International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

# A Simulation Scheme for Improving the Data Security in Mobile Ad-hoc Network

**Najiya Sultana[1], S. S. Sarangdevat[2]**

[1]Assistant Professor, Taibah University, Saudi Arabia

[2]Vice Chancellor, Department of CS & IT, Rajasthan Vidhyapeeth University, Udaipur, India

**Abstract:** ***With the modernization of the wireless communication system, mobile ad-hoc network (MANET) has gain a pace in the area of communication system. Conceptualized with infrastructureless networking system, every mobile nodes in MANET participate in the process of network behave both as host as well as router and therefore, it is guided by the communication principles to forward the packet to other nodes and hence formulate networking phenomenon. The area of MANET has already found its scope in Military Battlefield, Sensor Networks, Commercial Sector, Medical Service, and Personal Area Network. MANET possesses some inherent characteristics e.g. self-organizing capabilities, maximum degree of freedom, dynamic topology etc. Although, the research attempts in MANET is more than a decade old, but still commercialization of the technology are yet to be seen and therefore, due to novelty nature of the technology, MANET is also shrouded by various issues. Although, there are wide ranges of issues in MANET (Routing, power, bandwidth, Quality of Services), but the proposed study focuses on more critical issue e.g. security issues. Mobile ad-hoc network (MANET) is a self-configuring network that is formed automatically via wireless links by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. The mobile nodes allow communication among the nodes outside the wireless transmission range by hop to hop and the forward packets to each other. Due to dynamic infrastructure-less nature and lack of centralized monitoring points, the ad-hoc networks are vulnerable to attacks. The network performance and reliability is break by attacks on ad- hoc network routing protocols. AODV is a important on-demand reactive routing protocol for mobile ad- hoc networks. There is no any security provision against a "Black Hole" and "Wormhole" attacks in existing AODV protocol. Black hole nodes are those malicious nodes that conform to forward packet to destination. But they do not forward packet intentionally to the destination node. The black hole nodes degrade the performance of network by participating in the network actively. The propose watchdog mechanism detect the black hole nodes in a MANET. This method first detects a black hole attack in the network and then provides a new route to this node.***

**Keywords:** MAC, AODV, Black Hole, MANET, RREP, RREQ

## 1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the assistance of any stand-alone infrastructure or centralized administration [1]. Each node in mobile ad-hoc networks is fit out with a wireless transmitter and receiver, which permits it to communicate with other nodes in its radio communication range. Nodes usually share the similar physical media; they transmit and get signals at the same frequency band, and follow the same hopping sequence or spreading code. If the destination node is not within the transmission range of the source node, the source node takes help of the intermediate nodes to communicate with the destination node by relaying the messages hop by hop. In order for a node to transmit a packet to a node that is out of its radio range, the cooperation of other nodes in the network is required; this is called as multi-hop communication. Therefore, each node must act as both a host and router at the same time [2].

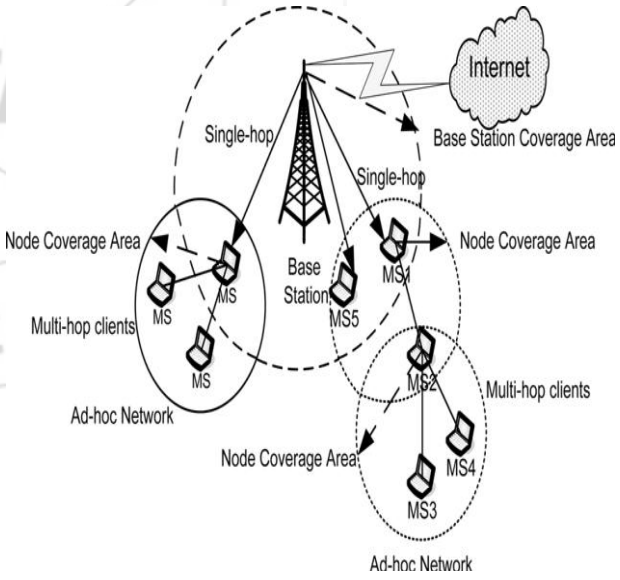


**Figure:** Multihop Scenario

## 2. Routing Protocol

Routing protocols can be categorized into proactive, reactive and hybrid protocols, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type of protocol are Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on demand protocols, in opposite, do not regularly update the routing information. It is circulated to the nodes only when

necessary. Example of this type of protocol is Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type of protocol is Zone Routing Protocol (ZRP) [3].

### 2.1 Proactive Routing Protocol

In a network utilizing a proactive routing protocol, every node keeps one or more tables representing the complete topology of the network. These tables are updated constantly in order to keep up-to-date routing information from each node to every other node.[4] To maintain the up to date routing information, topology information needs to be alternate between the nodes on a regular basis, leading to comparatively high overhead on the network. On the other hand, routes will be available on request. Many proactive protocols arise from conventional link state routing, along with the Optimized Link State Routing protocol (OLSR) [5].

**Table 1**(RREQ field):

| |
|---|
| Source address |
| Source Sequence |
| Broadcast Id |
| Destination address |
| Destination Sequence |
| Hop count |

### 2.2 Reactive Routing Protocol

Reactive routing protocols [6] are on-demand protocols. These protocols do not try to keep correct routing information on all nodes at all times. Routing information is collected only when it is required, and route determination based on sending route queries throughout the network. The primary benefit of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be consumed. While reactive protocols do not have the fixed overhead needed by keeping continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network because of query flooding. Because of these weaknesses, reactive routing is less applicable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes [7].

**Table 2:** (RREP field)

| |
|---|
| Source address |
| Destination address |
| Destination Sequence |
| Destination address |
| Hop count |
| Lifetime |

### 2.3 Hybrid Routing Protocol

Wireless hybrid routing is depends on the idea of organizing nodes in groups and then allowing nodes different functionalities inside and outside a group [8]. Both routing table size and update packet size are decreased by involving in them only part of the network (instead of the whole); thus, control overhead is decreased. The most popular way of building hierarchy is to group nodes geographically close to each other into definite clusters. Each cluster has a leading node (cluster head) to communicate to other nodes on behalf of the cluster. The other way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications pass across overlapping scopes. More efficient overall routing performance can be acquired through this flexibility. Since mobile nodes have only a single unidirectional radio for wireless communications, this type of hierarchical organization will be mentioned to as logical hierarchy to distinguish it from the physically hierarchical network structure [9].

### 2.4 Security Criteria for Mobile Ad-Hoc Network

While the security requirements for ad-hoc networks are the same the ones for fixed networks, namely availability, integrity, confidentiality, authentication, and non-repudiation.

#### 2.4.1 Availability

The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [9]. This security standard is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes do some of the network services unavailable, such as the routing protocol or the key management service [10].

#### 2.4.2 Integrity

Integrity guarantees the individuality of the messages when they are delivered. Integrity can be adjusted mainly in two ways-

- Malicious altering
- Accidental altering

A message can be deleted, replayed or revised by an adversary with malicious goal, which is admire as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is classified as accidental altering.

#### 2.4.3 Confidentiality

Confidentiality means that certain information is only use by those who have been authorized to access it. In other words, in order to keep the confidentiality of some confidential information, we require keeping them secret from all entities that do not have the privilege to access them.

#### 2.4.4 Authenticity

Authenticity is basically assurance that participants in communication are genuine and not impersonators [9]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to confidential resources, or even propagate some fake messages to disturb the normal network operations [11].

**2.4.5 Non Repudiation**

Non Repudiation guarantees that the sender and the receiver of a message cannot disavow that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

## 3. Proposed Work

In packet table, each node maintains track of the packets, it sent. It contains a unique packet ID, the address of the next hop to which the packet was forwarded, address of the destination node, and an expiry time after which a still-existing packet in the buffer is considered not forwarded by the next hop.

In node rating table, each node maintains rating of nodes, which are next to it (means nodes are within its communication range). This table includes the node address, a counter of dropped packets noticed at this node and a counter of successfully forwarded packets by this node [1]. The fourth field of the above node rating table is calculated by the ratio of dropped packets and successfully forwarded packets, if this ratio is greater than a given threshold value then this node misbehave value will be 1(means it is interpreted as a misbehaving node), otherwise it is deliberated as a legitimate node. An expired packet in the pending packet table causes the packet drops counter to increase for the next hop correlated with the pending packet table entry. Each node listens to packets that are inside its communication range, and only to packets associated to its domain. Then, it checks each packet and prevent forged packet. If it notices a data packet in its pending packet table, then it deletes this data packet from pending packet table after authenticating the packet. If it notices a data packet that exits in its pending packet table with source address different from the forwarding node address, then it increases the packet forwarding value in node rating table [1].

## 4. Wormhole Attacks

In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called “wormhole link”. They capture packets at one end and replay them at the other end using private high speed network. Wormhole attacks are relatively easy to deploy but may cause great damage to the network. Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets. Due to the recent performance advancements in computer and wireless communication technologies, mobile wireless computing is becoming increasingly widespread. One type of network that is most evolving is MANET (Mobile Ad-hoc Network).It is a wireless technology where the nodes are changing their topology with respect to time. MANET’s are dynamic, rapidly-changing random, multihop technologies composed of bandwidth constrained wireless links. This networking fundamental is mobility of nodes which is unrealized in world of networks.

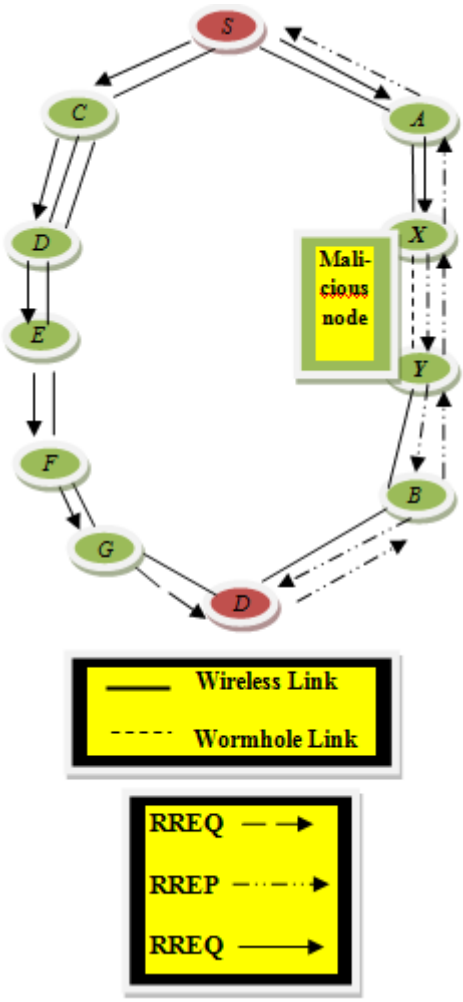


**Figure:** Wormhole Attack

## 5. Security

The 802.11 MAC Layer provides authentication and privacy. Since the signals are broadcast through the open air, the standard implementers should provide some level of security to prevent unauthorized users access to the network through which they might forge or steal information. The standard provides Open-system Authentication and Shared-key Authentication methods to enforce authentication and Wired Equivalent Privacy (WEP) to enforce privacy. In Open-System Authentication (OSA), both the station and the authenticator agree on exchanging data. The stations must be configured to use the same Service Set Identifier (SSID) in order to authenticate [16,17]. First, the initiating station

sends a MAC authentication frame to the authenticator station. This authentication frame states that it is an open-system authentication type. The authenticator responds to this frame with an authentication frame that indicates whether the authentication frame was accepted or rejected.

## 6. Countermeasures Against Wormhole Attacks

For detection and prevention of wormhole attacks, "Packet Leash" mechanism is suggested in which all nodes in the MANET can obtain authenticated symmetric key of every other node. The receiver can authenticate information like time and location from the received packet. "Time of Flight" is a technique used for prevention of wormhole attacks. It calculates the roundtrip journey time of a message; the acknowledgement estimate the distance between the nodes based on this time, and conclude whether the calculated distance is within the maximum possible communication range. If there is a wormhole attacker involved, packets end up travelling further, and thus cannot be returned within the short time [12, 13,14,15].

## 7. Conclusion

This research determines that the IEEE 802.1X could enhance the security level in authentication and privacy by enabling the rekeying process but would not prevent Denial of Service attacks via unauthenticated management frames. WEP and filtering are the security mechanisms provided by the current specification. If both mechanisms are applied correctly, they could protect WLANs from unauthorized access. However, when advanced, determined attackers are considered, there are many potential security leaks which may be exploited to access network services. MANET requires a reliable, efficient, and scalable and most importantly a secure protocol as they are highly insecure, self-organizing, rapidly deployed and they use dynamic routing. Mobile Ad-Hoc network is likely to be attacked by the black hole attack and wormhole attack. To solve this problem, here present a watchdog mechanism and time of flight to detect and overcome black hole attack and wormhole attack and improve the data security in mobile ad-hoc network.

## 8. Future Work

Management packets, such as deauthentication, disassociation, EAP-Success, EAPOL-Start, or EAPOL-Logoff could be generated to evaluate more types of these attacks. Tools for generating arbitrary management packets should be created by revising the source code of the HostAP. To secure MANETs against a plethora of often unpredictable attacks, security protocols are required that take the specific constraints and characteristics of MANETs into account. Efficient and light-weight security protocols are needed that can be handled by devices with limited computational capabilities. On the one hand, the requirements on efficiency and security are high, but on the other hand the devices' capabilities and bandwidth provided by the communication channel is limited. To this end, protocols must be designed to optimally exploit the available infrastructure and possibilities for pre-configuration of the respective MANET.

## References

[1] David B.Johnson and Dravid A. Maltz, "Dynamic Source routing in ad hoc wireless networks", *Technical report, Carneigie Mellon University*, 1996
[2] Harris Simaremare and Riri Fitri Sari, "Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks", International Journal of Computer Science and Network Security, VOL-11, June 2011, Page Number-6.
[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, *IEEE Communication magazine*, October 2002.
[4] Imrich Chlamtac, Marco Conti, Jennifer J. - N. Liu " Mobile ad hoc networking: imperatives and challenges ", School of Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.
[5] Lidong Zhou, Zygmunt J. Hass, "Securing Ad Hoc Networks*", IEEE Special Issue on Network Security*, Vol-13, Nov-Dec 1999, Page Number - 24-30L.
[6] P. Ning and K. Sum, "How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol", Tech Rep, TR- 2003-07, CS Department, NC University, April 2003
[7] Wenjia Li and Anupam Joshi, "Security Issues in Mobile Ad Hoc Networks", Department of Computer Science and Electrical Engineering, University of Maryland.
[8] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, Volume-2 Issue-3, pp. 18-29
[9] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, "MANET Routing Protocols and Wormhole Attack against AODV" , IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010
[10] Dongbin Wang, Mingzeng Hu and Hui Zhi, "A survey of secure routing in ad hoc networks", Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, PRC.
[11] Jesse R. Walker, "*Unsafe at Any Key Size: An analysis of the WEP Encapsulation"*, doc: IEEE 802.11-00/362, October 2000.
[12] W. Stallings, *Wireless Communications and Networks*, Prentice Hall 2002.
[13] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, creditbased system for mobile ad-hoc networks," in *Proc. 22nd Conf. Computer Commun. (INFOCOM 2003)*, vol. 3, Barcelona, Spain, Mar.-Apr. 2003, pp. 1987-1997.
[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Lecture Notes Computer Sci., Advances Cryptology -CRYPTO 2001*, vol. 2139. Springer-Verlag, 2001, pp. 213-229.
[15] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," *Wireless Netw. (WINET)*, vol. 13, no. 5, pp. 118-124, Oct. 2007.
[16] F. Zhang, R. Safavi-Nani, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Lecture Notes Computer Science, Proc. PKC 2004*, vol. 2947. Springer-Verlag, 2004, pp. 277- 290.
[17] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," *Wireless Netw. (WINET)*, vol. 13, no. 5, pp. 118-124, Oct. 2014