International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 10 October 2015

ADHOC routing Protocols and their Security Techniques for a Review

Vikas Yadav[1], Prof. Priyanka Dhasal[2]
Pursuing M.Tech[1], Asst. Professor[2]
Patel Group of Institution, Indore
vkyadav27june@gmail.com[1], priyanka.dhasal@yahoo.com[2]

Abstract- *Several routing protocols have been proposed in recent years for possible deployment of Mobile Ad hoc Networks (MANETs) in military, government and commercial applications. In this paper, we review these protocols with a particular focus on security aspects. The protocols differ in terms of routing methodologies and the information used to make routing decisions. Four representative routing protocols are chosen for analysis and evaluation including: Ad Hoc on demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and Temporally Ordered Routing Algorithm (TORA). Secure ad hoc networks have to meet five security requirements: confidentiality, integrity, authentication, non-repudiation and availability. The analyses of the secure versions of the proposed protocols are discussed with respect to the above security requirements.*

Keywords- *Ad hoc networks, routing protocols, security, wireless systems, mobile routing.*

1. Introduction

Mobile Ad hoc NETwork (MANET) [1] is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority. The member nodes are themselves responsible for the creation, operation and maintenance of the network. Each node in the MANET is equipped with a wireless transmitter and receiver, with the aid of which it communicates with the other nodes in its wireless vicinity. The nodes which are not in wireless vicinity, communicate with each other hop by hop following a set of rules (routing protocol) for the hopping sequence to be followed. The chief characteristics and challenges of the MANETs [2] can be classified as follows:

Cooperation: If the source node and destination node are out of range with each other then the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes is formed. This is known as multi hop communication. Hence each node is to act as a host as well as a router simultaneously. Dynamism of Topology: The nodes of MANET are randomly, frequently and unpredictably mobile within the network.[3] These nodes may leave or join the network at any point of time, thereby significantly affecting the status of trust among nodes and the complexity of routing. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable. So the management of the network environment is a function of the participating nodes

Lack of fixed infrastructure: The absence of a fixed or central infrastructure is a key feature of MANETs. This eliminates the possibility to establish a centralized authority to control the network characteristics. Due to this absence of authority, traditional techniques of network management and security are scarcely applicable to MANETs.

Resource constraints: MANETs are a set of mobile devices which are of low or limited power capacity, computational capacity, memory, bandwidth etc. by default. So in order to achieve a secure and reliable communication between nodes, these resource constraints make the task more enduring.

Albeit the security requirements (availability, confidentiality, integrity, authentication, nonrepudiation)[4] remain the same whether be it the fixed networks or MANETs, the MANETs are more susceptible to security attacks than fixed networks due their inherent characteristics.[5] Securitizing the routing process is a particular challenge due to open exposure of wireless channels and nodes to attackers, lack of central agency/infrastructure, dynamic topology etc.[6]. The wireless channels are accessible to all, whether meaningful network users or attackers with malicious intent. The lack of central agency inhibits the classical server based solutions to provide security. The dynamic topology entails that at any time any node whether legitimate or malicious can become a member of the network and disrupt the cooperative communication environment by purposely disobeying the routing protocol rules.

2. Routing Protocols in MANETS

The nodes in MANETs perform the routing functions in addition to the inherent function of being the hosts. The limitation on wireless transmission range requires the routing in multiple hops. So the nodes depend on one another for transmission of packets from source nodes to destination nodes via the routing nodes. The nature of the networks places two fundamental requirements on the routing protocols. First, it has to be distributed. Secondly, since the topology changes are frequent, it should compute multiple, loop-free routes while keeping the communication overheads to a minimum. Based on route discovery time, MANET routing protocols fall into three general categories:

a) Proactive routing protocols

b) Reactive routing protocols

c) Hybrid routing protocols

Proactive Routing Protocols: Proactive MANET protocols are table-driven and will actively determine the layout of the network. The complete picture of the network is maintained at every node, so route selection time is minimal. But the mobility of nodes if high then routing information in the routing table invalidates very quickly, resulting in many short lived routes. This also causes a large amount of traffic overhead generated when evaluating these unnecessary routes. For large size networks and the networks whose member nodes make sparse transmissions, most of the routing information is deemed redundant. Energy conservation being very important in MANETs, the excessive expenditure of energy is not desired. Thus, proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently. Examples of proactive MANET protocols include Optimized Link State Routing (OLSR)[7], Topology Broadcast based on Reverse Path Forwarding (TBRPF)[8], Fish-eye State Routing (FSR)[9], Destination-Sequenced Distance Vector (DSDV)[10], Landmark Routing Protocol (LANMAR)[11], Clusterhead Gateway Switch Routing Protocol (CGSR)[12].

Reactive Routing Protocols:Reactive MANET protocols only find a route to the destination node when there is a need to send data. The source node will start by transmitting route requests throughout the network. The sender will then wait for the destination node or an intermediate node (that has a route to the destination) to respond with a list of intermediate nodes between the source and destination. This is known as the global flood search, which in turn brings about a significant delay before the packet can be transmitted. It also requires the transmission of a significant amount of control traffic. Thus, reactive MANET protocols are most suited for networks with high node mobility or where the nodes transmit data infrequently. Examples of reactive MANET protocols include Ad Hoc On-Demand Distance Vector (AODV) [13], Dynamic Source Routing (DSR) [14], Temporally Ordered Routing Algorithm (TORA) [15], Dynamic MANET on Demand (DYMO) [16].

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) [17], Zone Routing Protocol (ZRP) [18], and Zone Based Hierarchical Link State Routing Protocol (ZHLS) [19].

3. Routing Attacks in MANETS

All of the routing protocols in MANETs depend on active cooperation of nodes to provide routing between the nodes and to establish and operate the network. The basic assumption in such a setup is that all nodes are well behaving and trustworthy. Albeit in an event where one or more of the nodes turn malicious, security attacks can be launched which may disrupt routing operations or create a DOS (Denial of Service)[20] condition in the network.

Due to dynamic, distributed infrastructureless nature of MANETs, and lack of centralized authority, the ad hoc networks are vulnerable to various kinds of attacks. The challenges to be faced by MANETs are over and above to those to be faced by the traditional wireless networks. The accessibility of the wireless channel to both the genuine user and attacker make the MANET susceptible to both passive eavesdroppers as well as active malicious attackers.

The limited power backup and limited computational capability of the individual nodes hinders the implementation of complex security algorithms and key exchange mechanisms. There is always a possibility of a genuine trusted node to be compromised by the attackers and subsequently used to launch attacks on the network. Node mobility makes the network topology dynamic forcing frequent networking reconfiguration which creates more chances for attacks.

The attacks on MANETs can be categorized as active or passive. In passive attacks the attacker does not send any message, but just listens to the channel. Passive attacks are non disruptive but are information seeking, which may be critical in the operation of a protocol. Active attacks may either be directed to disrupt the normal operation of a specific node or target the operation of the whole network.

A passive attacker listens to the channel and packets containing secret information (e.g., IP addresses, location of nodes, etc.) may be stolen, which violates confidentiality paradigm. In a wireless environment it is normally impossible to detect this attack, as it does not produce any new traffic in the network.

The action of an active attacker includes; injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets, and impersonating other nodes which violates availability, integrity, authentication, and nonrepudiation paradigm. Contrary to the passive attacks, active attacks can be detected and eventually avoided by the legitimate nodes that participate in an ad hoc network [21].

4. Security Measures Against Routing Attacks In Manets

In this section, we will discuss the countermeasures against the routing attacks and secured routing protocols in MANETS.

Solutions to the Flooding Attack: In [40], Yi et al. have proposed a simple mechanism to prevent the flooding attack in the AODV protocol. Here each node is to monitor its neighbors' RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. All future RREQs from the blacklisted nodes are then dropped. But this approach has limitations that a flooding threshold has to be set below which the attack cannot be detected. Also if a genuine nodes ID is impersonated by a malicious node and a large number of RREQs, are broadcast, other nodes might put the ID of this legitimate node on the blacklist.

In [41], Desilva et al. have proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. It uses a statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. The approach to attack detection is similar to that in [40.] with the difference that instead of a fixed threshold, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

Solutions to the Blackhole Attack: In [45] Tamilsevan et al. have proposed that the requesting node without sending the DATA packets to the reply node at once waits for other replies with next hop details from the other neighboring nodes. After receiving the first request a timer is set in the 'TimerExpiredTable', for collecting the further requests from different nodes. The 'sequence number', and the time at which the packet arrives is stored in a 'Collect Route Reply Table' (CRRT). Now the 'timeout' value based on arriving time of the first route request are calculated. Now CRRT is checked for any repeated next hop node which if found, it is assumed the paths are correct or the chance of malicious paths is limited. If there is no repetition then any random route from CRRT is selected.

In [46] Lee et al. have proposed the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack. The intermediate nodein addition to sending RREPs to the source node also sends CREQs to its next-hop node towards the destination node. The next-hop node on receipt of a CREQ looks up its cache for a route to the destination. If a route is found, it sends the CREP to the source. On receipt of the CREP, the source node compares the path in RREP and the one in CREP. If both are identical the source node pronounces the route to be correct. However in this proposal a blackhole attack is not resolved if two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker.

In [47], Shurman et al. have proposed the source node to wait until the arrival of a RREP packet from more than two nodes. On receiving multiple RREPs, the source node checks about a shared hop. If at least one hop is shared, the source node judges that the route is safe. The drawback here is the introduction of a time delay due to the wait till the arrival of multiple RREPs.

Solutions to the Worm Hole Attack: In [50], packet leashes are proposed to detect and defend against the wormhole attack. Hu et al. in their work have proposed temporal leashes and geographical leashes. For temporal leashes each node is to compute the packet expiration time (te) based on the speed of light c and is to include the expiration time (te') in its packet to prevent the packet from traveling further than a specific distance, L. At the receiving node, the packet is checked for packet expiry by comparing its current time and the te in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The constraint here is that all nodes have to be tightly clock synchronized. For the geographical leashes, each node must know its own position and may have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization is not critical.

Trust Based Security Solutions: Another active area of research in Mobile Ad Hoc and Sensor Network security in general is the Trust Based Security Solutions. In [54] Sun et al. have identified the role of Trust in MANETs. When a network entity establishes trust in other network entities, it can predict the future behaviors of others and diagnose their security properties. Trust helps in Assistance in decision making to improve security and robustness, Adaptation to risk leading to flexible security solutions, Misbehavior detection and Quantitative assessment of system-level security properties. Balakrishnan et al. in [44], [55],[56] have done extensive work on Trust based security solutions and have proposed Fellowship, TEAM (Trust Enhanced Security Architecture for Mobile Ad-hoc Networks) SMRITI (Secure MANET Routing with Trust Intrigue). In TEAM a trust model (SMRITI) is overlaid on other security models such as key management, secure routing and cooperation model (Fellowship) to enhance security. SMRITI assists the security models in making routing decisions, corresponding to the Trust evaluation of the involved nodes. The advantage of this approach is that no special/tamper proof hardware is required and there is no requirement of a central authority as well.

5. Conclusion

MANETs is an emerging technological field and hence is an active area of research. Because of ease of deployment and defined infrastructure less feature these networks find applications in a variety of scenarios ranging from emergency operations and disaster relief to military service and task forces. Providing security in such scenarios is critical. The primary limitation of the MANETs is the limited resource capability: bandwidth, power back up and computational capacity. Absence of infrastructure, vulnerability of channels and nodes, dynamically changing topology make the security of MANETs particularly difficult. Also no centralized authority is present to monitor the networking operations. Therefore, existing security schemes for wire networks cannot be applied directly to a MANETs, which makes them much more vulnerable to security attacks.

References

[1] C.S.R.Murthy and B.S.Manoj, Ad Hoc Wireless Networks, Pearson Education, 2008.

[2] George Aggelou, Mobile Ad Hoc Networks, McGraw-Hill, 2004.

[3] E. Ahmed, K. Samad, W. Mahmood, "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks," AusCERT2006 R&D Stream Program, Information Technology Security Conference, May 2006.

[4] A.Weimerskirch and G.Thonet, "Distributed Light-Weight Authentication Model for Ad-hoc Networks," Lecture Notes In Computer Science; Vol. 2288, pp. 341 354, 2001.

[5] I.Chlamtac, M.Conti, and J.Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1, pp. 13- 64, 2003.

[6] J.P.Hubaux, L.Buttyan, S.Capkun, "The Quest For Security In Mobile Ad Hoc Networks," Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), October, 2001.

[7] 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.

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

[9] 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.

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

[11] 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. [12] 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.

[12] 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.

[13] 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.

[14] 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.

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

[16] 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.

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

[18] 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.

[19] A.Shevtekar, K.Anantharam, and N.Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Commun. Lett., vol. 9, no. 4, pp. 363–65, April 2005.

[20] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, "Security in mobile ad hoc networks: Challenges and solutions," IEEE Wireless Communications, vol. 11, pp. 38-47, Feb., 2004.

[21] B.Wu, J.Chen, J.Wu, and M.Cardei, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[22] B.Kannhavong, H.Nakayama, Y.Nemoto, N.Kato, A.Jamalipour, "A Survey Of Routing Attacks In Mobile Ad Hoc Networks," IEEE Wireless Communications, vol. 14, issue 5, pp. 85-91, October 2007.

[23] Y.C.Hu and A.Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Security and Privacy, vol. 2(3), pp. 28-39, May 2004.

[24] D. Wang, M. Hu, H. Zhi, “A Survey of Secure Routing in Ad Hoc Networks,” IEEE Ninth International Conference on Web-Age Information Management, 2008, (WAIM '08), pp.482-486, July 2008.

[25] K.Sanzgiri, D.LaFlamme, B.Dahill, B.N.Levine, C.Shields, and E.M.Belding-Royer, “Authenticated Routing for Ad Hoc Networks,” Proceedings of IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, March 2005.

[26] Y.C.Hu, A.Perrig, and D.B.Johnson, “Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks,” Proc. MobiCom’02, Atlanta, GA, pp. 12-13 Se

[27] M.G.Zapata and N.Asokan, “Securing Ad-Hoc Routing Protocols,” Proceedings of ACM Workshop on Wireless Security, pp. 1–10, September 2002.

[28] Y.C.Hu, D.B.Johnson and A.Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks,” Proceedings of 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, pp. 3-13. June 2002.

[29] K.Sanzgiri, B.Dahill, B.N.Levine, C.Shields and E.M. Royer, “A Secure Routing Protocol for Ad hoc Networks”, Proceedings of 10th IEEE International Conference on Network Protocols (ICNP’02), IEEE Press, pp. 78-87, 2002.

[30] P.Papadimitratos, and Z.J.Haas, “Secure Link State Routing for Mobile Ad hoc Networks,” Proceedings of IEEE Workshop on Security and Assurance in Ad hoc Networks, IEEE Press, pp. 27-31, 2003.

[31] P.Yi, Z.Dai, S.Zhang, Y.Zhong., “A New Routing Attack in Mobile Ad Hoc Networks,” International Journal of Information Technology, vol. 11, no. 2, 2005.

[32] M.Drozda, H.Szczerbicka., “Artificial Immune Systems: Survey and Applications in Ad Hoc Wireless Networks,” Proceedings of International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'06), Calgary, Canada, pp. 485- 492, 2006.

[33] Y.C.Hu, A.Perrig, and D.B.Johnson, “Packet Leashes: A Defense Against Wormhole Attacks in Wireless Ad hoc Networks,” Proceedings of 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom’03), San Francisco, CA, vol.3, pp. 1976-1986, April 2003.

[34] Y.C.Hu, A.Perrig and D.Johnson, “Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,” Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, September 2003.

[35] L. Zhou and Z.J. Haas, “Securing Ad hoc Networks,” IEEE Network Magazine, vol. 6, no. 13, pp. 24-30, November/December 1999.

[36] B. Kannhavong, H. Nakayama, N.Kato, Y.Nemoto and A.Jamalipour, “Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks,” Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN' 06), pp. 30-35, June 2006.

[37] X.Lin, R.Lu, H.Zhu, P.H.Ho, X.Shen and Z.Cao, “ASRPAKE: An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks,” IEEE International Conference on Communications, ICC '07, pp. 1247 – 1253, June 2007.

[38] T.R.Andel and A.Yasinsac, “The Invisible Node Attack Revisited,” Proceedings of IEEE SoutheastCon 2007, pp. 686 – 691, March 2007.

[39] P.Yi, Z.Dai, S.Zhang, Y.Zhong., “A New Routing Attack In Mobile Ad Hoc Networks,” International Journal of Information Technology, vol. 11, no. 2, pp. 83-94, 2005.

[40] S.Desilva, and R.V.Boppana, "Mitigating Malicious Control Packet Floods In Ad Hoc Networks," Proceedings of IEEE Wireless Communications and Networking Conference 2005, , vol. -4, pp. 2112- 2117, March 2005.

[41] Y.Guo, S.Gordon, S.Perreau, "A Flow Based Detection Mechanism Against Flooding Attacks In Mobile Ad Hoc Networks," Wireless Communications and Networking Conference, IEEE (WCNC 2007), pp.3105-3110, March 2007.

[42] T.Peng, C.Leckie, R.Kotagiri, "Proactively Detecting Distributed Denial Of Service Attacks Using Source IP Address Monitoring," Proceedings of IFIP-TC6, 782 Athens, Greece, pp. 771-782, May 2004.

[43] V.Balakrishnan, V.Varadharajan, U.K.Tupakula, "Fellowship: Defense Against Flooding And Packet Drop Attacks In MANET," Network Operations and Management Symposium, NOMS 2006, pp. 1- 4, 2006.

[44] L.Tamilselvan, V.Sankaranarayanan, "Prevention of Blackhole Attack in MANET," The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, AusWireless, pp. 21- 26, August 2007

[45] S.Lee, B.Han, and M.Shin, "Robust Routing in Wireless Ad Hoc Networks," 2002 International. Conference on Parallel Processing Workshop, Vancouver, Canada, pp. 73-78, August 2002.

[46] M.A.Shurman, S.M.Yoo, and S.Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, pp. 96-97, 2004.

[47] S.Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, and Y.Nemoto, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, vol. 5, no. 3, pp. 338-346, November 2007.

[48] D.Dhillon, J.Zhu, J.Richards and T.Randhawa, "Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs," Proceedings Of The 2006 International Conference On Wireless Communications And Mobile Computing, pp. 45-50, 2006.

[49] Y.C.Hu, A.Perrig, and D.Johnson, "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, February 2006.

[50] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multi-path," IEEE Wireless Communication and Networking Conference '05, vol. 4, pp.2106-2111, March 2005.

[51] X.Su, R.V.Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks," IEEE International Conference on Communications, ICC '07, pp. 1136-1141, June 2007.

[52] M.A.Gorlatova, P.C.Mason, M.Wang, L.Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, MILCOM 2006, pp. 1-7, October 2006.

[53] Y.Sun, Z.Han and K.J.R.Liu, "Defense of trust management vulnerabilities in distributed networks," IEEE Communications Magazine, vol. 46, issue 2, pp.112-119, February 2008.

[54] V.Balakrishnan, V.Varadharajan, U.K.Tupakula and P.Lucs, "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks," 15th IEEE International Conference on Networks, ICON 2007, pp. 182-187, November 2007.

[55] V.Balakrishnan, V.Varadharajan, U.K.Tupakula and P.Lucs, "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks," 4th International Symposium on Wireless Communication Systems, ISWCS 2007, pp. 592-596, October 2007.