Possible Solutions of Different Security Issues and Challenges in Mobile Ad-Hoc Networks (MANETs)

Anum Aftab[1] and Ayma Aftab[2]
[1]Department of Computer Science and Engineering, UET Lahore, Pakistan
[2]University of the Punjab Lahore, Pakistan
[1]anumafab772@gmail.com

Abstract— **Today, the rising concern for flexible infrastructure services is a call for advanced researches in the emergence of 'Mobile Ad hoc Network'. It is a key technology that supports various ultramodern applications. Security is the important issue in every network. The security of MANET is important 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 a survey of security issues in this dynamic field such as denial of service attack, active and passive attacks, spoofing, eavesdropping, black hole attack, worm hole attack and rushing attack etc. This paper also presents a comprehensive survey of possible latest solutions available e.g. AODV (Ad hoc on demand distance vector), HMTI, Intrusion detection system, Fellowship etc.**

Keywords— **Issues of MANETs, Recent Solutions of MANETs, Challenges in Mobile Adhoc Networks, Security Issues and Requirement of MANETs**

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a self-governing system. It is also called mobile mesh network since mobile stations, termed as nodes, are associated through wireless network without a permanent framework. MANET is actually a batch of mobile nodes collaborating among one another that work individually and as a router too for moving data packets ahead. Frequent movement of each node is allowed moreover set up itself in system; this dynamically modifies topology of network. MANET is used in implementations that does not have centralized configuration. Technologies like IEEE 802.11, Bluetooth and Hyperlan are serving to make possible MANET deployments commercial so that it can be used outside the domain of military. This new progression has provoked the curiosity in research and improvement of MANET.

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. Ad hoc is a Latin word, which means *"for this or for this only"* [1]. 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 following section II describes the security issues regarding to mobile ad hoc networks which are important to be acknowledged to provide any solution. Section III gives the requirements for building security for MANET. Section IV presents a precise study of security attacks and their recent available solutions.

II. SECURITY ISSUES IN MANETS

MANET is highly vulnerable by security attacks caused by its self-governed infrastructure and hostile environment. Due to hostile environment some nodes are left unmonitored which are physically open to attack. Hence mobile nodes are exposed to the attacker to take over the control untraceably and security is compromised. The security issues for MANETs are as follows:

A. Security issue of nodes

Nodes are able to move in mobile ad hoc network that's why the infrastructure is not fixed. This mobility of nodes implies that nodes can move in hostile environment. So, in various conditions nodes can be left unmonitored. In these cases physical attack is mostly possible and nodes could work under the control of adversary. Precautions should be taken for securing information but even these precautions are not enough to protect a fraction of nodes that may be compromised and from inside of network attacks can be launched.

B. Security issue of flexible infrastructure

In mobile ad hoc network the nodes are allowed to move freely which makes the infrastructure flexible or in other words it is a lack of fixed infrastructure. This feature makes the authorized certificate security solutions inapplicable. A security protocol which should be adaptable to the present structure of network is required. Moreover, problems like packet dropping and transmission impairment occur.

C. Security issue of dynamic topology

Since the flexible infrastructure makes arrangement of network keep changing which makes the cryptographic protocols useless for this kind of dynamic infrastructure. Even routes are difficult to be distinguished due to the dynamic change in topology. Hence secure routing is compromised. Static configuration for security is not enough and a protocol is required which is compatible with each protocol that a node might have. Providing such kind of routing protocol with security is a challenging task in addition.

D. Security issue of channels

Eavesdropping, replay attacks, spoofing can be easily done even without any physical approach to components of network because it is easy for the attacker to intercept. Mobile ad hoc networks are unprotected from a wide range of attacks. Therefore, confidentiality is compromised.

E. Security issue of Limited Power Supply

Power consumption is the critical constraint to MANET. The limited power resource may cause breakage of connection. For instance if a node is being used as a router between two nodes and battery fails, then the two nodes would face a link breakage. Due to limited power denial of service and selfish manner of node attacks can be made.

III. SECURITY REQUIREMENTS

To attain security for MANETs familiar attributes are considered as for other networks. An effective security must ensure the following requirements.

A. Authenticity

Requirement of authenticity is necessary because a susceptible node can masquerade as a trusted network and can extract sensitive information or control the operation of nodes. Verifying the identity of peer entity to which node has to start communication prevents the nodes from attacks.

B. Availability

Loss of availability of services and resources is faced due to denial of service and misbehavior of node (selfishness of node in forwarding data packets) attacks. Even attackers can employ jamming technique on physical and MAC (medium access control) layer to jam or conflict communication over physical channel. On network layer routing protocol and on higher layers key management services and other high level services can be disrupted. Attribute of availability makes the services of network available even in the existence of these attacks [7].

C. Data Confidentiality

Securing data during the transmission from one node to another node or denial of unauthorized access is a way of maintaining confidentiality of data. Illegal access to sensitive data and eavesdropping should be blocked by using encryption techniques.

Routing of high sensitive data can occur by passing through many nodes before the destination point. This highlights the need of encryption of data thought out the transmission extended with the encryption of public sensor identities to protect from traffic analysis attack.

D. Integrity

Integrity involves affirmation that data or readings which are transferred cannot be modified by opponent node or any node which is acting as a router between sender and destination node. It needs employment of a strong mechanism of confidentiality which assures integrity easy as addition of one-way hashes prior to the message encryption [5].

E. Non-Repudiation

This requirement is for the security of the receiver node that the message it got has been from the node which it claims to be and vice versa. This is settled by the use of digital signatures [7].

F. Non-Fabrication

Use of wrong path to get access of information is fabrication through which attacks can be employed and these attacks are not easy to be distinguished.

IV. ATTACKS AND SOLUTIONS OF MANETS

MANETs are susceptible to various security attacks mainly due to its flexible infrastructure, unmonitored nodes, dynamic topology and highly constrained on energy and power. These limitations give a broad scope for attackers to attack. Attacks can be classified into two categories on the bases of nature, active and passive attacks.

A. Passive Attacks

It includes non disruptive attacks. Attackers espy the channels, location of nodes, packets and IP addresses. This observation is easy because of sharing nature of MANETs. So, attacker collects sensitive information from the all observed information and uses this collective information in setting up attacks. These attacks are impractical to identify because of no novel traffic generation and wireless environment.

1) Eavesdropping

It is an appropriate physical layer attack which hit the mobile ad hoc networks. Aim of this attack is to get secret data like public or private key, password, location or IP address of node. Two types of data can be caught by attacker that is data transmitted in a time section and collect source, destination, time of transmission, size and number by analyzing packets. This type of data should not be disclosed while communication is being done.

Solution:

Techniques of Frequency Hopping and Spread Spectrum Communication can protect the nodes from eavesdropping by preventing radio interface [8].

2) Traffic Analysis

It is an attack of data link layer. Attacker just require a wireless card operating in promiscuous mode and a software like traffic rate analysis or RF direction finder or time correlation monitor to analyze load or frequency of traffic in a communication. That's why this attack is not completely passive. Network topology, node location, activity of node, role of node, source and destination could be exposed by traffic analysis.

Solution:

Traffic analysis can be avoided by supporting link layer security and securing wireless MAC protocol [9].

3) Selfishness

Uncooperative role of nodes but distinct from evil behavior is named selfishness. Selfish nodes reject to send packets ahead and use services of network for its own transmission and saves power of battery. Selfish nodes does not try to corrupt other nodes, they take advantage of other nodes and consume their resources but don't let their resources to be used by other nodes.

Solution:

TWOACK is a very efficient scheme. It identifies the uncooperative behavior of nodes and explores to mitigate the cause through telling routing protocol [10].

4) Spoofing Attack

Spoofing is employed by nasty node that masks its own recognition in the network (changing its IP address or MAC in leaving packet) plus amends goal of the topology of network that a harmless mobile station may assemble. It produces forming routing packets that may divide the network [11].

B. Active Attacks

It includes disruptive attacks; distract routine processes of a node or entire network. Attackers can modify the packet contents, replay packets to get access by pretending as authentic node, generate fake packets towards worthless destination and attack using fabrication. These attacks are identifiable and evaded by the valid nodes [6].

1) Jamming

It is a physical layer attack. Attacker transmits signals exactly with same speed of that two communicating parties exchange data. This generates enormous troubles like low speed and no data retrieval during transmission. Regular forms of signal jamming are random noise and pulse [12].

Solution:

Use of Spread Spectrum Mechanism to block denial-of-service attacks could be a good solution.

2) Sleep Deprivation Attack

Resources of victim nodes are utilized by the attacker nodes. Nasty nodes make victim nodes busy continuously in sending packets to real or fake node or routing decisions. That's why the power of batteries end and bandwidth of the network could not be used properly [13].

3) Black Hole Attack

It is a critical security attack produced due to dynamic topology. It is a network layer attack. A routing protocol is broadcasted by malicious node which fakes it like shortened pathway for nodes whose information the malicious node needs to catch. As in protocol based on flooding, a fictitious route has been created when the attacker's node reply arrived at the demanding node earlier than the reply from the genuine node. After this it is up to attacker node that it mistreats the packet or modifies or blocks the packets which are routed through it.

Solution:

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 [14].

4) Worm Hole Attack

It is a network layer attack. Two attackers establish a worm hole link by capturing routing traffic on a position and tunnel that on different position in network which create private connection with high speed between them. Attacker afterward insert tunnel again in the network. Through this worm hole link the attackers can disfigure topology and create false routes [15].

Solution:

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 [16].

5) Node Isolation Attack

As the name suggests it is an attack on communicating nodes by detaching these nodes. This actually attacks on OLSR protocol. The communicating nodes are isolated by not spreading link information of particular or specific collection of nodes in the entire network. So these nodes are unknown for other nodes and hence route though these nodes could not be created. This leads towards the isolation of nodes, having no way to communicate [17].

Solution:

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 [18].

6) Denial of Service Attack & Flooding Attack

These are data link layer attacks. The purpose of these attacks is to make the services of network useless either by consuming all resources or by utilizing bandwidth much more that no one could use it. So, Attackers inject a lot of fake data in the network or transmit advertisements in excessive amount that the services are greatly degraded [9], [19].

Solution:

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 [20].

7) Rushing Attack

Attacker initiates a Discovery Route towards the victim node and request for forwarding packets through this route to be the first to reach the surrounding nodes, the path revealed via discovery route constitute step all the way from attacking node. This makes delivery to victim node of rushed request of attacker. Later requests are discarded from the legal nodes.

Solution:

Secure neighbor detection, Randomized ROUTE REQUEST forwarding, and Secure route delegation is a set of standard mechanisms that secure the network from rushing attacks [21].

V. CONCLUSION

The security of MANETs has been important challenge due to its unmonitored deployment nature and its inherent resources limitation. Because of restricted possessions of mobile stations, the MANET security has become more difficult to implement as compared to other traditional networks. Various techniques had deployed to resolve the security issues. In this paper, in a very comprehensive way, all the issues of security have been presented. This paper grasped all the required attributes for Mobile ad hoc networks which have become necessary for achieving the objective of security. A survey of security attacks in this dynamic field such as active, passive attacks and existing recent possible solutions has been conferred.

Advance research in security measures proposed many solutions to resolve security attacks but still some MANET is very susceptible to attacks of security due to no proper countermeasure developed against these security attacks. This work will help in finding those attacks and requirements on which research can be done in future and solutions can be suggested to the attacks.

REFERENCES

[1]. Pravin Ghosekar, Girish Katkar, Dr. 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” *Belgian science policy through IAP V/11 contract, by The Institute for the Promotion of Innovation by Science and Technology in Flanders (IWT).*

[5]. William Stallings, “Cryptography and Network Security: Principles and Practices”, *Pearson Education Inc*, 2003, Edition 3.

[6]. Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu and Lixia Zhang, “Security in mobile ad hoc networks: Challenges and solutions,” *IEEE Wireless Communications*, vol. 11, pp. 38-47, Feb., 2004.

[7]. Djamel Djenouri and Lyes Khelladi, ALGIERS Nadjib Badache, “A SURVEY OF SECURITY ISSUES IN MOBILE AD HOC AND SENSOR NETWORKS”, *IEEE Communications Surveys & Tutorials*, FOURTH QUARTER 2005, VOLUME 7, NO. 4

[8]. Hubaux J.-P., Buttyan L., Capkun S., “The Quest for Security in Mobile Ad Hoc Networks”, *ACM Symposium on Mobile Ad hoc Networking And Computing*, 2001.

[9]. Monika, Mukesh Kumar, Rahul Rishi, “Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review”, *International Journal of Computer Applications (0975 – 8887),* Volume 12– No.2, November 2010.

[10]. Kashyap Balakrishnan, Jing Deng, Pramod K. Varshney, “TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks”, *IEEE*, 2005.

[11]. K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” *10th IEEE Int’l Conf. Network Protocols (ICNP ’02),* Nov. 2002.

[12]. B. Wu, J. Chen, J. Wu, M. Cardei, “A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks,” Department of Computer Science and Engineering, Florida Atlantic university http://student.fau.edu/jchen8/web/papers/SurveyBookchapter.pdf

[13]. Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, “A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc

Networks", *JOURNAL OF COMPUTING*, VOLUME 3, ISSUE 1, JANUARY 2011, ISSN 2151-9617.

[14]. S.Kurosawa, H.Nakayama, N.Kato, A.Jamalipour, and Y.Nemoto, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, vol. 5, no. 3, pp. 338-346, November 2007.

[15]. Y.C.Hu, A.Perrig, and D.B.Johnson, "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks," Proceedings of 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, vol.3, pp. 1976-1986, April 2003.

[16]. M.A.Gorlatova, P.C.Mason, M.Wang, L.Lamont, R. Liscano, "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," Military Communications Conference, MILCOM 2006, pp. 1-7, October 2006.

[17]. B. Kannhavong, H. Nakayama, N.Kato, Y.Nemoto and A.Jamalipour, "Analysis of the Node Isolation Attack Against OLSR-based Mobile Ad Hoc Networks," *Proceedings of the Seventh IEEE International Symposium on Computer Networks (ISCN' 06)*, pp. 30-35, June 2006.

[18]. D.Dhillon, J.Zhu, J.Richards and T.Randhawa, "Implementation & Evaluation of an IDS to Safeguard OLSR Integrity in MANETs", Proceedings Of The 2006 International Conference On Wireless Communications And Mobile Computing, pp. 45-50, 2006.

[19]. P.Yi, Z.Dai, S.Zhang, Y.Zhong., "A New Routing Attack in Mobile Ad Hoc Networks," International Journal of Information Technology, vol. 11, no. 2, 2005.

[20]. V.Balakrishnan, V.Varadharajan, U.K. Tupakula, "Fellowship: Defense Against Flooding and Packet Drop Attacks In MANET," Network Operations and Management Symposium, NOMS 2006, pp. 1- 4, 2006.

[21]. Y.C.Hu, A.Perrig and D.Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proceedings of the ACM Workshop on Wireless Security (WiSe), SanDiego, California, pp. 30-40, September 2003.