Volume 4, Issue 5, May 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Load Balancing in MANETs: A Review

Vanita Sharma[*]
Computer Department
Galaxy Global Imperial Technical Campus ,Ambala

Saurabh Mittal
Computer Department
Galaxy Global Imperial Technical Campus ,Ambala

Abstract— Mobile Ad hoc Network (MANET) is an autonomous collection of mobile nodes that form a temporary network without of any existing network infrastructure or central access point. The popularity of these networks created security challenges as an important issue. In this paper, current challenges in an ad hoc environment which includes the different types of potential attacks that are possible in the Mobile Ad hoc Networks will be discussed. To develop proper security solutions for such environments, we must first recognize how MANETs can be attacked. This paper provides a broad study of attacks against mobile ad hoc networks.

Keywords— ***Load Balancing, Clustering, Efficient Routing, Congestion, MANETs***

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is an independent collection of mobile nodes that form a short-term network without of any existing network organization or central access point. The popularity of these networks created security challenges as an important issue. The old routing protocols perform well with dynamically changing topology but are not designed to protection against security challenges. In this paper we discuss about current challenges in an ad hoc situation which includes the different types of potential attacks that are likely in the Mobile Ad hoc Networks that can harm its working and operation. We have found that there is no universal algorithm that suits well against the most commonly known attacks. But the whole security solution requires the prevention, detection and reaction mechanisms applied in MANET. To develop suitable security solutions for such environments, we must first understand how MANETs can be attacked. This paper provides a broad study of attacks against mobile ad hoc networks. We present a detailed taxonomy of the attacks against MANETs.

II. SECURITY CHALLENGES IN MANET'S

Active attacks [1, 2, 3] in MANET range from erasing messages, inserting messages, imitate a node etc thus violating privacy, verification, obtain ability, integrity, and non-repudiation. Unlike the wired networks achieving security in MANETs is challenging. According to [4] Ad-hoc networks pose a number of nontrivial challenges to security design, such as the following:

i. Dynamic Topology
ii. Autonomous
iii. Scalability
iv. Bandwidth Optimization
v. Poor Transmission Quality
vi. Device Discovery
vii. Limited Resources
viii. Infrastructure less and Self Operated
ix. Topology Maintenance
x. Ad hoc Addressing
xi. Limited Physical Security

III. SECURITY ATTACKS

MANET provides network connectivity between mobile nodes over possibly multihop wireless channels mainly through Link Layer protocols that ensure one-hop connectivity, and Network Layer protocols that extend the connectivity to various hops. These dispersed protocols assume that all nodes are supportive. Because collaboration is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol terms.

A. Passive vs. Active

The Passive attacks take valuable information in the targeted networks. Examples of passive attacks are eavesdropping attacks, traffic analysis attacks. This kind of attack is difficult because neither the system resources nor the network functions are physically affected to prove the intrusions [5].

An Active attack attempts to modify system resources or disturb their operation [5]. These actively alter the data, with the intent of overworking the network, obstructing the operation or to cut off certain nodes from their neighbors so they cannot use the networks services well anymore. To perform active attacks, the attacker must be able to inject packets into the network.

B. External vs. Internal

External attacks are launched by adversaries that are not officially part of the network. These attacks typically aim to cause network congestion, denying access to specific network function or to disrupt the whole network operations. Fake packets injection, denial of service, and impersonation are some of the attacks that are usually introduced by the external attackers.

Internal attacks are sourced from inside a particular network. A cooperated node with access to all other nodes within its range poses a high threat to the functional effectiveness of the whole network. Attacks that are caused by the disobeying internal nodes are difficult to detect because to differentiate between normal network failures and misbehavior activities in the ad hoc networks is not an easy task.

C. Mobile vs. Wired Attackers

Mobile attackers have the same abilities as the other nodes in the ad hoc networks. Their abilities to harm the networks actions are also limited because of restricted resources. With the restricted communicating capabilities and battery powers, mobile attackers could only jam the wireless links within its vicinity but not the whole networks jobs. Wired attackers are attackers that are capable of acquisition access to the external resources such as the electricity. Since they have more resources, they could launch more severe attacks in the networks, such as jamming the whole networks or breaking exclusive cryptography algorithms.

D. Single vs. Multiple Attackers

Attackers might choose to launch attacks in contradiction of the ad hoc networks autonomously or by plotting with the other attackers. Single attackers usually generate a reasonable traffic load as long as they are not capable to reach any wired facilities. Since they also have similar abilities to the other nodes in the networks, their restricted resources become the weak points to them [6].

If several attackers are plotting to launch attacks, shielding the ad hoc networks against them will be much harder. Plotting attackers could easily shut down any single node in the network and be capable to humiliating the efficiency of network’s distributed operations including the security mechanisms.

IV. LAYER-WISE SECURITY ATTACKS

A. Physical Layer Attacks

1. Eavesdropping:

This is capturing and reading of messages and discussions by unintended receivers. The nodes share a wireless medium and the wireless communication use the RF spectrum and transmission by nature which can be easily captured with receivers tuned to the proper frequency. Signals broadcast in air can be easily captured with receivers tuned to the proper frequency. As a result conveyed message can be eavesdropped as well as fake message can be injected into the network.

2. Interference and Jamming:

Interference can happen with radio waves of MANETs, because WLAN use abandoned radio frequencies. Other electromagnetic devices operating in the infrared can overlap over the traffic. A controlling transmitter can generate signal that will be strong to overcome the target signal and can disrupting communications. This condition is called jamming. Pulse and random noise are the taken as most common type of signal jamming [6].

B. Data Link Layer Attacks

1. Traffic Analysis:

Traffic analysis attack adversaries monitor packet transmission to deduce important information such as a source, destination, and source-destination pair. Data on who is connecting with whom, how often, how much, and when is simply available to any listener within range of the wireless network. Even if the payload is encoded, standard MANET protocols transmit sufficient header and routing evidence in the clear making traffic study relatively relaxed for attackers.

2. Disruption MAC (802.11):

Many attacks can be thrown in link layer by unsettling the teamwork of the protocols of this layer. MAC protocols have to coordinate the transmission of the nodes on the shared communication or transmission medium. The IEEE 802.11 MAC is susceptible for DoS attacks. To launch the DoS attack, the attacker may exploit the binary exponential backoff scheme.

3. WEP weakness:

The WEP was designed for pointing at giving some layer of security to wireless networks. IEEE 802.11 WEP joins Wired Equivalent Privacy (WEP) to provide WLAN systems unsure level of privacy by encoding radio signals. The WEP protection technique recommended for adhoc network fall short of the objective of data privacy, data integrity and authentication. Various security standards such as IEEE 802.11i, WPA, and IEEE 802.1 X were recommended to enhance the security issues in 802.11. In spite of their efficiency, these standards do not provide any strength to the security approach for monitoring of the verification in a disseminated architecture.

C. Network Layer Attacks

1. Wormhole Attack:

The wormhole attack [7] is one of the most cultured and severe attacks in MANETs. The wormhole attack is possible even if the attacker has not negotiated any hosts and even if all statement provides authenticity and confidentiality. In this attack, a pair of conniving attackers record packets at one location and replay them at another location using a private network

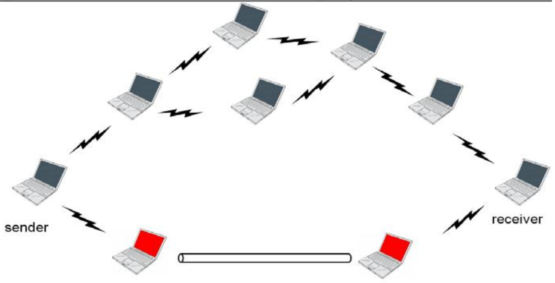

Fig 1: Wormhole attack

The Fig 1 shows the Wormhole attack. It is also possible for the attacker to forward each bit by the wormhole directly, without waiting for a whole packet to be received before start to tunnel the bits of the packet, in order to lessen delay introduced by the wormhole. The attacker is unseen at higher layers; unlike a nasty node in a routing protocol, which can often easily be named, the existence of the wormhole and the two planning attackers at either end- point of the wormhole are not visible in the route.

2. *Blackhole Attack:*

In this attack, a malicious nodes trick all their adjoining nodes to attract all the routing packets to them. It exploits the routing protocol to promote itself as having a good and valid path to a endpoint node. It tries to become an element of an active route. As in the wormhole attacks, nasty nodes could launch the black hole attacks by publicizing themselves to the adjoining nodes as having the most optimal route to the requested destinations. The blackhole attack is shown in Fig 2. However, unlike in the wormhole attacks where many attackers colluded to attack one neighboring node, in the black hole attacks, only one attacker is involved and it threatens all its adjoining nodes.

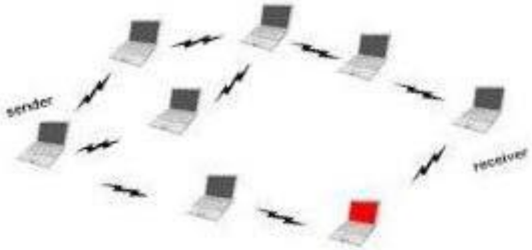

Fig. 2: Blackhole attack

3. *Byzantine attack:*

Byzantine attack can be thrown by a single nasty node or a group of nodes that work in collaboration. A negotiated intermediary node works alone or set of compromised intermediary nodes works in collusion to form attacks. The negotiated nodes may create routing loops, advancing packets in a long route instead of optimal one, even may drop packets. This attack reduces the routing performance and also disrupts the routing services [8].

4. *Flooding attack:*

In this attack, attacker consumes the network resources, such as bandwidth and to consume a node's resources, such as battery power and computational or to upset the routing process to root severe degradation in network performance.

5. *Resource consumption attack*:

In MANETs energy is a serious parameter because the battery-powered devices try to save energy by transmitting only when absolutely needed [9]. The target of resource consumption attack is to send request of excessive route detection or needless packets to the victim node in order to consume the battery life. An attacker or negotiated node thus can upset the normal functionalities of the MANET.

6. *Location disclosure attacks:*

This attack is a part of the information expose attack. The nasty node leaks information regarding the location or the structure of the network and uses the information for further attack. It gathers the node location information such as a route map and knows which nodes are positioned on the target direction and then plans further attack situations. The leakage of such information is overwhelming in security subtle scenarios Traffic analysis is one of the unresolved security attacks against MANETs.

D. Transport Layer Attacks

1. *Session hijacking:*

Session hijacking is a serious error and gives a nasty node the chance of behaving as a authentic system. The attacker takes the advantage that, all the communications are authentic only at the beginning of session setup and does the session hijacking attack. At first, the attacker spoofs the IP address of target machine and regulates the correct sequence number that is predictable by the target and performs a DoS attack on the victim. As a result, the target system becomes inaccessible for some time. The attacker now remains in the session with the other system as a real system.

2. *SYN flooding:*

The SYN flooding attack is also Denial of Service (DoS) attack which is completed by generating a large number of half-opened TCP connections with a victim node. For two nodes to interconnect using TCP, they must first launch a TCP connection using a three-way handshake. The three messages traded during the handshake. The sender sends a SYN message to the receiver with a aimlessly generated ISN (Initial Sequence Number). The receiver also produces another ISN and sends a SYN message including the ISN as an acknowledgement of the received SYN message. The sender sends acknowledgement to the receiver. In this way the connection is established between two interactive parties using TCP three way handshakes.

E. Application Layer Attacks

1. Repudiation:

Firewalls are used to keep packets in or keep packets out in the network layer. In the transport layer, entire connections can be encoded, end-to-end. But these solutions taken to solve confirmation or non-repudiation attacks in network layer or in transport layer are not enough to solve the problems. Repudiation refers to a denial of participation in the communication.

F. Multilayer Attacks

1. Denial of Service:

Attacker injects a large amount of rubbish packets into the network. These packets overspend a significant portion of network resources, and announce wireless channel contention and network contention in the MANET. The limitation of the wireless links is utilized in resource exhaustion attacks. The attackers transfer big, needless volumes of data between them to deplete the bandwidth of the links. The resource exhaustion attack is shown in the Figure 4. During this transfer A and B might send and receive only with a limited efficiency.

Denial of service attacks aim at the complete disruption of the routing function and therefore the entire operation of the ad hoc network. Specific instances of denial of service attacks include the routing table overflow [10] and the sleep deficiency torture [11]. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the contributing nodes and disrupt the establishment of real routes. The sleep deprivation torture attack aims at the consumption of batteries of a specific node by continually keeping it engaged in routing decisions.

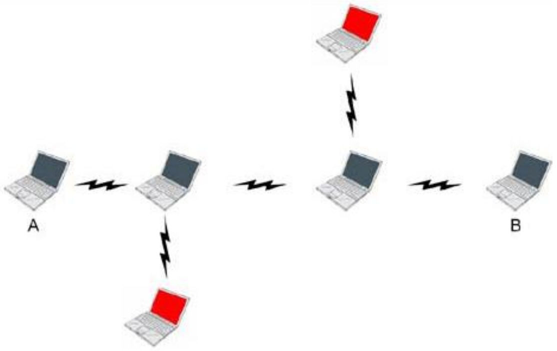

Fig. 4: Resource Depletion Attack

2. Impersonation:

Impersonation attacks are also called spoofing attacks. Spoofing is a special case of integrity attacks whereby a negotiated node imitates a real one due to the lack of authentication in the ad hoc routing protocols. Dependent on the access level of the imitated node, the intruder may even be able to reconfigure the network so that other attackers can easily join or he could remove security measures to allow succeeding attacks. A negotiated node may also have access to encryption keys and authentication information. In many networks, a malicious node could obstruct proper routing by injecting false routing packets into the network or by altering routing information. As described in [20], an intruder may try to imitate a node within the path of the data flow of interest. This can be achieved by altering routing data or implying itself as a trustworthy communication partner to adjoining nodes in parallel.

A spoofing attack allows forming loops in routing packets which may also result in partitioning network. In many cases, lighter solutions like key hashed functions, priori negotiated and certified key and session identifiers are used. However, by using good verification algorithms, strong data encryption and secure routing protocols, the effects of impersonation can be reduced significantly.

3. Man in the Middle Attack:

In this attack, the attacker sits between the sender and the receiver and smells any information being sent between two ends. In some cases the attacker may imitate the sender to communicate with the receiver, or imitate the receiver to reply to the sender.

V. CONCLUSION

In this study, we discussed the security threats in the MANETs. It is clear that the security features related to MANETs are much higher due to the dynamic and impulsive nature of most MANETs. On the other hand, ad hoc networks vary from each other significantly from the viewpoint of the area of submission. Some ad hoc networks may not need security explanations other than simple encryption and username-password authentication scheme, as in the classroom example.

REFERENCES

[1] Nishu Garg and R.P. Mahapatra, “MANET Security Issues”. In IJCSNS International Journal of Computer Science and Network Security, 9, No.8, August 2009.

[2] Arun Kumar Bayya, Siddhartha Gupte, Yogesh Kumar Shukla, Anil Garikapati. “Security in Ad-hoc Networks”. Computer Science Department University of Kentucky.

[3] Sanzgiri K, Dahill B, Levine B.N and Belding-Royer E.M, “A secure routing protocol for Ad-hoc networks,” Proc. Of IEEE ICNP, 2002.

[4] Er. Tushar Gohil “Overview of Security Threats in Mobile Ad-hoc Network”, Journal of High Performance Communication Systems and Networking Volume. 2 (1-2), January-December 2010, pp. 1–10.

[5] S. Bouam and J. B. Othman, “Data Security in Ad hoc Networks using MultiPath Routing,” in Proc. of the 14th IEEE PIMRC, pp. 1331-1335, Sept. 7-10, 2003.

[6] G. Schäfer, “Research Challenge in Security for Next Generation Mobile Networks,” Position Papers PAMPAS '02 - Workshop on Requirements for Mobile Privacy & Security, Sept. 16-17, 2002.

[7] Y.C.Hu, A. Perrig, and D. Johnson, “Wormhole Attacks in Wireless Networks,” IEEE JSAC, vol. 24, no. 2, Feb. 2006.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, An On-demand Secure Routing Protocol Resilient to Byzantine Failures. Proceedings of the ACM Workshop on Wireless Security, pp.21-30, ‘02.

[9] H. Deng, W. Li, Agrawal, D.P., “Routing security in wireless ad hoc networks,” Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.

[10] J.-F. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues and Open Problems,” Proc. Wksp. Design Issues in Anonymity and Unobservability, Berkeley, CA, July ‘00, pp. 7–26.

[11] K. Sanzgiri et al., “A Secure Routing Protocol for Ad hoc Networks,” Proc. 10th IEEE Int’l. Conf. Network Protocols (ICNP’02), 2002, pp. 78–87.