Review on Challenges and Security Issues in Mobile Ad Hoc Networks

Ms. Rashmi Dongre
Research Scholar
Tilak Maharashtra Vidyapeeth, Pune, India

Abstract— A mobile ad hoc network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without the help from a network infrastructure. MANET faced lots of challenges allegorically routing, security and clustering. Security is actually an essential issue for the secured conversation in between mobile nodes in a dangerous ecosystem. Although security issues in mobile ad hoc networks have been a major focus in the recent years, the development of fully secure schemes for these networks has not been entirely achieved till now. MANET has no definite defensive structure, so that, it is easily accessible to both trustworthy networking end-users as well as destructive assailants. This paper, presents an elaborate view of issues in MANET security. Based on MANET's special characteristics, we define three security parameters for MANET. Also in addition MANET security is divided into two different aspects and types of various attacks are also discussed in details.

Keywords: Mobile Ad Hoc Network (MANET), Security Attacks in MANET, Denial of Service Attack

I. INTRODUCTION

A MANET is a self configuring network formed by mobile hosts having wireless communication devices Figure-1. MANETs consist of mobile nodes interconnected by multihop communications paths or radio links which are free to move at any speed in any direction and organize themselves randomly Figure-2. And can act as both routers and hosts [2]. The nodes in the network function as routers, clients, and servers. These nodes are constrained in power consumption, bandwidth, and computational power. MANETs lack central administration and prior organization, so the security concerns are different than those that exist in conventional networks [1].

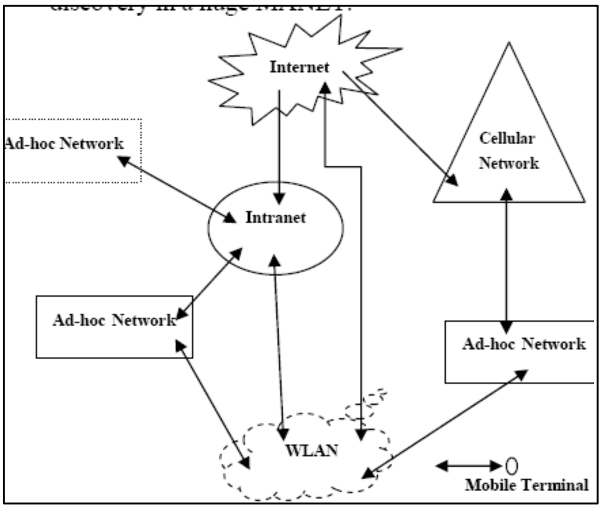

Fig. 1: Architecture of MANET

MANET is more susceptible compared to wired network because of to mobile nodes, hazards coming from affected nodes within the network, restricted physical security, compelling topology, scalability as well as shortage of centralized administration. As a result of these types of vulnerabilities [3] MANET tend to be more susceptible to destructive assaults. The principle focus of this particular task is to present a study upon a lot of different attacks that influence the MANET behavior as a result to virtually any explanation. MANET security involves authentication, key establishment and distribution, and encryption. The aim of this paper is to provide a brief discussion and analysis on MANET security. Based on MANET characteristics, three important security parameters for MANET are defined. Furthermore, analysis and discussion in security attacks and defeating approaches are elaborated. Moreover, the most effective defeating approaches for MANET and their limitations are introduced.

II. LITERATURE REVIEW

A MANET is a most appealing and also growing rapidly innovation that is based upon a self-organized and swiftly implemented network [5]. MANET appeals to separate real-world application segments where in actuality the networks topology variations extremely at a fast rate. The present safeguards possibilities of wired networks cannot be practiced straight away to MANET, which in turn is really a MANET allot more susceptible to security assaults.

Because for the significance of routing standards inside vibrant Multi hop networks, a lot of MANET routing standards have been recommended within the last couple of years [8]. Along with the specialized characteristics of MANET, the subsequent characteristics tend to be expected.

- A routing communications protocol for the MANET should always be dispersed within form in order to really boost their trustworthiness
- A routing protocol need to become tailored contemplating unidirectional connections mainly because wireless media could potentially cause a wireless associate to become exposed in unidirectional just because actual physical aspects.
- The routing protocol ought to be power streamlined
- The routing protocol ought to give consideration to their protection.
- A routing protocol should really be familiar with excellent Service

Some security challenges in MANET were inherited from ad hoc networks that were research interests since 1999. Because of MANET's special characteristics, there are some important metrics in MANET security that are important in all security approaches, which are termed as "Security Parameters" [6]. Figure 2 shows the relation between security parameters and security challenges. Each security approach must be aware of security parameters as shown in Figure 2.

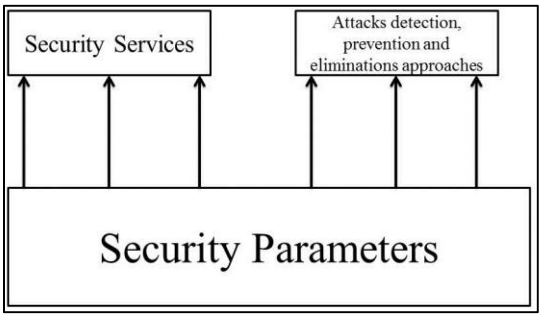

Fig. 2: Relation between Security Parameters and Security aspects

All mechanisms proposed for security aspects, must be aware of these parameters and don't disregard them, otherwise they may be useless in MANET. Security parameters in MANET are as follows:

A. *Network Overhead:*

This parameter refers to number of control packets generated by security approaches. Due to shared wireless media, additional control packets may easily lead to congestion or collision in MANET. High packet overhead increases packet lost and the number of retransmitted packets. This will easily wastes nodes energy and networks resources [10].

B. *Processing Time:*

Each security approach needs time to detect misbehaviors and eliminate malicious nodes. Due to MANET's dynamic topology it's strongly possible that routes between two different nodes break because of mobility. Therefore, security approaches must have as low as possible processing time in order to increase MANET flexibility and avoid rerouting process.

C. *Energy Consumption:*

In MANET nodes have limited energy supply. Therefore, optimizing energy consumption is highly challengeable in MANET. High energy consumption reduces nodes and network's lifetime. Security protocols that disregard these parameters aren't efficient as they waste network resources.

Ad hoc networking is not a new concept. As a technology for dynamic wireless networks, it has been deployed in military since 1970s. A new working group for MANET has been formed within the Internet Engineering Task Force (IETF), aiming to investigate and develop candidate standard Internet routing support for mobile, wireless IP autonomous segments and develop a framework for running IP based protocols in ad hoc network.

III. MANET SECURITY CHALLENGES

Generally there are two important aspects in security: Security services and Attacks. Services refer to some protecting policies in order to make a secure network, while attacks use network vulnerabilities to defeat a security service.

A. *Security Services*

The aim of a security service is to secure network before any attack happened and made it harder for a malicious node to breaks the security of the network. Due to special features of MANET, providing these services faced lots of challenges. For securing MANET a trade-off between these services must be provided, which means if one service guarantees without noticing other services, security system will fail [4]. Providing a trade-off between these security services is depended on network application, but the problem is to provide services one by one in MANET and presenting a way to guarantee each service. The important security services and their challenges are discussed as follows:

1) *Availability:*

According to this service, each authorized node must have access to all data and services in the network. Availability challenge arises due to MANET's dynamic topology and open boundary. Accessing time, which is the time needed for a node to access the network services or data is important, because time is one of the security parameters. By using lots of security and authentication levels, this service is disregarded as passing security levels needs time.

2) *Authentication:*

The goal of this service is to provide trustable communications between two different nodes. When a node receives packets from a source, it must be sure about identity of the source node. One way to provide this service is using certifications, whoever in absence of central control unit, key distribution and key management are challengeable.

3) *Data confidentially:*

According to this service, each node or application must have access to specified services that it has the permission to access. Most of services that are provided by data confidentially use encryption methods but in MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible.

4) *Integrity:*

According to integrity security service, just authorized nodes can create, edit or delete packets. As an example, Man-In-The-Middle attack is against this service. In this attack, the attacker captures all packets and then removes or modifies them.

5) *Non-Repudiation:*

By using this service, neither source nor destination can repudiate their behavior or data. In other words, if a node receives a packet from node 2, and sends a reply, node 2 cannot repudiate the packet that it has been sent.

B. *Attacks on MANET*

Due to special features like hop-by-hop communications, wireless media, open border and easy to setup, MANET became popular for malicious nodes [6]. Some of the most important attacks in MANET are as follows:

1) *Black Hole Attack:*

This dangerous node advertises its availableness about refreshed channels regardless of verifying it's routing table. In this particular approach assailant node will usually experience the accessibility in responding to the route ask for and therefore intercept the information packet and preserve it. In protocol formulated upon flooding [9]. The malware node response will likely be accepted through the requesting node just before the reception of respond back from genuine node; consequently a malicious and forged route is planned. The moment this path is establish, now it's up to the node regardless of whether to decrease all of the packets or forwards it to the unidentified target

2) Worm Hole Attack:

Wormhole attack is a sort of replay attack that is especially frustrating in MANET to shield against. Even if, the routing facts is sensitive, encoded or perhaps authenticated, it could be extremely effective furthermore detrimental. An assailant can easily tunnel a request packet RREQ immediately towards desired destination node without worrying about enhancing the hop-count benefits. The wormhole attack can be combined with all the information shedding attack to protect against the desired destination node from acquiring packets. Wormholes tend to be harmful because they could undertake damage without worrying about even determining the network.

3) Routing Attack:

In this attack, malicious node tries to modify or delete node's routing tables. Using this attack, malicious node destroys routing information table in ordinal nodes. Therefore, packet overhead and processing time will increase.

4) Denial of Service:

In this attack, malicious node prevents other authorized nodes to access network data or services. Using this attack, a specific node or service will be inaccessible and network resources like bandwidth will be wasted. In addition, packet delay and congestion increases.

5) Jamming Attack:

Jamming attack is a kind of DOS attack. The objective of a jammer is to interfere with legitimate wireless communications. A jammer can achieve this goal by either preventing a real traffic source from sending out a packet, or by preventing the reception of legitimate packets.

6) Gray Hole Attack:

This attack is similar to black hole. In black hole, malicious node drops all packets, while in this attack; malicious node drops packets with different probabilities. As it relays some packets, detecting this attack is more complicated than black hole and some detection approaches like sniffing or watchdog will be useless in it.

IV. Incorporating Security Goals and Other Challenges

One way to provide security in MANET, besides decreasing network overhead, is to incorporate security approaches with other challenges [7]. In this way, both challenges are solved by improving security parameters in total. These combinational approaches as follows:

A. Secure Routing Protocols:

The aim of these approaches is to provide security in routing phase. When a node wants to create a path to a destination, it uses some mechanisms to find a secure path and detect malicious nodes in the selected path before sending packets or after sending a number of packets.

B. Privacy:

Secrecy will help to make sure that computer related resources tend to be utilized exclusively by certified person. That is, exclusively those people that really should have accessibility a little something will in reality get that accessibility. In order to maintain privacy of individual's sensitive facts, we have to keep them mystery from all agencies which do not have exclusive right to gain access to them. Privacy is frequently known as secrecy or solitude

Integrity: Ethics implies that resources tend to be altered exclusively by authorized people or perhaps merely as part of certified way. Alteration consists of crafting, switching state, erasing as well as producing. Ethics guarantees that a information currently being transmitted has never been corrupted.

C. Security in QOS:

Using security mechanisms increase packet delivery time and processing time in each node. As a result, security has negative impacts on QOS. Therefore providing QOS beside security in MANET is highly challengeable. Authors in presented a game theory to make a trade-off between security and QOS. Authors in provided an approach that creates QOS aware multipath between source and destination with link information. By providing security in QOS, a level of security and QOS will be guaranteed with low time or network overhead.

D. Authentication:

Verification makes it possible for a node to ensure the identity of equal node it is communicating with. Verification is primarily belief just that people in interaction are authenticated and not impersonators. Reliability is actually ascertained because only the trustworthy transmitter may establish a communication that will decrypt perfectly because of the shared key.

V. Conclusion

In this paper, a comprehensive review in MANET security challenges is presented. Based on MANET characteristics and security requirements, three important security parameters are introduced. A single hand, the security-sensitive programs of an ad-hoc networks need to get extreme level of safety on the other side, Ad Hoc network are inevitably susceptible to safety assaults. There exists an intend to make all of them safer as well as resilient in order to accommodate the strenuous specifications among these networks. The foreseeable future concerning to ad- hoc networks is genuinely enticing, offering the experience of ―at any time, everywhere as well as inexpensive communications. Routing information and encryption defeating approaches are the most effective approaches for MANET security

References

[1] Dinesh, Ajay Kumar, "Security Attacks in Mobile Ad hoc Networks (MANET): A Literature Survey", International Journal of Computer Applications (0975 – 8887) Volume 122 – No.20, July 2015

[2] Ali Dorri, Seyed Reza Kamel, and Esmail kheyrkhah, "Security challenges in mobile ad hoc Networks: a survey," International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015

[3] Sachin Lalar, "Security in MANET: vulnerabilities, Attacks & Solutions", International Journal of Multidisciplinary and Current Research, 10 January

2014, Vol.2 (Jan/Feb 2014 issue), ISSN: 2321-3124 Available at: http://ijmcr.com

[4] Kirti Gupta and Dr. Pardeep Kumar Mittal, "An Overview of Security in MANET," International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-6) June 2017

[5] Mamatha. T, "Network Security for MANETS", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[6] Tripathi Lalit Kumar, Dr. Kanojia Sindhuben, "MANET: Security and Challenges", International Journal of Computer Science and Information Technologies, Vol. 7 (5), 2016, 2381-2384, ISSN: 0975-9646.

[7] Mrs. R. Saraswathi, Dr. A. Subramani, "Increasing the Route Stability for MANET through BTSNA-DS Algorithm", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 2, February 2018, ISSN: 2278 – 1323.

[8] Kavita Khatkar, Neera Batra, "Fault Tolerance Approach for Improving Connectivity in Vehicular Ad Hoc Network", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 2 (2018) pp. 823-829 © Research India Publications. http://www.ripublication.com.

[9] Ranjana Kumari, Achint Chugh, "Distributed Denial of Service Attack Detection, Prevention and Secure Communication in MANET", International Journal of Computer Science Trends and Technology (IJCST) – Volume 6 Issue 1, Jan - Feb 2018.

[10] Dimpal Joshi, Nisha Velani, "A Study of Modified Routing Protocols in MANET", International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN: 2456-3307