An enhanced Scheme for Reducing Vertical handover latency

Mohammad Faisal, Muhammad Nawaz Khan
Department of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science & Technology (SZABIST),
Islamabad, Pakistan.

Abstract- Authentication in vertical Hand over is a demanding research problem. Countless methods are commenced but all of them have insufficiencies in term of latency and packet loss. Standard handover schemes (MIPv4, MIPv6, FMIPv6, and HMIPv6) also practice these shortages when a quick handover is desirable in several genuine circumstances like MANETs, VANETs etc. This paper will evaluate the literature of the work done in past and present for undertaking the authentication concerns in vertical handover and will put down a basis for building the latency and packet loss more effective in such a huge shared situation that can produce to an extremely bulky level. This effort will mostly focus on the existing tendency in vertical handover mostly with the authentication, latency and packet loss issues.

Keywords: Vertical hand over, Authentication, FMIPv6, HMIPv6, reactive, proactive, latency and packet loss.

I. INTRODUCTION

Future generation heterogeneous wireless networks (FGHWNs) are facing with service continuity challenge for which vertical handoff is indispensible. So its assurance by means of rapid and efficient vertical handover that recognize service connection and seamless mobility maintaining the security and QoS is demand of the day [4]. Administered by diverse operators like WiMax,WiFi ,UMTS,GSM etc each in the run to achieve the highest quality and data rates, dynamically to choose for the always best connected network. Same technology networks switching are called horizontal while different technology networks switching are called vertical handover.

As shown:

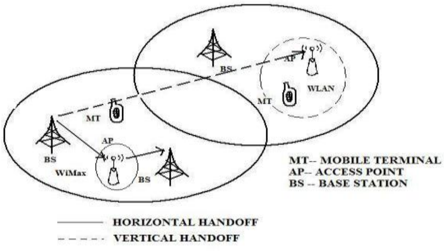

Figure 1. Vertical and Horizontal Handoff

[K.Savitha et al:1]

Four stages are accomplished during handover mechanism

- Handoff Initiation stage: Signal strength, link quality etc initiated the handover procedure.
- System discovery stage: Discovering the neighbor networks, sharing Quality of Service (QoS) information offered by these networks.
- Handover Decision stage: Comparing QoS of all available networks leads the user toward best network selection.
- Handoff Execution stage: Relinquishing old and establishing new connection and security services is done in this phase [1].

FGHWN are the result of overlapping of diverse wireless networks. The heterogeneity of FGHWN needs the realization of a vertical authentication method that trim down the handover delay whereas safeguarding the security perspective of the enduring communication. To uphold the continuing connections still after the home network is no longer accessible, vertical handover methods must be put into practice. Today, subscribers turn into additional challenges in conditions of omnipresent services availability and security. Furthermore, the installed fourth generation (4G) networks are illustrated by several wireless access networks expertise. To assure availability at the same time as preserving the security level, operators and service providers be supposed to harmonize and facilitate a mobile subscriber steadily using the services he is subscribed to regardless of his position and the access network expertise that is obtainable in his region, for which novel inter-networks roaming and vertical handover means ought to be cleared. To provide effective mobility with security all generation technologies (2G, 3G, and 4G) should be interoperable to facilitating the subscribers with ubiquitous wireless communication with high data rates. In case of loose coupling between WiMAX and WiFi networks operators have to describe supplementary mechanisms to implement network intelligence be capable to execute vertical handovers, as WiFi networks are incapable of management. In case of tight coupling, WiMax apparatus will be utilized to tackle subscribers' mobility and seamless connection shift, as they are capable of intelligent management [5].

II. LITERATURE REVIEW

In this paper the author's K.Savitha et al illustrated three different designs namely centralized, distributed and trusted distributed for vertical handoff decision, by means of three parameters; Throughput, Decision Processing and End-End delay [1]. The strength of the paper is that, it validates that among the each outcome of all the three designs the trusted distributed for vertical handoff decision having best performance among all. The limitation of the paper is that, a lot of delay time both in decision processing and End-End transmission. Secondly, there are many inappropriate judgments attempted by the mobile nodes to decide their target network due to data flooding which leads to network congestion.

In this paper the author's Bao Guo et al compared and contrast two schemes (Encrypt-and-MAC, Encrypt- then-MAC) to achieve the confidentiality and integrity for the Short Message Services Networks [2]. The Encrypt-and-MAC scheme using CTR and CMAC modes while Encrypt-then-MAC scheme using EAX mode, both characterize by AES. Strength of the paper is that, output of each scheme in terms of operation time is almost similar but the Encrypt-then-MAC scheme offer more assurance, because appending MAC of the encrypted plaintext. Secondly Encrypt-then-MAC scheme also demonstrating best performance during online processing's. The limitation of paper is that, implementation of transmitter flow (SE/ES) will create the I/O obstruction if input data is increased. Secondly, Python 2.6 executables codes functionality is platform restricted.

In this work the author's Jakub Szefer et al suggested a flexible hardware mechanism (FPGA) that facilitates in time operations for encryption and hashing algorithms [3]. Strength of the paper is that, the Design is compatible with any portable devices and sensor nodes. Secondly, its implementation doesn't compromise its performance at the cost of its area and time [3]. Thirdly, the design can be used for other security services not just ciphering and hashing. Limitations of the paper are that, the mechanism of the FPGA policy is fixedly predefined. Secondly mechanism is adjustable with a limited and fixed quantity of Parameters. Thirdly, its efficiency is variable for cipher-to-cipher or hash-to-hash; maximum for whirlpool and block ciphers.

In this paper the author's wafaa bou diab et al proposed a new Seamless vertical handover solution for real-time data transfer with fast authentication. while analyzing the results with conventional schemes in terms of signaling cost (handover and authentication) and packet loss [4] It proved better results than its predecessor (IMS, MIPv6, FMIPv6) although quality and security services both maintained. Strength of the paper is that, it decreased the number of authentication messages, because both handover and authentication amalgamated in a single message, which reduced handoff latency as well. Resultantly the chances of packet loss also diminished. The limitation of the paper is that, this model is very sensitive to packet loss. Any loss of packet will lead to miss-synchronization, resultantly either to reinstate a new security association or roll back to the initial state.

In this paper the author's Neila KRICHENE et al discussed a vertical authentication method among the GSM, UMTS, WiFi and WiMAX technologies, regardless of any previous subscription to the visited network [5]. Strength of the paper is that, the authors proposed a global authentication protocol authorizing vertical handover between 4G architecture networks and proved the strength of the protocol against man-in-the-middle and denial of service attacks during vertical handover. The limitation of the paper is that, this protocol is only compatible with mesh topology 4G networks and does not bother for Quality of Service.

In this paper the author's Ahmed H. Zahran et al described a broker-based design for integrated heterogeneous networks to enhance the vertical handoff management, utilizing novel resource query method for Media Independent Handover [6]. The strength of the paper is that, it focuses on the decline in signaling load, MT configuration time, power consumption, user authentication delay, VHO delay, and the probability of VHO interruption, although guarantying seamless transitions as well. The limitation of the paper is that, almost all of its work is least cited which degrade its authenticity.

In this paper the author's Ali Al Shidhani et al put forward two re-authentication protocols (FUAR,LFR) comparing them to existing protocols(EAP-AKA, UMTS-AKA) in the 3G Home Networks [7]. The strength of the paper is that, It considerably spawning less signaling traffic and enduring less delay, accomplishing secured key management and mutual authentication, demanding no adjustments to the interworking architecture. The limitations of the paper is that,FAUR's security and performance depends upon the lifetime of security keys (TK, nCK, nIK).while security keys neither can be shared nor it can be reused, one time the session expired. The paper only focused on 3G networks

In this paper the author's Hoyeon Lee et al, have done efforts to enhance SIP, for vertical handover design (WiFi-to-UMTS) to reduce the IMS delay, comparing the results with conventional SIP [8].The strength of the paper is that, it enabling make-before-break vertical handover for IMS, successfully defined and operated two new headers in SIP, as sustaining for delay-sensitive real time applications, presenting compatibility with traditional. The limitation of the paper is that, it does not bother about the Layer 2 and 3 handover latency, secondly neglecting the forecasted troubles due to increase in header size.

In this paper the author's Jaeho Jo et al have focused on vertical handover via layer 2 and layer 3 signaling messages connecting mobile WiMAX and 3G networks [9].

The strength of the paper is that, it sort out L2 and L3 signaling messages as merging them resultantly limiting handover latency and UDP packet loss ratio while enhancing the TCP throughput. The limitation of the paper is that, it implemented the idea of predictive mode fast handover in which chances of failure are always open.

In this paper the author's chan-Kyu Han et al, assessed the signaling load, authentication procedures and compatibility of vertical handover in the EPS architecture networks [10]. The strength of the paper is that, it introduces the EPS network release 8 concentrating on security, secondly allowing random processes in authentication arrival, thirdly discovering new authentication generation processes other than routine, fourthly enhancing authentication signals as required. Limitations of the paper are that, mandatory parameters like mobility organization, security strategies, and a variety of haphazard arrival processes are ignored in the current model.

In this paper the author's Liming Hou et al, introduced a pre-authentication design, based on the EAPTLS protocol, between WiFi and WiMAX hybrid networks, comprises of two stages; pre-authentication and re-authentication [11]. Strength of the paper is that, authentication delay is considerably reduced, while introducing pre-authentication stage. The design can be used for real time services as well. Limitation of the paper,EAPTLS is based on a public key infrastructure for its authentication, which reduces its portability.

In this paper the author Mario Marchese, integrate the interconnection and (Delay Tolerant Networks) DTN gateways architectures for wireless ubiquitous networks [12]. The strength of the paper is that, it shared successfully the functionalities of QoS mapping, and resource control from interconnection Gateways while extended delays and momentary link unavailability from DTN Gateways. The limitation of the paper is that, essential functionalities like well-organized mobility operates on broad territory coverage and guarantee of end-to-end data deliverance for elongated delay corridor and momentary link distraction are ignored.

In this paper the author Shih-Jung Wu specify (Host Identity Protocol) HIP-based vertical handover scheme via integrated architecture for seamless mobility of diverse wireless networks [13]. The strength of the paper is that, it used effectively HIP to tackle the problems of mobility and multi-homing while Diameter Protocol for registered users authentication. Limitations of the paper is that, as the local scope identifier (LSI) is a 32-bit identifier of host identity which is incompatible for IPv6 so collision probability is enviable, and its scope will be also controlled. Lastly results are not simulated or proved.

In this paper the author's Gabriele Tamea et al have provided an algorithm which makes its vertical handover decision on the basis of probability to avoid ping-pong effect [14]. Strength of the paper is that, the suggested algorithm evaluating the (WDP) wrong decision probability on the basis of: improving the collective goodput, and dropping of redundant and needless vertical handovers (PPE), was empowering the Mobile Terminal (MT) for the commencement and restriction of VHO that is why it is distinct as a Mobile Terminal-Controlled Handover scheme. Limitations of the paper is that, it didn't bother other estimations of good put , and analysis of its correlation at different intervals.

In this paper the author's Pedro J. Fern´andez Ruiz et al, portrayed a testbed setup installed over inter and intra technology vertical handover (WiFi,WiMAX and UMTS) to testify the secure mobility on vehicular networks [15]. Strength of the paper is that, it successfully experienced the authentication process on vehicular networks using IKEv2 and EAP3 for dynamic IP allocation and authentication respectively, exclusive of losing connectivity. Limitation of the paper is that, due to vehicular network there must be overlapping and no overlapping zones for which the selection and authentication procedures are not discussed.

III. Critical Analysis

TABLE 1.

Author	Working	Problems	Solution
K.Savitha et al	Validates that the trusted distributed for vertical handoff decision having best performance among all.	Delay time both in decision processing, End-End transmission, many inappropriate judgments which lead to network congestion.	By replacing the reactive routing protocol, Ad hoc On Demand Distance Vector (AODV) with a proactive routing protocol like, Highly Dynamic Destination-Sequenced Distance Vector routing protocol (DSDV), to reduce the delay time.
Bao Guo et al	Encrypt-then-MAC scheme offer more assurance, because appending MAC of the encrypted plaintext.	Implementation of transmitter flow (SE/ES) will create the I/O obstruction if input data is increased. Python 2.6 executables codes functionality is platform restricted.	If we implement MAC-then-encrypt scheme, will enhance security services. And if python 2.6 is replaced by PERL or ruby programming language then the platform independence issue will also be resolved
Jakub Szefer et al	The Design is compatible with any portable devices and sensor nodes. Its implementation doesn't compromise its performance at the cost of its area and time. The design can be used for other security services not just ciphering and hashing.	The mechanism of the FPGA policy is fixedly predefined. Mechanism is adjustable with a limited and fixed quantity of Parameters. Its efficiency is variable for cipher-to-cipher or hash-to-hash; maximum for whirlpool and block ciphers.	We can design FPGA user defined while assigning unlimited parameters according to the need and situation dynamically.
wafaa bou diab et al	It decreased the number of authentication messages, because both handover and authentication amalgamated in a single message, which reduced handoff latency as well. Resultantly the chances of packet loss also diminished.	This model is very sensitive to packet loss. Any loss of packet will lead to miss-synchronization, resultantly either to reinstate a new security association or roll back to the initial state.	A mechanism can be introduced so that, on each and every mobile node SCID (Session Context ID) routing table should be fully updated with full header packets rather only destination IP addresses.
Ali Al Shidhani et al	It considerably spawning less signaling traffic and enduring less delay, accomplishing secured key management and mutual authentication,	FAUR's security and performance depends upon the lifetime of security keys (TK,nCK,,nIK).while security keys	Consequence of additional security keys for each session is required to be investigated. Proper confirmation of the security and

	demanding no adjustments to the interworking architecture.	neither can be shared nor it can be reused, one time the session expired. The paper only focused on 3G networks	performance of FUAR will be carried out with constraint of life time.
Hoyeon Lee et al	It enabling make-before-break vertical handover for IMS, successfully defined and operated two new headers slots in SIP.	It does not bother about the Layer 2 and 3 handover latency, secondly neglecting the forecasted troubles due to increase in header size.	Large bandwidth allocation to solve the header size problem.
Jaeho Jo et al	It sort out L2 and L3 signaling messages as merging them resultantly limiting handover latency and UDP packet loss ratio while enhancing the TCP throughput.	It implemented the idea of predictive mode fast handover in which chances of failure are always open.	predictive mode can be replaced with reactive mode fast handover
chan-Kyu Han et al	Allowing random processes in authentication arrival, discovering new authentication generation processes other than routine, enhancing authentication signals as required.	Parameters like mobility organization, security strategies, and a variety of haphazard arrival processes are ignored in the current model.	Several features like haphazard walk mobility model, associations with every authentication activation and different random process generation are to be examined for the compatibility with the real world scenarios.
Liming Hou et al	Authentication delay is considerably reduced, while introducing pre-authentication stage. The design can be used for real time services as well.	EAPTLS is based on a public key infrastructure for its authentication, which reduces its portability.	we can replace the protocol by any other of EAP family member like EAP-MD5, EAP-OTP, EAP-GTC, EAPTLS and EAP-SIM etc.
Mario Marchese	It shared successfully the functionalities of QoS mapping, and resource control from interconnection Gateways while extended delays and momentary link unavailability from DTN Gateways.	Essential functionalities like well-organized mobility operates on broad territory coverage and guarantee of end-to-end data deliverance for elongated delay corridor and momentary link distraction are ignored.	A novel illumination relating to architectures and protocols is obligatory
ih-Jung Wu	It used effectively HIP to tackle the problems of mobility and multi-homing while Diameter Protocol for registered users authentication.	As the local scope identifier (LSI) is a 32-bit identifier of host identity which is incompatible for IPv6 so collision probability is enviable, and its scope will be also controlled. Lastly results are not simulated or proved.	Its results should be simulated so that to assess its presentation and should also be compared with its predecessor work.
Gabriele Tamea et althe	Improving the collective good put, and dropping of redundant and needless vertical handovers (PPE),empowering the Mobile Terminal (MT) for the commencement and restriction of VHO	It didn't bother other estimations of good put, and analysis of its correlation at different intervals.	To include the other goodput parameters and enhance correlation among them.
Pedro J. Fern´andez Ruiz et al	it successfully experienced the authentication process on vehicular networks using IKEv2 and EAP3 for dynamic IP allocation and authentication respectively, exclusive of losing connectivity.	As it is vehicular network there must be overlapping and no overlapping zones, for which the selection and Authentication procedures are not discussed.	To set pre-established security and mobility policy that will allow the user to opt the appropriate interface in each and every situation.

IV. Proposed Solution

The above observations reveal that many schemes were introduced but all of them have deficiencies. Hand over process takes time in address acquisition and on time calculations which increases latency and hence leads to packet loss. For fast and smooth hand over between homogeneous and heterogeneous networks, a modified and fast hand over mechanism always needed. Hand over is more critical in some conditions like in ad hoc networks such as MANETs and VANETs. In ad hoc networks the hand off need very few time for changing point of attachment to the access point and with routers as mobile nodes move very fast. The horizontal handover between different network such as WiFi, WIMax, UMTS also leads latency and packet loss. Latency created in the hand over process because the difference in the band width. When a node leaves from one network and inters into the premises of another network such as from WiFi to WiMax, the difference between band widths leads latency. The queue becomes full at the bridge of the network and waiting packets feel delay in term of latency and as a result all this lead to packet loss. In horizontal hand over on time calculations also takes timing to change from point to point.

The Standard IEEE 802.11 Handover process of consist into following six phases: triggering, discovery, authentication, association, IP address acquisition, and home agent (HA) registration [16]. The first four phases related to the data link layer and called layer two (L2) while the last two phases done it the network layer and called layer three (L3) handover [17]. In the whole process there is on time calculation and awake the moment of the mobile node. The moment of the mobile node from one network premises to another continuously monitor from its Received Signal Strength Indicator (RSSI) value. When RSSI value decrease in area the mobile node start scanning for other network having better RSSI value. IEEE 802.11 had over two types of scan modes are define: active scan and passive scan. In active scanning, the MN transmits a probe request massage on a channel and then waits for a while. If no response from other side, mobile node continues to sends a probe massage on the next channel and wait for response from other access router. While in passive scanning, the mobile node sequentially listens to beacons on different channels instead of transmitting massages for request. When mobile node listen all the channel, it choose a channel with better RSSI value and start massages to shift from one access router to another.

In our proposed scheme passive scanning mode, the mobile node start hand over procedure rather network. Nearly all parameters are set prior starting the connection establishment of new connection with another access router. While some very necessary calculation still performed at time of changing access routers.

In the proposed scheme total focus is on proactive mechanism rather than reactive all time. Proactive means much of the work been done by the system before actually hand over been starting. First, when mobile node experience weak RSSI value, it starts searching for better RSSI network value. The mobile node starts discovery and section for new access routers. Once the mobile is performed authentication to entering at premises of the new network. Then no need for re-authentication, when changing from one access point to other (horizontal handover). At the association process the mobile node define itself prior to association and almost all massages shared between new router and mobile node.

Therefore for a mobile node tack very little time to associate with access router. After association the mobile node trying to get new IP address. Two variations either Router Advertisement messages are periodically broadcasted by new router or the mobile node sends Router Solicitation messages to new router to obtain the Router Advertisement messages. Care of Address (CoA) has been assign to mobile node for time being, duplication address detection (DAD) process ensure unique addresses in the same network premises. When a mobile node obtains its CoA in new network then mobile node informs it's Home Agent about the new CoA by sending a binding update message to home agent. The home agent also sends a binding acknowledgement massages to the mobile node to complete the process [18].

The standard scheme shows that latency turn outs because of the on board calculation. Nearly all schemes needs on time calculations for completing the hand over procedure. But these calculations can be decrease by dividing the whole process into two parameters. Some necessary parameters are still calculated on time but most of the parameters should set before the actual process being start.

The proactive mechanism reduces the delay in term of reducing latency. Reactive mechanisms are applied when some parameters need some on line calculating values otherwise the proactive mechanism. Proactive mechanisms reduce the hand over latency by applying pre-define parameters values. Proactive parameters including pre-define calculations by the mobile node for smooth roaming in the same network with different access points or roaming between different routers of the different networks, pre-define pool of address for mobile nodes which decrease on time calculation for address acquisition and duplication address detection.

V. Conclusion And Future Work

While evaluating all the above mentioned work it can be concluded that almost all of the time reactive protocols are used when a node shift from one entrance point to a new one, while executing estimations in terms of handover and authentication. As handover massages are exchanged, the actual data packets experiences extensive average delay, which amplify latency and lastly leads to packet loss in few cases. In our proposed scheme, a few parameters will be pre-defined, which will assist in calculation at hand over process. The proposed scheme will be helpful as it is based on preceding standard approaches with improvements. The proposed elucidation will be a hybrid approach of reactive and proactive.

Aknowledgment

We are very thankful to Almighty Allah; whose grace and blessed mercy enabled us to complete this work with full devotion and legitimacy. We are grateful to Mr. Mohammad Ibrahim, Lecturer in Computer Science, Virtual University of Pakistan, for their invaluable support and guidance throughout this research work. We also want to thank our friends and family for their encouragement; without whose support we could not have lived through this dream of ours.

References

[1] K.Savitha and Dr.C.Chandrasekar "VERTICAL HANDOFF DECISION SCHEMES IN HETEROGENEOUS WIRELESS NETWORK USING MADM", JGRCS 1(5), December 2010, 16-20.

[2] Bao Guo and William Emmanuel Yu "Comparison between Encrypt-and-MAC Composite (CMAC CTR) and Encrypt-then-MAC Composite (AES EAX) Modes of Operation in Cryptography Systems for Use in SMS-based Secure Transmission". Proceedings of the international multi conference of Engineers and Computer Scientists 2011 Vol I, IMECS 2011 March 16-18, 2011, Hong Kong.

[3] Jakub Szefer, Yu-Yuan Chen and Ruby B. Lee "General-Purpose FPGA Platforms for Efficient Encryption and Hashing"

[4] Wafaa Bou Diab and Samir TohmeSeamless "Handover and Security Solution for Real-Time Services" 2009 11th IEEE International Symposium on Multimedia 978-0-7695-3890-7/09 $26.00 © 2009 IEEE

[5] Neila KRICHENE and Noureddine BOUDRIGA "Securing roaming and vertical handover in fourth generation networks "Third International Conference on Network and System Security" 978-0-7695-3838-9/09 $26.00 © 2009 IEEE

[6] Ahmed H. Zahran and Cormac J. Sreenan "Extended Handover Keying and Modified IEEE 802.21 Resource Query Approach for Improving Vertical Handoff Performance" 978-1-4244-8704-2/11/$26.00 ©2011 IEEE

[7] Ali Al Shidhani and Victor C. M. Leung "Reducing Re-authentication Delays during UMTS-WLAN Vertical Handovers "978-1-4244-2644-7/08/$25.00 ©2008 IEEE

[8] Hoyeon Lee, Bongkyo Moon, and A. H. Aghvami "Enhanced SIP for Reducing IMS Delay under WiFi-to-UMTS Handover Scenario The Second International Conference on Next Generation Mobile Applications, Services, and Technologies "978-0-7695-3333-9 /08 $25.00 © 2008 IEEE

[9] Jaeho Jo and Jinsung Cho "A Cross-layer Vertical Handover between Mobile WiMAX and 3G Networks"978-1-4244-2202-9/08/$25.00 © 2008 IEEE

[10] Chan-Kyu Han, Hyoung-Kee Choi,Jung Woo Baek, Ho Woo Lee "Evaluation of Authentication Signaling Loads in 3GPP LTE/SAE Networks"2009 IEEE 34th Conference on Local Computer Networks (LCN 2009) Zürich, Switzerland; 20-23 October 2009 978-1-4244-4487-8/09/$25.00 ©2009 IEEE [11] LimingHou and Kai X.

[11] Miao "A Pre-authentication Architecture in WiFi & WiMAX Integrated System.

[12] Mario Marchese, "Wireless Pervasive Networks for Safety Operations and Secure Transportations" IEEE 2010 International Symposium on Wireless Pervasive Computing (ISWPC)

[13] Shih-Jung Wu "A New Integrated Mobile Architecture for Heterogeneous Wireless Networks 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing" 2010 IEEE.

[14] Gabriele Tamea, Anna Maria Vegni, Tiziano Inzerilli, Roberto Cusani "A Probability based Vertical Handover Approach to Prevent Ping-Pong Effect" ISWCS 2009.

[15] Pedro J. Fern´andez Ruiz Cristian A. Nieto Guerra Antonio F. G´omez Skarmeta "Deployment of a Secure Wireless Infrastructure oriented to Vehicular Networks 2010 24th IEEE International Conference on Advanced Information Networking and Applications "

[16] Daehan Kwak, Jeonghoon Mo, Moonsoo Kang, "Investigation of Handoffs for IEEE 802.11 Networks in Vehicular Environment".

[17] Yao-Tung Chang, Jen-Wen Ding, Jen-Wen Ding, Ing-Yi Chen. "A Survey of Handoff Schemes for Vehicular Ad-Hoc Networks".

[18] R. Koodli, Ed. "Mobile IPv6 Fast Handovers", Request for Comments: 5268 Starent Networks Obsoletes: 4068 June 2008.

Authors Profile

Mohammad Faisal received his B.S. degree in Computer Science (Hons) from University of Malakand at Chakdara, Dir lower, KPK, Pakistan. He is currently pursuing his MS in Information Security management system at Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology (ZABIST) Islamabad Pakistan. Since November 2006, he is working as Network Engineer in Pakistan Revenue Automation Limited (PRAL), Motorway Department.
His research areas focuses on Handoff, forensics, cryptography and networks (SENSOR, WIRELSS, MANETS) security. He intended to precede his studies (PhD) in any of the above mentioned fields.

Muhammad Nawaz Khan is lecturer in Computer Science in Govt. College of Management Science. In 2008, he received Silver Medal in B.S. (Hons) degree in Computer Science from University of Malakand, K.P.K. Pakistan. He partially completed MS in Computer Communication Security at School of Electrical Engineering & Computer Science (SEECS), National University of Science & Technology (NUST) Islamabad, Pakistan. In 2010, he worked as a Research Assistant in a project on "Distributed Computing" supported by Higher Education Commission of Pakistan. Currently he is working as Research Assistant at Shaheed Zulfikar Ali Bhutto Institute of Science & Technology Islamabad. His research is focused on Computer Information Security especially Computer Communication Security. He has also showed keen interest in Ad-hoc networks (MANETs, VANETs), wireless communications security and security related issues in distributed computing. He intended to proceed his studies (PhD) in any of the above mentioned fields.