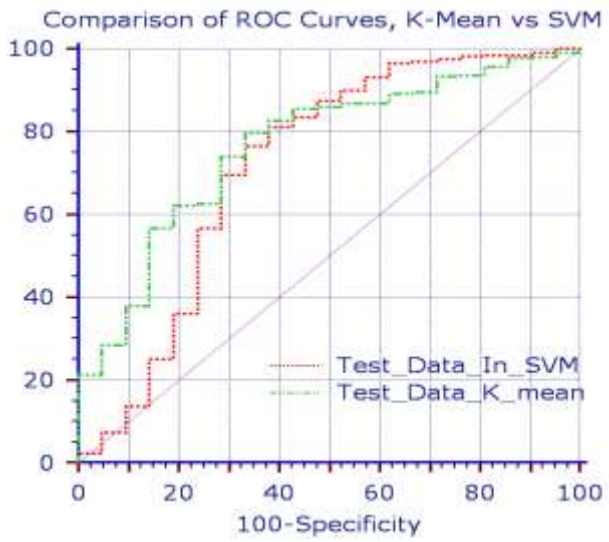


Figure 1. The comparison of ROC curves for the datasets

IV. CONCLUSION

In this Paper' goal was to provide the scientific evidence that one-class SVMs and K-Means algorithm can be regarded as suitable method for detecting intrusions in flow-based network data The performance of K-Means algorithm is comparable to that of other reported unsupervised anomaly detection approaches. Especially, our approach achieve higher detection rate when the false positive rate is low. It is more significant for NIDSs, since high false positive rate will make NIDSs useless. Due to high complexity of the unsupervised anomaly detection algorithm, low detection speed performance of the approach makes real time detection impossible. However, the approach can detect novel intrusions without attack-free training data. The detected novel intrusions can be used to train real time supervised misuse detection systems. Therefore, the trained misuse detection systems can detect the novel intrusions in real time.

The results also show that the performance tends to be reduced with increasing number of attack connections. That is a problem of unsupervised systems. Some attacks (e.g., DoS) produce a large number of connections, which may undermine an unsupervised anomaly detection system. To overcome the problem, we will incorporate both anomaly based and misuse based approaches into the NIDS in the future. Misuse approach can detect known attacks. By removing known attacks, the number of attacks can be reduced significantly in datasets for unsupervised anomaly detection. Misuse detection has high detection rate with low false positive rate. Anomaly detection can detect novel attacks to increase the detection rate. Therefore, combining misuse and anomaly detection can improve the overall performance of the NIDS.

REFERENCES

[1] Bhawana Pillai, Mr. Vineet Rechhariya Network Intrusion Detection For Unsupervised Authentication RecordsIn Matlab icices-2011

[2] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo, "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data", Applications of Data Mining in Computer Security, Kluwer, 2002.

[3] Rasheda Smith, Alan Bivens, Mark Embrechts, Chandrika Palagiri, and Boleslaw Szymanski, "Clustering Approaches for Anomaly Based Intrusion Detection", Walter Lincoln Hawkins Graduate Research Conference 2002 Proceedings, New York, USA, October 2002.

[4] Susan M.Bridges, and Rayford B. Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection", Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, MD, October, 2000.

[5] Alan Bivens, Mark Embrechts, Chandrika Palagiri, Rasheda Smith, and Boleslaw Szymanski, "Network-Based Intrusion Detection Using Neural Networks", Artificial Neural Networks In Engineering, St. Louis, Missouri, November 2002.

[6] Q.A. Tran, H. Duan, and X. Li, "One-class Support Vector Machine for Anomaly Network Traffic Detection", The 2nd Network Research Workshop of the 18th APAN, Cairns, Australia, 2004.

[7] A. Lazarevic, L. Ertoz, A. Ozgur, J. Srivastava & V. Kumar, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection", Proceedings of Third SIAM Conference on Data Mining, San Francisco, May 2003.

[8] J. Zhang and M. Zulkernine, "Network Intrusion Detection Using Random Forests", Proc. of the Third Annual Conference on Privacy, Security and Trust, St. Andrews, New Brunswick, Canada, October 2005.

[9] Kingsly Leung and Christopher Leckie, "Unsupervised Anomaly Detection in Network Intrusion Detection Using Clusters", Australasian Computer Science Conference, Newcastle, NSW, Australia, 2005.

[10] M. Ramadas, S. Ostermann and B. Tjaden, "Detecting Anomalous Network Traffic with Self-Organizing Maps", RAID, 2003.

[11] Ian H. Witten, and Eibe Frank, Data Mining: Practical Machine Learning Tools and Techniques with Java Implementations, Morgan Kaufmann publishers, October 1999.

[12] V. Barnett and T. Lewis, Outliers in Statistical Data, John Wiley, 1994.

[13] C. T. Lu, D. Chen, and Y. Kou, "Algorithms for Spatial Outlier Detection", Proceedings of 3rd IEEE International Conference on Data Mining, Melbourne, Florida, November 2003.

[14] K. Tan, K. Killourhy, and R. Maxion, "Undermining an anomaly based intrusion detection system using common exploits", RAID, Zurich, Switzerland, Oct. 2002.

[15] Snort, Network Intrusion Detection System, http://www.snort.org.

[16] L. Breiman, "Random Forests", Machine Learning 45(1):5–32, 2001.

[17] Lan Guo, Yan Ma, Bojan Cukic, and Harshinder Singh, "Robust Prediction of Fault-Proneness by Random Forests", Proceedings of the 15th International Symposium on Software Reliability Engineering (ISSRE'04), pp. 417-428, Brittany, France, November 2004.

[18] Bogdan E. Popescu, and Jerome H. Friedman, Ensemble Learning for Prediction, Doctoral Thesis, Stanford University, January 2004.

[19] J. D. Cannady. An adaptive neural network approach to intrusion detection and response. PhD thesis, Nova Southeastern University, 2000.

[20] Yimin Wu, High-dimensional Pattern Analysis in Multimedia Information Retrieval and Bioinformatics, Doctoral Thesis, State University of New York, January 2004.

[21] M. Mahoney and P. Chan, "An Analysis of the 1999 DARPA/Lincoln Laboratory Evaluation Data for Network Anomaly Detection", Proceeding of Recent Advances in Intrusion Detection (RAID), Pittsburgh, USA, September 2003.

[22] J. D. Cannady. Next generation intrusion detection: Autonomous reinforcement learning of network attacks. In NISSC '00: Proc. 23rd National Information Systems Security Conference, 2000.

[23] MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation, http://www.ll.mit.edu/IST/ideval/, MA, USA.

[24] Daniel Barbarra, Julia Couto, Sushil Jajodia, Leonard Popyack, and Ningning Wu, "ADAM: Detecting Intrusions by Data Mining", Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, T1A3 1100 United States Military Academy, West Point, NY, June 2001.

[25] WEKA software, Machine Learning, http://www.cs.waikato.ac.nz/ml/weka/, The University of Waikato, Hamilton, New Zealand.

[26] Charles Elkan, "Results of the KDD'99 Classifier Learning", SIGKDD Explorations 1(2): 63-64, 2000

[27] KDD'99 datasets, The UCI KDD Archive, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, Irvine, CA, USA, 1999

[28] Ting-Fan Wu, Chih-Jen Lin, and Ruby C. Weng, "Probability Estimates for Multi-class Classification by Pairwise Coupling", The Journal of Machine Learning Research, Volume 5, December 2004.

[29] D. Sarjon and Mohd Noor Md Sap, "Association Rules using Rough Set and Association Rule Methods", Proceedings of 7th Pacific Rim International Conference on Artificial Intelligence (PRICAI-02), Tokyo, Japan, August 18-22, 2002, pp. 238-243.

RSS based Vertical Handoff algorithms for Heterogeneous wireless networks - A Review

Abhijit Bijwe
Electronics & Comm. Engg. Deptt
P.I.E.T.Nagpur

Dr. C.G.Dethe
Electronics & Telecom Engg. Deptt
Principal,
P.I.E.T. Nagpur

***Abstract*—Heterogeneous networks are integrated in fourth generation. To have seamless communication and mobility between these heterogeneous wireless access networks, support of vertical handoff is required. Vertical handover is convergence of heterogeneous networks for e.g.:- handover between WLAN and cellular networks.**

In this paper, three algorithms on RSS based vertical handoff are discussed. First, algorithm is adaptive lifetime based vertical handoff, which combines RSS and estimated lifetime (expected duration after which the MT will be able to maintain its connection with WLAN) to decide the vertical handover. Second algorithm, is based on dynamic RSS threshold which is more suitable for handover from WLAN to 3G network. Third algorithm is a traveling distance prediction method, which works well for WLAN to cellular networks and vice versa. This avoids unnecessary handoff and also minimizes failure probability.

Keywords- RSS; WLAN; 3G; VHD.

I. INTRODUCTION

Convergence of heterogeneous network is getting a lot of attention. To be precise, in 4G network, a mobile terminal incorporated with multiple interfaces will be able to choose the appropriate available access links. In 4G systems, handoff management is more complex, as it covers not only horizontal handoff but also vertical handoff. In horizontal handoff, where an MT moves between two different cells or access points within the same wireless communication system. While in vertical handover, MT moves from one wireless system to another wireless system, for example, from cellular network to wireless LAN system. In this paper, we do not address the horizontal handoff, as traditional RSS based algorithms which works good to support the horizontal handoff . RSS based handoff algorithm is generally applied to homogeneous network and can be extended to heterogeneous network. Numerous Vertical handover decision algorithms are proposed in various research papers which takes into account several parameters such as Bandwidth, Power consumption, Cost, Security etc. Based on these parameters, cost function algorithm and multiple attribute decision algorithms may be used. These algorithms use different set of parameters [5] to provide better handoff.

Some of the problems associated with these algorithms are

1) Too many parameters may affect the performance of VHD algorithms and relationship between these parameters is very complicated, therefore, how to select those most important parameters as decision factors, and also take into account the effects of other parameters, so that handoff performance can be guaranteed and proper performance tradeoff can be achieved is an important & difficult problem.

2) MADM algorithms are the most challenging ones because of their pre training requirements. Hence it suffers from longest handover delay. Also the system is complex.

RSS based algorithms are less complex and can be used between macro cellular and microcellular networks.

High handover failure probability is observed for algorithm without inclusion of RSS.

In this paper, we will be focusing on various Mathematical Models in RSS based vertical handover decision algorithms.

We make an attempt to provide a comparative analysis of three RSS based vertical handoff algorithms.

II. RSS BASED VHD ALGORITHMS

In this, the handoff decisions are made by comparing RSS (received signal strength) of the current network with the preset threshold values. These algorithms are less complex and may be combined with other parameters such as bandwidth, cost etc. to have a better handover decisions. We describe here three RSS based algorithms in the following sections.

A. ALIVE-HO (adaptive lifetime based vertical handoff) algorithm. –

Zahran , Chen and Sreenan [6]proposed algorithm for handover between 3G Networks and WLAN by combining the RSS with an estimated life time (duration over which the current access technology remains beneficial to the active applications). ALIVE-HO always uses an uncongested network whenever available. It continues using the preferred network (i.e. WLAN) as long as it satisfies the QoS requirements of the application.

Two different vertical handoff scenarios are discussed: Moving out of the preferred network (MO) and Moving in to the preferred network (MI), where the preferred network is usually the underlay network that provides better and economical service. Hence, extending the utilization of the WLAN, as long as it provides satisfactory performance is the main considerations of vertical handoff algorithm design.

We observe the method through the following scenarios.

In first scenario, when the MT moves away from the coverage area of a WLAN into a 3G cell, a handover to the 3G network is initiated. The handover is done under the conditions that

(a) RSS average of the WLAN falls below predefined threshold. (MO threshold) and (b) the estimated life time is atleast equal to the required handoff signaling delay. The MT continuously calculate the RSS mean using the moving average method.[4]

$$\overline{RSS}\,[K] = \frac{1}{Wav} \sum_{i=0}^{Wav-1} \overline{RSS}[k-i]$$

Here $\overline{RSS}$ [k] is RSS mean at time instant k, and W_{av} is the window size, a variable that changes with velocity of the velocity of mobile terminal. Then, the lifetime metric EL [k] is calculated by using $\overline{RSS}$ [k], ASST Application signal strength threshold),S[k],RSS change rate.

$$EL[k] = \frac{\overline{RSS}\,[k] - ASST}{S[k]}$$

ASST (Application signal strength threshold) chosen to satisfy the requirements of the active applications. S [K] represents RSS decay rate.In second scenario, when the MT moves towards a WLAN cell, the handover to the WLAN is done if the average RSS is larger than MI Threshold. WLAN and the available bandwidth of the WLAN meet the bandwidth requirement of the application. Table given below shows lost frames during the handoff transition area for the received stream.

ASST (in dBs)	-90	-89	-88	-87	-86	-85
Lost frames_100kbit/s	13.3	5	3	0.67	0	0
Lost frames_300kbit/s	38	28	4	0.33	0	0

TABLE 1.1 FRAMES LOST CORRESPONDING TO ASST

Based on the obtained results and subjective testing, the optimal value for UDP based streaming is chosen as -86dB.

By introducing EL[k] the algorithm adapts to the application requirements and reduces unnecessary handovers. Second, there is an improvement on the average throughput for user because MT prefers to stay in WLAN cell as long as possible.

However packet delay grows, due to the critical fading impact near the cell edges, which may result in severe degradation in the user perceived QoS. This phenomenon results in a tradeoff between improving the system resource utilization and satisfying the user Qos requirements. This issue can be critical for delay sensitive applications and degrade their performance. ASST is tuned according to various system parameters, including delay thresholds, MT velocities, handover signaling costs and packet delay penalties.

B. Algorithm on Adaptive RSS Threshold

Mohanty and Akyildiz[2] in paper "A cross-layer (Layer 2 + 3) Handoff Management Protocol" proposed a WLAN to 3G handover decision method. In this method, RSS of current network is compared with dynamic RSS threshold (S_{th}) when MT is connected to a WLAN access point. We observe the following notations with reference to fig 1.1 which shows a handoff from current network (AP) referred as WLAN, to the future network (BS), referred as 3G.

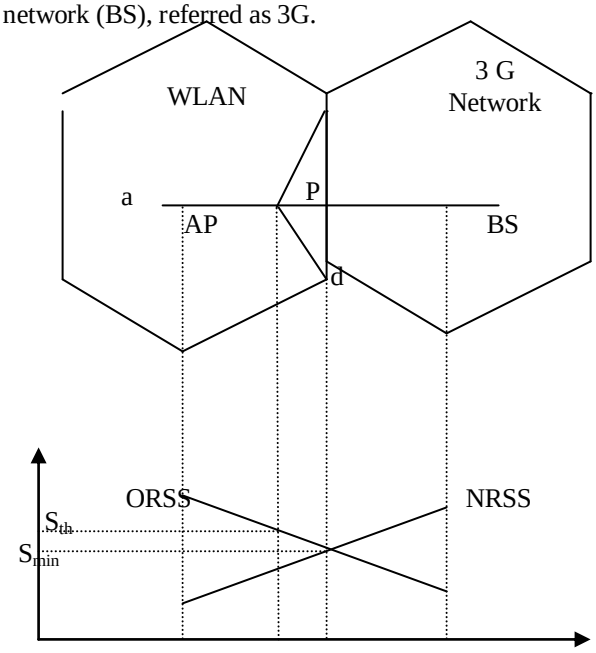


Fig 1.1 Analysis of handoff process

* S_{th} : The threshold value of the RSS to initiate the handover process. Therefore, when the RSS of WLAN referred to as ORSS(old RSS) in fig drops below S_{th}, the registration procedures are initiated for MT's handover to the 3G network.

* a :The cell size we assume that the cells are of hexagonal shape.

d: is the shortest distance between the point at which handover is initiated and WLAN boundary. We observe the Path loss Model [1] given by

$$P_r(x) = Pr\,(d_0) \left(\frac{d_0}{x}\right)^{\alpha} + \varepsilon$$

Where x is the distance between the AP and MT, and $P_r(d_0)$ is the received power at a known reference distance (d_0) . The typical value of d_0 is 1 km for macrocells, 100m for outdoor microcells, and 1 m for indoor picocells.

The numerical value of $P_r\,(d_0)$ depends on different factors, such as frequency, antenna heights, and antenna gains, α is the path loss exponent. The typical values of α ranges from 3 to 4 and 2 to 8 for macrocellular and microcellular environment.

ε - is a Zero mean Gaussian random variable that represents the statistical variation in $P_r(x)$ caused by Shadowing. Typical std. deviation of ε is 12 dB.

We observe the path loss model applied to the scenario.

$$P_r(a-d) = P_r(a)\left(\frac{a}{a-d}\right)^{\alpha} + \varepsilon$$

$$P_r(a-d) = P_r(a) + 10\alpha \log_{10}\left(\frac{a}{a-d}\right) + \varepsilon$$

$$S_{th} = S_{min} + 10\alpha \log_{10}\left(\frac{a}{a-d}\right) + \varepsilon$$

When the MT is located at point P, the assumption is that it can move in any direction with equal probability, i.e. the pdf of MT's direction of motion θ is

$$f_{\theta}(\theta) = \frac{1}{\Pi-(-\Pi)} = \frac{1}{2\Pi} \quad -\Pi < \theta < \Pi \quad \ldots\ldots\ldots\ldots(1)$$

As per assumption, that MT's direction of motion and speed remains the same from point P until it moves out of the coverage area of WLAN. As the distance of P from WLAN boundary is not very large, this assumption is realistic.

The need for handoff to cellular network arises only if MTs direction of motion from P is in the range [θ ε $(-\theta_1, \theta_1)$]

Where θ_1 = arctan $\left(\frac{a}{2d}\right)$, otherwise the handoff initiation is false. The probability of false handoff initiation is

$$P_a = 1 - \int_{-\theta_1}^{\theta_1} f_{\theta}(\theta)\,d\theta$$

P (unfavourable event) = 1 – P (favourable event)

$$= 1 - \frac{1}{2\Pi}(2\theta_1)$$

$$= 1 - \frac{1}{\Pi} arc\ \tan\left(\frac{a}{2d}\right) \quad \ldots\ldots\ldots\ldots\ldots..(2)$$

When the direction of motion of MT from P β ε $[(-\theta_1, \theta_1)]$ the time it takes to move out of the coverage area of WLAN cell is given by

$$\text{time} = \frac{dis\tan ce}{speed}$$

From fig $\text{Cos}\,\beta = \frac{d}{x}$

$$\text{Sec}\ \beta = \frac{x}{d} \quad , \ x = d \sec \beta$$

$$\text{Hence } t = \frac{x}{v}$$

$$t = \frac{d\sec\beta}{v} \quad \ldots\ldots\ldots\ldots.. (3)$$

Pdf of β is

$$f_{\beta}(\beta) = \begin{cases} \frac{1}{2\theta_1} & -\theta_1 < \beta < \theta_1 \\ 0 & \text{otherwise} \end{cases}$$

From (3), t is a function of β i. e. t = g (β) in $[-\theta_1, \theta_1]$

$$g(\beta) = \frac{d\sec\beta}{v}$$

Therefore pdf of t is given by

$$f_t(t) = \sum_i \frac{f_{\beta}(\beta_i)}{g'(\beta_i)}$$

Where β_i are the roots of equation t = g (β) in [$-\theta_1, \theta_1$]

And for each of these roots

$$f_{\beta}(\beta_i) = \frac{1}{2\theta_1} \quad \text{for i = 1 and 2}$$

$$f_t(t) = \frac{1}{2\theta_1\left|g'(\beta_i)\right|} + \frac{1}{2\theta_1\left|g'(\beta_i)\right|}$$

$$f_t(t) = \frac{1}{\theta_1\left|g'(\beta_i)\right|}$$

where $g'(\beta)$ is derivative of $g(\beta)$ given by

$$g'(\beta) = \frac{d\sec\beta\tan\beta}{v}$$

$$= \frac{d\sec\beta\left(\sqrt{\sec^2\beta - 1}\right)}{v}$$

$$= \frac{vt\left(\sqrt{\left(\frac{vt}{d}\right)^2 - 1}\right)}{v}$$

$$g'(\beta) = t\sqrt{\frac{v^2t^2}{d^2}} - 1 \quad \text{from (3) ……7}$$

Using (6) & (7), the pdf of t is given by

$$f_t(t) = \begin{cases} \dfrac{d}{\theta_1 t\sqrt{v^2t^2 - d^2}}, & \dfrac{d}{v} < t < \dfrac{\sqrt{\frac{a^2}{4} + d^2}}{v} \\ 0 & \text{otherwise} \end{cases}$$

The probability of handoff failure is given by

$$P_f = \begin{cases} 1 & \tau > \sqrt{\frac{a^2}{4} + d^2} \\ P(t < \tau) & \dfrac{d}{v} < \tau < \dfrac{\sqrt{\frac{a^2}{4} + d^2}}{v} \\ 0 & \tau \le \dfrac{d}{v} \end{cases} \quad \text{…… (9)}$$

τ - Handoff signaling delay
and $P(t < \tau)$ - is the probability that $t < \tau$

when $\dfrac{d}{v} < \tau < \dfrac{\sqrt{\frac{a^2}{4} + d^2}}{v}$ using(8)

$$P(t < \tau) = \int_0^{\tau} f_t(t)\,dt$$

$$= \int_{\frac{d}{v}}^{\tau} \frac{d}{\Pi t\sqrt{v^2t^2} - d^2}\,dt$$

$$= \int_{\frac{d}{v}}^{\tau} \frac{d}{\Pi dt\sqrt{\frac{v^2t^2}{d^2} - 1}}\,dt$$

$$= \int_{\frac{d}{v}}^{\tau} \frac{1}{\Pi \frac{vt}{d}.\frac{d}{v}\sqrt{\frac{v^2t^2}{d^2} - 1}}\,dt$$

$$\approx \frac{1}{\theta_1}\arccos\left(\frac{d}{vt}\right) \quad \text{…………10}$$

Now using (9) & (10)

$$P_f = \begin{cases} 1 & \tau > \dfrac{\sqrt{\frac{a^2}{4} + d^2}}{v} \\ \dfrac{1}{\theta_1} arc\cos\left(\dfrac{d}{v\tau}\right) & \dfrac{d}{v} < \tau < \dfrac{\sqrt{\frac{a^2}{4} + d^2}}{v} \\ 0 & \tau \le \dfrac{d}{v} \end{cases} \quad \text{…………………(8)}$$

$$P_f = \frac{arcCos\left(\frac{d}{v\tau}\right)}{\arctan\left(\frac{d}{v\tau}\right)}$$

$$P_f = \frac{\frac{\Pi}{2} - \frac{d}{v\tau}}{\frac{\Pi}{2} - \frac{2d}{\sqrt{4d^2 + a^2}}}$$

The use of adaptive RSS threshold helps reducing the handoff failure probability and also reducing unnecessary handovers. The exact value of S_{th} will depend on MT's speed and handoff signaling delay at a particular time. Adaptive S_{th} is used to limit handoff failure. However, in this algorithm, the handover from 3G network to a WLAN is not efficient when MTS traveling time inside a WLAN cell is less than the than the handover delay. This may lead to wastage of network resources.

C. A Traveling Distance Prediction Based Method.

To minimize unnecessary handover over Mohanty's Method. Yan et al[3] developed VHD algorithm that takes into consideration the time the mobile terminal is expected to spend within a WLAN cell. A handover to a WLAN is initiated if the WLAN coverage is available and the estimated traveling time. Inside the WLAN cell is larger than the time threshold.

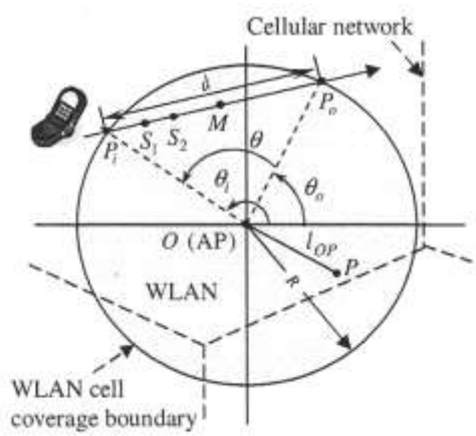


Fig 1.2 Prediction of traveling distance in WLAN cell

Assume that the MT starts receiving a sufficiently strong signal at point P_i and the signal strength drops below the usable level at point P_0.

Angles θ i and θ_0 are both uniformly distributed in $[0, 2\Pi]$ where $\theta = \theta i - \theta_0$

The probability density function (pdf) of θ as fallows

$$f_0(\theta) = \frac{1}{\Pi}\left(1-\frac{\theta}{2\Pi}\right), \quad 0 \le \theta \le 2\Pi$$

By replacing l with θ, d with 2Π l ranges from 0 to d

From the geometric configuration in fig

$$\text{Sin}\ \frac{\theta}{2} = \frac{d/2}{R}$$

$$\text{Sin}\ \frac{\theta}{2} = \frac{d}{2R}$$

$$\text{Sin}^2\frac{\theta}{2} = \left(\frac{d}{2R}\right)^2$$

$$\text{Sin}^2\frac{\theta}{2} = \frac{d^2}{4R^2}$$

$$2\ \text{Sin}^2\frac{\theta}{2} = \frac{d^2}{2R^2}$$

$$2R(1-\text{Cos}\theta) = d^2$$

$$d^2 = 2R^2(1-\cos\theta)$$

The Pdf of d is expressed as from (3) & (4)

$$f_D(d) = \frac{2}{\Pi\sqrt{4R^2-d^2}} \quad 0 \le d \le 2R$$

The cdf of d can be derived by integrating

$$f_D(d) = \frac{2}{\Pi}\frac{1}{\sqrt{1-\left(\frac{d}{2R}\right)^2}}$$

$$P(d \le D) = \begin{cases} \frac{2}{\Pi}Sin^{-1}\left(\frac{D}{2R}\right), & 0 \le D \le 2R \\ 1 & 2R < D \end{cases}$$

We observe a distance threshold parameter L whichwill be used to make handover decisions. Whenever the estimated traveling distance d is greater than L, the MT will initiate the handover procedures. L may be calculated by using spanning algorithm.

$$P = \frac{2}{\Pi}\left[Sin^{-1}\left(\frac{v\tau_i}{2R}\right) - Sin^{-1}\left(\frac{L}{2R}\right), 0 \le L \le v\tau\right]$$

$$\{ \quad 0 \qquad v\tau < L$$

Thus the value of L for a maximum tolerable failure or unnecessary handover probability as

$$L = 2R\ \text{Sin}\left(\text{Sin}^{-1}\left(\frac{v\tau}{2R}\right) - \frac{\Pi}{2}P\right.$$

The time threshold (T_{WLAN}) is calculated as

$$T_{WLAN} = \frac{2R}{v}Sin\left(Sin^{-1}\left(\frac{v\tau}{2R}\right) - \frac{\Pi}{2}P\right)$$

P $\rightarrow$ is maximum tolerable handover failure or unnecessary handover probability.

τ is the handover delay from cellular network to WLAN. In this method, VEPSD algorithm can be used to estimate v and τ respectively

The traveling time (t_{WLAN})

$$t_{WLAN} = \frac{R^2 - los^2 + v^2(t_s - t_{in})^2}{v^2(t_s - t_{in})}$$

Where R $\rightarrow$ radius of WLAN Cell,

l_{os} $\rightarrow$ distance between access point and where the MT takes RSS.sample.

t_s & t_{in} $\rightarrow$ are the times at which RSS sample is taken and MT enters the WLAN cell coverage respectively.

$t_{WLAN} > T_{WLAN}$ $\rightarrow$ handover is initiated.

Even though the speed of the MT increases, the probabilities remain in the same. For higher speeds, our method yields lower probability of handover failures and unnecessary handover than the Mohanty's Method.

But the method relies on sampling and averaging RSS points, which introduces increased handover delay.

III. CONCLUSION

As per the discussion above, we conclude that Adaptive lifetime based method gives an Improvement in average throughput for user because MT prefers to stay in WLAN cell. But, packet delay grows near edges of the WLAN cell due to fading of signal which results in degradation of Qos. To solve this issue ASST is tuned according to various parameters such as delay thresholds, MT velocities, handover signaling costs and packet delay penalties. Adaptive RSS threshold algorithm works good for handover from WLAN to 3G network .It helps in reducing handoff failure probability and also reducing

unnecessary handover between WLAN to 3G as dynamic RSS threshold is dependent on MTs speed and handoff signaling delay. This algorithm is not efficient when handover is from 3G to WLAN, if traveling time inside WLAN cell is less than the handover delay. For this case traveling distance prediction based method works fine.

These algorithms minimize unnecessary handover for handover from 3G to WLAN. But the method relies on sampling and averaging RSS points which introduce increased handover delay. But, the sampling of RSS periodically will eliminate the assumption of MTs speed being fixed in WLAN cell.

IV. Future Directions

A improvement to the scheme is to periodically sample the RSS, recalculate and refine the estimations for v to improve the performance, and eliminate the assumption that the MTS speed remains fixed inside the WLAN cell. Based on the application and economic point of view (i.e cost) the handover decision inside the WLAN Cell can be taken. User can be given the choice of selecting the network depending on the factors such as cost or critical application which requires cellular network.

References

[1] T. S. Rappaport, Wireless Communications: Principles and Practice.Prentice Hall, July 1999.

[2] S. Mohanty and I. F. Akyildiz, "A cross-layer (Layer 2 + 3) handover management protocol for next-generation wireless systems," *IEEE Trans. Mobile Computing*, vol. 5, pp. 1347–1360, Oct. 2006.

[3] Xiaohuan Yan,N,Nallasamy Mani, and Y.Ahme S¸ ekercio˘glu, " A Traveling Distance Prediction Based Method to minimize Unnecessary Handovers from Cellular Networks to WLANs," *IEEE communication letters*, vol. 12, pp. 14–16 , 2008.

[4] Ahmed H. Zahran and Ben Liang "Performance Evaluation Framework for Vertical Handoff Algorithms in Heterogeneous Networks",in :Proceedings of the 2005 *IEEE International Conference on Communications(ICC05),Seoul,Korea,May2005. pp.173-178*

[5] Xiaohuan Yan,.Ahmet S¸ ekercio˘glu, Sathyanarayan "A Survey of vertical decision algorithms in fourth generation heterogeneous networks"*Elsevier,2010,* pp.1848-1863

[6] A. H. Zahran and B. Liang, "ALIVE-HO: Adaptive lifetime vertical handoff for heterogeneous wireless networks," *Technical Report, University of Toronto.*

Authors Profile

Abhijit Bijwe is PhD student at the Department of Electronics & Communication engineering at Nagpur university.Has received B.E.from Amravati university and received M.E. from Mumbai university.His current research area is vertical handover algorithm in heterogeneous networks.

Dr.C.G.Dethe has done Doctrate from Amravati University. Has done B.E. & M.E. from Amravati and Nagpur University. Currently, He is Principal in Priyadarshini Institute of Engineering & Technology, Nagpur. His research area is Measurement of Traffic in Mobile Networks. He is guiding 10 PhD students.

A Novel Architecture for Intrusion Detection in Mobile Ad hoc Network

Atul Patel
Charotar University of Science & Technology
Changa, India

Ruchi Kansara
Charotar University of Science & Technology
Changa, India

Dr. Paresh Virparia
Sardar Patel University
Vallabh Vidyanagar,
India.

***Abstract*— Today's wireless networks are vulnerable in many ways including illegal use, unauthorized access, denial of service attacks, eavesdropping so called war chalking. These problems are one of the main issues for wider uses of wireless network. On wired network intruder can access by wire but in wireless it has possibilities to access the computer anywhere in neighborhood. However, securing MANETs is highly challenging issue due to their inherent characteristics. Intrusion detection is an important security mechanism, but little effort has been directed towards efficient and effective architectures for Intrusion Detection System in the context of MANETs. We investigate existing Intrusion Detection Architecture design Issues, challenges and proposed a novel architecture based on a conceptual model for an IDS agent that lead to a secure collaboration environment integrating mobile ad hoc network and the wired backbone. In wireless/mobile ad hoc network, the limited power, weak computation capabilities of mobile nodes, and restricted bandwidth of the open media impede the establishment of a secure collaborative environment.**

Keywords- Ad hoc network; Intrusion Detection System; Mobile Network.

I. INTRODUCTION

Mobile ad hoc networks are complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organise into arbitrary and temporary, ''adhoc'' network topologies. They allow people and devices to seamlessly internetwork with no pre-existing communication infrastructure and central administration [1].

Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. The goal is to investigate the development of a suite of protocols and algorithm that enables to securely collaborate over mobile ad hoc networks as well as the wired backbone. Collaboration requires secure information sharing and communication among a large number of academic, governmental, and military sites. A series of experiments in key management, malicious intruder identification, and detection of denial of service attacks will be conducted to provide the secure networking.

Ubiquitous access to information anywhere, anyplace, and anytime, will characterize whole new kinds of information systems in the 21st Century. These are being enabled by rapidly emerging wireless communication systems, based on radio and infrared transmission mechanisms, and utilizing such technologies as cellular telephony, personal communication systems, wireless PBXs, and wireless local area networks. These systems have the potential to dramatically change society as workers become "untethered" from their information sources and communication mechanisms. While there is a rich body of knowledge associated with radio system engineering, the needed expertise must build upon this to encompass network management, integration of wireless and wire line networks, system support for mobility, computing system architectures for wireless nodes/base stations/servers. User interface appropriate for small handheld portable devices, and new application that can exploit mobility and location information.

Enormous amounts of data are collected from the network for network based intrusion detection. This poses a great challenge. Raw network traffic needs to be summarized into higher-level events, described by some features, such as connection records before feeding the data to a machine learning algorithm. Selecting relevant features is a crucial activity and requires extensive domain knowledge.

In this paper, we propose the novel conceptual architecture for IDS agent for detecting Intrusions effectively. Section 2 gives the general information regarding Intrusion Detection Systems, Section 3 gives the problems with the current Intrusion Detection Techniques, Section 4 gives the novel conceptual model for intrusion agent and finally we conclude in section 5 and give future directions for this work.

II. INTRUSION DETECTION

The concept behind intrusion detection is a surprisingly simple one: Inspect all network activity (both inbound and outbound) and identify suspicious patterns that could be evidence of a network or system attack. Nowadays, network based computer plays an important role in society. There are many advantages of network: one can easily connect anyone on the network, one can share and use the files, folders, and data, they can also call their loved once on the net. At the same time,

there are many disadvantages of it too. One welcomes one's enemy, hackers, criminals. There may be chance of misuse of the data. When an intrusion (defined as "any set of actions that attempt to compromise the integrality, confidentially, or availability of a resource [2]) takes place, intrusion prevention technique, such as encryption and authentication (e.g., using passwords or biometrics), are usually the first line of defense[3]. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

A. *Wireless Vs Wired Intrusion*

Wired – Physically attached: Intruder/attacker needs to plug directly into the network

Wireless – Intruder can stay anywhere and intrude unseen

No exact "border" between internal and external network-losing exact classification to insider and outsider attacks

Sometimes people assume that host based systems prevent insider attacks where as network based system invites outsider attacks. We may not agree with this practice, but as soon as you add a Wi-Fi signal, the border of defense becomes unclear and not sharply defined.

The primary assumptions of intrusion detection are: user and program activities are observable, for example via system auditing mechanism; and more importantly, normal and intrusion detection activities have distinct behavior. In the network based IDS, normally, it runs on the gateway of a network packets that go through the network hardware interface.

In misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS looks for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies [4].

III. Problems of Current IDS Techniques

There are two different types of networks - wireless and wired network. There has always been having problem of security, collaboration, management and integration. Thus there is a need of intrusion detection system as there may be chances of misusing of data while communicating between these two. There is a big problem to fix IDS between Wired and Wireless network as the wireless network perhaps may not have fix infrastructure.

There is a big difference between how the data transfer in Wireless Ad-Hoc network and Wired network. There is always some limitation while communicating through wireless Ad-Hoc network. One may face the problem of bandwidth, data may be loss, high cost, slower links etc. Intrusion detection in MANETs, however, is challenging for a number of reasons [12,13,14].

The major limitations with the current Intrusion Detection Systems are[5]

- Noise can severely limit an Intrusion detection systems effectiveness. Bad packets generated from software bugs, corrupt DNS data, and local packets that escaped can create a significantly high false-alarm rate.
- It is not uncommon for the number of real attacks to be far below the false-alarm rate. Real attacks are often so far below the false-alarm rate that they are often missed and ignored.
- Many attacks are geared for specific versions of software that are usually outdated. A constantly changing library of signatures is needed to mitigate threats. Outdated signature databases can leave the IDS vulnerable to new strategies.

A. *NIDS Performance Issues*

It is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. Network intrusion detection systems NIDS [6,7,8] gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap. In an NIDS (figure 1), sensors are located at choke points in the network to be monitored, often in the demilitarized zone (DMZ) or at network borders. Sensors capture all network traffic and analyze the content of individual packets for malicious traffic[9]. An example of an NIDS is Snort.

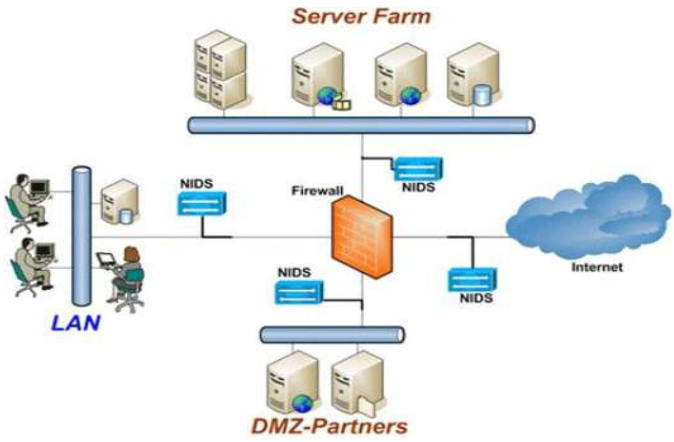


Figure 1. A Network Based IDS

Network Intrusion Detection Systems are usually deployed as a dedicated component on a network segment. There is some debate as to where to place a single NIDS (inside or outside of a firewall), but most agree that multiple NIDS are better. It will then compare captured network data to a file of known malicious signatures. If there is a match, the IDS will log and send an alert according to how it was configured by the network or security administrator[10].

A major difficulty is that true performance statistics are very hard to obtain, especially in a lab. However, a recent test by NSS Labs is probably one of the best[11]. The issue is not how many attacks that an NIDS can detect that is the most

important factor (and often the only bench mark used in lab tests), but how effectively the NIDS can pick out one attack in a mass of normal background traffic. It is often not the mass of attacks that an NIDS has problems dealing with, but the proverbial "finding a needle in a haystack". This becomes especially difficult when SSL (Secure Socket Layer) traffic is involved, because the NIDS cannot read encrypted traffic. It wastes valuable CPU cycles realizing that it can't do anything with the traffic and then discards it!

A second core performance element to consider is the size of packets. In tests, NIDS vendors usually look at an average packet size of 1024 bytes, however if the packet sizes are smaller, the NIDS will run a lot slower (e.g. consider the negative impact when monitoring a large DNS server).

A third key driver in how fast an NIDS can run is the actual policy that is running on the NIDS. Typically NIDS have hundreds of attack signatures that they are looking for at any given time. The more signatures they are looking for in a stream of data, the longer it will take to look at the next stream. This is more critical for pattern matching based systems than those that utilize protocol analysis.

The nature of mobile computing environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any node. Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless ad-hoc network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly.

IV. New Architecture

Though many IDS architecture have been designed for infrastructure-based networks, they are not applicable in Mobile Environment. Motivated by this consideration, we propose the modified architecture based on a conceptual model for an IDS agent proposed by Yongguang Zang and Wenke Lee[3]. The model is extended by introducing two novel ideas, the Data collection is divided in two parts and one Global Data Collection Module is introduced as the outer most layer of the model.

IDS should be both cooperative and distributed to satisfy the need of the wireless Ad-Hoc network. In the proposed architecture, every node in the wireless Ad-Hoc network participate in intrusion detection and response. Each of these nodes is responsible for signaling the intrusion locally and independently. Also this IDS model identifies the black list and white list requests.

The internal of an IDS agent can be fairly complex, but conceptually it can be structured in eight pieces (Figure 2). The data collection module is responsible for gathering local audit trace and activity logs. Next the Identifier will use this data to identify the detection; Notification will take the appropriate action if the intrusion occurs. The Global Data Collection will store all the calls which have been occurred.

A. Data Collection Module

This has been further divided into black list and white list. It gathers all the necessary streams of the data that has been arrive at a time of request. The black list Module stores all the details of the source that may lead to misuse. That is there may be chance of intrusion. Whereas the white list module will store all the details of the most frequently calls and which are authentic. Depending on the intrusion detection algorithms, these useful data streams can include system and user activity within the mobile node. Multiple data collection modules cab consist in one IDS agent to provide multiple audit streams for a multi-layer integrated intrusion detection method.

B. Identifiers

Identifiers can be a local Identifier or Group detection. The local Identifier uses the data from the Data Collection module and identifies whether the intrusion is occurred or not. If yes, then, it sends the signal to the Notification module where it will be proceed. As the days going, there will always been created a newer attacks for the system and to secure a system is not an easy task even more and more devices become wireless so security must be increased accordingly. To establish a new and best security for the mobile Ad-Hoc network is not so easy. So IDS model should be used different statistical and mathematical model to solve the problems.

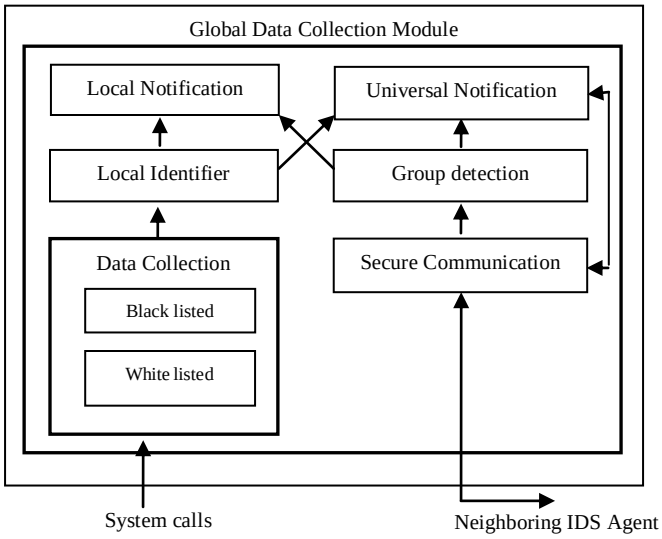


Figure 2. A Conceptual model for IDS Agent

C. Notification

Notification can be local notification or universal notification. According to the type of network the notification has been made to the system. When the system is in the network at that time it will notified universally i.e. it will broadcast the message to its neighbor alongwith the details of the intrusion description and the address of that particular system which initiates the intrusion. In this case, all the system updates their data collection module and put this description in the black list of that module. Also they can refer it in the future to identify the intrusion.

In the Local Notification, it will notify itself that the intrusion has occur then it will terminate the connection with that particular system and update the black list data collection module.

When an intrusion occurs, at that time, it will send the intrusion state information to its neighboring node. Then each node can update the Data Collection module and can initiate appropriate action against that Intruder.

D. Global Data Collection Module

The core and the heart of the new Intrusion detection system as it is centralized and stores all the streams and actions carried out by the system in the network. When any system initiates, the request, at that time, first it will store in this module which can be further used to identify the intrusion by the Data collection module. This module also implements the Cache concepts as it is updated at every interval by itself. The cross checking will be done for every instance of the node to secure the Ad-hoc network and to identify the unauthorized user.

V. CONCLUSION

Here the argument is that any system on the network may find intrusion and their privacy may be exploited. This is especially true for wireless Ad-hoc network. Intrusion detection can help intrusion prevention technique to improve intrusion technique. So that new technique must be developed to solve this problem.

By the continuous investigation, it is shown that how a new model can be developed and how a Global Data Collection module will help IDS Agent to identify the occurrences of the intrusion. Firstly when any system initiates the request, it will be checked in the Global Data Collection Module if it will not found in that it will be put in the Black list and the broad cast of the message is made thus all the neighboring node can know the intrusion point, and can take appropriate action.

At present time, the investigation of the architecture issues is still going on to solve it, implementing it practically and studying its performance issues. In short we are focuses more on the issues that raises in the IDS and try to identify the best solution among all.

In future, the algorithm which supports the model will be developed to identify the Intrusion in cost effective way.

REFERENCES

[1] I.Chlamtac, M. Conti, Jennifer J.-N. Liu., Mobile ad hoc networking: imperatives and challenges, Ad Hoc Networks, 1 (2003), 13-64.

[2] R. Heady, G. Luger, A. Maccabe, and M. Servilla. The architecture of a network level intrusion detection system. Technical report, Computer Science Department, University of New Mexico, August 1990.

[3] Wenke Lee and Yongguang Zhan, Intrusion Detection in wireless Ad-Hoc Networks, Technical report, Department of Computer Science, North Carolina State University, Raleigh, NC 27695.

[4] Web site of the Webopedia http://www.webopedia.com/term/i/intrusion_detection_system.html

[5] Anderson, Ross (2001). "Security Engineering: A Guide to Building Dependable Distributed Systems". New York: John Wiley & Sons. pp. 387–388. ISBN 9780471389224.

[6] T. Heberlein, et al. A Network Security Monitor, In Proc. IEEE Symp. Research in Security and Privacy, pp. 296-304, 1990.

[7] B. Mukherjee, L T. Heberlein, and K. N. Levitt, Network Intrusion Detection. IEEE Network, 8(3): 26–41, May/June 1994.

[8] S. R. Snapp, et al, The DIDS (Distributed Intrusion Detection System) prototype. In Proc. Summer USENIX Conference, pp. 227-233, San Antonio, Texas, 8-12 June 1992.

[9] Web site of the Wikipedia – The free encyclopedia : http://en.wikipedia.org/wiki/Intrusion_detection_system

[10] Northcutt, Stephen and Novak, Judy Network Intrusion Detection An Analyst's Handbook Second Edition New Riders 2001. P203-213

[11] Web site of NSS lab : http://www.nss.co.uk/ids/index.htm

[12] P. Brutch and C. Ko, "Challenges in Intrusion Detection for Ad Hoc Networks," IEEE Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.

[13] Konrad Wrona, "Distributed Security: Ad Hoc Networks & Beyond," PAMPAS Workshop, Sept. 16/17 2002, London

[14] Vesa Karpijoki, "Security in Ad Hoc Networks," http://citeseer.nj.nec.com/karpijoki01security.html

AUTHORS PROFILE

Atul Patel received Bachelors degree in Science (Electronics), M.C.A. degree from Gujarat University, India. M.Phil. (Computer Science) Degree from Madurai Kamraj University, India. Now he is an Associate Professor and Head, Charotar Institute of Computer Applications – Changa, India. He is pursuing Ph.D. in wireless networks. His main research areas are wireless communication and Network Security.

Ruchi Kansara received B.Sc. Degree from Sardar Patel University, V. V. Nagar. Now she is pursuing MCA programme at Charotar University of Science & Technology, Changa. Her area of research is Wireless networks.

Dr. Paresh Virparia received B.Sc. (Maths), M.C.A. and Ph. D. Degree from Sardar Patel University, V. V. Nagar, India. Now he is a Associate Professor at G. H. Patel PG Department of Computer Science and Technology, Sardar Patel University, India His main research areas are Computer Simulation & Modeling and Networks.

Agent based Congestion Control Performance in Mobile ad-hoc Network:A Survey paper

Vishnu Kumar Sharma
Department of CSE,
JUET,India

Dr. Sarita Singh Bhadauria
Department of Elex,
MITS,India

***Abstract*— A Congestion control is a key problem in mobile ad-hoc networks. The standard TCP congestion control mechanism is not able to handle the special properties of a shared wireless channel. Many approaches have been proposed to overcome these difficulties. ideas and show their interrelations. mobile agent based congestion control Technique routing is proposed to avoid congestion in ad hoc network. Some mobile agents are added in ad hoc network, which carry routing information and nodes congestion status. When mobile agent travels through the network, it can select a less-loaded neighbor node as its next hop and update the routing table according to the node's congestion status. With the aid of mobile agents, the nodes can get the dynamic network topology in time. In this paper, we give an overview over existing proposals, explain their key ideas, TCP Issues, Reduce the Congestion, delay in mobile ad-hoc network and proposed solution**

Keywords- Mobile Ad hoc Networks (MANETs); mobile agents (MA); TCP.

I. INTRODUCTION

An ad hoc network is also called as infrastructure less networks which is a collection of mobile nodes which forms a temporary network without the help of central administration or standard support devices regularly available in conventional networks. Mobile ad hoc wireless networks have the ability to establish networks at anytime, anywhere to possess the assurance of the future. These networks do not depend on irrelevant hardware because it makes them ideal candidate for rescue and emergency operations. The constituent wireless nodes of these network build, operate and maintain these networks. Each node asks the help of its neighboring nodes to forward packets because these nodes usually have only a limited transmission range [1].

Congestion occurs in mobile ad hoc networks (MANETs) with limited resources. In such networks, packet transmissions suffer from interference and fading, due to the shared wireless channel and dynamic topology. Congestion leads to packet losses and bandwidth degradation, and wastes time and energy on congestion recovery. A congestion-aware routing protocol can preempt congestion through bypassing the affected links [2]. Several distinct congestion-related problems have been identified and tracked down, including severe throughput degradation and massive fairness problems. They have been shown to originate from the MAC, routing, and transport layers [4].

TCP congestion control works very well on the Internet. But MANETs exhibit some unique properties that greatly affect the design of appropriate protocols and protocol stacks in general, and of congestion control mechanism in particular. As it turned out, the vastly differing environment in a mobile ad-hoc network is highly problematic for standard TCP.

- Route failures trigger inappropriate TCP congestion control reactions.
- The standard TCP retransmission timeout grows too fast in MANET environments.
- The locally shared medium induces unfairness between TCP flows.
- TCP has a long feedback path.
- Data and acknowledgment packets interfere on the shared medium.
- TCP over saturates the network.
- On the shared medium, there is intra-flow contention between successive data packets.
- The TCP acknowledgment scheme generates a lot of packets.
- TCP traffic is bursty.
- TCP's basic design decisions do not fit a MANET environment well. [4]

TCP congestion control has an implicit assumption, which is that any packet loss is due to network congestion. However, this assumption is no longer valid in the MANET as packet losses may well be due to channel bit errors, medium contention, and route failures. [14]

Congestion is a major cause for packet loss in MANETs and reducing packet loss involves congestion control running on top of a mobility and failure adaptive routing protocol at the network layer. Congestion non-adaptive routing in MANETs may lead to the following problems:

- Long delay: It takes time for a congestion to be detected by the congestion control mechanism. In severe congestion situations, it may be better to use a new route. The problem with an on-demand routing protocol is the delay it takes to search for the new route.
- High overhead: In case a new route is needed, it takes processing and communication effort to discover it. If multipath routing is used, though an alternate route is readily found, it takes effort to maintain multiple paths.

- Many packet losses: Many packets may have already been lost by the time congestion is detected. A typical congestion control solution will try to reduce the traffic load, either by decreasing the sending rate at the sender or dropping packets at the intermediate nodes or doing both. The consequence is a high packet loss rate or a small throughput at the receiver [3].

Flow control is a good mechanism to avoid the congestion problem. But it is another major challenge in the network research that adapts the transmission rate to the available resources capacities in order to avoid congestion [13].

II. Related Work

This section presents a brief review of the work already done in this field.

Kazuya Nishimura et al [5] have discussed a routing protocol that uses multi-agents to reduce network congestion for a Mobile Ad hoc Network (MANET). They have extended a dynamic routing protocol using mobile agent's protocol to be more generic, so that it can be effective in the face of network congestion. They have developed both simulation environment and protocols, and performed simulations under different conditions of mobility and traffic patterns to demonstrate the effectiveness of their approach.

Yao-Nan Lien et al [6] proposed a new TCP congestion control mechanism by router-assisted approach. Based on the information feed backed from routers, a TCP sender is able to adjust its sending speed dynamically in order to avoid overshooting problem.

Wei Sun et al [7] have compared the general AIMD-based congestion control mechanism (GAIMD) with Equation-based congestion control mechanism (TFRC TCP-Friendly Rate Control) over a wide range of MANET scenario, in terms of throughput fairness and smoothness. Their results have shown that TFRC and GAIMD are able to maintain throughput smoothness in MANET, but at the same time, they require only a less throughput than the competing TCP flows. Also their results show that TFRC changes its sending rate more smoothly than GAIMD does, but it gets the least throughput compares with TCP and GAIMD.

Consolee Mbarushimana et al [8], have exposed the performance of MANETs routing protocols is highly dependent on the type of traffic generated or routed by intermediate nodes. They have proposed a Type of Service Aware routing protocol (TSA), an enhancement to AODV, which uses both the ToS and traditional hop count as route selection metrics. TSA avoids congestion by distributing the load over a potentially greater area and therefore improving spatial reuse. Their simulation study reveals that TSA considerably improves the throughput and packet delay of both low and high priority traffic under different network operational conditions.

Yung Yi et al [9] have developed a fair hop-by-hop congestion control algorithm with the MAC constraint being imposed in the form of a channel access time constraint, using an optimization-based framework. In the absence of delay, they have shown that their algorithm is globally stable using a Lyapunov-function-based approach. Next, in the presence of delay, they have shown that the hop-by-hop control algorithm has the property of spatial spreading. Also they have derived bounds on the "peak load" at a node, both with hop-by-hop control, as well as with end-to-end control, show that significant gains are to be had with the hop-by-hop scheme, and validate the analytical results with simulation.

Umut Akyol et al [10] have studied the problem of jointly performing scheduling and congestion control in mobile adhoc networks so that network queues remain bounded and the resulting flow rates satisfy an associated network utility maximization problem. They have defined a specific network utility maximization problem which is appropriate for mobile adhoc networks. They have described a wireless Greedy Primal Dual (wGPD) algorithm for combined congestion control and scheduling that aims to solve this problem. They have shown how the wGPD algorithm and its associated signaling can be implemented in practice with minimal disruption to existing wireless protocols.

S.Karunakaran et al [11] have presented a Cluster Based Congestion Control (CBCC) protocol that consists of scalable and distributed cluster-based mechanisms for supporting congestion control in mobile ad hoc networks. The distinctive feature of their approach is that it is based on the self-organization of the network into clusters. The clusters autonomously and proactively monitor congestion within its localized scope.

Kazuya Nishimura et al [12] have discussed a routing protocol that uses multi-agents to reduce network congestion for MANET. In their work, two kinds of agents are engaged in routing. One is a Routing Agent that collects information about network congestion as well as link failure. The other is a Message Agent that uses this information to get to their destination nodes.

III. The Proposed Work

Congestion adaptive routing has been investigated in several studies as we explained in section 2. The approaches in all the cited studies converge in evaluating or assessing the level of activity in intermediate nodes by measuring either the load or the delay. Based on the gathered information, the optimal path is established trying to avoid the already or likely to become congested nodes. However, none of the research reported has evaluated the effect service type of the traffic carried by intermediate nodes has on the performance of routing protocols [8].

The route discovery process of most of MANETs routing protocols do not consider the status of their queues, before advertise themselves as candidate to route traffic to the destination. This might result into long delays or packet drops for newly arriving traffic, failing to be transmitted ahead of the already queuing traffic [8].

The performance of the mobile ad hoc networks is strongly influenced by the congestion problem. A congestion control scheme consists of a routing algorithm and a flow control scheme. In earlier research, the routing and the flow control problems have been considered separately. To achieve better

performance and better congestion control, the routing and the flow control must be considered jointly [13].

In this paper, we propose to design and develop an agent based congestion control architecture in fig.-1, In this architecture, all the nodes are mobile and information about network congestion is collected and distributed by mobile agents (MA). Each node has a routing table that stores route information for every destination. MA starts from every node and moves to an adjacent node at every time. The MA updates the routing table of the node it is visiting.

In this proposal, the node is classified in one of the four categories depending on whether the traffic belongs to background, best effort, video or voice AC respectively. Then MA at each node estimates the congestion level for each traffic class by checking the queue status and a priority is assigned for the node based on the measured congestion level. Using this classification, a node with no traffic or with delay-insensitive traffic is considered more priority so that it can receive more traffic than a low priority node. The congestion level of every node is updated every time there is change in traffic type, and it is periodically propagated to neighbors.

IV. Agent Based Congestion Control Routing

The agent based congestion routing can be explained from the following figure:

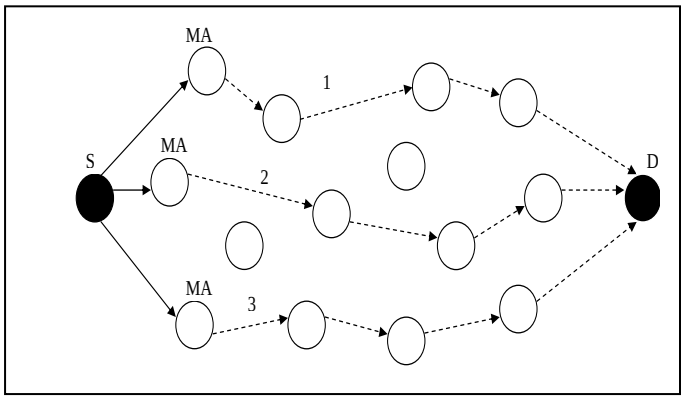


Figure 1. Agent Based Congestion Routing

Step 1: The source S checks the number of available one hop neighbors and clones the Mobile Agent (MA) to that neighbors.

Step 2: The Mobile Agent selects the shortest path of the route to move towards the destination D as given in the figure 1 such as P1, P2 and P3.

Step 3: The MA1 moves towards the destination D in a hop-by-hop manner in the path P1 and MA2 in P2 and MA3 in P3 respectively.

Step 4: Then the MA1 calculates the Total Congestion Metric(TCM), TCM1 of that path P1 and similarly MA2 calculates the TCM2 of P2 and MA3 calculates the TCM3 of P3.

Step 5: Now the destination D sends the total congestion metrics TCM1, TCM2 and TCM3 of the paths P1, P2 and P3 respectively to the source.

Step 6: Now the source selects path using min (TCM1, TCM2, and TCM3) and sends the data through the corresponding path which has the minimum congestion.

V. Mobile Agents Technique

Mobile agents are software entities that act on behalf of their creators and move independently between hosts. In general, a mobile agent executes on a machine that hopefully provides the resources or services that it needs to do its work. If a machine does not contain the needed resources or services, the mobile agent can transfer itself to a new machine. Lange and Oshima [15] enumerate several beets of using mobile

agents. Of particular interest to MANET routing are:

• Mobile agents are able to upgrade protocols in use by moving to a destination and setting up communications operating under revised policies.

• After being dispatched, mobile agents become indecent-dent of the process that created them and can operate asynchronously and react dynamically and autonomously to environmental changes.

• Mobile agents can reduce network load and latency by running remotely.

Recently, a number of mobile agent systems have been developed to address applications in areas including telecom-munication services, E-commerce and personal assistance. Included among these are Agent TCL [16] (later D'Agents),ARA [17], Concordia [18], and Aglets [19]. All such systems provide common functions including agent migration, inter-agent communication and security. One potential drawback of using mobile agents is that the agents require an "execution environment" in which to run. This has become less of an issue in recent years as mobile devices become more capable and the execution environments become somewhat leaner.

A. Routing Using Mobile Agents

Early work on routing in dynamic networks using mobile agents by Kramer et al. [20] concentrated on route discovery using agents to continuously track the network topology and update routing tables at all mobile hosts reached. When a route is requested, an agent is sent to discover routes to the destination.

These agents analyze the routing tables on the hosts they arrive at and either return a discovered route to the sender or move on to another machine if no route is found. Unfortunately, this method increases network load

B. Mobile Agent Technology

Mobile Agent is a novel way of building distributed software system. Traditional distributed systems are built out of

stationary programs that pass data back and forth across a network [21]. It is usually kept a certain state. It is able to exchange information for its owners and other nodes in order to work together.

VI. CONCLUSION

In this paper, we have discussed an agent based congestion control technique and TCP issues. In our technique, the information about network congestion is collected and distributed by mobile agents (MA). A mobile agent starts from every node and moves to an adjacent node at every time. A node visited next is selected at the equivalent probability. The MA brings its own history of movement and updates the routing table of the node it is visiting. The MA updates the routing table of the node it is visiting. In this technique, the node is classified in one of the four categories depending on whether the traffic belongs to background, best effort, video or voice AC respectively. our proposed technique attains high delivery ratio and throughput with reduced delay when compared with the existing technique

REFERENCES

[1] S.Santhosh baboo and B.Narasimhan, "A Hop-by-Hop Congestion-Aware Routing Protocol for Heterogeneous Mobile Ad-hoc Networks", International Journal of Computer Science and Information Security, 2009

[2] Xiaoqin Chen, Haley M. Jones and A.D.S. Jayalath, "Congestion-Aware Routing Protocol for Mobile Ad Hoc Networks", IEEE 66th Conference in Vehicular Technology, 2007.

[3] Duc A. Tran and Harish Raghavendra, "Congestion Adaptive Routing in Mobile Ad Hoc Networks", IEEE Transactions on Parallel and Distributed Systems, November 2006

[4] Christian Lochert, Bjorn Scheuermann and Martin Mauve, "A Survey on Congestion Control for Mobile Ad-Hoc Networks", Wireless Communications and Mobile Computing, InterScience, 2007.

[5] Kazuya Nishimura and Kazuko Takahashi, "A Multi-Agent Routing Protocol with Congestion Control for MANET", Proceedings 21st European Conference on Modeling and Simulation, 2007

[6] Yao-Nan Lien and Ho-Cheng Hsiao, "A New TCP Congestion Control Mechanism over Wireless Ad Hoc Networks by Router-Assisted Approach", 27th IEEE International Conference on Distributed Computing Systems Workshops, 2007.

[7] Wei Sun, Tao Wen and Quan Guo, "A Performance Comparison of Equation-Based and GAIMD Congestion Control in Mobile Ad Hoc Networks", International Conference on Computer Science and Software Engineering, 2008

[8] Consolee Mbarushimana and Ali Shahrabi, "Congestion Avoidance Routing Protocol for QoS-Aware MANETs", Proceedings of IEEE International Wireless Communications and Mobile Computing Conference, 2008.

[9] Yung Yi and Sanjay Shakkottai, "Hop-by-Hop Congestion Control Over a Wireless Multi-Hop Network", IEEE/ACM Transactions on Networking, February 2007

[10] Umut Akyol, Matthew Andrews, Piyush Gupta, John Hobby, Iraj Saniee and Alexander Stolyar, "Joint Scheduling and Congestion Control in Mobile Ad-Hoc Networks", Proceedings of IEEE INFOCOM, 2008.

[11] S.Karunakaran & P.Thangaraj , "A CLUSTER BASED CONGESTION CONTROL PROTOCOL FOR MOBILE ADHOC NETWORKS" , International Journal of Information Technology and Knowledge Management , July-December 2010, Volume 2, No. 2, pp. 471-474.

[12] Kazuya NISHIMURA and Kazuko TAKAHASHI, "A Multi-Agent Routing Protocol with Congestion Control for MANET", Proceedings 21st European Conference on Modelling and Simulation ,2007.

[13] Belkadi Malika, Lalam Mustapha, M'zoughi Abdelaziz, Tamani Nordine, Daoui Mehammed, Aoudjit Rachida , "Intelligent Routing and FloControl In MANETs" , Journal of Computing and Information Technology, doi:10.2498/cit.1001470

[14] Hongqiang Zhai, Xiang Chen and Yuguang Fang, "Rate-Based Transport Control for Mobile Ad Hoc Networks", Proceedings of IEEE WCNC'05.

[15] D. Lange and M. Oshima: "Seven Good Reasons for Mobile Agents". Communications of the ACM 42(3) (1999) 88–89.

[16] R. Gray: "Agent Tcl: A flexible and secure mobile agent system". In Proceedings of the 4th Annual Tcl/Tk workshop. Monterey, USA,July 1996, pp. 9–23.

[17] H. Peine and T. Stolpmann: "The Architecture of the Ara Platform for Mobile Agents". In Proceedings of the 1st International Workshop on Mobile Agents. Berlin, Germany, April 1997, pp. 50–61.

[18] D. Wong, N. Paciorek, T. Walsh, and J. DiCelie: "Concordia: An Infrastructure for Collaborating Mobile Agents". In Proceedings of the 1st International Workshop on Mobile Agents. Berlin, Germany,April 1997, pp. 86–97.

[19] D. Lange, M. Oshima, G. Karjoth, and K. Kosaka: "Aglets: Programming Mobile Agents in Java". In Proceedings of Worldwide Computing and Its Applications. Tsukuba, Japan, March 1997, pp.253–266.

[20] K. Kramer, N. Minar, and P. Maes:"Mobile Software Agents from Dynamic Routing".Mobile Computing and Communications Review 3(2) (1999) 12–16.

[21] WOOK C, SAJAL K D, LEE I. Nomadic Control Packet- Based Dynamic Route Maintenance Scheme for Adaptive Routing in Mobile Ad Hoc Networks[EB/OL]. http:// csdl.computer.org/comp/proceedings/lcn /2003/ 20 37/00/20370140abs.html.

32 x 10 and 64 × 10 Gb/s transmission using hybrid Raman-Erbium doped optical amplifiers

Shveta Singh[1], M.L.Sharma[2]
Department of Electronics and Communication,
B.G.I.E.T, Sangrur, India

Ramandeep Kaur[3],
Department of Electronics and Communication, Thapar University, Patiala, India

***Abstract*— We have successfully demonstrated a long-haul transmission of 32 × 10 Gbit/s and 64 × 10 Gbit/s over single-mode fiber of 650 km and 530 km respectively by using RAMAN-EDFA hybrid optical amplifier as inline and preamplifier amplifiers. The measured Q-factors and BER of the 32 and 64 channels after 650 and 530 km respectively (16.99–17 dB) and (10^{-13}) were higher than the standard acceptable value, which offers feasibility of the hybrid amplifiers including EDFA optical amplifiers for the long-haul transmission.**

Keywords- HOA; RAMAN; EDFA; BER; Q-FACTOR; EYE-OPENING; DISPERSION; TRANSMISSION DISTANCE; WDM and DWDM.

I. INTRODUCTION

Wavelength division multiplexing (WDM) is basically frequency division multiplexing in the optical frequency domain, where on a single optical fiber there are multiple communication channels at different wavelengths [1]. A WDM system uses a multiplexer at the transmitter to join the signals together and a demultiplexer at the receiver to split them apart. By using WDM and optical amplifiers, they can accommodate several generations of technology development in their optical infrastructure [2]. Optical gain depends on the frequency of the incident signal and also on the local beam intensity. Dense wavelength division multiplexing (DWDM) is a technology that puts data from different sources together on an optical fiber, with each signal carried at the same time on its own separate light wavelength [3]. Optical amplifiers have several advantages over regenerators. Optical amplifiers can be more easily upgraded to a higher bit rate. In an optical communication system, as the optical signals from the transmitter propagate through optical fiber are attenuated by it and losses are added by other optical components, such as multiplexers and couplers which causes the signal to become too weak to be detected. Before this the signal strength has to be regenerated [4]. Most optical amplifiers amplify incident light through stimulated emission, its main ingredient is the optical gain realized when the amplifier is pumped to achieve population inversion. The optical gain, in general, depends not only on the frequency of the incident signal, but also on the local beam intensity at any point inside the amplifier [5]. To understand how optical amplification works, the mutual or reciprocal action of electromagnetic radiation with matter must be understood [6]. Optical amplification uses the principle of stimulated emission same as used in a laser. Optical amplifiers can be divided into two basic classes: optical fiber amplifiers (OFAs) and semiconductor optical amplifiers (SOAs) [1]. An amplifier can boost the (average) power of a laser output to higher levels. It can generate extremely high peak powers, particularly in ultra short pulses, if the stored energy is extracted within a short time. It can amplify weak signals before photo detection, and thus reduce the detection noise, unless the added amplifier noise is large. In long fiber-optic links for optical fiber communications, the optical power level has to be raised between long sections of fiber before the information is lost in the noise [7]. The combination of an erbium-doped fiber amplifier (EDFA) and a fiber Raman amplifier (FRA or RA) is called a hybrid amplifier (HA), the RAMAN-EDFA. Hybrid amplifier provides high power gain. Raman amplifier is better because it provides distributed amplification within the fiber. Distributed amplification uses the transmission fiber as the gain medium by multiplexing a pump wavelength and signal wavelength. It increases the length of spans between the amplifiers and regeneration sites. So this provides amplification over wider and different regions [8]. HYBRID Raman/erbium-doped fiber amplifiers (HFAs) are an advance technology for future. Hybrid Raman/erbium-doped fiber amplifiers are designed to maximize the long-haul transmission distance [9].

H.S. Chung *et al*. [10] have successfully demonstrated a long-haul transmission using cascaded Raman and linear optical amplifiers as inline amplifiers of 16 × 10 Gbit/s over single-mode fiber of 1040 km. Q-factors of the 16 channels after 1040 km (12.7–14.5 dB) were higher than the error-free threshold of the standard forward-error correction, which offers feasibility of the hybrid amplifiers including semiconductor optical amplifiers for the long-haul transmission.

Tetsufumi Tsuzaki *et al*. [11] have successfully developed a 64nm hybrid optical repeater amplifier for a long-distance WDM transmission system. The gain variation after 40 concatenations was reduced below 3dB with the optimal equalization techniques. Using these repeaters, transmitted 3.2Tb/s (1 60 x 20 GB/s RZ) over 1,500 km using 64nm hybrid optical repeater amplifier for a long-distance WDM transmission system.

Seung Kwan Kim *et al*. [12] describes the multiple channel amplification, using commercially available pump laser diodes and fiber components, they determined and optimized the conditions of three-wavelength Raman pumping for an amplification bandwidth of 32 nm for C-band and 34 nm for L-band using design of a hybrid amplifier composed of a

distributed Raman amplifier and erbium- doped fiber amplifiers for C- and L-bands.

T.N.Nielsen *et al.* [13] has demonstrated ultra-high capacity WDM transmission systems based on either dual C- and L-band transmission, or distributed Raman amplification with aggregate capacities of more than 1 Tbls. In this paper they demonstrate a record capacity of 3.28-Tb/s by, for the first time, combining these three techniques in one system. The 3.28-Tb/s is comprised of forty 100-GHz spaced WDM channels in the C-band and forty-two 100-GHz spaced WDM channels in the L-band.

Unlike the previous work [9] with the hybrid amplifiers based on LOAs, we used RAMAN- EDFA and a variable span R of different lengths, which includes the transmission of 32 × 10 Gb/s and 64 × 10 Gb/s upto 650 and 530 km respectively using raman/edfa hybrid optical amplifiers, which offers feasibility of the hybrid amplifiers including EDFA optical amplifiers for the long-haul transmission.

This paper is divided into different sections for transmission of 32 × 10 and 64 × 10 Gb/s using hybrid raman/edfa amplifiers. In section 2, the simulation set up for the transmission of 32 and 64 channels at 10 Gb/s speed. Section 3 gives the discussion of the results observed after the simulation. And section 4 gives the conclusion of the system performance.

II. Simulation Setup

In the figure shown below, 32 and 64 channels are transmitted at 10 Gb/s speed. Input signals are pre-amplified by a booster and these signals are transmitted over optical fiber of different transmission distances. The figure shows the compound component composed of RAMAN/EDFA at different distance and dispersion. This transmitter compound component consists of the data source, electrical driver, laser source and external Mach-Zehnder modulator in each transmitter section. The data source is generating signal of 10 Gb/s with pseudo random sequence. The electrical driver converts the logical input signal into an electrical signal. The CW laser sources generate the 16 laser beams at 191.9 THz to 193.4 THz with 100 GHz channel spacing. These beams have random laser phase and ideal laser noise bandwidth. The signals from data source and laser are fed to the external Mach-Zehnder modulator, where the input signals from data source is modulated through a carrier. optical output signal is transmitted over different distance for 100,100,100,90,90,90,80 km for 32 channel and 100,90,90,90,80,80 km for 64 channels at 2 ps/nm/km dispersion. Optical power meter and optical spectrum analyser with splitter are used for calculating signal power and spectrum. Receiver is used to receive 32/64 output signals and these signals are then converted into electrical signal. Optical Power meter and Optical probe with splitters are used for measuring the signal power at different levels. Optical signals are amplified using EDFA amplifier. The signal power is measured by power meter and optical probe. The modulated signal is converted into original signal with the help of PIN photodiode and filters. A compound receiver is used to detect all signals and converts these into electrical fo R is the variable span length of 100, 100, 100, 90, 90, 90, 80 km for 32 channel and 100, 90, 90, 90, 80, 80 km for 64 channels for long hual transmission of optical fiber using raman/edfa Optical amplifiers.

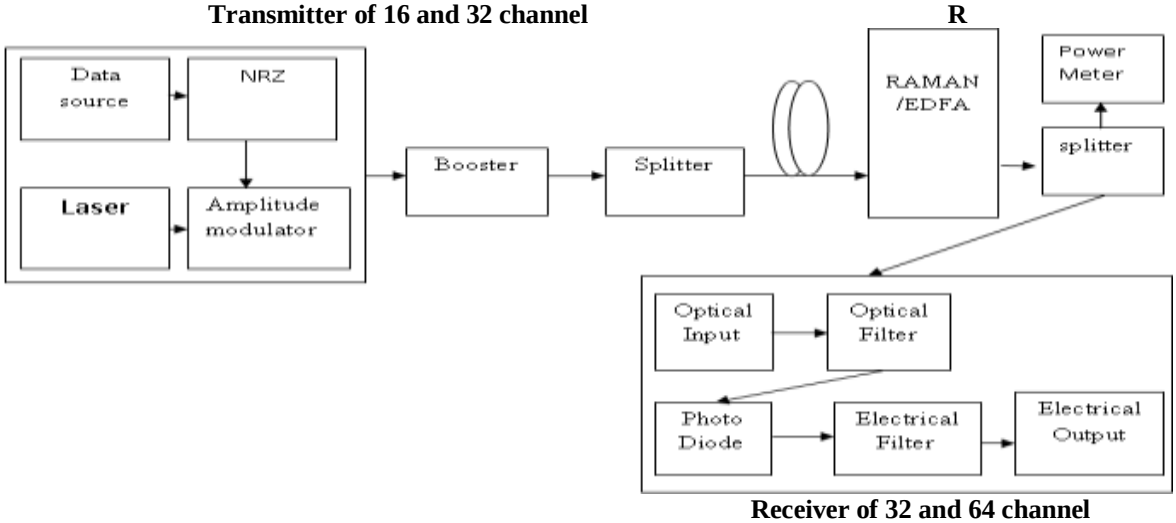


Figure 1: Block Diagram of Simulation Setup

III. Results and Discussions

In the previous section, we have discussed various components used in the simulation setup. Using this setup we are taking measurements of BER, Q-factor, eye closure and output power at 10Gbps with respect to the length. The result discussed below gives optimized parameters of hybrid optical amplifiers (RAMAN-EDFA). The optimization is done on the basis of BER, Q-factor, eye closure and output power for hybrid optical amplifier by changing the transmission distance varying from 100 to 650 km and 100 to 530 km for 32 and 64 channel respectively.

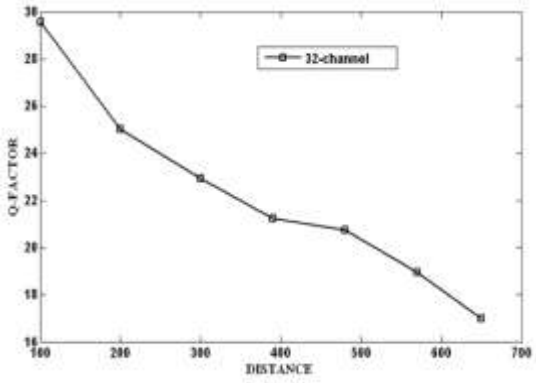


Figure 2: Quality factor vs. distance for 32 channels

In order to observe the performance of RAMAN-EDFA, the quality factor versus transmission distance are shown in figure 2.This graph shows that as we increase the transmission distance from 100 to 650 km, the quality factor decreases simultaneously. The transmission distance is varied with R (R= 100, 100, 100, 90, 90, 90, 80 km). The quality factor decreases from 29.5 to16.9 db for 32 channels.

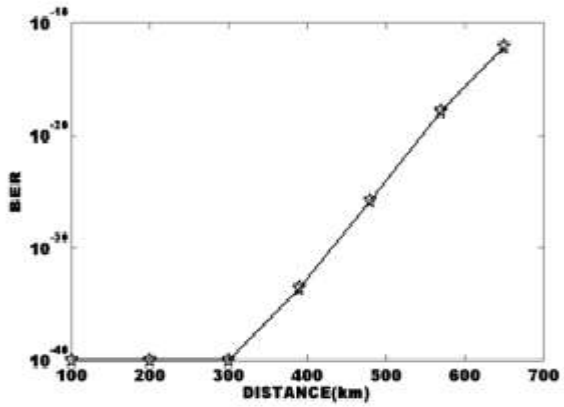


Figure 3: BER vs. distance for 32 channels.

As shown in figure 3, BER increases with distance from 10^{-40} to 10^{-13}. The acceptable bit error rate (BER) for optical transmission is 1×10^{-10}. The BER versus transmission distance for different dispersion is shown in figure. It is observed that by increasing the transmission distance from 100 to 650 km, BER is also increasing.

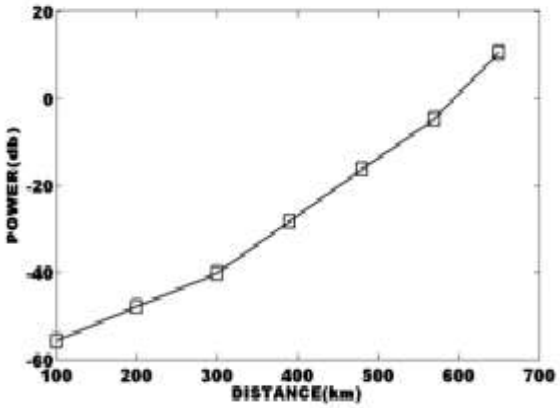


Figure 4: power vs. distance for 32 channels

The power vs. distance is shown in figure 4, Power increases with distance from -55.525 to 10.658 db for 32 channel and quality factor decreases from 29.5 to 16.9 db. The acceptable power for optical transmission is 10 db. It is observed that by increasing distance from 100 to 650 km, power is also increasing.

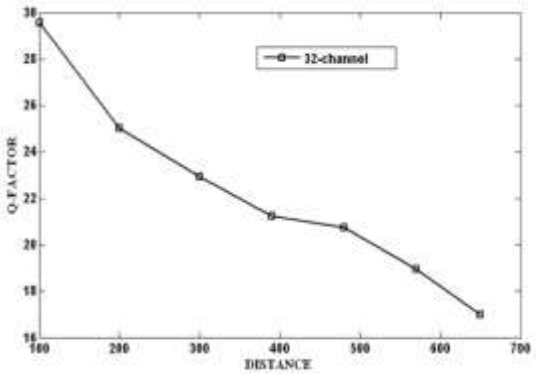


Figure 5: Q-factor vs. distance for 64 channels Figure 7: Power vs. distance for 64 channels

In order to observe the performance of RAMAN-EDFA, the quality factor versus transmission distance are shown in figure 5.This graph shows that as we increase the transmission distance from 100 to 530 km, the quality factor decreases simultaneously. The quality factor decreases from 28 to 17db for 64 channels.

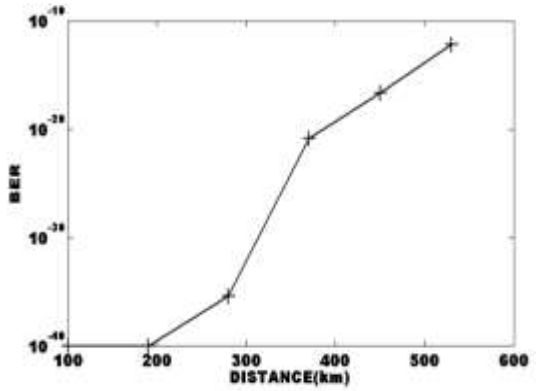


Figure 6: BER vs. distance for 64 channels

As shown in figure 6 BER increases with distance from 10^{-40} to 10^{-13}. The acceptable bit error rate (BER) for optical transmission is 1×10^{-10}. The BER versus transmission distance for different dispersion is shown in figure. It is observed that by increasing the transmission distance from 100 to 530 km, BER is also increasing.

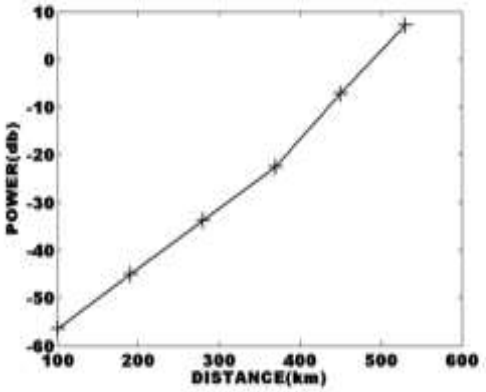


Figure 7: Power vs. distance for 64 channels

As shown in figure 7, Power vs transmission distance from 100 to 530 km, Power increases with distance from -56.415 to 7.178 db for 64 channel and quality factor decreases from 28 to 17 db. The acceptable power for optical transmission is 10 db. It is observed that by increasing distance from 100 to 650 km, power is also increasing. The performance of Raman amplification depends on the properties of the transmission fibers used. The Raman gain efficiency, determining how much Raman gain can be obtained from a given amount of pump power, depends on a number of factors, including the Raman effective area, the composition of the fiber, and the pump and signal wavelengths.

The output power characteristics of the HA are determined by the EDFA. EDFA's offer available output powers of up to 30dBm, the main determining factor is the pump power. Raman amplifiers are broad-band and wavelength agnostic. Raman amplifiers can be distributed, lumped or discrete, or hybrid. Also, in Raman amplifiers the amplification and dispersion compensation can be combined in the same fiber length.

For high channel count systems, as will be deployed in the next few years, Raman amplifiers' efficiency actually exceeds even 1480-nm pumped -band EDFAs. Consequently, Raman amplifiers should see a wide range of deployment in the next few years.

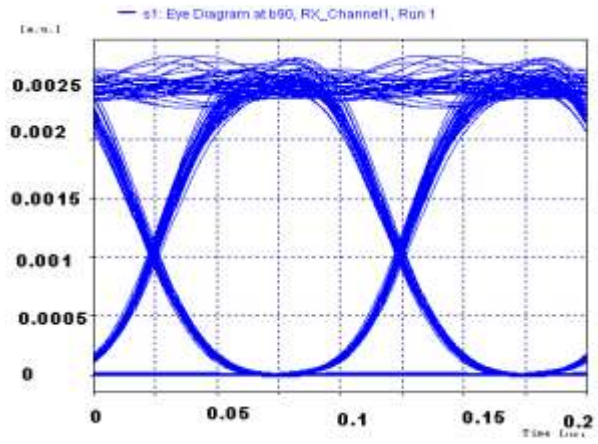


Figure 8: Eye Diagram for RAMAN/EDFA at 100 km for 32 channel

As shown in figure 8, Eye diagram of signal after RAMAN/EDFA at 32 channels with 100 km distance is shown in figure 8.

The eye opening for 100 km is 0.002316, quality factor decreases from 29.5 to 16.9 db and BER is also increasing.

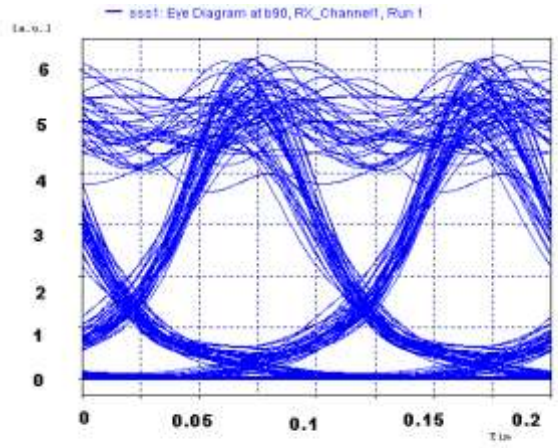


Figure 9: Eye Diagram for RAMAN/EDFA at 650 km at 32 channel

Eye diagram of signal after RAMAN/EDFA at 32 channels with 650 km distance is shown in figure 9.

The eye opening for 650 km is 3.18696, quality factor decreases from 29.5 to 16.9 db and BER is also increasing.

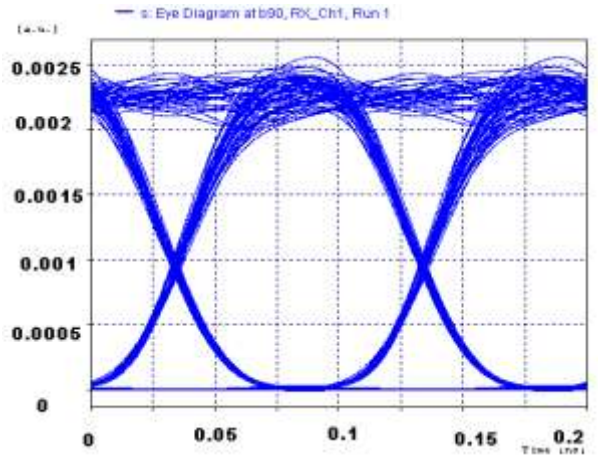


Figure 10: Eye Diagram for RAMAN/EDFA for 64 channel at 100 km

It is observed from the simulation result from the figure 10, that maximum eye opening is obtained from RAMANEDFA at 64 channel is 0.00206 and 2.25773 at 100 km and 530 km transmission distance respectively.

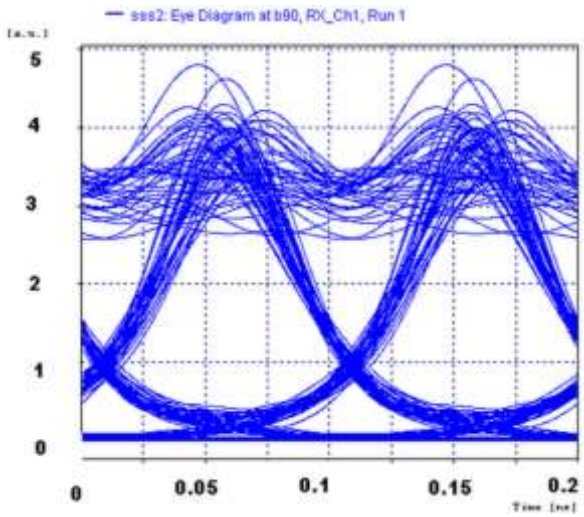


Figure 11: Eye Diagram for RAMAN/EDFA for 64 channel at 530 km

As shown in figure 11, it is observed from the simulation result from the figure 10, that maximum eye opening is obtained from RAMANEDFA at 64 channel is and 2.25773 at 530 km transmission distance.

IV. CONCLUSION

In this Paper, we have successfully demonstrated long-haul WDM transmissions using RAMAN/EDFA as the inline amplifiers.The results offered the feasibility of the Raman/EDFA as inline amplifiers for long distances of 650 and 530 km. We have been observed that before 650 and 530 km, we have an acceptable BER, Q-factor, Power and eye-opening.

After that we observed that the quality factor and ber increases. The performance of optical amplifiers was evaluated using the eye patterns, BER measurement, eye opening, Q factor and power. The simulation results show that RAMAN-EDFA has quality factor of 16.99 db, BER of 7.01×10^{-13}, Eye-Opening of 4.928 and power of 10.65 at 650 km for 32 channel at 10 Gb/s and Quality factor of 17 db, BER of 6.5×10^{-13}, power of 7.17 at 530 km for 64 channel at 10 Gb/s.

The output power, Q factor and eye opening are decreasing. Also there is an increment in BER after 650 Km and 530 km for 32 and 64 channels respectively.

REFERENCES

[1] K. H. Liu, 'IP over WDM', New York: John Wiley and Sons, (2002), Pages 147-151.

[2] Biswanath Mukherjee, 'Optical WDM Networks', Springer, New York, (2006).

[3] P.E. Green, "Fiber-Optic Networks", Prentice-Hall, Cam- bridge, MA, (1992).

[4] Rajiv Ramaswani and Kumar N. Sivarajan, "Introduction to Optical Networks", 2nd Edition, Pages 151-153.

[5] G.P. Agrawal, "Fiber Optic Communication Systems", John Wiley and Sons, New York, (1997), Pages 226-251.

[6] H Ghafouri-Shiraz, "Semiconductor Laser & Amplifiers", Imperial College Press, London, Pages-15.

[7] P.Urquhart (ed.), "Advances in optical amplifiers", an open-access book from In Tech, (2011).

[8] Simranjit singh, "Performance Evolution of Hybrid Optical Amplifiers for WDM Systems", ISTE sponsored IDEA, Pages-7.

[9] A. Carena, "On the Optimization of Hybrid Raman/Erbium-Doped Fiber Amplifiers", (2001), V13, pages 1170-1172.

[10] H.S. Chung, J.Han, S.H. Chang, K. Kim. "A Raman plus linear optical amplifier as an inline amplifier in a long-haul transmission of 16 channels × 10 Gbit/s over single-mode fiber of 1040 km", (2005), V244, pages 141-145.

[11] Tetsufumi Tsuzaki, Michiko Harumoto, Motoki Kakui, Kozo Fujii, "3.2 Tb/s - 1,500 km WDM transmission experiment using 64nm hybrid repeater amplifiers",(2000), V4, Pages 239-241.

[12] Seung Kwan Kim, Sun Hyok Chang, Jin Soo Han, and Moo Jung Chu, "Design of Hybrid Optical Amplifiers for High Capacity Optical Transmission" (2002), V24, Pages 81-96.

[13] T.N.Nielsen, A.J.Stentz, K.Rottwitt, D.S.Vengsarkar, "3.28-Tbh (82~40Gbht) transmission over 3x100 km non zero dispersion fiber using dual C-and L-band hybrid Raman/Erbium-doped inline amplifiers", (2000).