International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 4, April-2014, pp: (108-114), Impact Factor: 1.252, Available online at: www.erpublications.com

# A Conventional and proposed model for comparative study of security breach attack in Mobile Adhoc Network

Indrajeet Kumar[1], Varun Prabhakar[2], Jyoti Rawat[3], Noor Mohd.[4]
[1,2,3,4]Research Scholar, GBPEC, Pauri, Uttrakhand, INDIA

**Abstract: A mobile ad-hoc network consists of mobile nodes that can move freely in an open environment. Communicating nodes in a Mobile Ad-hoc Network usually seek the help of other intermediate nodes to establish communication channels. In such an environment, malicious intermediate nodes can be a threat to the security of conversation between mobile nodes. So that This paper is based on the bibliography of security issues of networks, especially mobile ad hoc networks. The purpose of this note is to give a quick review on the security related problems in MANETs, types of possible attack and comparison between available security protocols.**

**Key terms**: **MANET, Routing protocol, Attacks.**

## Introduction

Mobile Ad-Hoc Networks are autonomous and infrastructure less wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network. Mobile nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance and personal computer that can participate in the network and are mobile in nature. These nodes can act as host/router or both at the same time. MANET is self governing, where there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes on each other. The network can be set up anywhere without any geographical restrictions [07]. Mobile Ad-Hoc network topology is dynamic and can change rapidly because the nodes are able to move freely and can organize themselves randomly [06,07]. This property of the nodes makes the mobile Ad-Hoc networks unpredictable from the point of view of scalability and topology.

Most important networking operations include routing and network management. Routing protocols can be divided into proactive, reactive and hybrid protocols, depending on the routing topology [08,10,15]. Fig. 1elobarte the protocol suite for MANET. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV), WRP, CGSR etc. Reactive or source-initiated on-demand protocols [20], in contrary, do not periodically update the routing information [03,04,05]. Routing information is propagated to the nodes only when necessary. Example of this type includes 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 includes Zone Routing Protocol (ZRP), EIGRP.
Area of application for MANET includes emergency services such as disaster recovery and relief activities, where traditional wired network is already destroyed. It can be also used for automated battlefield and war games. There are so many other application areas such as entertainment, education and commercial where MANET play their role for connecting people.

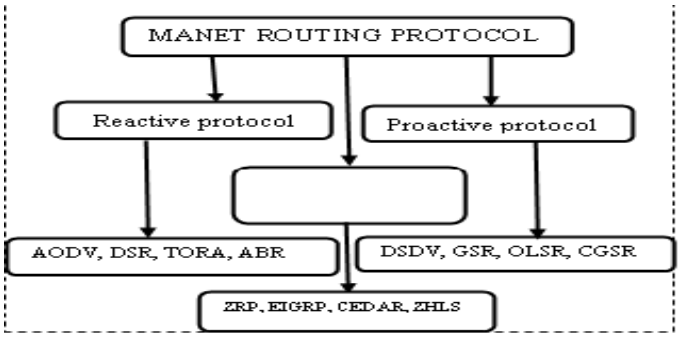


**Fig. 1: MANET Protocol SUITE**

As the nodes are dynamic and work without centralized control, they are more prone to attacks thus the MANETs work without a centralized administration where the nodes communicate with each other on the basis of mutual trust [01, 07]. This characteristic makes MANETs more vulnerable to be exploited by an attacker inside the network. Wireless links also makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Mobile nodes present within the range of wireless link can overhear and even participate in the network[01].

## Security Challenges in MANET

Like all other networks, MANETs need security assurance for its normal operations [13]. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism[02]. However, securing MANETs is particularly challenging due to its unique features described as below.

- The network topology is constantly changing as a result of nodes joining in and moving out.
- Network nodes have limited resources (e.g., battery power, CPU capacity, memory and bandwidth).
- Wireless links between nodes are unreliable.
- Mobile nodes lack for sufficient physical protection.
- There is the absence of a centralized monitoring or management point.

## Security Issues in MANET

Security in Mobile Ad-Hoc Network (MANET) is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by managing security issues[13].

### Flaws in MANETS

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is nobody that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed bellow [13].

### Non Secure Boundaries

MANET is vulnerable to different kind of attacks due to no clear secure boundary. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity[13].

### Compromised Node

Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Due to behaviour of this autonomous nodes it is very difficult for the nodes to prevent malicious activity of the with which it is communicating. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network are more dangerous than attacking threats from outside the network[13].

### No Central Management

MANET is a self-configurable network, which consists of Mobile nodes where the communication among these nodes is done without a central control. Each and every node act as router and can forward and receive packets. MANET works without any pre-existing infrastructure. This lack of centralized management leads MANET more vulnerable to attacks. Detecting attacks and monitoring the traffic in highly dynamic and for large scale Ad-Hoc network is very difficult due to no central management [13.

## CLASSIFICATION OF ATTACKS

The attacks can be categorized on the basis of the source of the attacks i.e. Internal or External, and on the behavior of the attack i.e. Passive or Active attack. This classification is important because the attacker can exploit the network either as internal, external or as well as active or passive attack against the network [14].

### External and Internal Attack

External attackers are mainly outside the networks who want to get access to the network and once they get access to the network they start sending fake packets, denial of service in order to disrupt the performance of the whole network. This attack is same, like the attacks that are made against wired network. These attacks can be prevented by Implementing security measures such as firewall, where the access of unauthorized person to the network can be mitigated [09].

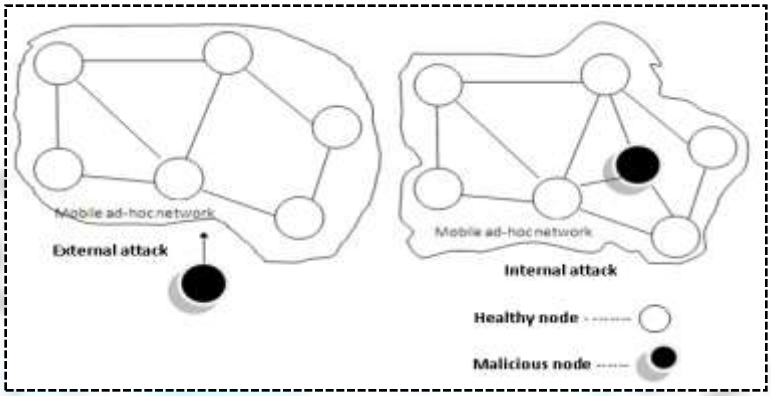


**Fig. 2: External and internal attack**

In internal attack the attacker wants to have normal access to the network as well as participate in the normal activities of the network. The attacker gain access in the network as new node either by compromising a current node in the network or by malicious impersonation and start its malicious behavior. Internal attack is more severe attacks then external attacks.

### Active and Passive Attack

In active attack the attacker disrupts the performance of the network, steal important information and try to destroy the data during the exchange in the network. Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of network in such case the active attack act as internal node in the network. Being an active part of the network it is easy for the node to exploit and hijack any internal node to use it to introduce bogus packets injection or denial of service [09]. This attack brings the attacker in strong position where attacker can modify, fabricate and replays the massages. Attackers in passive attacks do not disrupt the normal operations of the network. In Passive attack, the attacker listen to network in order to get information, what is going on in the network. It listens to the network in order to know and understand how the nodes are communicating with each other, how they are located in the network. Before the attacker launch an attack against the network, the attacker has enough information about the network that it can easily hijack and inject attack in the network [18].

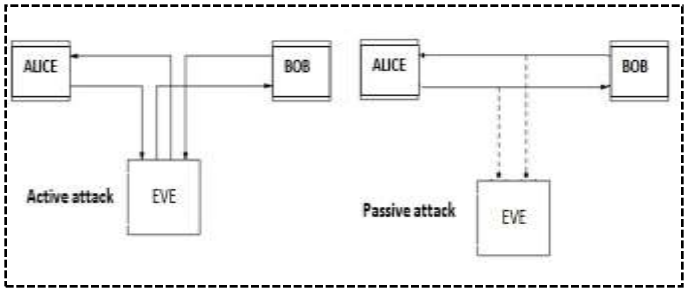


**Fig. 3: Active attack and Passive attack**

**Black Hole Attack**

An black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [12, 49].

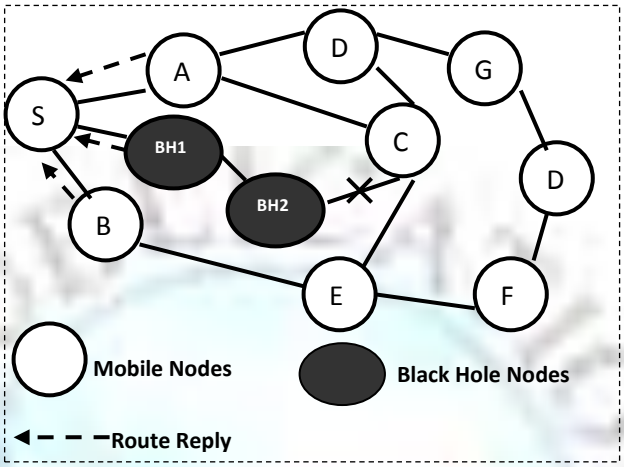


**Fig. 4: Black Hole Attack**

**Gray Hole Attack**

In this kind of attack the attacker misleads the network by agreeing to forward the packets in the network. As soon as it receive the packets from the neighboring node, the attacker drop the packets. This is a type of active attack. In the beginning the attacker nodes behaves normally and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray-hole attacks the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack [09].

**Flooding Attack**

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time [09].

**Wormhole Attack**

Wormhole attack is a severe attack in which two attackers placed themselves strategically in the network. The attackers then keep on hearing the network, record the wireless data. The figure bellow shows the two attackers placed themselves in a strong strategic location in the network [12].

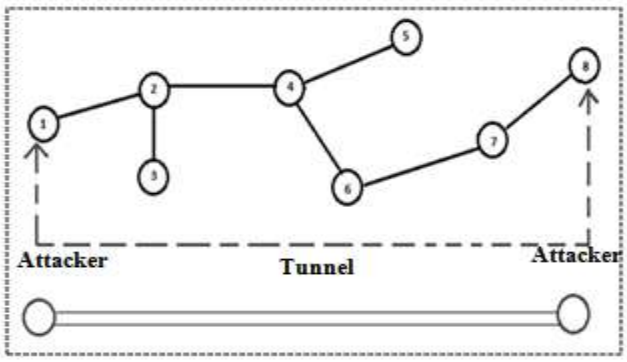


**Fig. 5: Wormhole Attack**

**Sleep Deprivation Torture Attack**

One of the most interesting attack in MANETs, where the attacker tries to keep the nodes awake until all its energy is lost and the node go into permanent sleep. This attack is known as sleep Deprivation torture attack. The nodes operating in MANETs have limited resources i.e. battery life, the node remain active for transmitting packets during the communication. When the communication cease these nodes go back to sleep mode in order to preserve their resources. The attacker exploit this point of the nodes by making it busy, keeping it awake so as to waste all its energies and make it sleep for the rest of its life. When nodes went to sleep for ever an attacker can easily walk into the network and exploit rest of the network.

**Jellyfish Attack**

In jellyfish attack, the attacker attacks in the network and introduce unwanted delays in the network. In this type of attack, the attacker node first get access to the network, once it get into the network and became a part of the network. [09] The attacker then introduce the delays in the network by delaying all the packets that it receives, once delays are propagated then packets are released in the network. This enables the attacker to produce high end-to-end delay, high delay jitter and considerably effect the performance of the network.

**Modification Attack**

The nature of Ad-Hoc network is that any node can join freely the network and can leave it. Nodes which want to attack join the network. The malicious node then later exploits the irregularities in the network amongst the nodes. It participates in the transmission process and later on some stage launches the message modification attack. Misrouting and impersonation attacks are two types of modification attack [09].

**Misrouting Attack**

In misrouting attack a malicious node which is part of the network, tries to reroute the traffic from their originating nodes to an unknown and wrong destination node. As long as the packets remain in the network make use of resources of the network. When the packet does not find its destination the network drops the packet [18].

**Selfish Node**

In MANETs the nodes perform collaboratively in order to forward packets from one node to another node. When a node refuse to work in collaboration to forward packets in order to save its limited resources are termed as selfish node, this cause mainly network and traffic disruption. The selfish nodes can refuse by advertising non existing routes among its neighbor nodes or less optimal routes. The concern of the node is only to save and preserves it resources while the network and traffic disruption is the side effect of this behavior. The node can use the network when it needs to use it and after using the network it turn back to its silent mode. In the silent mode the selfish node is not visible to the network. The selfish node can sometime drop the packets. When the selfish node see that the packets need lot of resources, the selfish node is no longer interested in the packets it just simply drop the packets and do not forward it in the network [18].
Proposed Secure Routing protocol for MANET

Recently, a lot of research has focused on the cooperation issue in MANET. Several related issues are briefly presented here. Researchers have proposed solutions to identify and eliminate a single black hole node

**Watchdog and The Path Rater:** Misbehavior detection and reaction are described, by Marti, Giuli, Lai and Baker. The paper presents two extensions to the DSR algorithm: the watchdog and the path rater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission. This technique is imperfect due to collisions, limited transmit power and partial dropping. However, according to simulations, it is highly effective in source routing protocols, such as DSR. The path rater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. The path rating is calculated by averaging the rating of the nodes in the path, where each node maintains a rating for all the nodes it knows in the network. Watchdog is used intensively in many solutions for the cooperation problem. The main drawback of this idea is that it enables selfishness and misbehaving nodes to transmit packets without punishing them, and thus encourages misbehavior.

**CONFIDANT protocol:** Buchegger and Le Boudecs [19] present the CONFIDANT protocol .Each node Monitor the behavior of its next hop neighbors in a similar manner to watchdog. The information is given to the reputation system that updates the rate of the nodes. Based on the rating, the trust manager makes decisions about providing or accepting route information, accepting a node as part of a route and so on. When a neighbor is suspicious in misbehaving, a node informs its friends by sending them an ALARM message. If a node's rating turns out to be intolerable, the information is relayed to the path manager, which proceeds to delete all routes containing the intolerable node from the path cache. This does not address partial packet dropping.

**CORE scheme:** Michiardi and Molva propose the CORE [16] scheme and various related issues. In his scheme, every node computes a reputation value for every neighbor, based on observations that are collected in the same way as watchdog. The reputation mechanism differs between subjective reputation, indirect reputation, and functional reputation. Subjective reputation is calculated directly from neighbors past and present observations, giving more relevance to past observations in order to minimize false detection influence. Indirect reputation is the information collected through interaction and information exchange with other nodes using positive values only. Functional reputation is the global reputation value associated with every node. By avoiding the spread of negative rating, the mechanism resists attacks, such as denial of service. When a neighbor reputation falls below a predefined value, the service provided to the misbehaving node is suspended.

**Comparison of Various Secure Routing Protocols**

On the basis of the various studied protocols a comparison table is given below [01, 12, 17] :

| Proposed Protocol | Routing Strategy | Security from | | | |
|---|---|---|---|---|---|
| | | Rushing attack | DoS | Tunnelling | Routing table modification |
| ARIADNE | On-Demand | Yes | Yes | Yes | Yes |
| SLSP | Table driven | Yes | Yes | No | Yes |
| SAODV | On demand | Yes | No | No | Yes |
| CORE | Table driven | No | Yes | No | No |
| CONFIDANT | On demand | Yes | No | Yes | No |
| WATCHDOG & PATHRATER | On demand | No | No | Yes | No |

Above table displays that a lot of work is done for rushing attacks, Denial –of- service and Table modification attacks but for Tunnelling attacks a lot of secure protocols are required. Also, every secure routing protocol can handle only limited attacks.

## Conclusion

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. With the importance of MANET comparative to its vast potential it has still many challenges left in order to overcome. Security of MANET is one of the important features for its deployment. In our thesis, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks with solution finding technique. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. So there is a requirement of routing protocol which not only provide efficient routing but can also provide security to the mobile ad-hoc network (MANET).

## References

[1]. A. Menaka Pushpa, "Trust Based Secure Routing in AODV Routing Protocol", IEEE, 2009.
[2]. A Mishra and K.M Nadkarni, security in wireless Ad -hoc network, in Book. The Hand book of Ad Hoc Wireless Networks (chapter 30), CRC press LLC, 2003.
[3]. C.E.Perkins and E.M.Royer, "Ad-Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
[4]. C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-684, May, 2003.
[5]. C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and protocol Second Edition, Low price Edition, Pearson Education, 2007.
[6]. Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003,pp. 13–64.
[7]. F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol. 35, pp. 22-26, Apr, 2002.
[8]. G. S. Mamatha and Dr. S. C. Sharma "Analyzing the MANET Variaitons, Challenges, Capacity and Protocol Issues", International Journal of Computer Science & Engineering Survey (IJCSES), Vol. 1, no.1, August 2010.
[9]. H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks," International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.
[10]. http://en.wikipedia.org/wiki/ Mobile_ad hoc network, last visited 12, Apr, 2010.
[11]. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang, " Security in mobile ad hoc networks : challenges and solutions ", IEEE Wireless Communications, February 2004.
[12]. http://www.ijca online.org /volume12 /number4 / pxc3872250.pdf.
[13]. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology," Sweden, March 2007.
[14]. Kevin Hoffman,David Zage,and Cristina Nita-Rotaru. A Survey of Attack and Defense Techniques for Reputation Systems. Department of Computer Science and CERIAS Purdue University. April 2008,pages 19.
[15]. M.Abolhasan, T.Wysocki, E.Dutkiewicz, " A Review of Routing Protocols for Mobile Ad-Hoc Networks," Telecommunication and Infromation Research Institute University of Wollongong, Australia, June, 2003.
[16]. Michiardi P, Molva R. " Core : a collaborative reputation mechanism to enforce node Corporation in Mobile Ad Hoc Networks ", In Proceeding of the sixth IFIP Conf. on Security Communications and Multimedia (CMS), 2002.
[17]. Ming Yu, Mengchu Zhou and Wei Su, " A Secure Routing Protocol Against Byzantine Attacks for MANETs in Adversarial Environments ", IEEE Transactions on Vehicular Technology, Vol 58, no. 1, pp 449-460, 2009.
[18]. Po-Wah Yau and Chris J. Mitchell, "Reputation methods for routing security for mobile ad-hoc network" http:// www.isg.rhul.ac.uk/ ~cjm/ rmfrsf.pdf.
[19]. S. Buchegger, C. Tissieres, and J. Y. Le Boudec. A testbed for misbehavior detection in mobile ad-hoc networks - how much can watchdogs really do. Technical Report IC/2003/72, EPFL-DI-ICA, November 2003.
[20]. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks, Architectures and protocol Second Edition, Low price Edition, Pearson Education, 2007.