INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY (IJCET)

ISSN 0976 – 6367(Print)
ISSN 0976 – 6375(Online)
Volume 4, Issue 6, November - December (2013), pp. 145-155
© IAEME: www.iaeme.com/ijcet.asp
Journal Impact Factor (2013): 6.1302 (Calculated by GISI)
www.jifactor.com

IJCET

©IAEME

# REVIEW OF MOBILE AD HOC NETWORKS SECURITY ATTACKS AND COUNTERMEASURES

**Nada M. Badr[1] and Noureldien A. Noureldien[2]**

[1]PhD Student, Department of Computer Science, University of Science and Technology, Omdurman, Sudan.
[2]Associate Professor, Department of Computer Science, University of Science and Technology, Omdurman, Sudan

## ABSTRACT

In recent years mobile ad hoc networks (MANETs) have become a very popular top research area. By providing communications in the absence of a fixed infra-structure. MANETs are an attractive technology for many applications such as rescue operations, tactical operations, environmental monitoring, conferences, and the like. Unlike the wired networks, the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security issues; however, MANET is susceptible to attacks due to its mobility nature.

In this paper we provide based on a layered driven analysis a review of common attacks against MANET's and their proposed countermeasures.

**Keywords:** MANETs Security, Security Attacks, Countermeasures, Intrusion Detection.

## 1. INTRODUCTION

The MANETs, as a technology for dynamic wireless networks, had been deployed in military since 1970s, and thereafter it had been applied in various applications such as; patient monitoring, airplane exhaustion breakage supervision, business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference, remote landscapes monitoring, and emergency disaster relief personnel coordinating efforts after an earthquake [28]. The other possible applications [29] include personal area and home networking, location-based services, and sensor networks.

Although MANETs is promising technology but it has certain features that are considered vulnerable, which leads to security weakness in this technology such as; lack of centralized management, resource availability, scalability, cooperativeness, dynamic topology, limited power

supply, bandwidth constraint, adversary inside the network and no predefined boundary. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging.

The goal of this paper is to provide a review to MANETs attacks and the currently proposed countermeasures. The rest of the paper is organized as follows. Section 2 is dedicated to the attacks against MANETs and section 3 for common countermeasures. Conclusion and future work are given in section 4.

## 2. SECURITY ATTACKS

Classification of MANET security attacks can be done using different criteria such as attacks domain and techniques applied in attacks. One common domain classification, classifies MANET attacks into external and internal attacks [24].

External attacks are carried out by nodes that do not belong to the network. These attacks can cause congestion, sends false routing information or causes unavailability of services.

Internal attacks are launched by compromised nodes that are part of the network. In an internal attack the malicious node from the network gains unauthorized access and impersonates as a genuine node. It can analyze traffic between other nodes and may participate in other network activities. External and internal attacks are further classified as either passive or active. In a passive attack an adversary spies the data exchanged in the network without disrupting the network normal communication.

A common passive attack in MANETs that applied to physical layer of the Internet model is eavesdropping, in which an adversary can intercept and read messages and communication conversations. Another passive attack is traffic analysis, where adversaries collect traffic between communicating nodes and apply some analysis tools to reveal some information about the communication.

In an active attack, unlike passive attacks, an adversary attempt to modify or disrupting data being exchanged in the network or attempt to affect the normal functioning of the network. One typical classification to active attacks that ease the understanding the nature of these attacks is based on the TCP/IP stack model.

### 2.1. Active Attacks

Active attacks can be launched in each of the TCP/IP model layers. Attacks at each layer are examined in the following subsections.

#### 2.1.1. Physical Layer Attacks

Attacks at this layer aims to disrupt the service of wireless network physically, common active attacks applied in this layer is jamming, in which a jammer use an equipment to interfere with legitimate wireless communication, which causes the legitimate message to be corrupted or lost [25].

#### 2.1.2. Mac Layer Attacks

Attacks objective at this layer is to disrupt the cooperation of the layer's protocols. Efficient attacks in this layer include Selfish Misbehavior of Nodes in which the selfish node is not participating in forwarding or dropping in order to conserve resources. This attack affects the nodes performance but not interfere with network operation [27].

### 2.1.3 Network Layer Attacks

This layer represents a pool of attacks due to the fact that MANETs nodes acts as host and routers at the same time and this requires cooperation and reactions between nodes. Variety of attacks scenarios at this layer is possible such as absorbing network traffic, adversaries may inject themselves into the path between source and destination, control network traffic flow, packets can be forwarded to non optimal path, multi adversaries may colluding or prevent certain source node from finding routes to destination ...etc. These scenarios lead to the following attacks.

- **Wormhole attack**: The wormhole attack [22] [23], is a severe type of attacks in which two malicious nodes can forward packets through a private "tunnel" in the network as shown in Figure 1.

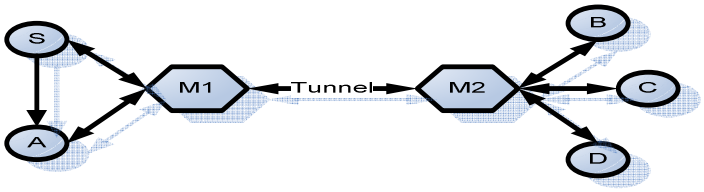


**Figure 1:** Wormhole attack [16]

Here, $M_1$ and $M_2$ are two malicious nodes which link through a private connection. Every packet that $M_1$ receives from the network is forwarded through "wormhole" to node $M_2$, and vice versa. This attack disrupts routing protocols by short circuiting the normal flow of routing packets. Such a type of attack is difficult to detect in a network, and may severely damages the communication among the nodes. Such an attack can be prevented by using packet leashes [16], which authenticate the timing information in the packets to detect faked packets in the network.

- **Black-hole attack**: In this attack anode advertises a zero metric for all destinations causing all nodes around it to route data packets towards it [30] [31] [32]. As in the wormhole attacks, malicious nodes could launch the black hole attacks by advertising themselves to the neighboring nodes as having the most optimal route to the requested destinations. However, unlike in the wormhole attacks where multiple attackers cooperated to attack one neighboring node, in the black hole attacks, only one attacker is involved.
- **Gray-hole attack**: This attack is also known as routing misbehavior attack which leads to dropping of messages. Gray-hole attack has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain probability.
- **Byzantine attack:** In this attack a compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion, 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 [14].
- **Routing Attacks**: These are attacks based on routing protocols on MANET which include the following attacks.

  - ***Modification Attacks***

In this type of attacks, some of the protocol fields of the messages passed among the nodes are modified, thereby resulting in traffic subversion, redirection or Denial of Service (DoS) attacks. Modification attacks include;

**Modification of sequence numbers**: This attack is possible against the AODV protocol. The malicious node can change the sequence number in the route request packets or route reply packets in order to make the route fresh. Figure 2, shows a malicious node M that receives a route request message RREQ originates from node S and broadcasted by node B to the destined node X. M uncast a route replay message RREP to B with a higher destination sequence number than the value last advertised by X. The node S accepts the RREP and then sends the data to X through M. When the legitimate RREP from X gets to S, if the destination number is less than the one advertised by M, then it will be discarded as a stale route. The situation will not be corrected until a valid RREP with higher sequence number than that of M reach to S.

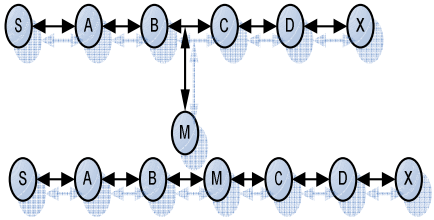


**Figure 2:** An example of route modification attack [15]

**Modification of hop count**: This type of attacks is possible against the AODV protocol in which a malicious node can increase the chance that they are included in a newly created route by resetting the hop count field of a RREQ packet to a lower number or even zero. Similar to route modification attack with sequence number, the hop count field in the routing packets is modified to attract data traffic.

**Modification of source route**: This attack is possible against DSR which uses source routes and works as follows. In Figure 2, it is assumed that the shortest path exists from S to X. It is also assume that C and X cannot hear each other, that nodes B and C cannot hear each other, and that M is a malicious node attempting a denial-of-service attack. Suppose S sends a data packet to X with the source route S-A-B-C-D-X. If M intercepts this packet, it removes D from the list and forwards it to C. C will attempt to forward this packet to X which is not possible since C cannot hear X. Thus M has successfully launched a DoS attack on X.

- ***Impersonation attacks***

This type of attacks violates authenticity and confidentiality in a network. A malicious node can impersonate or spoof the address of another node in order to alter the vision of the network topology as perceived by another node. Such attacks can be described as in Figure 3.

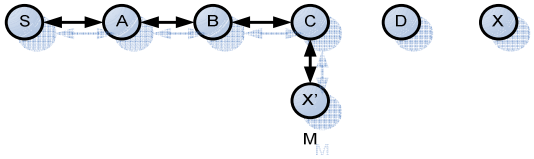


**Figure 3:** Impersonation Attack [17]

Node S wants to send data to node X and initiates a Route Discovery process. The malicious node M, closer to node S than node X, impersonates node X as X'. It sends a route reply (RREP) to node S. Without checking the authenticity of the RREP, node S accepts the route in the RREP and starts to send data to the malicious node. This type of attacks can cause a routing loop within the network.

- ***Fabrication attacks***

In this type of attack, a malicious node tries to inject fake messages or routing packets to disrupt the routing mechanism. These attacks are difficult to detect in a MANET since the routing packets appear to be legitimate packets to the nodes processing them. Figure 4 is an example of a fabrication attack. Node S wants to send data to node X, so it broadcasts a route request in order to find a route to node X. Malicious node M pretends to have a cached route to the destination X, and returns route reply message (RREP) to the source node (S).

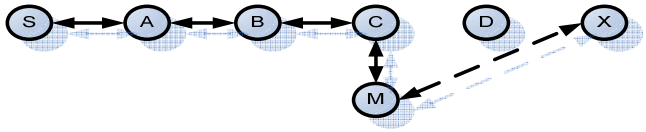


**Figure 4.** Fabrication attack [17]

The source node S, without checking the validity of the RREP, accepts the RREP and starts to send data through M. Furthermore, malicious nodes can fabricate RERR to advertise a link break to a certain node in a MANET with AODV or DSR protocols.

- ***Interception Attacks***

In this attack, attackers can get an unauthorized access to the routing messages that are not intentionally sent to them. This kind of attack put in dangers the integrity of the packets because such packets might be modified before being forwarded to the next hop. Examples of attacks that can be classified under the interception attacks are wormhole attacks, black hole attacks.

- ***Replay Attacks***

In a replay attack on the routing infrastructure an adversary sends old route advertisements to a node causing it to update its routing table with stale routes. The attacker may also record packets sent between legitimate network nodes on the application layer and replay these recorded packets in order to gain unauthorized access to network services or overload a node with outdated information resulting in denial of service attack.

- **Sleep deprivation torture (Resource consumption attack):** An adversary may interact with a node in a "legitimate" way with the purpose of consuming its battery power (energy resources). In ad hoc networks and particularly in sensor networks, energy resources are severely limited. In order to conserve power these nodes go into sleep mode in which the channel is only periodically scanned for signals. During a sleep deprivation torture attack, nodes are prevented from going into sleep mode until the battery of the target device is fully depleted, leaving the node disabled.
- **Sybil Attacks:** If a strong one-to-one binding between the identity and physical entities does not exist in a communication system, it is always possible for an unfamiliar entity to adopt more than one identity [2]. In a Sybil attack, a single inconsistent or malicious entity presents multiple identities and therefore potentially controls a substantial fraction of the system**.**
- **Rushing attack:** Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g. a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne [18].

#### 2.1.4 Transport Layer Attacks

Attacks in this layer are characterized by degrading the performance of MANETs significantly [26], since they result in what called DOS attack. Attacks of this class include SYN Flooding Attack, in which half opened TCP connections was stored in the victim node in a fixed size table and waits for acknowledgement for three way handshake, the pending connections overflow the buffer and made the victim node unable to accept any legitimate attempts to open a connection**,** and TCP Session Hijacking Attack, in which the hijacker impersonates the victim node and perform DOS attack, the objective of the hijacker is to determine the sequence number expected by the target through spoofing the victim's IP address.

#### 2.1.5 Application Layer Attacks

This layer is concerned with semantics of data i.e. what data means to application , and support many important protocols such as HTTP, SMTP, TELNET and FTP which makes this layer is the target for attackers who seeks access to information. Attacks that are common in application layer are malicious code attacks which can be a viruses, worms, spyware and Trojans which can affect both the user applications and operating system and widely spread through network, and repudiation attacks which disrupt MANETs merit cooperation and reaction between nodes.

## 3. MANETS ATTACKS COUNTERMEASURES

In this section we discuss the most common countermeasures to MANETs security attacks based on attack layers.

### 3.1 Physical layer defense

By nature wireless communication is broadcast. A common radio signal is easy to jam or intercept. To counter jamming attack, spread spectrum technology, such as frequency hopping (FHSS) or direct sequence (DSSS) [33], can be used to make signals difficult to detect. The spread spectrum technology either changes frequency in a random way that makes signal capturing difficult or spreads the energy to a wider spectrum so the transmission power is hidden behind the noise level.

### 3.2 Link layer defense

Although it is still an open challenge to prevent selfishness attack, some schemes are proposed, such as ERA802.11 [34], where detection algorithms are proposed, also the traffic analysis attack can be prevented by encryption at data link layer.

### 3.3 Network layer defense

As stated above, this layer is largely overwhelmed with different security attacks. In the following subsections we present the proposed security countermeasures to defend against or to eliminate these attacks.

#### 3.3.1 Defending Wormhole attack

A **v**ariety of mechanisms are proposed to counter a wormhole attacks such as Wormhole Attack Prevention (WAP) [31], True Link, which is timing mechanism, Packet Leashes (temporal and geographical) [32], SECTOR [35], Directional Antenna[36] and Cluster-based Intrusion Detection Algorithm [37].

#### 3.3.2 Defending black-hole attack

Two mechanisms that are based on demand protocols are utilized to countermeasure this serious attacks, namely the Detection Prevention and Reactive AODV (DPRAODV) [38] and Security Aware adhoc Routing protocol (SAR) [39].

Furthermore two authentication mechanisms based on the hash function are proposed in [41] to identify multiple black holes cooperating with each other. TOGBAD [39] is an approach that can detect and identify the nodes that attempt to create blackhole attack. Also wait and check the replies mechanism which aims to find a safe route for packets is proposed to detect blackhole attack [42].

### 3.3.3 Defending Gray-hole attack

One proposed countermeasure to gray-hole attack is the Aggregate Signature Algorithm [40], which is a mechanism, supported by DSR protocol, and contains three algorithms**:** creating proof algorithm, the checkup algorithm and the diagnosis algorithm. This algorithm main purpose is to track the dropping packets nodes.

### 3.3.4 Defending Byzantine attack

Robust source routing protocol (RSR) [43] is a secure on demand routing protocol which has the ability to mitigate dropped and modified packets.

### 3.3.5 Defending Routing attacks

Routing protocols use various security mechanisms to ensure robustness of the routing scheme. Some of these mechanisms are redundancy exploitation and diversity coding.

- **Redundancy exploitation**

Routing schemes may exploit redundancy by establishing multiple routes from source to destination [1], as easily achieved by ZRP [5], DSR [3], TORA [4], AODV [6], by sending data via all these routes, the redundancy will ensure that all data arrives at the destination.

- **Diversity coding**

An alternative mechanism to sending data via redundant routes is diversity coding [9]. Diversity coding takes advantage of redundant routes in a more bandwidth efficient way by not re-transmitting the messages. Rather, it transmits limited redundant information through additional routes for the purpose of error detection and correction.

## 3.4 Transport layer defense

TCP is guaranteed and reliable protocol that provides valuable security mechanism, but in MANET this protocol is inefficient, therefore many adhoc transmission control protocols have been innovated. Examples include; Adhoc Transmission Control protocol ATCP [44], Adhoc Transmission Protocol (ATP) [44], TCP-feedback [44], TCP explicit failure notification (TCP-ELFN) [44]. Further, SSL/TLS and private communication transport (PCT) [45] can offer secure communication through public key cryptography techniques.

## 3.5 Application layer defense

The strategy of defense in this layer is based on layered defense so as to build a robust security strategy. The most common application layer defense mechanisms are firewalls and intrusion detection systems.

### 3.5.1 Firewall Mechanism

This mechanism is considered as the first layer of defense and can perform packet filtering, user authentication, logging and access control. Although it solves many security problems but it has some shortcomings such as its lack of preventing of insider attacks.

### 3.5.2 Intrusion Detection Mechanism

Another layer of defense is the Intrusion Detection System (IDS), which can complement firewall shortcomings**.** Intrusion detection systems can detect the intrusions using certain techniques such as anomaly based, statistical, artificial intelligence and neural network techniques.

Applying intrusion detection in MANETs is different to that in conventional network due to the fact that MANETs have no central devices, mobile, wireless linked and have limited resources.

Therefore certain intrusion detection systems architectures have been proposed to suit the characteristics of MANETs, as it can be configured as flat or multi layer, the common architectures for IDS in MANETs are:

- **Stand-alone intrusion detection systems:** in this architecture, each node has its own detection engine to identify the intrusion without cooperation from other nodes in the network.
- **Distributed and cooperative intrusion detection systems:** this architecture is compatible to MANETs nature as the detection of intrusion is occurred locally by IDS agent and globally through cooperation between neighboring nodes.
- **Hierarchical intrusion detection systems**: this architecture is inevitable in multilayer infrastructure as the network is already clustered. The cluster heads bear the workload of detection of intrusion locally for its node and globally for the cluster through monitoring packets and issues global response when malicious activities are detected.

There are widely common schemes used by intrusion detection systems in MANETs to detect misbehaving, identify malicious nodes and isolate them, the most common are**:**

- **Watchdog and Pathrater:** watchdog method allows detecting misbehaving nodes [44]. When a node forwards a packet, the watchdog set in the node ensures that the next node in the path also forwards the packet. The watchdog does this by listening to all nodes within transmission range promiscuously. If the next node does not forward the packet then it is tagged as misbehaved. If a packet is not forwarded within a timeout period, then a failure tally for the node responsible for forwarding the packet is incremented. If this tally exceeds a predetermined threshold, then the node is termed as malicious.

  In the Pathrater approach, each node uses the information provided by watchdogs to rate neighbors isolate or punish the misbehaved node by decreasing trust rate.

- **Confidant**: this scheme [19] is similar to watchdog and Path rater in that it can observe the behavior of neighboring nodes within its transmission range. But it is different in that; in watchdog and Path rater scheme misbehaving nodes whose packets are forwarded before certain period of time does not penalized, with Confidant the misbehaving nodes are prohibited from forwarding packets. In Confidant each node has four components: a monitor, a reputation system, a trust manager, and a path manager. This protocol has a risky feature as it allows sending alarms between nodes in the network, where attackers can benefit from this and sending false alarms.

- **Virtual currency or nuglets**: it is a credit based scheme [20] which is used to encourage cooperation. Each packet is loaded with nuglets by the source node, each relay node charges a nuglet from the packet before forwarding it. This scheme is able to handle watchdog and pathrater weakness by detecting misbehavior nodes and lock them out, since it is not letting them to send and receive packets as watchdog and pathrater scheme.

- **Token-based Mechanism: this** scheme is designed to work on AODV protocol [21], and it composed of neighbor verification, neighbor monitoring, intrusion reaction and enhanced routing protocol.

Defending Dos Attack at application layer can be achieved by using some proposed techniques are mitigation techniques that use digital signatures to drop the illegitimated packets which are not verified, others are build on firewall to distinguish packets attacks, some trace Dos attacker like on-the fly scheme [46], and Dos-Mac protocol [45] are used as tool to ensure the network performance improves.

## 4. CONCLUSIONS

In this review we focused on MANET attacks and security countermeasures of these attacks. As MANET works in vulnerable environment different attacks at different layers are exist. The review is based on a layer driven taxonomy and classification of MANETs attacks and their corresponding security countermeasure.

## 5. REFERENCES

[1] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," IEEE Network: special issue on network security, vol. 13, no. 6, pp. 24–30, 1999.

[2] J. R. Douceur, "The Sybil Attack," in proc. 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), March, 7-8 2002.

[3] S. Murphy and J. J. Garcia-Luna-Aceves, "An efficient routing algorithm for mobile ad hoc networks," MONET, vol. 1, no. 2, pp. 183–197, 1996.

[4] V. D. Park and M. S. Corson, "A Highly Adaptable distributed Routing Algorithm for Mobile Wireless Networks," in proc. Sixteenth Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM'97), 1997.

[5] Z. J. Haas and M. Perlman, "The Performance of Query control Schemes for Zone Routing Protocol," in proc. Annual Conf. of the ACM Special Interest Group on Data Communication (SIGCOMM'98), September 2-4 -1998.

[6] C. E. Perkins and E. M. Belding-Royer, "Ad-hoc On-demand Distance Vector Routing," in proc. The Second IEEE Workshop on Mobile Computing Systems and Applications (IEEE WMCSA'99), February 1999.COMM'98), September 2-41998.

[7] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook in Applied Cryptography. CRCPress, 1996.

[8] M. Steiner, G. Tsudik, and M. Waidner, "Key Agreement in Dynamic Peer Groups," IEEE Transactions on Parallel and Distributed Systems, vol. 11, no. 8, pp. 769–780, 2000.

[9] E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo, "Diversity Coding for Transparent Self-healing and Fault-Tolerant Communication Networks," IEEE Transactions on Communications,vol. 41, no. 11, pp. 1677–1686, 1993.

[10] G. Ateniese, M. Steiner, and G. Tsudik, "Authenticated Group Key Agreement and Friends,"in proc. 5th ACM Confernce on Computer and Communications Security, November, 2-51998.

[11] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault-Tolerant Key Agreement for Dynamic Collaborative Groups," in proc. 7th ACM Conf. on Computer and communications security (CCS'00), November, 1-4 2000.

[12] Y. Kim, A. Perrig, G. Tsudik, "Tree-based Group Key Agreement," ACM Transactions on Information Systems Security(TISSEC), vol. 7, no. 1, pp. 60 – 96, 2004.

[13] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions," in proc. ACM Workshop on Wireless Security (WiSe'02), September, 28 2002.

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

[15] K. Sanzgiri, B.Dahill, Brian N. Levine, and Elizabeth M. Belding-Royer. "A Secure Routing Protocol for Ad Hoc Networks". Proceedings of 10th IEEE International Conference on Network Protocols(ICNP'02),Paris, France, November 2002, pp.78-90.

[16] Y. Hu, A. Perrig, D. Johnson. "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks". Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM2003), March 2003.

[17] Yi-an Huang and Wenke Lee. "Attack analysis and Detection for Ad-hoc Routing protocols". Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID'04), French Riviera, France. September 2004.

[18] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. of MobiCom2002, Atlanta, 2002.

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

[20] L. Buttyan and J. Hubaux, Nuglets: A Virtual Currency to Simulate Cooperation in Self-organized Ad Hoc Networks. Technial Report DSC/2001/001, Swiss Federal Institute of Technology - Lausanne, 2001.

[21] H. Yang, X. Meng, and S. Lu, Self-organized Network Layer Security in Mobile Ad Hoc Networks, ACM MOBICOM Wireless Security Workshop (WiSe'02).

[22] M. Ilyas, The Handbook of Ad Hoc Wireless Networks, CRC Press, 2003.

[23] 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

[24] A. Cardenas, N. Benammar, G. Papageorgiou, and J. Baras, Cross-Layered Security Analysis of Wireless Ad Hoc Networks, *Proc. of 24th Army ScienceConference*, 2004.

[25] T. Karygiannis and L. Owens, Wireless Network Security-802.11, Bluetooth and Handheld Devices. National Institute of Standards and Technology. TechnologyAdministration, U.S Department of Commerce, *Special Publication* 800-848, 2002.

[26] H. Hsieh and R. Sivakumar, Transport Over Wireless Networks. *Handbook of Wireless Networks and Mobile Computing*, Edited by Ivan Stojmenovic. JohnWiley and Sons, Inc., 2002.

[27] Vikrant Gokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey".

[28] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer, 2006.

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

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

[31] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung," WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.

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

[33] W. Stallings, Wireless Communication and Networks, Pearson Education, 2002.

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

[35] 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.

[36] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", *Proc. of Networks and Distributed System Security Symposium* (NDSS), 2004.

[37] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki,"A New Cluster based wormhole intrusion detection algorithm for MANET", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009).

[38] Payal N. Raj and Prashant B. Swades, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET" , IJCSI International Journal of Computer Science Issues, Vol. 2, 2009 .

[39] Elmar Gerhards-Padilla, Nils Aschenbruck, Peter Martini, "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs Networks ," 32nd IEEE Conference on Local Computer Networks 0742-1303/07 $25.00 © 2007 IEEE.

[40] Gao Xiaopeng and Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks", 2007 IFIP International Conference on Network and Parallel Computing – Workshops @ 2007 IEEE.

[41] Zhao Min and Zhou Jiliu1, "Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks", 2009 International Symposium on Information Engineering and Electronic Commerce.

[42] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007).

[43] Claude Cr´epeau, Carlton R. Davis and Muthucumaru Maheswaran, "A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes ", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07).

[44] S. Marti, T.J. Giuli, K. Lai, and M. Baker. "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annual Int. Conf.on Mobile Computing and Networking (MobiCom'00),* Boston, MA, August 2000, pp.255-265.

[45] R. Gunasekaran and V. Rhymend Uthariaraj, "Prevention of Denial of Service Attacks and Performance Enhancement in Mobile Ad hoc Networks ", 2009 Sixth International Conference on Information Technology:

[46] Yongjin Kim, Vishal Sankhla, Ahmed Helmy1," Efficient Traceback of DoS Attacks using Small Worlds in MANET", Proc. 2004 IEEE.

[47] Prof. S.B. Javheri and Shwetambari Ramesh Patil, "Attacks Classification in Network", International Journal of Information Technology and Management Information Systems (IJITMIS), Volume 4, Issue 3, 2013, pp. 1 - 11, ISSN Print: 0976 – 6405, ISSN Online: 0976 – 6413.

[48] Kusum Nara and Aman Dureja, "A Dynamic Approach For Improving Performance of Intrusion Detection System Over Manet", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 4, 2013, pp. 61 - 81, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[49] M. Ahmed, S. Yousef and Sattar J Aboud, "Bidirectional Search Routing Protocol for Mobile Ad Hoc Networks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 1, 2013, pp. 229 - 243, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[50] Poonam Pahuja and Dr. Tarun Shrimali, "Routing Management for Mobile Ad-Hoc Networks", International Journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 464 - 468, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.

[51] Neha Kaushik and Ajay Dureja, "A Comparative Study of Black Hole Attack in Manet", International Journal of Electronics and Communication Engineering & Technology (IJECET), Volume 4, Issue 2, 2013, pp. 93 - 102, ISSN Print: 0976- 6464, ISSN Online: 0976 –6472.