Network Layer Attacks and Defense Mechanisms in MANETS- A Survey

G.S. Mamatha
Assistant Professor, ISE Dept.
R.V. College of Engineering
Bangalore

Dr. S.C. Sharma
Vice Chancellor
Tumkur University
Tumkur, Karnataka

ABSTRACT

The foremost concerned security issue in mobile ad hoc networks is to protect the network layer from malicious attacks, thereby identifying and preventing malicious nodes. A unified security solution is in very much need for such networks to protect both route and data forwarding operations in the network layer. Without any appropriate security solution, the malicious nodes in the network can readily act to function as routers. This will solely disturb the network operation from correct delivering of the packets, like the malicious nodes can give stale routing updates or drop all the packets passing through them. In this paper a study that will through light on such attacks in MANETS is presented. The paper also focuses on different security aspects of network layer and discusses the effect of the attacks in detail through a survey of approaches used for security purpose.

General Terms

Security, MANETS, Attacks

Keywords

Mobile ad hoc network, network-layer attacks, cryptographic security, malicious nodes.

1. INTRODUCTION

Mobile ad hoc network (MANET) is a type of wireless ad hoc network, and is a self-configuring network of mobile devices connected by any number of wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate, packet drop rate, the overhead introduced by the routing protocol, and other measures. Security is an essential service for wireless network communications. However, the characteristics of MANETS pose both challenges and opportunities in achieving security goals, such as confidentiality, authentication, integrity, availability, access control, and non-repudiation [1]. The countermeasures can be considered as features or functions that reduce or eliminate security vulnerabilities and attacks. First, in this paper an overview of network layer attacks is given, and then the security counter measures.

Since in MANETS the nodes dynamically set up paths among themselves to transmit the packets, it is referred as infrastructure less network. The nodes in MANET can communicate directly if they are in within each other's wireless transmission ranges otherwise they have to rely on some other nodes to transmit messages if the nodes are outside each other's transmission range [2]. Thus, several intermediate hosts relay the packets which are sent by the source host before they reach the destination host, which in turn leads to a multi-hop scenario I.e. each node, will act as a router. The nodes cooperation is very much important for a successful communication. Thus, a MANET has several salient characteristics [3]: dynamic topologies, resource constraints, limited physical security, and no infrastructure. Possible applications of MANET include: Soldiers relaying information for situational awareness on the battlefield, business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference; and emergency disaster relief personnel coordinating efforts after a fire, hurricane, or earthquake [1]. The other possible applications [2] include personal area and home networking, location-based services, and sensor networks. There are a wide variety of attacks that target the weakness of MANETS. For example, routing messages are an important component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination. Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV [4] [5]. More sophisticated and subtle routing attacks have been identified in recent published papers, such as the black hole (or sinkhole) [6], Byzantine [7], and wormhole [8] [9] attacks. Currently routing security is one of the hottest research areas in MANET, so only the research initiative is taken for a specific layer like network layer in OSI model [1]. This paper is organized as follows. In Section 2, description about the network layer attacks is given. In Section 3, proposed solutions for the different network layer attacks are discussed, including multilayer attacks. In section 4, a discussion on open challenges and future directions is given.

2. NETWORK SECURITY ATTACKS

The connectivity of mobile nodes over a wireless link in MANETS which is multihop in nature strongly relies on the fact that ensures cooperation among the nodes in the network. Since network layer protocols forms connectivity from one hop neighbors to all other nodes in MANET, the assurance of cooperation among nodes is required. Recently variety of network layer targeted attacks have been identified and heavily studied in research papers. As a consequence of attacking network layer routing protocols, adversaries can easily disturb and absorb network traffic, inject themselves into the selected data transmission path between the source and destination, and thus control the network traffic flow, as shown in Figure 1, where a malicious node M can interfere itself in between any of the intermediate nodes participating in the communication in the chosen path (in the figure 1 to N represents the number of intermediate nodes) between source S and destination D [1].

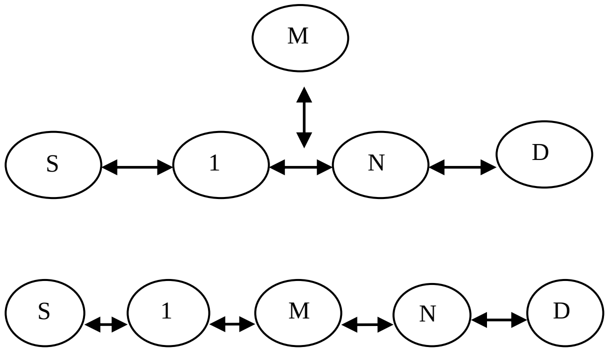

Figure 1: Interference of malicious node in between source and destination communication

The packets in the network traffic could be forwarded to a sub-optimal path or to a not existing path, which introduces significant delay and packet losses in the network. The adversaries send some fictitious routing updates to create routing loops or to introduce severe congestion in some portions of the network or to make some parts of the network inaccessible. The main effect of the presence of malicious nodes in the network is excessive network control traffic which intensifies the network congestion and as a result the performance of the network degrades. The principle idea behind this paper is to evaluate what security measures have been considered till date for identification of malicious nodes and preventing them in the network. Through a relative study, it can be revealed the research work carried using different cryptographic techniques considered for the security purposes to avoid malicious nodes in MANETS. Finally it can be concluded with a note that what precautions can be applied to ensure confidentiality and integrity in the network to upgrade the network performance.

The attacks in MANETS are classified into two major categories, namely passive attacks and active attacks, according to the attack means [10] [11]. Passive attacks are those, launched by the adversaries solely to snoop the data exchanged in the network. These adversaries in any way don't disturb the operation of the network. Such attacks identification becomes very difficult since network itself does not affected and they can reduced by using powerful encryption techniques. But an active attack tries to alter or destroy the information that is being exchanged, thereby disturbing the normal functionality of the network. Table 1 shows the classification of Network security attacks against MANETS. Passive attacks can be listed as eavesdropping, traffic analysis, and traffic monitoring. Active attacks include wormhole, black hole, gray hole, information disclosure, resource consumption, routing attacks and others include jamming, impersonating, modification, denial of service (DoS), and message replay.

Table 1: Network Security Attacks against MANETS

Passive Attacks	Snooping, eavesdropping, traffic analysis, monitoring
Active Attacks	Wormhole, black hole, gray hole, information disclosure, resource consumption, routing attacks

The attacks can also be classified into two categories, namely external attacks and internal attacks. External attacks are those, launched by the adversaries that do not belong to the network. Such attacks can be prevented by using powerful encryption techniques and firewalls. Internal attacks are launched by the compromised nodes within the network. This node tries to collect security information and can access the protected rights of the network. Since the compromised node is an authorized one in the network, it is very difficult to identify the internal attacks. The following figure 2 shows the exact classification of security attacks for MANETS for different layers of the OSI model [12].

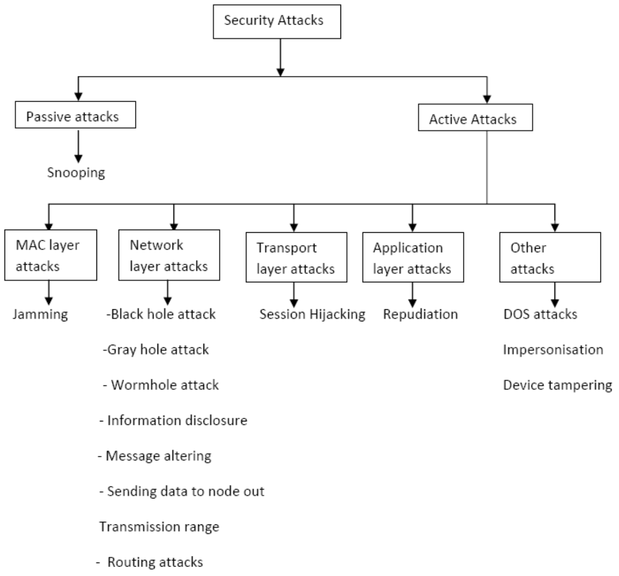

Figure 2: Classification of Security Attacks for different layers.

2.1 Network Layer Attacks Description

Black hole Attack:

In routing mechanism of ad hoc networks three layers namely physical, MAC and network layers plays a major role. As MANETs are more vulnerable to various attacks, all these three layers suffer from such attacks and cause routing disorders. The variety of attacks in the network layer differs such as not forwarding the packets or adding and modifying some parameters of routing messages; such as sequence number and hop count. The most basic attack executed by the nodes in the network layer is that an adversary can stop forwarding the data packets. The consequence caused by this is that, whenever the adversary is selected as an intermediate node in the selected route, it denies the communication to take place. Most of the times the black hole attack is launched by the adversaries, whenever AODV is used as the data forwarding protocol. Consider a malicious node which keeps waiting for its neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all the data packets [13] [14].

Gray hole Attack:

A variation of black hole attack s is the gray hole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). Both types of gray hole attacks seek to disrupt the network without being detected by the security measures in place [15].

Byzantine Attack:

In this type of attack the compromised or malicious nodes tries to create routing loops or routing of the data packets on the non-optimal routes or selectively drop packets. This kind of failures is not easy for identification, since the network seems to be operating very normally in the view of the user.

Wormhole Attack:

Wormhole attack takes place when two geographically separated adversaries create a tunnel called wormhole tunnel. Consequently, aim of the attackers is to create a man-in-the-middle attack which can drop packets, listen to confidential information or change the transferred data packets or to destroy the proper operation of the AODV in a MANET, by advertising shorter routes to a destination. The tunnel is created either using a wired link or by having a long range high bandwidth wireless link operating at a different frequency band [16].

Information Disclosure:

This type of attacks is mainly executed by the compromised nodes in the network by leaking the confidential or important information to the unauthorized nodes in the network.

Message Tampering:

This type of attack is launched by the adversaries acting as compromised nodes during communication. They tend to take all the data packets and modify the data which may be regarding the network topology, optimal routes etc; either by adding additional bytes or by deleting existing bytes. A small change in the data may obviously cause abnormalities or havoc in the network.

Routing Attacks:

1. Packet Replication attack: In this type of attack the adversary replicates the stale packets. As a result much of the network bandwidth and battery power of the nodes are consumed, which creates confusion in the routing process.
2. Route Cache Poisoning: Here a compromised node in the network send some fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. This result in sub-optimal routing, congestion in the portions of network or some parts of the network becomes inaccessible.
3. Rushing attack: Most of the on-demand protocols are more vulnerable to this kind of attack. An adversary which takes the RREQ packet from source node floods the packet quickly to all the other nodes in the network, before they get the same packet from the source. Once the original RREQ packet comes to the nodes, they assume it is a duplicate one and rejects it since they already have the packet from adversary.

Multilayer Attack:

Denial of Service Attack (DOS): Here an adversary tries to prevent all the legitimate and authorized users of the network from the services offered by the network. Especially in the network layer this attack is carried by flooding packets through a centralized resource to make it unavailable for all other nodes in the network. This makes failure in the delivery of guaranteed services to the end users. Other examples of multilayer DoS attacks are jamming, SYN flooding, DDoS (Distributed DoS) etc; [12].

3. DEFENSE AGAINST NETWORK LAYER ATTACKS

The previous section reveals the possibility of various attacks on the network layer and now the focus is on the several security measures taken to overcome these attacks. As it is a known fact, cryptography is one of the most common and reliable means to ensure security in MANETS. The main notions for cryptography are confidentiality, integrity, authentication and non-repudiation. The cryptography is discussed in detailed in [17].

MANETS have certain challenges in key management due to lack of infrastructure, absence of dedicated routers and mobility of nodes, limited processing power and limitation of battery power, bandwidth and memory. The main requirement to ensure security in MANETS is to have a secure routing protocol which should have properties to detect malicious nodes, guarantee of exact route discovery process, maintaining confidential network topological information and to be self-stable against attacks.

SAR (Secure-Aware Ad Hoc Routing protocol), which defines a level of trust as a metric for routing and as an attribute for security for routing. SAR using AODV uses encryption and decryption process using a common key [18]. The main drawback with SAR protocol is whenever the levels of security rise; it needs different keys for different levels, thereby increasing the number of keys [12].

SEAD (Secure Efficient Ad Hoc Distance Vector Routing protocol) is mainly designed for DSDV (Destination-Sequenced Distance Vector). This protocol can overcome DoS, all types of routing attacks and resource consumption attacks. It uses one-way hash function without the usage of asymmetric cryptographic mechanism. The mechanism uses authentication to differentiate between malicious and non-malicious nodes, which in turn reduces resource consumption attacks launched by malicious nodes. SEAD avoids routing loops, but the drawback lies whenever the attacker uses the same metric and sequence number used for authentication were same by the recent update message and updates with new update message [19]. The research update message from this mechanism is that it can also be used for other distance vector routing protocols.

ARAN (Authenticated Routing for Ad Hoc Networks) is a security protocol based on cryptographic certificates which overcomes all types of attacks in the network layer. Three major properties of cryptography, authentication, integrity and non-repudiation are supported with both DSR (Dynamic Source Routing) and AODV protocols [20] [12]. Even though this protocol mechanism is quite robust against attacks, it is mainly based on prior security coordination among nodes which cannot be correctly assured always. The issue of a false certificate to a node violates the non-repudiation and authentication property directly.

CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks is mainly used for selfishness detection in the MANETS through node co operation mechanism [21]. CONFIDENT Protocol: Cooperation Of Nodes---Fairness In Distributed Ad hoc NeTworks provides trust based routing security in MANETS [22]. Timed efficient stream loss-tolerant authentication (TESLA) protocol proposes a security mechanism to avoid attacks in MANETS [23].

Some approaches that detect malicious behavior in the data forwarding phase are, WATCHERS (Watching for Anomalies in Transit Conservation: a Heuristic for Ensuring Router Security) [24] is a protocol designed to detect disruptive routers in fixed networks through analysis of the number of packets entering and exiting a router. In this approach each router executes the WATCHERS protocol at regular intervals in order to identify neighboring routers that misroute traffic and avoid them [15].

SCAN (self-organized network layer security in mobile ad hoc networks) [25] focuses on securing packet delivery. It uses AODV, but argues that the same ideas are applicable to other routing protocols. SCAN assumes a network with sufficient node density that nodes can overhear packets being received by a neighbor, in addition to packets being sent by the neighbor. SCAN nodes monitor their neighbors by listening to packets that are forwarded to them. The SCAN node maintains a copy of the neighbor's routing table and determines the next-hop node to which the neighbor should forward the packet; if the packet is not overheard as being forwarded, it is considered to have been dropped [15].

Off late a system that can mitigate the effects of packet dropping has been proposed. This is composed of two mechanisms that are kept in all network nodes: a watchdog and a pathrater. The watchdog mechanism identifies any misbehaving nodes by promiscuously listening to the next node in the packet's path. If such a node drops more than a predefined threshold of packets the source of the communication is notified. The pathrater mechanism keeps a rate for every other node in the network it knows about. A node's rate is decreased each time a notification of its misbehavior is received. Then, nodes' rates are used to determine the most reliable path towards a destination, thus reducing the chance of finding a misbehaving node along the selected path. Moreover, the watchdog might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions or nodes capable of controlling their transmission power. Such weaknesses are the result of using promiscuous listening to determine whether a node has forwarded a packet or not [26].

DPRAODV: Detection, Prevention and Reactive AODV, provides a mechanism against security threats of black hole attack [14]. Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks also presents a mechanism to overcome black hole attack without the protocol implementation [15]. Some other related works for black hole attacks include Security-Aware Ad Hoc Routing for Wireless Networks [18], Routing Security in wireless ad hoc networks [27], and Collaborative security architecture for black hole attack prevention in mobile ad hoc networks provides a method to detect and exclude the nodes launching this type of attacks [28].

Packet Leashes which proposes a defense mechanism against wormhole attacks using hash function by sharing a set of keys for authentication [29]. MEPA method proposes a minimum exposed path to attacks which reduces impact of attacks but cannot handle attacks [30]. AODV-WADR (Wormhole Attack Detection Reaction) proposes a method to avoid the attack using Diffie-Hellman key exchange algorithm [16]. SECTOR uses the distance bounding algorithm to detect the wormhole attacks [31]. MDS-VOW uses multidimensional scaling to reconstruct the network and to detect worm holes [32]. WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks without using any specialized hardware wormholes can be detected and isolated within the route discovery phase [33]. Wormhole attacks detection in wireless ad hoc networks: a statistical analysis approach has been proposed [34].

A Secure Routing Protocol against Byzantine Attacks for MANETs in Adversarial Environments provides a method to overcome byzantine attacks using public key cryptographic algorithm for secure multimedia communications in emergency MANETS [35]. An on-demand secure routing protocol resilient to byzantine failures uses adaptive probing technique to reduce byzantine failures in MANETS [7]. Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks also presents a mechanism to overcome gray hole attack without the protocol implementation [15].

SMT (Secure Data Transmission in MANETS), proposes a method for overcoming information disclosure attack [36]. ARIADNE is a well-known secure on-demand ad hoc network routing protocol, which proposes a mechanism to avoid routing attacks and DoS attacks [5].

4. OPEN CHALLENGES AND FUTURE DIRECTIONS

Security in MANETS is such a hot topic among the research communities, if it is assured properly it can be used as a success factor and for the widespread deployment of the network. Several types of attacks in network layers have been identified and analyzed recently in most research papers. Security countermeasures and the defense against for each of the network attacks so far designed and implemented for MANETS are presented in the above sections. The research proposals till date, in MANETS are based upon a specific attack. They could work well in the presence of designated attacks, but there are many unanticipated or combined attacks that remain undiscovered. A lot of research is still on the way to identify new threats and create secure mechanisms to counter those threats. More research can be done on the robust key management system, trust-based protocols, integrated approaches to routing security, and data security at network layer. Here are some research topics and future work in the area:

a) Cryptography is the fundamental security technique used in almost all aspects of security. The strength of any cryptographic system depends on proper key management. The public-key cryptography approach relies on the centralized CA (certifying authority) entity, which is a security weak point in MANET. Some papers propose to distribute CA functionality to multiple or all network entities based on a secret sharing scheme, while some suggest a fully distributed trust model, in the style of PGP (Pretty Good Privacy). Symmetric cryptography has computation efficiency, yet it suffers from potential attacks on key agreement or key distribution. For example, the Diffie-Hellman (DH) scheme is vulnerable to the man-in-the-middle attack. Many complicated key exchange or distribution protocols have been designed, but for MANET, they are restricted by a node's available resources, dynamic network topology, and limited bandwidth. Efficient key agreement and distribution in MANET is an ongoing research area. Most of the current work is on preventive methods with intrusion detection as the second line of defense [1]. One interesting research issue is to build a mechanism which uses many approaches together without the use of key management to ensure more level of security in MANET. Building a sound robust semantic security approach and integrating it into the current preventive methods can be done in future research. Since most attacks are unpredictable, a resiliency-oriented security solution will be more useful, which depends on a multi-fence security solution.

5. ACKNOWLEDGMENTS

My sincere thanks to my honorable guide Dr. S. C. Sharma and others who have contributed towards the preparation of the paper.

6. REFERENCES

[1] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, WIRELESS/MOBILE NETWORK SECURITY, pp. – - –, © 2006 Springer

[2] C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications, pp. 38-47, 2004.

[4] M. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.

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

[6] Y. Hu and A. Perrig, A Survey of Secure Wireless Ad Hoc Routing. IEEE Security & Privacy, pp. 28-39, 2004.

[7] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of theACM Workshop on Wireless Security, pp. 21-30, 2002.

[8] Y. Hu, A Perrig, and D. Johnson, Packet Leashes: A Defense Against Wormhole Attacks inWireless Ad Hoc Networks. Proc. of IEEE INFORCOM, 2002.

[9] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks. Proc. of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, 2002 .

[10] S. Yi and R. Kravets, Composite Key Management for Ad Hoc Networks.Proc. of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services(MobiQuitous'04), pp. 52-61, 2004.

[11] R. Oppliger, Internet and Intranet Security, Artech House, 1998.

[12] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and Protocols", Low Price Edition, Pearson Education, 2007, pp. 521.

[13] Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity, September 2006.

[14] Payal N. Raj, Prashant B. Swadas. "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET", IJCSI International Journal of Computer Science Issues, 2:54-59, 2009.

[15] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks", Journal of Internet Engineering, 2:1, 2008.

[16] Emmanouil A. Panaousis, Levon Nazaryan, Christos Politis, " Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", Mobimedia'09, September 7-9, 2009, London, UK.

[17] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

[18] S. Yi, P. Naldurg and R. Kravets, "Security-Aware Ad Hoc Routing for Wireless Networks", Proceedings of ACM MOBIHOC 2001, pp. 299-302, October, 2001.

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

[20] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks", In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP' 02), pp. 78-87, November 2002.

[21] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", IFIP-Communication and Multimedia Security Conference 2002.

[22] S. Buchegger and J. Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks", Proc. of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, Canary Islands, Spain, 2002.

[23] A. Perrig, R. Canetti, J. Tygar, and D. Song, "The TESLA Broadcast Authentication Protocol", Internet Draft, 2000.

[24] K. A. Bradley, S. Cheung, N. Puketza, B. Mukherjee, and R. A. Olsson, "Detecting disruptive routers: a distributed network monitoring approach", in Proc. Symposium on Security and Privacy, May 1998.

[25] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-organized network-layer security in mobile ad hoc networks," IEEE Journal on Selected Areas in

Communications, Vol. 24, No. 2, February 2006, pp. 261-273.

[26] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad hoc Networks", in Proc. 6th ACM International Conference on Mobile Computing and Networking, , Boston, USA, August 2000, pp. 255-265.

[27] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Ad Hoc Networks", IEEE Communications Magazine, vol. 40, no. 10, 2002.

[28] Patcha, A; Mishra, A. "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks", In Proceedings of Radio and Wireless conference, RAWCON apos; 03, Vol. 10, Issue 13, pp. 75–78, Aug 2003.

[29] Y. Hu, A Perrig, and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks. Proc. of IEEE INFOCOM, 2002.

[30] Khurana, S.; Gupta, N.; Aneja, N, "Minimum Exposed Path to the Attack (MEPA) in Mobile Ad Hoc Network (MANET)", 6th International Conference on Networking (ICN'07), April 2007, pp: 16.

[31] S. Capkun, L. Buttyan, and J. Hubaux, Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[32] W. Wang and B. Bhargava. Visualization of Wormholes in Sensor Networks. In Proceedings of the ACM workshop on Wireless security (Wise'04), 2004. pp. 51-60.

[33] Sun Choi, Doo-young Kim, Do-hyeon Lee and Jae-il Jung, "WAP: Wormhole Attack Prevention Algorithm In Mobile Ad Hoc Networks", In Proceedings of International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, Vol. 0, ISBN = 978-0-7695-3158-8, pp. 343-348, 2008.

[34] N. Song, L. Qian and X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", In proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, 2005.

[35] Ming Yu; Mengchu Zhou; Wei Su, "A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments", IEEE Transactions on Vehicular Technology, Volume 58, Issue 1, Jan 2009,pp: 449 – 460.

[36] P. Papadimitratos and Z. Haas, Secure Data Transmission in Mobile Ad Hoc Networks. Proc. of the 2003 ACM Workshop on Wireless Security, pp. 41-50, 2003.