A Review on MANETs: its attack types, intrusion detection systems, Black-hole attack and its effect on the AODV routing protocol

Baishali Goswami
Department of Computer Science and Engineering
Sikkim Manipal Institute of Technology
Sikkim, India
baishaligoswami3@gmail.com

Abstract-Mobile ad-hoc networks (MANETs) are autonomous, infrastructure less, self-organized networks. In MANETs, nodes are not stationary and thus move arbitrarily, resulting into rapid and unpredictable topology changes in the network. Due to the limited transmission range of the nodes in the MANETs, these nodes are not capable of directly communicating with each other. Hence, routing paths in MANETs potentially contain multiple hops, and every node in it has the responsibility to act as a router. So, presence of any intermediate node in the route, which is either highly congested or behaving as a malicious node, is likely to drop the packets. In computer networking, this type of attack is known as a packet drop attack or black hole attack which is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them.

Keywords: *Ad-hoc AODV, Black Hole Attack, MANET, Destination sequence Number.*

1. MANET (Mobile Ad-Hoc Network)

A mobile ad-hoc network (MANET) is a self-configuring infrastructure-less network of mobile devices. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently [1].

Mobile ad hoc networks (MANET) are wireless networks in which the mobile nodes exchange information without the help of any predefined network infrastructure. In such networks, also called spontaneous networks, the nodes collaborate to provide the basic network services. Nodes in a MANET may, at any time, disappear from, appear into or move within the network. The resulting dynamic nature of the network topology [4], along with the unreliability of the wireless links, require for the configuration of MANET services to be highly adaptable. Moreover, the availability of an individual node cannot be assured and therefore, services cannot rely on a central entity and must be provided in a distributed and adaptive manner. Moreover, the wireless access links makes the network more vulnerable to many attacks (e.g. passive eavesdropping, active impersonation, denial of service) than wired networks. These features make the provision of security services in MANET particularly challenging. Nevertheless, some solutions for security services in MANET have been presented in recent literature. Most existing solutions consist in some kind of preventive security, usually based in authentication. These preventive security mechanisms can usually be reinforced by proactive security services, such as intrusion detection.

1.1. Why it is called an Ad-hoc network?

A wireless ad-hoc network is a decentralized type of wireless network. The network is ad-hoc because it does not rely on a pre-existing infrastructure [10], such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad-hoc networks can use flooding for

forwarding data.An ad-hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range.

1.2. Merits of MANET

i. **Low cost of deployment**: Ad-hoc networks can be deployed on the fly, thus requiring no expensive infrastructure such as copper wires, data cables, etc.

ii. **Fast deployment:** When compared to WLANs, ad -hoc networks are very convenient and easy to deploy requiring less manual intervention since there are no cables involved.

iii. **Dynamic Configuration***:* Ad-hoc network configuration can change dynamically with time. For many scenarios such as data sharing in classrooms, etc., this is a useful feature. When compared to configurability of LANs, it is very easy to change the network topology [1] [4].

1.3. **Vulnerabilities of MANET**

MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

i. **Lack of centralized management**: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

ii. **Resource availability**: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures.

iii. **Scalability**: Due to mobility of nodes, scale of ad-hoc network keeps on changing all the time. So scalability is a major issue concerning security.

iv. **Cooperativeness**: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

v. **Dynamic topology**: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised.

vi. **Limited power supply**: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

vii. **Bandwidth constraint:** Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

viii. **Adversary inside the Network**: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious.

ix. **No predefined Boundary**: In mobile ad-hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network [1] [4].

1.4. Security goals of MANET

The goals to evaluate if mobile ad- hoc network is secure or not are as follows:

i. **Availability**: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

ii. **Confidentiality**: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access.

iii. **Integrity**: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

iv. **Authentication**: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and

not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

v. **Non repudiation**: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message .This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

vi. **Anonymity**: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

vii. **Authorization**: This property assigns different access rights to different types of users.

1.5. **Broadcasting Approaches in MANETs**

In MANET, a number of broadcasting approaches on the basis of cardinality of destination set is present:

i. **Unicasting:** Sending a message from a source to a single destination.

ii. **Multicasting**: Sending a message from a source to a set of destinations.

iii. **Broadcasting**: Flooding of messages from a source to all other nodes in the specified network.

iv. **Geocasting**: Sending a message from a source to all nodes inside a geographical region.

1.6. Applications of MANET

Typical applications include:

i. **Military Battlefield**: - hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters.

ii. **Commercial Sector**: Ad hoc can be used in emergency/ rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed. Information is relayed from one rescue team member to another over a small hand-held. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

iii. **Local Level**: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, mobile ad hoc communications will have many applications.

iv. **Personal Area Network (PAN):** Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). Tedious wired cables are replaced with wireless connections. Such an ad hoc network can also extend the access to the Internet or other networks by mechanisms e.g. Wireless LAN (WLAN), GPRS, and UMTS.

v. **MANET-VoVoN:** A MANET enabled version of JXTA peer-to-peer, modular, open platform is used to support user location and audio streaming over the JXTA virtual overlay network. Using MANET-JXTA, a client can search asynchronously for a user and a call setup until a path is available to reach the user. The application uses a private signaling protocol based on the exchange of XML messages over MANET-JXTA communication channels.

1.7. **Challenges of MANET**

Regardless of the attractive applications, the features of MANET introduce several challenges. These include:

i. **Routing***:* Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

ii. **Security and Reliability**: An ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium (e.g. hidden terminal problem), mobility-induced packet losses, and data transmission errors**.**

iii. **Quality of Service (QoS**):Providing different quality of service levels in a constantly changing environment will be a challenge.

iv. **Inter-networking:** In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

v. **Power Consumption**: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

vi. **Multicast**: Multicast is desirable to support multiparty wireless communications. Since the multicast tree is no longer static, the multicast routing protocol must be able to cope with mobility including multicast membership dynamics (leave and join).

vii. **Location-aided Routing:** Location-aided routing uses positioning information to define associated regions so that the routing is spatially oriented and limited. This is analogous to associatively-oriented and restricted broadcast in ABR [2] [3].

1.8. Characteristics of MANET

i. **Autonomous and infrastructure less:**MANET is a self-organized network, independent of any established infrastructure and centralized network administration. Each node acts as a router and operates in distributed manner.

ii. **Multi-hop routing:**Since there exists no dedicated router, so every node also acts as a router and aids in forwarding packets to the intended destination. Hence, information sharing among mobile nodes is made available.

iii. **Dynamic network topology:**Since in MANET, nodes move randomly in the network, the topology of MANET changes frequently, leading to regular route changes, network partitions, and possibly packet losses.

iv. **Variation on link and node capabilities:**Every participating node in an ad hoc network is equipped with different type of radio devices having varying transmission and receiving capabilities. They all operate on multiple frequency bands. Asymmetric links may be formed due to this heterogeneity in the radio capabilities.

v. **Energy-constrained operation:**The processing power of node is restricted because the batteries carried by portable mobile devices have limited power supply.

vi. **K-scalability:**A wide range of MANET applications may involve bulky networks with plenty of nodes especially that can be found in strategic networks. Scalability is crucial to the flourishing operation of MANET.

2. Attacks on Mobile Ad-hoc Networks

The attacks in MANETs are divided into two major types:

2.1. Internal Attacks

Internal attacks directly lead to the attacks on nodes present in the network and link interfaces between them [26]. These type of attacks may broadcast wrong type of routing information to the other nodes. Internal attacks are sometimes more difficult to handle as compared to external attacks, as the compromised nodes are able to generate the valid signature using their private keys [27].

2.2. External Attacks

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and produces additional overhead to the network [31].

The Internal and External attacks can further be classified into two categories:

i. Passive Attack

In this type of attack, the intruder only performs some kind of monitoring on certain connections to get

information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully [33]. The type of passive attacks are eavesdropping or more often called as Denial of Service attack (DoS), traffic analysis and snooping.

ii. Active attack

In this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; causing routing disruption,

3. Black-hole attack

In a black-hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. This attack drops the data packets in the network. Thus the packets in the network from source never reach the destination [10].

A Black Hole node forges the sequence number and the hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all the data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

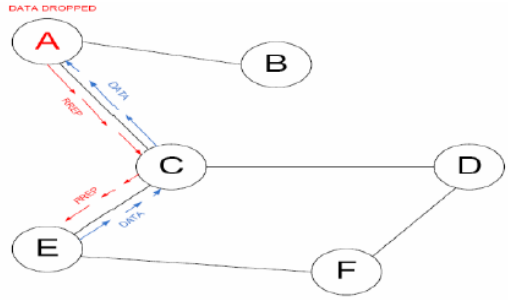

Fig 1: Black-hole attack

3.1. Properties of a Black Hole node

1. The node exploits the ad-hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is fake, with the intention of intercepting packets.

2. The node consumes the intercepted packets [11].

It is a DoS attack possible in wireless ad-hoc networks. In this attack, an attacker sends a false RREP packet to a source node that initiated a route

network resource depletion, and node breaking [34]. The following are the types of active attacks over MANET : Flooding attack, Black-hole attack, Rushing attack, Link spoofing attack, Selective forwarding attack, Sleep deprivation, Node isolation attack, Routing table poisoning attack, Blackmail, Snare attack, The Invisible node attack, Wormhole attack, Cloning attack, Jamming.

The various active attacks can also be categorized according to their effect in the different layers of the network protocol stack.

discovery, posing itself as a destination node or an immediate neighbor to the actual destination node. In such a case, the source node would forward all of its data packets to the attacker, which originally was intended for the genuine destination. The attacker, eventually may never forward any of the data packets to the genuine destination. As a result, therefore, the source and the destination nodes became unable to communicate with each other. Black hole attacks mostly affect proactive protocols and with a great effect on AODV protocol [10, 4]. Since AODV treats RREP messages having higher value of destination sequence number to be fresher, the malicious node will always send the RREP having the highest possible value of destination sequence number. Such RREP message, when received by source node is treated afresh. The malicious node always sends RREP as soon as it receives RREQ without performing standard AODV operations, while keeping the Destination Sequence number very high. Thus, malicious nodes succeed in injecting Black Hole attack [12] [13].

3.2. Types of Black-Hole attack

i. Internal black-hole attack

It is present in the network internally. Here the internal malicious node fits in between the routes of source and destination. As it is present internally so this node makes itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is called an internal attack because here node itself belongs to the network internally. Internal attack is more severe because here malicious node is present inside the network actively [15] [16].

ii. External black-hole attack

External black hole node physically stays outside of the network and denies access to network traffic or creates congestion in network or disrupts the entire network. External attack can become a kind of internal attack when it takes control of internal malicious nodes and control it to attack other nodes in the MANET.

4. Existing Techniques for preventing attacks caused by misbehaving nodes [20][21]

i. Intrusion Detection Systems

Intrusion Detection Systems (IDS) [2] are one of the basic techniques in use to prevent any attacks against security threats. Intrusion detection can be categorized as network based IDS and host based IDS. Network based IDS (NIDS) can be set up on data concentration points of a network such as switches and routers.

ii. Route Confirmation Approach (RCA)

In [3], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) technique to avoid the black hole attack in the network. In this approach, the intermediate node not only sends RREP messages to the source node but also sends CREQ messages to its next-hop node towards the destination node. This is to enquire about the route to the destination node. After receiving a CREQ message, the next-hop node searches its cache for a route to the destination. If it has the route, it sends the CREP to the source. On receiving the CREP message, the source node confirms the validity of the route by comparing the route in RREP message and the one in CREP. If both are the same, the source node confirms that the route is correct. One drawback of this approach is that it cannot avoid the black hole attack in which two consecutive nodes work in agreement with each other, that is, when the next-hop node is an attacker working together with the malicious node sending CREPs that supports the incorrect path.

iii. Multiple Route Replies (MRR)

In [4], the authors have discussed the AODV protocol that suffers from the Black hole attack in MANETs and has proposed a realistic solution for the black hole attacks, which can be implemented on the AODV protocol. This mechanism expects a source node to wait until an RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node confirms that the route is safe and can be used. The main drawback of this solution is that it introduces time delay, because it has to wait until multiple RREPs arrive.

iv. Statistical Anomaly Detection (SAD)

In [5], the authors investigate the effects of black hole attack in MANETs and shows that a malicious node must increase the destination sequence number adequately to persuade the source node that the route provided is amply enough. Based on this investigation, the authors suggest a statistical based anomaly detection approach to detect the black hole attack in the network, based on the difference between the destination sequence numbers of the multiple received RREPs. The advantage of this approach is that it can detect the black hole at low cost without launching extra routing traffic, and it does not require any modification to the existing protocol. However, false positives, where the malicious node raises a false alarm indicating that a given condition has been fulfilled when it actually has not been, are the main drawbacks of this approach due to the nature of anomaly detection.

v. Further Request Approach (FRA)

In [6], according to the author's solution, when any intermediate node replies for an RREQ message, information regarding the next hop to the destination should be included in the RREP packet. The source node then sends a further request (FREQ) message to the next hop of the node that replied to the RREQ message and asks about the node that replied as well as the route to the destination. By using this method the credibility of the responding node can be identified, only if the next hop is trusted. However, this solution cannot prevent cooperative black hole attacks on MANETs. For instance, if the next hop also obliges with the replied node, the reply for the FREQ will be simply answered "yes" for both the questions. Then the source will believe the next hop and transmit data through the replied node which is a black hole node.

vi. Prior - Receive Reply Method

The paper [1] proposes an algorithm that identifies the malicious node which is responsible for the black hole attack. In this method we can check whether there is any large difference between the sequence number of the source nodes and intermediate nodes who has sent back RREP messages or not. Naturally, the first route reply in the routing table will be from the malicious node with high destination sequence number. The first destination sequence number can be compared with the source sequence number. If there exists much difference between source and destination sequence number, then the destination node is a malicious node, allowing the elimination of that entry from the routing table immediately. This is done as 5 different processes which include the initialization process, storing process, identification and removal of the malicious node, node selection process and finally the default process.

5. Intrusion Detection System

An IntrusionDetection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts, identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.

5.1. Requirements for IDS in MANET

The difference between wireless and wired network as regard of IDS are as follows:

i. IDS for MANET must work with localized and partial audit data. In MANET, the audit data is always localized and partial because MANET does not have a fixed infrastructure such as firewall or gateway that is used in wired network to collect complete and global audit data. To deal with local and partial audit data, IDS may need to sense anomaly happened on other hops.

ii. Network-based IDS does not work for wireless network.

iii. It is more difficult for IDS in MANETs to distinguish between normal and intrusion traffic. In wireless network, there is often no clear line between normal/abnormal activities. In wireless network the connection is not stable and mobile nodes can join and leave the network at any time.

iv. IDS should utilize minimum resources. The wireless network does not have stable connection and physical resource of network and devices, such as bandwidth and power, are limited. Disconnection can happen at any time. In addition, the communication between nodes for IDS purpose should not take too much bandwidth resources.

v. Encryption in communication is difficult to achieve. The communication between IDS on different nodes must be secure to not allow attacks gain the access to such communication. However, encryption in MANETs is a difficult task itself.

vi. IDS cannot assume any node is secure. Unlike in a wired network, MANET nodes can be very likely compromised. Therefore, in cooperative algorithm, the IDS must not assume that any nodes can be fully trusted.

vii. IDS must address high false alarm rate problem. It is difficult to obtain enough audit data to make an intrusion detection decision, because the bandwidth of MANET is much restricted compared with wired network. As a result, IDS in MANET can easily result in either having too much false alarm or missing many attacks.

viii. The IDS be truly distributed, which means IDS must detect intrusion on each node, but nodes can collaborate in making decision on whether to issue an alarm.

6. Routing protocol types

The routing protocols in MANETs can be classified into three categories based on their update mechanisms: proactive routing protocols, reactive routing protocols and hybrid routing protocols.

6.1. Pro-Active Table Driven Routing Protocols

Proactive routing protocols maintain routing information of all the nodes in the network and add new routes or update existing routes by periodically distributing routing information among each other. One advantage of doing so is that routes to any destination are ready to use when needed. However,

this is offset by the overhead of route updates in response to mobility, for which nodes may have to wait anyway [45]. Routing tables grow with the size and density of the network, rather than the number of routes actually needed.

6.2. Reactive On-Demand Routing Protocols

Unlike proactive routing protocols, reactive routing protocols construct routes only when they are required [46]. Thus the nodes using reactive routing protocols do not need to update their routing tables as frequently and do not maintain routes for all nodes in the network. When a node using a reactive protocol requires a route to a new destination, it initiates a route request and must wait until the route is discovered. Reactive routing protocols have the disadvantage of delay in finding routes to new destinations traded against the savings of not needing to maintain tables for all possible routes.

6.3. Hybrid Protocols

Hybrid routing protocols aggregates a set of nodes into zones in the network topology. Then, the network is partitioned into zones and proactiveapproach is used within each zone to maintain routing information. To route packets between different zones, the reactive approach is used [57].Consequently, in hybrid schemes, a route to a destination that is in the same zone is established without delay, while a route discovery and a route maintenanceprocedure is required for destinations that are in other zones. These protocols can provide a better trade-off between communicationoverhead and delay [55], but this trade-off is subjected to the size of a zone and the dynamics of a zone. Thus, the hybrid approach is an appropriate candidate for routing in a large network. At network layer, routing protocols are used to find rote for transmission of packets.

7. AODV Routing Protocol (Ad-hoc On-Demand Distance-Vector Routing)

The Ad-hoc On-Demand Distance Vector (AODV) routing protocol is designed for use in ad-hoc mobile networks. AODV is a reactive protocol [36]: the routes are created only when they are needed. It uses traditional routing tables, one entry per destination, and sequence numbers to determine whether routing information is up to date and to prevent routing loops. An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired [38]. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicast back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors [40] [45].

Whenever routes are not used they get expired and get discarded. It helps in reducing stale routes and also reduces need for route maintenance. It minimizes number of active routes between an active source and destination. AODV can determine multiple routes between a source and a destination, but implements only a single route, because it is difficult to manage multiple routes between same source/destination pair. If one route breaks, it is difficult to know whether other route is available. Lot of book-keeping is involved in AODV.

Sequence Numbers are used in AODV to:

1. To avoid using old/broken routes.
2. To determine which route is newer.
3. To prevent formation of loops.

7.1. Limitations of AODV

AODV besides being an efficient routing algorithm possesses some limitations due to which it is easily attacked by the external intruders. Following are a few limitations of the AODV protocol [50] [51].

1. If the sequence number of source node is lower than that of intermediate nodes, it may lead to inconsistent routes.

2. Multiple route reply packets and periodic beaconing may result in heavy routing overhead [48].

3. The overall performance starts degrading as network grows.

4. There is noacknowledgement procedure that ispresent and hence no validation.

8. References

[1] A. Salomaa, *Public-Key Cryptography*, Springer-Verlag, 1996.

[2] A. Tanenbaum, *Computer Networks*, PH PTR, 2003.

[3] L. Zhou and Z. Haas, Securing Ad Hoc Networks, *IEEE Network Magazine*Vol.13 No.6 (1999) pp. 24-30.

[4] S. Yi, P. Naldurg, and R. Kravets, Security Aware Ad hoc Routing forWireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002.

[5] H. Luo and S. Lu, URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks, *IEEE/ACM Transactions on Networking* Vol.12 No.6 (2004) pp. 1049-1063.

[6] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions. *Ad Hoc Wireless Networks*, edited by X. Chen, X. Huang and D. Du. Kluwer Academic Publishers, pp. 319-364, 2003.

[7] S. Burnett and S. Paine, *RSA Security's Official Guide to Cryptography*, RSA Press, 2001.

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

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

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

[11] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing in Mobile Wireless Ad-Hoc Networks. *Proc. of the 4th IEEE Workshopon Mobile Computing Systems and Applications* (WMCSA'02), pp. 3-13,2002.

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

[13] P. Papadimitratos and Z. Haas, Secure Routing for Mobile Ad Hoc Networks. *Proc. of the SCS Communication Networks and Distributed Systems Modelingand Simulation Conference* (CNDS 2002), 2002.

[14] W. Mehuron, Digital Signature Standard (DSS). U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL). FIPS PEB 186, 1994.

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

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

[17] 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.

[18] 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.

[19] Y. Hu, A. Perrig, and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. *Proc. of the ACM Workshop on WirelessSecurity* (WiSe), pp. 30 40, 2003.

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

[21] 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.

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

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

[24] B.Wu, J.Wu, E. Fernandez, S. Magliveras, and M. Ilyas, Secure and Efficient Key Management in Mobile Ad Hoc Networks. *Proc.*

[25] L. Buttyan and J. Hubaux, Report onWorking Session on Security inWirelessAd Hoc Networks. *Mobile Computing and Communications Review*, vol. 6, 2002.

[26] S. Ravi, A. Raghunathan, and N. Potlapally, Secure Wireless Data: System Architecture Challenges. *Proc. of International Conference on System Synthesis*, 2002.

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

[28] N. Borisov, I. Goldberg and D.Wagner, Interception Mobile Communications: The Insecurity of 802.11. *Conference of Mobile Computing and Networking*,2001.

[29] P. Kyasanur and N. Vaidya, Detection and Handling of MAC Layer Misbehavior in Wireless Networks. *Proc. of the International Conference on DependableSystems and Networks*, pp. 173-182, 2003.

[30] A. Crdenas, S. Radosavac, and J. Baras, Detection and Prevention of MAC layer Misbehavior in Ad Hoc Networks. *Proc. of the 2nd ACM Workshop onSecurity of Ad Hoc and Sensor Networks*, pp. 17-22, 2004.

[31] C. Murthy and B. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall PTR, 2005.

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

[33] K. Ng andW. Seah, Routing Security and Data Confidentiality for Mobile Ad Hoc Networks. *Proc. of Vehicular Technology Conference*(VTC), Jeju, Korea, 2003.

[34] M. Jakobsson, S. Wetzel, and B. Yener, Stealth Attacks on Ad Hoc Wireless Networks. *Proc. of IEEE Vehicular Technology Conference* (VTC), 2003.

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

[36] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, *Proc. of the Sixth Annual International Conferenceon Mobile Computing and Networking* (MOBICOM), Boston, 2000.*of 19th IEEE International Parallel & Distributed Processing Symposium*, Denver, 2005.

[37] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, Proc. of the Sixth Annual International Conference on Mobile Computing andNetworking (MOBICOM), Boston, 2000.

[38] P. Kyasanur and N. Vaidya, Detection and Handling of MAC Layer Misbehavior in Wireless Networks, Proc. of Dependable Computing and CommunicationsSymposium (DCC) at the International Conference on DependableSystems and Networks (DSN), 2003.

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

[40] H. Yang, X. Meng, and S. Lu, Self-Organized Network-Layer Security in Mobile Ad Hoc Networks. Proc. of ACM MOBICOM Wireless Security Workshop (WiSe'02), Atlanta, 2002.

[41] 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.

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

[43] P. Ning and K. Sun, How to Misuse AODV: A Case Study of Inside Attacks against Mobile Ad-Hoc Routing Protocols, Proceedings of the 2003 IEEEWorkshop on Information Assurance, United States Military Academy, West Point, NY, 2003.

[44] V. Park and S. Corson, Temporally-Ordered Routing Algorithm (TORA) Ver. 1 Functional Specification, IETF draft, 2001.

[45] T. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR) Project, Hipercom, INRIA, www.ietf.org/rfc/rfc3626.txt, RFC-3626, 2003.

[46] X. Wang, D. Feng, X. Lai, and H. Yu, Collisions for Hash Functions MD4, MD5, HAVAL 128 and RIPEMD, Cryptology ePrint Archive, Report 2004/199, http://eprint.iacr.org/, 2004.

[47] 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.

[48] R. Nichols and P. Lekkas, Wireless Security-Models, Threats, and Solutions, McGraw-Hill, Chapter 7, 2002.

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

[50] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham, "A Taxonomy of Computer Worms", First Workshop on Rapid Malcode(WORM), 2003.

[51] C. Kaufman, R. Perlman, and M. Speciner, Network Security Private Communication in a Public

World, Prentice Hall PTR, A division of Pearson Education,Inc., 2002
[52] S. Capkun, L. Buttyan, and J. Hubaux, Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop onSecurity of Ad Hoc and Sensor Networks, 2003.