ISSN 2047-3338

Suggesting the Possible Solution of the Most Probable Security Attacks of MANETs

Anum Aftab[1], Junaid Arshad[2] and Muhammad Fuzail[3]
[1,2,3]Department of Computer Science and Engineering, UET, Lahore, Pakistan
[1]anumafab772@gmail.com, [2]mjunaiduet@gmail.com, [3]m.fuzail@ymail.com

***Abstract*– The MANETs security is vital challenge due to its unmonitored deployment nature and its inherent resources limitation. Mobile Ad hoc Network is used in very sensitive fields such as rescue operations, home and enterprise network, education military and airports. Therefore the addressing of security issues of network is most challenging task. Because of restricted possessions of mobile stations, the MANET security is more difficult to implement as compared to other traditional networks. Today huge research is going on in the field of security. Various techniques are now deployed to resolve the security issues. This paper provides possible solution of attacks of security in this evolving arena such as active and passive attacks. This paper also presents an inclusive survey of possible solutions available at a single platform. Suggested solution provide strong wall against problems and enhances the efficiency of security.**

***Index Terms*– Security, MANET, Survey, Attacks and Solution**

I. INTRODUCTION

THIS paper is about Mobile Ad Hoc Networks [1], and how they are created, the attacks MANETS are vulnerable to and also provides the reader with a comprehensive study of the possible solutions of these attacks.

Mobile ad hoc network is an independent system. Also referred as mobile mesh network. The mobile stations are labeled as nodes. These nodes are linked through wireless network without a permanent framework. A set of mobile nodes, interacting together and working individually, and as a router moreover for moving data packets is actually MANET. Common programs of individual node is permitted additionally take part itself in system; this is the reason of MANETs of having a dynamic topology. MANETs are implemented in those configurations which does not have unified structure. IEEE 802.11, Bluetooth and Hyperlan are aiding for possible MANET organizations marketable, so that it can be used outside the domain of military. This innovative advancement triggered the curiosity in research and improvement of MANET [1].

In wireless network a centralized system restricts the malleability. The places where no central infrastructure exist the technologies do not work effectively. Initiation of MANET is based on Bluetooth technology. Ad hoc networks can work even without fixed infrastructure. MANETs are autonomous systems consists of movable nodes linked through wireless network. Nodes collaborate with each other and also act as path between the nodes which cannot communicate directly and route the packet to proper destination. The self-configuring and fully distributed property makes ad hoc network robust [2]. Today mobile ad hoc network is becoming popular due to the requirement of quick hobnob of persons that are out of range of transmission from each other. Network topology is modified according to the movement of nodes in geographical area and parameters of transmission and reception are adjusted [3].

Security is a major concern in a potentially hostile environment for the protection of communication among nodes. MANETs are greatly vulnerable to attacks as compare to the wired networks because of its limitations of unstable topology, physical security, battery inhibited functions in addition to mismanagement and unmonitored environment. Features of Mobile ad hoc networks are Autonomous Terminal Infrastructure-less and Self Operated Distributed operation Dynamic network topologies, Multi-hop routing, Energy constrained Operation, Light–weight Terminal, Ease of deployment, Limited physical security, Network scalability. These features have made MANETs to be used in tactical networks, emergency services, commercial and civilian environments, sensor network, location aware services and informal messages during gathering or lecture [4].

The biggest challenge is securing the adhoc networks. Initial task is to understand the problems and issues properly for suggesting a good solution. Problems of mobile adhoc networks regarding security attacks are not only complex but are diverse too. So compilation of each challenge and attack is not possible at one platform. Considering this fact, all conceivable security issues are studied in detail for mobile adhoc networks. In addition to that issues their respective requirements for providing security are accounted in a definite way in this paper. Hitches faced by MANETs related to all dimensions of security are argued and imaginable solution is suggested.

II. SECURITY PROBLEMS IN MANETS

Limitations in the infrastructure of the MANETs have provided an extensive range to fake nodes for launching a variety of attacks. The two sorts of attacks are passive and active attacks depending on the nature of attacks.

A) Limitations in Passive Attacks

Passive attacks are non-disruptive, just by accumulating the susceptible data from observation of node positions, data being transferred, addresses of IP and channels. No novel generation of traffic makes the detection of attack impossible.

Eavesdropping is an attack on physical layer by analysis of positions of source, destination, duration of communication and amount of packets [5].

Traffic Analysis is an attack on data link layer. Much sensitive information is exposed to attacker by accounting time relationships, load or frequency of traffic.

Selfishness of nodes leads to the correlation rupture by using the network services for transmitting its own data but not let others to use its resources for their transmission [6].

Spoofing attack masks its own IP or MAC address and change the destination of transmission.

B) Limitations in Active Attacks

Active attacks are disruptive includes modification in the content of packet, fake packet generation, masking as authentic node of a fake node etc. these active attacks are identifiable.

Jamming a physical layer active attack causes low speed or failure in the transmission and retrieval of data [7].

Sleep deprivation attack make other nodes to transfer fake data packets frequently which intend to more battery and resource utilization. This leads to improper use of bandwidth [8].

Black Hole attack is employed on network layer that misguides the victim nodes in adapting the short path to destination. In this way attacker grabs the packets of victim node and mistreats packets.

Worm Hole attack is employed by inserting tunnel in topology and use it with high speed afterwards attackers damage topology and introduce wrong routes [9].

Node isolation attack is also a network layer attack. This is actually an attack on OLSR protocol that causes the communicating nodes to be isolated and get no path to communicate [10].

DOS attacks are launched to degrade services of network either by using bandwidth a lot more than normal that no one can use or by utilizing all resources [11].

Rushing attack is by discovery route to victim node and other requests are denied by the node [12].

Byzantine is generated through midway nodes that route alone in infrastructure creates routing rings like loop, drops particular packets, route packets through worst path and network services are corrupted [13].

Table 1 comprises all the attacks that are faced by MANETs.

Table 1: Attacks Faced by MANETs

Type of Attack	Attack	Description
Passive Attacks	Eavesdropping	Eavesdropping is an attack on the physical layer on the mobile ad hoc networks. The main target of eavesdropping is to obtain confidential and private information that the user might intend to keep a secret.
	Traffic Analysis	The attacker tries to extract critical and important information from the target system through monitoring and listening on to the communication between nodes within the mobile ad hoc network.
	Selfishness	Can be described as a node that is has unwillingness to share its resources with other nodes. The main purpose of selfish nodes is to not destroy or bring down the whole network, but on the same hand take benefit from other nodes. They usually can be categorized into four different types: They may appear as a normal node, Another type of selfish nodes will not send Route Reply message to other nodes, third type will intentionally cause delay in relay of route request messages and the fourth kind will relay routing packets but will reject or drop data packets.
	Spoofing Attack	A spoofing attack is done in order to change the appearance of the topology of the mobile adhoc network. The attack is done by masking the malicious node by making it appear as a genuine host node of the network.
Active Attacks	Jamming	Jamming Attack is a form of a Denial of Service attack that causes interferences between the nodes that are communicating with each other. The main goal of the attacker using this type of the attack is to stop an authorized sender or receive to transmit data packets or to receive them through effective communication
	Sleep Deprivation Attack	The attacker in the sleep deprivation attack misuses the process of the discovery of the route in the AODV routing protocol commonly used in MANETS. The attacker continues to broadcast the packets of RREQ so that it can notify every node constantly and therefore utilize the specific nodes source of energy that is already in a very limited form.

	Black Hole Attack	The black hole attack is a form of a denial of service attack in which the mischievous node is able to attract all the packets in the network by wrongly stating itself as a new route for the available packets and then is able to consume the packets without actually forwarding them to their destinations
	Worm Hole Attack	Wormhole attack occurs, where two nodes that conspire against the network, and are at a greater distance apart, are connected through a tunnel giving the rest of the nodes a delusion that the two nodes are actually neighbors. Different kinds of wormhole attacks are: In band wormhole attack, Out of band wormhole attack, Hidden attack, Exposed attack.
	Node Isolation Attack	The node isolation attack results from the denial of service attack on the OLSR protocol. The main objective of this attack is to isolate the node and prevent the node from establishing any form of communicating link between other nodes that may be present on the network.
	Denial of Service Attack	A denial of service attack is a form of attack that eradicates and lessens the capability of a system to provide its relevant services. There can be many reason s that may cause a DoS attack, that includes failure of the hardware to function properly, bugs present in the software, and other environmental conditions, but the main and primary reason behind a Do is the attack by a malicious person that wants to compromise the overall network in order to achieve its personal goals.
	Rushing Attack	Another kind of a Denial of Service (DOS) attack, Rushing attack is an effective way to perform an attack on a MANET. It is known as an efficient form of attack that effects even the safest of the protocols that do exist.

Table 2: Possible solutions of Attacks on MANETs

Type of Attack	Attack	Solution
Passive Attacks	Eavesdropping	Techniques of Frequency Hopping and Spread Spectrum Communication can protect the nodes from eavesdropping by preventing radio interface
	Traffic Analysis	Traffic analysis can be avoided by supporting link layer security and securing wireless MAC protocol
	Selfishness	TWOACK is a very efficient scheme. It identifies the uncooperative behavior of nodes and explores to mitigate the cause through telling routing protocol
	Spoofing Attack	A combination of encryption, steganography and modified frame of data can successfully lead to overcome the spoofing attack.
Active Attacks	Jamming	Use of Spread Spectrum Mechanism to block denial-of-service attacks could be a good solution.
	Sleep Deprivation Attack	The Dynamic Source Routing protocol (DSR) is a basic and proficient directing protocol composed particularly for utilization in multi-hop remote specially appointed systems of mobile nodes.
	Black Hole Attack	The sequence number of destination should be adequately amplified by the node of attacker so that it looks authentic to source node. Ad hoc On Demand Distance Vector (AODV) is a scheme that finds out the black hole attack depending upon the received RREPs having difference in sequence numbers to destination
	Worm Hole Attack	An approach HMTI (HELLO Message Timing Interval) finds nodes of attacker. HMTI has a profile of frequency which is set, a contravention in specification of OLSR protocol. The timing among packets becomes frequently bigger a lot as compare to the interval for legitimate node
	Node Isolation Attack	Intrusion Detection System (IDS) is local module of intrusion detection for OLSR. This module does non-conformance evaluation of each node in network and reveals the existence of attack on routing protocol
	Denial of Service Attack	Fellowship is a model based on obligation proposed in the direction of alleviating the packet flooding and dropping of packet in network. Limitation rate of packets, Restoration as well as Enforcement are defined as the good constraints in this model
	Rushing Attack	Secure neighbor detection, Randomized ROUTE REQUEST forwarding, and Secure route delegation is a set of standard mechanisms that secure the network from rushing attacks

III. SOLUTIONS, SUGGESTIONS AND DISCUSSIONS

Possible solutions of both passive and active attacks are comprises in Table 2 in an extremely comprehensive way. Table 2 shows the possible solutions to both passive and active attacks inclusively.

All these solutions can be enhanced by adding a small layer of encryption depending on the architecture where the security is the matter of concern. Prevention of Active attacks is somewhat all about Cryptography but the use of Steganography can be very useful so that the intruder is kept busy in analyzing that if the communication is taking place. Again the trade off about the architecture will have to be considered. With rapid growth of security algorithms there are many techniques that use encryption even before steganography. These schemes in some cases are impossible to breach unless intruder intends to destroy the data. However these techniques can be a strong barrier for passive attacks as in this case the purpose is only to analyze the information that is being transferred. Steganography techniques are available for all kinds of data formats as it is concerned with the byte stream only. However some data formats that do not support byte stream processing are excluded from this list.

Vernam Cipher is an advance security solution if this scheme is added on all solutions this enhances a security layer of possible solutions of active attacks. As in all passive attacks this scheme will make attacker to believe that no transfer of data or communication is taking place, so, this becomes a strong protection wall.

IV. CONCLUSION

To conclude this research, a lot of work has been done by various institutes to assess the vulnerabilities MANETS are exposed to and the possible solutions. However as these solutions are being implemented, the attackers and hackers are also working in order to overawe these protective measures so that they can attack the Mobile Ad Hoc Networks.

Strict vigilance and monitoring is required over the behavior of MANETS and nodes and any form of misbehavior or anomaly should be immediately be investigated so as to determine the cause and hence necessary action should be taken place.

All the solutions can be enhanced by adding a layer of encryption before steganography depending on the architecture. These techniques provide improvement for all solutions of active attacks. Plus for all the passive attackers a protection like encryption before steganography becomes a strong wall which shows off that no communication or data transfer is taking place.

Moreover, constant work should be done to find ways to improve the security mechanisms that are already been implemented so as to not only improve the existing security of the MANETS, but also to explore the further possibilities that can be unleashed in this regard

.

REFERENCES

[1]. Pravin Ghosekar, Girish Katkar, Pradip Ghorpade, “Mobile Ad Hoc Networking: Imperatives and Challenges”, IJCA Special Issue on “Mobile Ad-hoc Networks”, MANETs, 2010

[2]. G. Jaya kumar and G. Ganapathy, “Performance Comparison of Mobile Ad-hoc Network Routing Protocol”, International Journal of Computer Science and Network Security (IJCSNS), VOL.7 No.11, pp. 77-84, November 2007.

[3]. I. Chlamtac, M. Conti, and J.-N. Liu, “Mobile ad hoc networking: imperatives and challenges,” Elsevier Ad Hoc Networks Journal, vol. 1, pp. 13–64, 2003.

[4]. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad Hoc Networks: Applications and Challenges IAP V/11 contract, by The Institute for the Promotion of Innovation by Science and Technology in Flanders (IWT).

[5]. S. P. Gulhane, R. K. Solanki and N. A. Timande, "A Survey of Black hole and Worm hole Attack on Routing Protocol AODV in MANET," International Journal of Computer Applications, 2012.

[6]. M. Dhivya and A. Kanimozhi, "Improved Routing for Protection against Denial Of Service Attack in Ad Hoc Networks," International Journal of Engineering Research & Technology, vol. 3, no. 3, 2014.

[7]. Y.C. Hu, A. Perrig and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols," in WiSe '03 Proceedings of the 2nd ACM workshop on Wireless security, New York, 2003.

[8]. D. Kidston and Li Li, "Mitigating Security Threats in Tactical Networks," Communications Research Centre (CRC).

[9]. I. S. Mariana, M. Panagiotis and G. Dilintas, "Securing Mobile Ad Hoc Networks Using Spread Spectrum Technology and CDMA".

[10]. M. M. Islam, R. Pose and C. Kopp, "A Link Layer Security Protocol for Suburban Ad-Hoc Networks," School of Computer Science and Software Engineering, Monash University, Australia.

[11]. J. J. and H. K. J, "Mitigating Inside Jammers in Manet Using Localized Detection Scheme".

[12]. M. B. Jani and P. H. Patel, "Mitigation of Blackhole for AODV (Ad hoc On Demand Distance Vector)," International Journal of Computer Science and Mobile Computing, vol. 2, no. 5, pp. 338-345, 2013.

[13]. J. Thalor and M. Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review," International Journal of Advanced Research in, Vols. vol. 3, no. 2, 2013.

[14]. R. Shah, R. L. and S. Sumathy, "Node Monitoring with Fellowship Model against Black Hole Attacks in MANET," International Journal of Computer Science and Business Informatics, vol. 14, no. 1, pp. 14-21., 2014.

[15]. L. TamilSelvan and V Sankaranarayanan, "Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks," in Ad Hoc and Ubiquitous Computing, 2006. ISAUHC '06. International Symposium.