A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks

K.P.Manikandan
HOD/MCA
Chirala Engineering College
Chirala-523157.A.P. India
+919908847047
manikandankp@yahoo.com

Dr.R.Satyaprasad
CSE Department
Achariya Nagarjuna University
Nagarjuna Nager-522 510,A.P.,India
+919848487478
profrsp@gmail.com

Dr.K.Rajasekhararao
PRINCIPAL
KL University
Vadeshwaram-522502,A.P.,India
+919848452344
krr_it@yahoo.co.in

***Abstract*-A Mobile Ad hoc Network (MANET) is a dynamic wireless network that can be formed infrastructure less connections in which each node can act as a router. The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. Although the ongoing trend is to adopt ad hoc networks for commercial uses due to their certain unique properties, the main challenge is the vulnerability to security attacks. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. Different mechanisms have been proposed using various cryptographic techniques to countermeasure the routing attacks against MANET. As a result, attacks with malicious intent have been and will be devised to exploit these vulnerabilities and to cripple the MANET operations. Attack prevention measures, such as authentication and encryption, can be used as the first line of defense for reducing the possibilities of attacks. However, these mechanisms are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. In this paper, we identify the existent security threats an ad hoc network faces, the security services required to be achieved and the countermeasures for attacks in routing protocols. To accomplish our goal, we have done literature survey in gathering information related to various types of attacks and solutions. Finally, we have identified the challenges and proposed solutions to overcome them. In our survey, we focus on the findings and related works from which to provide secure protocols for MANETs. However, in short, we can say that the complete security solution requires the prevention, detection and reaction mechanisms applied in MANET.**

Keywords- MANET; Routing Protocol; Security Attacks; Routing Attacks and Defense Metrics

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is an autonomous system that consists of a variety of mobile hosts forming temporary network without any fixed infrastructure. Since it is difficult to dedicate routers and other infrastructure in such network, all the nodes are self-organized and collaborated to each other. All the nodes as well as the routers can move about freely and thus the network topology is highly dynamic. Due to self-organize and rapidly deploy capability, MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive computing environments. There are 15 major issues and sub-issues involving in MANET [10] such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. The routing protocol sets an upper limit to security in any packet network. If routing can be misdirected, the entire network can be paralyzed. The problem is enlarged by the fact that routing usually needs to rely on the trustworthiness of all the nodes that are participating in the routing process. It is hard to distinguish compromised nodes from nodes that are suffering from bad links.

The main objective of this paper is to discuss ad hoc routing security with respect to the area of application.

II. ROUTING PROTOCOLS IN MANETS

Many protocols have been proposed for MANETs. These protocols can be divided into three categories: *proactive, reactive, and hybrid*. Proactive methods maintain routes to all nodes, including nodes to which no packets are sent. Such methods react to topology changes, even if no traffic is affected by the changes. They are also called table-driven methods. Reactive methods are based on demand for data transmission. Routes between hosts are determined only when they are explicitly needed to forward packets. Reactive methods are also called on-demand methods. They can significantly reduce routing overhead when the traffic is lightweight and the topology changes less dramatically, since they do not need to update route information periodically and do not need to find and maintain routes on which there is no traffic. Hybrid methods combine proactive and reactive methods to find efficient routes, without much control overhead.

A. Proactive Routing Protocols

Proactive MANET protocols are table-driven and will actively determine the layout of the network. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology propagating updates throughout the network in order to maintain a consistent network view.

The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. Examples of proactive MANET protocols include Optimized Link State Routing (OLSR)[11], Topology Broadcast based on Reverse Path Forwarding (TBRPF)[12], Fish-eye State Routing (FSR)[13], Destination-Sequenced Distance Vector (DSDV)[14], Landmark Routing Protocol (LANMAR)[15], Cluster head Gateway Switch Routing Protocol (CGSR)[16].

B. Reactive Routing Protocols

Reactive protocols are on- demand protocols, create routes only when desired by source nodes. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined. Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired. Examples of reactive MANET protocols include Ad Hoc On-Demand Distance Vector (AODV) [17], Dynamic Source Routing (DSR) [18], Temporally Ordered Routing Algorithm (TORA) [19], and Dynamic MANET On Demand (DYMO) [20].

C. Hybrid Routing Protocols

Since proactive and reactive routing protocols each work best in oppositely different scenarios, there is good reason to develop hybrid routing protocols, which use a mix of both proactive and reactive routing protocols. These hybrid protocols can be used to find a balance between the proactive and reactive protocols.

The basic idea behind hybrid routing protocols is to use proactive routing mechanisms in some areas of the network at certain times and reactive routing for the rest of the network. The proactive operations are restricted to a small domain in order to reduce the control overheads and delays. The reactive routing protocols are used for locating nodes outside this domain, as this is more bandwidth-efficient in a constantly changing network. Examples of hybrid routing protocols include Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR) [21], Zone Routing Protocol (ZRP) [22], and Zone Based Hierarchical Link State Routing Protocol (ZHLS) [23].

D. Proactive vs. Reactive vs. Hybrid Routing

The tradeoffs between proactive and reactive routing strategies are quite complex. Which approach is better depends on many factors, such as the size of the network, the mobility, the data traffic and so on. Proactive routing protocols try to maintain routes to all possible destinations, regardless of whether or not they are needed. Routing information is constantly propagated and maintained. In contrast, reactive routing protocols initiate route discovery on the demand of data traffic. Routes are needed only to those desired destinations. This routing approach can dramatically reduce routing overhead when a network is relatively static and the active traffic is light. However, the source node has to wait until a route to the destination can be discovered, increasing the response time.

The hybrid routing approach can adjust its routing strategies according to a network's characteristics and thus provides an attractive method for routing in MANETs. However, a network's characteristics, such as the mobility pattern and the traffic pattern, can be expected to be dynamic. The related information is very difficult to obtain and maintain.

This complexity makes dynamically adjusting routing strategies hard to implement.

III. TYPES OF SECURITY ATTACKS

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors.

The security attacks in MANET can be roughly classified into two major categories, namely passive attacks and active attacks. The active attacks further divided according to the layers.

A. Passive Attacks

A passive attack does not disrupt the normal operation of the network; the attacker snoop's the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, and thereby making it impossible for the attacker to get useful information from the data overhead.

1) Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

2) Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

B. Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks.

Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

IV. Types Of Routing Attacks And Defense Metrics On Manet

A. Routing Attacks

An attacker can absorb network traffic, inject themselves into the path between the source and destination and thus control the network traffic flow. For example, as shown in the *fig 1(a) and (b)*, a malicious node ***M*** can inject itself into the routing path between sender ***S*** and receiver ***R***.

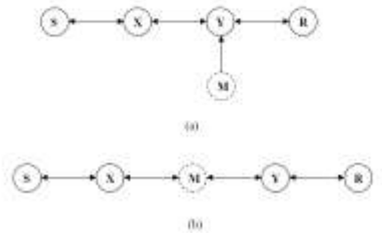

Figure 1: Routing attack

Network layer vulnerabilities fall into two categories: routing attacks and packet forwarding attacks [5]. The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocols. The specific attack behaviors are related to the routing protocol used by the MANET.

The venomous routing nodes can attacks in MANET using dissimilar ways, so that, the following subsections are discussed various issues of routing attacks and its defense methods to mitigating route security attacks vulnerability on MANET.

B. Types of Routing Attacks

1) Routing Table Overflow Attack

This attack is basically happens to proactive routing algorithms, which update routing information periodically. To launch routing table overflow attack, the attacker tries to create routes to nonexistent nodes to the authorized nodes present in the network. It can simply send excessive route advertisements to overflow the target system's routing table. The goal is to have enough routes so that creation of new routes is prevented or the implementation of routing protocol is overwhelmed.

2) Routing Table Poisoning

Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. Routing table poisoning may result in suboptimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

3) Packet Replication

In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

4) Rushing Attack

On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. An adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes which also receive the same Route Request packet can react. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks [3].

5) Routing Cache Poisoning Attack

Routing cache poisoning attack uses the advantage of the promiscuous mode of routing table updating. This occurs when information stored in routing tables is either deleted, altered or injected with false information. Suppose a malicious node ***M*** wants to poison routes node to ***X***. ***M*** could broadcast spoofed packets with source route to ***X*** via ***M*** itself, thus neighboring nodes that overhear the packet may add the route to their route caches [6].

C. Attacks on Specific Routing Protocol

There are many attacks in MANET that target the specific routing protocols. This is due to developing routing services without considering security issues. Most of the recent research suffers from this problem. In this section, we describe about the security threats, advantage and disadvantage of some common routing protocols.

1) AODV

The Ad-hoc On-demand Distance Vector (AODV) routing algorithm is a reactive algorithm that routes data across wireless mesh networks. The advantage of AODV is that it is simple, requires less memory and does not create extra traffic for communication along existing links. In AODV [2], the attacker may advertise a route with a smaller distance metric than the original distance or advertise a routing update with a large sequence number and invalidate all routing updates from other nodes.

2) DSR

Dynamic Source Routing (DSR) protocol is similar to AODV in that it also forms route on-demand. But the main difference is that it uses source routing instead of relying on the routing table at each intermediate node. It also provides functionality so that packets can be forwarded on a hop-by-hop basis. In DSR, it is possible to modify the source route listed in the RREQ or RREP packets by the attacker. Deleting a node from the list, switching the order or appending a new node into the list is also the potential dangers in DSR.

3) ARAN

Authenticated Routing for Ad-hoc Networks (ARAN) is an on-demand routing protocol that detects and protects against malicious actions carried out by third parties and peers in particular ad-hoc environment [4]. This protocol introduces authentication, message integrity and non-repudiation as a part of a minimal security policy. Though ARAN is designed to enhance ad-hoc security, still it is immune to rushing attack.

4) ARIADNE

ARIADNE is an on-demand secure ad-hoc routing protocol based on DSR that implements highly efficient symmetric cryptography. It provides point-to-point authentication of a routing message using a message authentication code (MAC) and a shared key between the two communicating parties. Although ARIADNE is free from a flood of RREQ packets and cache poisoning attack, but it is immune to the wormhole attack and rushing attack [3].

5) SEAD

Specifically, SEAD builds on the DSDV-SQ version of the DSDV (Destination Sequenced Distance Vector) protocol. It deals with attackers that modify routing information and also with replay attacks and makes use of one-way hash chains rather than implementing expensive asymmetric cryptography operations. Two different approaches are used for message authentication to prevent the attackers. SEAD does not cope with wormhole attacks [3].

D. Advanced Attacks

1) Wormhole attack

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole [1].

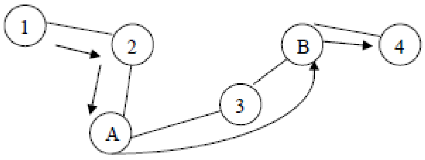

Figure 2: Wormhole attack

2) Blackhole attack

The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV [1], to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

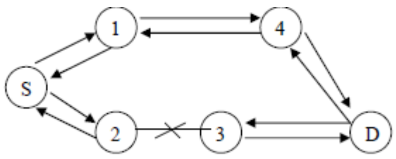

Figure 3: Blackhole attack [1]

3) Byzantine attack

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services [3].

4) Rushing Attack

In wormhole attack, two colluded attackers form a tunnel to falsify the original route. If luckily the transmission path is fast enough (e.g. a dedicated channel) then the tunneled packets can propagate faster than those through a normal multi-hop route, and result in the rushing attack. Basically, it is another form of denial of service (DoS) attack that can be launched against all currently proposed on-demand MANET routing protocols such as ARAN and Ariadne [3] [8].

5) Resource Consumption Attack

Energy is a critical parameter in the MANET. Battery-powered devices try to conserve energy by transmitting only when absolutely necessary [7]. The target of resource consumption attack is to send request of excessive route discovery or unnecessary packets to the victim node in order to consume the battery life. An attacker or compromised node thus can disrupt the normal functionalities of the MANET. This attack is also known as sleep deprivation attack.

6) Location Disclosure Attack

Location disclosure attack is a part of the information disclosure attack. The malicious node leaks information regarding the location or the structure of the network and uses the information for further attack. It gathers the node location information such as a route map and knows which nodes are situated on the target route. Traffic analysis is one of the unsolved security attacks against MANETs.

E. Defense Metrics against Routing Attacks in MANET

Network layer is more vulnerable to attacks than all other layers in MANET. A variety of security threats is imposed in this layer. Use of secure routing protocols provides the first line of defense. The active attack like modification of routing messages can be prevented through source authentication and message integrity mechanism. For example, digital signature, message authentication code (MAC), hashed MAC (HMAC), one-way HMAC key chain is used for this purpose. By an unalterable and independent physical metric such as time delay or geographical location can be used to detect wormhole attack. For example, packet leashes are used to combat this attack [9]. IPSec is most commonly used on the network layer in internet that could be used in MANET to provide certain level of confidentiality. The secure routing protocol named ARAN protects from various attacks like modification of sequence number, modification of hop counts, modification of source routes, spoofing, fabrication of source route etc [4]. The research by Deng [7], et al presents a solution to overcome blackhole attack. The solution is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node.

V. Related Work

The major task of the routing protocol is to discover the topology to ensure that each node can acquire a recent map of the network to construct routes to its destinations. Several efficient routing protocols have been proposed for MANET.

These protocols generally fall into one of the two major categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as Ad hoc On Demand Distance Vector (AODV) protocol [2], nodes find routes only when they must send data to the destination node whose route is unknown. In contrast, in proactive routing protocols, such as OLSR [11], nodes obtain routes by periodic exchange of topology information with other nodes and maintain route information all the time. Based on the behavior of attackers, attacks against MANET can be classified into passive or active attacks. Attacks can be further categorized as either outsider or insider attacks. With respect to the target, attacks could be also divided into data packet or routing packet attacks. In routing packet attacks, attackers could not only prevent existing paths from being used, but also spoof non-existing paths to lure data packets to them. Several studies [1],[2],[24], [25], [26] have been carried out on modeling MANET routing attacks. Typical routing attacks include black-hole, fabrication, and modification of various fields in routing packets (route request message, route reply message, route error message, etc.). Some research efforts have been made to seek preventive solutions [8], [27],[28] for protecting the routing protocols in MANET. Although these approaches can prevent unauthorized nodes from joining the network, they introduce a significant overhead for key exchange and verification with the limited intrusion elimination. Besides, prevention-based techniques are less helpful for defending from malicious insiders who possess the credentials to communicate in the network.

Numerous intrusion detection systems (IDS) for MANET have been recently introduced. Due to the nature of MANET, most IDS are structured to be distributed and have a cooperative architecture. Similar to signatured-based and anomaly based IDS models for wired network; IDS for MANET use specification-based approaches and statistics-based approaches. Specification-based approaches, for example DEMEM [30], C. Tseng et al. [29] and M. Wang et al. [32], monitor network activities and compare them with known attack features, which are impractical to cope with new attacks. On the other hand, statistics-based approaches, such as Watchdog and Lipad , compare network activities with normal behavior patterns, which result in higher false positives rate than specification-based ones. Because of the existence of false positives in both MANET IDS models, intrusion alerts from these systems always accompany with alert confidence, which indicates the possibility of attack occurrence. Intrusion response systems (IRS) for MANET are inspired by MANET IDS [31] isolate malicious nodes based on their reputations. Their work fails to take advantage of IDS alerts and simple isolation of nodes may cause unexpected network partition [33] brings the concept of cost-sensitive into MANET intrusion response which considers topology dependency and attack damage. The advantage of our solution is that we integrate evidences from IDS, local routing table with expert knowledge to estimate risk of attacks, and countermeasures with a mathematical reasoning approach.

VI. Conclusion

Mobile Ad Hoc Networks have the ability to setup networks on the fly in a harsh environment where it may not possible to deploy a traditional network infrastructure. Whether ad hoc networks have vast potential, still there are many challenges left to overcome. Security is an important feature for deployment of MANET. In this paper, we have overviewed the challenges and solutions of the routing security threats in mobile ad hoc networks. Of these attacks, the passive attacks do not disrupt the operation of a protocol, but is only information seeking in nature whereas active attacks disrupt the normal operation of the MANET as a whole by targeting specific node(s). In this survey, we reviewed the current state of the art routing attacks and countermeasures MANETs. The advantages as well as the drawbacks of the countermeasures have been outlined. It has been observed that although active research is being carried out in this area, the proposed solutions are not complete in terms of effective and efficient routing security. There are limitations on all solutions. They may be of high computational or communication overhead (in case of cryptography and key management based solutions) which is detrimental in case of resource constrained MANETS, or of the ability to cope with only single malicious node and ineffectiveness in case of multiple colluding attackers. Furthermore, most of the proposed solutions can work only with one or two specific attacks and are still vulnerable to unexpected attacks. A number of challenges like the Invisible Node Attack remain in the area of routing security of MANETs. Future research efforts should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment.

References

[1] Pradip M. Jawandhiya et. al. / International Journal of Engineering Science and Technology Vol. 2(9), 2010, 4063-4071.

[2] Nishu Garg and R.P.Mahapatra, “MANET Security Issues ,” IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[3] Ping Yi, Yue Wu and Futai Zou and Ning Liu, “A Survey on Security in Wireless Mesh Networks”, Proceedings of IETE Technical Review, Vol. 27, Issue 1, Jan-Feb 2010.

[4] K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, “*Secure routing protocol for ad hoc networks,”* In Proc. of 10th IEEE International Conference on Network Protocols, Dept. of Comput. Sci., California Univ., Santa Barbara, CA, USA. 12-15 Nov. 2002, Page(s): 78- 87, ISSN: 1092-1648.

[5] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang, “*Security in mobile ad hoc networks: challenges and solutions,”* In proc. IEE Wireless Communication, UCLA, Los Angeles, CA, USA; volume- 11, Page(s):38- 47, ISSN: 1536-1284

[6] B. Wu, J. Chen, J. Wu, M. Cardei, “*A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,”* Department of Computer Science and Engineering, Florida Atlantic University, http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[7] H. Deng, W. Li, Agrawal, D.P., “*Routing security in wireless ad hoc networks,”* Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804

[8] Y. Hu, A. Perrig, and D. Johnson, “*Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,”* Proc. of MobiCom 2002, Atlanta, 2002.

[9] Y. Hu, A. Perrig, and D. Johnson, *"Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad Hoc Networks,"* Proc. of IEEE INFORCOM, 2002.

[10] C. R. Dow, P. J. Lin, S. C. Chen*, J. H. Lin*, and S. F. Hwang. A Study of Recent Research Trends and Experimental Guidelines in Mobile. Ad-hoc Networks. 19th International Conference on *Advanced Information Networking and Applications, 2005. AINA 2005***,** *Volume: 1, On page(s): 72- 77 vol.1*.

[11] T.H.Clausen, G.Hansen, L.Christensen, and G.Behrmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments and Simulation," *Proceedings of IEEE Symposium on Wireless Personal Mobile Communications 2001*, September 2001.

[12] R. Ogier, F. Templin, M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", *IETF Internet Draft*, v.11, October 2003.

[13] A.Iwata, C.C.Chiang, G.Pei, M.Gerla and T.W.Chen, "Scalable Routing Strategies for Ad Hoc Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1369-1379, August 1999.

[14] C.E.Perkins and P.Bhagwat, "Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) For Mobile Computers," *Proceedings of ACM SIGCOMM 1994*, pp. 233-244, August 1994.

[15] M.Gerla, X.Hong, L.Ma and G.Pei, "Landmark Routing Protocol (LANMAR) for Large Scale Ad Hoc Networks", *IETF Internet Draft*, v.5, November 2002.

[16] C.C.Chiang, H.K.Wu, W.Liu and M.Gerla, "Routing in Clustered Multi Hop Mobile Wireless Networks with Fading Channel," *Proceedings of IEEE SICON 1997*, pp. 197-211, April 1997.

[17] C.E.Perkins and E.M.Royer, "Ad Hoc On-Demand Distance Vector Routing," *Proceedings of IEEE Workshop on Mobile Computing Systems and Applications 1999*, pp. 90-100, February 1999.

[18] D.B.Jhonson and D.A.Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, Kluwer Academic Publishers, vol.353, pp. 153-181, 1996.

[19] V.D.Park and M.S.Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Ad Hoc Networks," *Proceedings of IEEE INFOCOM 1997*, pp. 1405-1413, April 1997.

[20] I. Chakeres and C. Perkins, "Dynamic MANET On-demand (DYMO) Routing Rrotocol", *IETF Internet Draft*, v.15, November 2008, (Work in Progress).

[21] P.Sinha, R.Sivakumar and V.Bharghavan, "CEDAR: A Core Extraction Distributed Ad Hoc Routing Algorithm," *IEEE Journal on Selected Areas in Communications*, vol.17, no.8, pp. 1454-1466, August 1999.

[22] Z.J.Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks," *Proceedings of ICUPC 1997*, vol. 2, pp. 562-566, October 1997.

[23] M.Joa-Ng and I.T.Lu, "A Peer -to-Peer Zone-Based Two-Level Link State Routing for Mobile Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1415-1425, August 1999.

[24] B. Kannhavong, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto.

A study of a routing attack in OLSR-based mobile ad hoc networks. *International Journal of Communication Systems*, 20(11):1245–1261, 2007.

[25] B. Kannhavong, H. Nakayama, N. Kato, Y. Nemoto, and A. Jamalipour.

A collusion attack against olsr-based mobile ad hoc networks. In *GLOBECOM*, 2006.

[26] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour.

A Survey of routing attacks in mobile ad hoc networks. *IEEE Wireless Communications*, page 86, 2007.

[27] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad Hoc Networks*, 1(1):175–192, 2003.

[28] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. *Wireless Networks*, 11(1):21–38, 2005.

[29] C. Tseng, T. Song, P. Balasubramanyam, C. Ko, and K. Levitt. A Specification-Based Intrusion Detection Model for OLSR.

LECTURE NOTES IN COMPUTER SCIENCE, 3858:330, 2006.

[30] C. Tseng, S. Wang, C. Ko, and K. Levitt. Demem: Distributed evidence driven message exchange intrusion detection model for manet.

In *Recent Advances in Intrusion Detection*, pages 249–271. Springer, 2006.

[31] T. View. Information theoretic framework of trust modeling and evaluation for ad hoc networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):305–317, 2006.

[32] M.Wang, L. Lamont, P. Mason, and M. Gorlatova. An effective intrusion

detection approach for OLSR MANET protocol. In *Secure Network Protocols, 2005.(NPSec). 1st IEEE ICNP Workshop on*, pages 55–60, 2005.

[33] S. Wang, C. Tseng, K. Levitt, and M. Bishop. Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks. *LECTURE NOTES IN COMPUTER SCIENCE*, 4637:127, 2007.

[34] Ramasamy, U. (2010). Classification of Self-Organizing Hierarchical Mobile Adhoc Network Routing Protocols - A Summary. International Journal of Advanced Computer Science and Applications - IJACSA, 1(4).

[35] Nayak, C. K., Dash, G. K. A. K., & Das, S. (2011). Detection of Routing Misbehavior in MANETs with 2ACK scheme. International Journal of Advanced Computer Science and Applications - IJACSA, 2(1), 126-129.