Survey on Various Security Attacks and the Mitigation Techniques for MANET

Ashima Mittal[1] and Satwinder Singh[2]
[1,2]*Department of Computer Science,*
Guru Nanak Dev University, Regional Campus, Jalandhar, India
E-mail: [1]er.ashimamittal2013@gmail.com, [2]er.satwindermehmi@gmail.com

***Abstract*—Mobile ad-hoc network is a network of Mobile nodes that are connected with a wireless Link. There is no centralized node that controls the Network. The recent trend in mobile ad-hoc networks is on-demand routing where routes are established on Demand. Various security threats come into existence these days. Mobile ad-hoc networks are highly dynamic in nature. So, secure routing is a major issue now days. This paper is a survey on various security attacks, various mitigation techniques proposed by various researchers protocols for secure routing and the research on current trends.**

Keywords: MANETs, Routing, Denial of service (DoS)

I. Introduction

Wireless communication is growing day by day due to its Increasing applications. In recent years, MANETs (mobile ad-hoc Networks) have received more attention due to its self-creation and self-maintenance nature. Each device in MANET is free to move in any direction which results the change in link table frequently. The member nodes are itself responsible for all the link management. Each node in a MANET has its own wireless transmitter and receiver so that nodes can communicate with each other in their wireless range. The nodes which are not within the wireless range communicate with other nodes hop by hop by following some rules known as routing protocols. The latest work is done in wireless technology achieve a lot of attention. An ad-hoc network is one of such advancement in wireless technology which gives a new platform to wireless self-organized networks. The ad-hoc networks are not infrastructure networks and create routes when required. They are peer-to-peer network. They are mainly used for military oriented purposes. Confidentiality, integrity, availability, non-repudiation and authentication are the basic requirements of information security [2]. The dynamic nature of mobile ad-hoc networks creates a problem in finding multi-hop routes for communication path. In ad-hoc networks mobile node can move randomly because each node act as a router, so it is very difficult to find an optimal route. Security is still the main topic for many researchers. They provide various security routing protocols for secure communication.

II. Various Routing Protocols

In MANETs, some form of routing protocol is required in order to dynamically detect the multi-hop paths through which packets can be sent from one node to another [1]. Basically, there are two types of routing protocols for MANETs.

A. Table Driven (Proactive)

In this, every node maintains a table that represents the entire network topology. Various proactive protocols are DSDV, GSR and WRP.

B. On-Demand (Reactive)

In this, routes are not predefined for routing. Here, The Source node initiates the route discovery procedure when needed. Some reactive protocols are ABR, AODV, DSR and LAR. Much of the research has been done working in efficiency and stable routing of the MANETs. Because of the previous research, now we have huge number of routing protocols that are marvelous in terms of efficiency. But the situation changes when we focus on the security requirements of these protocols. The more detailed research is under the way to find a secure routing protocols. Due to the Open medium communication and dynamically changing behavior of MANETs, they are more vulnerable to attacks. Researchers have provided various secure routing protocols by watching their resistance towards various security attacks. Various proposes protocols by researchers are Secure Efficient Distance Vector Routing SEAD), Authenticated Routing for Ad-hoc Networks (ARAN), Secure Routing protocol (SRP) and many more.

III. Some Security Attacks

There exist some potential loopholes in MANETs that can be exploited by undesirable nodes to destroy the smooth functioning in the network. In MANETs, attacks are classified into two types: active attacks and passive attack. Brief introduction about both the attacks is given below.

A. Passive Attacks

In this attack intruder snoop packet that contain secret information by listening only to the channel e.g. IP addresses, location of nodes etc., without disturbing the operation of network. These attacks are very difficult to identify.

1. *Eavesdropping:* In this attack, the malicious node obtain some secret information e.g. password of the node that is very important to kept secret, location, private key and public key.

2. *Traffic Analysis:* In this attack, attacker detects transmission to inflict important information such as source-destination pair.
3. *Jellyfish Attack:* In this attack, attacker breakdown the performance of the network by introduces the delay in sending packets that it receives.

B. *Active Attacks*

In active attacks, malicious nodes confuse the network topology by introducing false information to it. They can do two things either attract the traffic or compromise the packets. They can send packet to the wrong node.

1. *Denial of Service (DoS) Attack:* In this, attacker does not corrupt data; he can just disable services by replacing them with the virtual services.
2. *Wormhole Attack:* An attacker took the packet from one location in the network, tunnels the packet to another location and again resends the packet in the network but at different location. Wormhole attack is a big threat to security of MANETs. The wormhole attack can be detected and prevented by implementing digital signature.
3. *Sinkhole Attacks:* In this, a sinkhole node becomes the attraction point for all the nodes and attracts the data toward itself from other neighboring nodes. Sinkhole node maintains the route according to itself, create complicated network and finally destroy the network.
4. *Gray-Hole-Attack:* In this, malicious node behaves like it is an actual node during the discovery process. After route discovery process when sender sends the packet it silently drop the packets sent to it.
5. *Fabrication Attack:* It is an active attack which breaks the network authenticity by acting like it is a source node. It then sends an error message to the nodes to inform that the network is no more exists. Other nodes update their table with false information. In this way it drops the routing performance of a network.

IV. Related Work on Various Security Techniques

The Authors in [3] presented a design and performance evaluation of new on-demand ad hoc network routing protocol known as Ariadne. Ariadne helps the protocol by preventing attacker from altering with uncompromised routes consisting of such uncompromised nodes. Ariadne also helps to prevent Denial-of-Service attacks. Some more features of Ariadne is that it is efficient and using only efficient symmetric cryptographic operations. They also compared Ariadne to a version of Dynamic source routing (DSR) by disabling all protocol optimizations that are not present in Ariadne and then calculate the effect of optimization and security separately. They prove that Ariadne lowers the packet overhead by 41% than for unoptimized DSR. However Ariadne added some cost for security that was not present on unoptimized DSR.

Cheng Yong, Huang Chuanhe and Shi Wenming in 2007 suggested novel secure routing protocol for mobile ad-hoc networks known as trusted dynamic source routing (TDSR) [4]. In this a trust score is calculated on the basis of direct trust and indirect trust. When the trust value of the node falls below the threshold then it is added to the blacklist. The nodes that performs below the threshold or present in blacklist are not b forwarded.

Dhurandher and Mehra in 2009 [5] introduced the approach that can be used to calculate the trust value of node in a dynamic manner and also protects message modification by attacker. The result is calculated by doing simulations in packet delivery ratio and the number of times packet was broken into parts. By considering behavior of a node a trust value is given to a node. it can be incremented and decremented according to the behavior of node. Trust value can be of three types that are: positive, negative or zero that shows that node is known, malicious or unknown behavior respectively.

Pallavi and Trivedi in 2011[6] gave solution to prevent serious attack that is a wormhole attack by the use of digital signatures. In this if a sender wants to send packet to destination node it will create a secure path with the help of digital signature verification. Node sends a packet along with a digital signature and if it matched with the digital signature stored in their database of other nodes then the request is from authentic source.

Kamini Nalavade and Dr. B.B. Meshram in June, 2014 gave the layered approach for preprocessing of data in intrusion detection system [7]. To remove unwanted and redundant data from packets, the layered approach of TCP/IP model is used for the faster preprocessing of data in intrusion detection system.

S. Saravanakumar, Umamaheshwari, D. Jayalakshmi and R. Sugumar [8] in 2010 handles the issue of complexity and throughput that are the problems in Intrusion Detection System (IDS). The authors compare various IDS systems and then suggests a scheme that uses the combination of artificial neural network algorithms. This combination of algorithm gives better performance.

Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU [9] in 2010 proposed the algorithm to detect black hole and gray hole attacks in adhoc networks. The researchers demonstrates the adaptive approach using cross layer design. The authors proved their theory by using path-based method to overhear the next node. So, it saves system resources by not sending out extra control messages. A collision rate reporting system is established to reduce the false positive rate under high network load.

TABLE 1 A BRIEF SUMMARY OF VARIOUS KINDS OF SECURITY ATTACKS ON MANETS AND THEIR MITIGATION TECHNIQUES

Security Attack	A Brief Description of the Security Attack	Techniques Proposed to Mitigate the Attacks
1. Black-Hole Attack	Also called Packet drop attack in which intruder drop all the packets advances to it.	1. The technique in [12] makes use of creditable routing table to detect the black-holes and eliminate them. 2. The authors in [9] verify the control messages sent by the attacker and check if the black-hole attack is executed. 3. In [13] a two-stage technique is followed. In the first stage detection of the malicious nodes is done and in the second stage the removal of malicious node is done.
2. Wormhole Attack	In this attack, an intruder records the packets at one location and forwards them to another location.	1. The wormhole attack can be detected and prevented by implementing digital signature. This is proposed by [6]. 2. In [14] the researchers use a cooperative approach among the distributed nodes to detect and minify the wormhole attack.
3. Sink-Hole Attack	In a Sink-Hole attack, the intruder node/malicious node sends fake routing information claiming that it has an optimum route to the target which causes other nodes in the Ad Hoc Network to route data packets through it.	1. A trust based algorithm is implemented in [15] to diminish sink-hole attack. 2. In [10] they make use of technique in which the mobile agents are used to detect and reduce the sink-hole technique. 3. The authors in [16] implement scheme which include three variables: Sequence Number, Route Add Ratio and Previous Image Ratio to prevent and mitigate the Sink-hole Attacks.
4. Grey hole attack	It drops the part of the data and cheats the previous node.	1. In [17], author proposed mechanism to detect gray hole attack. The detection involves proactively invoking of collaborative and distributive algorithm involving neighbors. The detection decision is based on threshold cryptography.
5. Route Fabrication	In this attack the wrong routing massages are sent into the network by the intruder.	1. In [18] the authors use fuzzy logic, a soft computing method to establish a quantifiable trust value among the nodes of the network. This approach prevents the route fabrication attack.

QuanJia, Kun Sun and Angelos Stavrou [11] in 2011 designed an approach to prevent Denial of Service (DoS) attack. This approach is designed for multipath communication in mobile ad hoc networks (MANETs). They defined the capability messages that are exchanged in between the nodes of network. This enables the each node to maintain overall throughput of flows in the network and then dynamically adjust local constraints. it helps to prevents DoS attacks against a specific node.

Following Table I show the brief survey on different kind of security attacks and some mitigation techniques to minify the effects of these attacks.

V. RESEARCH GAPS

As we all know MANETs are always very attractive for the military purposes and lot of research is going on this topic. Security is always a major topic in research field. As MANETs use is increasing day by day, new attacks are also coming forth continuously. So, the main research gap in the field of security is that researchers are only focusing on some nodes and some routing protocols. None of the existing system is a complete solution for the security attacks. As we have limited resources in MANETs, this topic is also less explored. Researchers should examine more security risks to explore the topic of security and also to find its solution.

VI. CONCLUSION

This paper gave all the stock information about the security of ad hoc networks. In the introduction section we discussed about the MANETs. We also discussed about the routing protocols and its types. In the next part, we discussed some of the main security attacks that are vulnerable to ad hoc networks. This paper proposed the related work on the security threat by many researchers and the research gap in this field. Lot of work is going on the security attacks by intruder.This paper is a survey on various methods that are proposed by researchers to prevent security attacks and the what the researchers should more focus about security of MANETs.

ACKNOWLEDGMENT

We would like to thank almighty for his constant blessings. We would also like to thank Dr. Jyoteesh Malhotrawho provide valuable advices and our friends for helping and supporting us throughout the making of this paper.

REFERENCES

[1] Jayraj Singh, Arunesh Singh, Raj Shree “An Assessment of Frequently Adopted Security Patterns in Mobile Ad hoc.

[2] Stallings W [2000], Network Security Essentials: Security Attacks. Prentice Hall. (pp. 2-17).

[3] YIH-CHUN HU∗and ADRIAN PERRIG Carnegie Mellon University, USA DAVID B. JOHNSONRice University, USA.in 2005.

[4] CHENG Yong, HUANG Chuanhe, SHI Wenming, “Trusted Dynamic Source Routing Protocol”, Wireless Communications, International Conference on Networking and Mobile Computing, WiCom2007, Sept. 21-25,2007,pp.1632-1636.

[5] Sanjay K. Dhurandher, VijetaMehra, “Multi-path and Message Trust-Based Secure Routing in Ad Hoc Networks”, International Conference on Advances in Computing, Control, andTelecommunication Technologies, ACT '09. Dec. 28-29,2009,pp.189-194.

[6] Pallavi Sharma, Aditya Trivedi, “An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN), May 27-29 2011, pp.307-311.

[7] International Journal of Computer Applications Technology and Research (IJCATR) Volume 3 Issue 6 June 2014 Layered Approach for Preprocessing of Data in Intrusion Prevention SystemsKamini Nalavade,Dr. B. B. Meshram.

[8] S. Saravanakumar, Umamaheshwari, D. Jayalakshmi, R. Sugumar, “Development and implementation of artificial neural networks for intrusion detection in computer network”, Int. Journal of Computer Science and Network Security2010. vol. 10, no. 7, pp. 271-275.

[9] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU, “An Adaptive Approach to Detecting Black and GrayHole Attacks in Ad Hoc Network”, 2010 24th IEEE International Conference on Advanced Information Networking and Applications (AINA),Perth, Australia,April 20-23, 2010, pp.775-780.

[10] D.Sheela, Naveen Kumar. C, G.Mahadevan, “A Non-Cryptographic method of Sink HoleAttack Detection in WirelessSensor Networks”, 2011 International Conference on Recent Trends in InformationTechnology(ICRTIT),Chennai, India,June 3-5, 2011, pp.527-532.

[11] Quan Jia, Kun Sun, Angelos Stavrou, “CapMan:Capability-based Defense against Multi-Path Denial of Service (DoS) Attacks in MANET”, Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN), Maui, HI, USA 2011, July 31-August 4, 2011, pp.1-6.

[12] Japing Wang, Haoshan Shi, “A Secure DSR Protocol Based on the Request Sequence-Number”, 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009 (WiCom '09), Beijing, China, Sept. 24-26, 2009, pp. 1-4.

[13] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, Attique Ahmed, “Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks”, International Seminar on Future Information Technology and Management Engineering, (FITME '08), Leicestershire, UK, Nov. 20. 2008, pp.568-572.

[14] Gunhee Lee, Dong-kyoo Kim, Jungtaek Seo, “An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks”, International Conference on Information Security and Assurance (ISA 2008), April 24-26, 2008, pp.220-225.

[15] Thanachai Thumthawatworn, Tapanan Yeophantong, Punthep Sirikriengkrai, “Adaptive Sinkhole Detection on Wireless Ad Hoc Networks”, Proceedings of IEEE Aerospace Conference, 2006,Big Sky, Montana, USA, 4-11 March 2006,pp.1-10.

[16] Benjamin J. Culpepper, H. Chris Tseng, “Sinkhole Intrusion Indicators in DSR MANETs”, Proceedings of First International Conference on Broadband Networks(BroadNets 2004),San Jose, USA, Oct. 25-29, 2004, pp. 681- 688.

[17] Jaydip sen et. al “A Mechanism for Detection of Gray Hole Attack in Mobile AD Hoc Networks” ICICS 2007, IEEE.

[18] H. Hallani, S.A. Shahrestani, “Trust Assessment in Wireless Ad-hoc Networks”, Wireless Days, 2008 (WD '08). 1st IFIP, Dubai, Nov. 24-27, 2008, pp.1-5.