International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 5

Review on Various Security Attacks in Ad-Hoc Networks

Vaishali Tyagi[1], **Dr. Parul Tomar**[2]
[1]M.Tech Scholar, [2]Asisstant Professor
YMCA University of Science and Technology, Faridabad, Haryana, India

ABSTRACT

Importance of security in ad-hoc networks is increasing due to a tremendous boon in mobile equipment usage. Due to the characteristic of ad hoc network being decentralized, wireless and infrastructure-less makes it vulnerable to various attacks that cause disruption in the network. In order to provide possible security measures to handle the malicious activity in the network, security services are made sure to be implied. This paper includes a study of the required security goals to be achieved by the network and possible attacks that might result in alteration of network functionality.

Keywords: *Ad hoc, MANET, Security Attacks, Security Goals.*

INTRODUCTION

An ad-hoc network is a type of decentralized, peer-to-peer, wireless network. It is composed of individual devices communicating with each other directly. These networks do not rely on pre-existing infrastructure like access points. Mobile ad-hoc network (MANET) is a type of ad-hoc network that is a self-organizing, self-configuring and infrastructure-less network of mobile devices connected without wires [1]. The highly dynamic and infrastructure-less nature of ad-hoc networks makes it more susceptible to security attacks as compared to networks with pre-existing infrastructure. Providing security in MANET is difficult to achieve considering its lack of centralized control and limited availability of resources.

SECURITY SERVICES

Routing in MANET requires secure data transmission. There are five standard goals to achieve the complete security that are; Authentication, Availability, Confidentiality, Integrity, Non-Repudiation. [2].

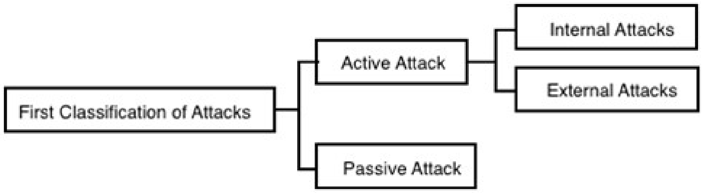
1. Authentication- This ensures that the data transmission and communication occurs only between authorized nodes. The goal of this service is to provide a trusted connection between the end nodes. With the use of certification, authentication can be achieved [4].
2. Availability- According to this, every authorized node in the network should have access to the data and the services. The data should be available to the network when in need. A technique called trust-based clustering approach is used to achieve availability of services and data in the network [4].
3. Confidentiality- Nodes in the network can only access the data that they are permitted to. Any other node that does not have the permission to access, cannot breach the security protocol [2]. This can be achieved using encryption techniques [4].
4. Integrity- This ensures that the data that is being transmitted should not be altered during the routing between nodes in the network. Only the authorized nodes are permitted to modify the data.
5. Non-Repudiation- This ensures the data transmitted in the network cannot be denied by the nodes sending or receiving it [3]. None of the authors can refuse to admit the authorization. It is a confirmed evidence of the participation of each party in the process of communication.

SECURITY ATTACKS

On the basis of studying various authors, the security attacks have been concluded into three major kinds of categories, which are as follows:

First Category:

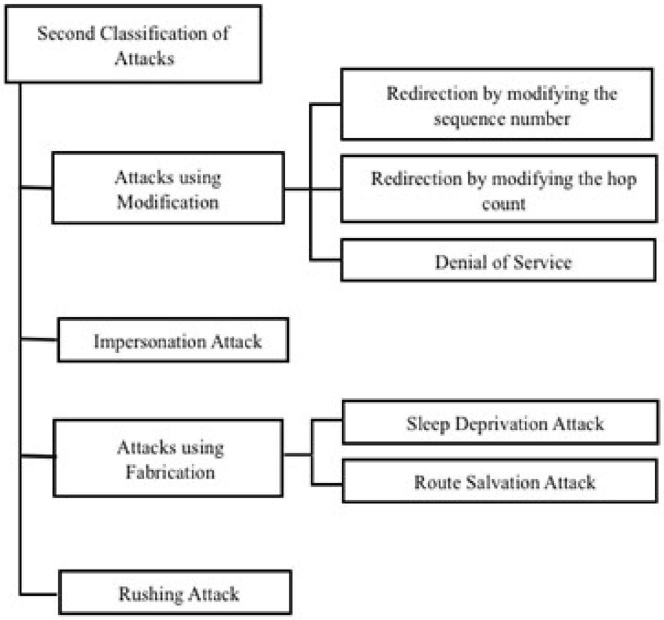
The attacks on ad hoc networks are categorized into two groups- Active and Passive. [2]



In an active attack, the attacker actively participates in trying to disrupt the proper functionalities of the net network. These attacks prevent the flow of messages between the nodes. Although, they can be either internal or external attacks [1]. Active internal attacks are caused by the nodes which were once a legitimate part of the network. These attacks enable the attacker to generate unauthorized access to the network that helps to make changes like, modification of the packet, Denial-of-Service, congestion et cetera. Active external attacks are carried out by the nodes from outside that do not belong to the network. These attacks are easier to detect than internal attacks.

In a passive attack, the intruder node exchanges the data without altering it [3]. These attacks do not modify the normal functionalities of the network. The malicious actions are not actively initiated by the attacker. The goal of the attacker is to obtain information by silently listening without authorization and retrieving the vital information into the data packet. Since no disruption is caused in the network, these attacks make it difficult for the attacker to be detected as they are spying on the network without leaving any footprint.

Second Category:

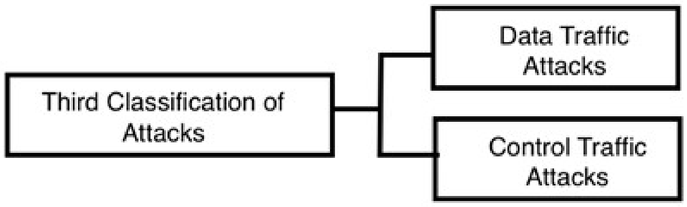

Second Classification of Attacks
Attacks using Modification
Redirection by modifying the sequence number
Redirection by modifying the hop count
Denial of Service
Impersonation Attack
Attacks using Fabrication
Sleep Deprivation Attack
Route Salvation Attack
Rushing Attack

These security attacks can be further classified into four other categories, which are; attacks using modification, impersonation attack, attacks using fabrication and rushing attacks [2].

- ➢ Attacks using Modification- Attacker customizes the data that is to be exchanged between the nodes accordingly through which the integrity of the network is endangered. It can be done by the following possible ways [7]:
- • Redirection by modifying the route sequence number- A route with a greater value is chosen. The node may advertise the higher value to alter the route of the data.
- • Redirection by modifying the hop count- The malicious node alters the hop count of the route between nodes to exchange messages to cause unnecessary traffic.
- • Denial of service- It refers to complete repudiation of the routing functions. The attacker could jam the network with traffic to block the sender to exchange data within the network.
- ➢ Impersonation Attack- These can be referred to Spoofing attacks in the ad hoc network [2]. The attacker impersonates the identity of being an authorized node of the network to cause malicious activity. It can create a possibility of reconfiguring topology in the network or isolate an active node from the network.
- ➢ Attacks using Fabrication- Creating a concoction by adding unauthorized messages to the existing data packet is known as fabricating the network. These can be done in two possible ways [8]:
- ➢ Sleep Deprivation Attack- This attack causes complete depletion of the battery of nodes by flooding huge size of unnecessary packets along with the data. Which, in turn, ends up using more processing time leading to more battery usage.
- ➢ Route Salvation Attack- They can be caused by the nodes which are a legitimate source of the network by behaving mischievously. The internal nodes may disrupt the functionality of the network without notifying with an error message. This causes unnecessary use of bandwidth.
- ➢ Rushing Attacks- This attack implies to the On-Demand routing protocol [2]. This routing technique uses a single route request packet to be sent to establish a path in the network. If the attacker sends a route request first to discover the path, then any other route that will be discovered will include a hop through the attacker node as well. This attack might lead to scarcity of resources and isolation of legitimate nodes of the network [20].

Third Category [6]:

Another classification of these attacks has been defined as- Data Traffic Attacks and Control Traffic Attacks.



The data traffic attacks usually take place on those nodes that either drop data packet that passes through them or when the data is delayed while forwarding it to other nodes. Some attacks in this category may choose to drop packets that are a victim, whereas, some might drop all of the packets irrespective of the node sending them. This leads to degradation of the quality of service and even exceed end-to-end delay. This category includes attacks like- Black hole attack, Grey-hole attack, and Jellyfish attack.

A pre-requisite of any attack to launch itself is that the node should be a legitimate source of the network. Because ad hoc networks include the autonomous participation of the nodes and lack of centralized authority, there is no control over what kind of node becomes part of the network. This way, any malicious node could join the network causing its threat, which leads to network disruption. This node could possibly hijack the network and hamper its expected functionality. Also, it could silently eavesdrop on the data packets in order to prevent themselves from being detected. The control attacks include- Wormhole attack, Hello flood attack, Rushing attack, or Sybil attack.

Security Attacks at Different Layers [16]

Every layer of the network comes across different type of attacks according to their specific functionalities provided. Following is a detailed description of the possible attacks a network may encounter while going through each layer.

Layers	Attacks
Physical	Jamming, Tampering
Data Link	Collision, Exhaustion
Network	HELLO Flood, Wormhole, Sybil, Sinkhole
Transport	Session Hijacking, Flooding
Application	Denial-of-Service

Attacks on Physical Layer

Jamming – It can be called an intentional interference attack with the radio frequencies of the network. A type of DoS attack whose objective is to interfere with the wireless communications [16]. It affects the availability of the services in the network. This is a type of physical layer attack.

- Tampering – Another physical layer attack, also referred as node capturing. Tampering is the act of manipulating the data. The node is compromised and physically modified by the attacker node. This attack is very harmful and easy to implement [16].

Attacks on Data Link Layer

- Collision – It is caused by data link layer that handles neighbor-to-neighbor communication along with channel arbitration. It can occur when messages are transmitted by two nodes on same frequency simultaneously. It affects the network by corrupting the data/control packets. Entire packet can be disrupted if an adversary is able to generate collisions of even part of a transmission. There are two types of collision; Environmental and Probabilistic collision [5]. Error correction codes, like CRC, can be used as a defensive mechanism against collision in the network.
- Exhaustion – It can be defined as repeated collisions and continuous retransmission of data until the victim node dies. A compromised node could repeatedly send/receive data thus consuming the battery power more than required [5]. It consumes all the resource of the victim node, by obliging it to receive or transmit unnecessary data.

Attacks on Network Layer

- Hello flood attack – Routing protocols use HELLO packets for node discovery to establish a network topology. This is the simplest attack for an attacker with high transmission power to flood beacon packets in the network to prevent other messages from being exchanged [15]. In this way, the attacker creates an illusion of being a neighbor to other nodes and underlying routing protocol can be disrupted which facilitate further types of attacks.
- Wormhole attack – One of the challenging attacks to be defended, occurs in the network layer. Attackers place themselves strategically in the network at different endpoints. A private network connection is enabled between the compromising nodes for communication to exchange messages. The attacker retrieves the data from one of the ends of the network and tunnels the packet to another end through low-latency link formation

that allows the packet to travel faster than a usual multi-hop route [5]. The message is then replayed at another delivery location of the network where it was tunnelled. The private connection creating the tunnel is referred to as a wormhole. This attack can either drop the packet or forward it selectively in order to avoid being detected. This can also be found guilty of eavesdropping in the network which makes it even more difficult to detect and prevent the attack [5].

- Sybil attack – This attack is manifested by pretending to be multiple identities [17]. The attacker node claims to impersonate false identities in the network. It can depict itself to be a group of false nodes that can hamper the network functionality. It usually only occurs during broadcasting and operates without identity verification. Attacker node possesses malefic identities which target network topology, hop-count, and distribution of the network by monitoring and modifying the functionality of the network. There are four classifications of Sybil attack; Direct vs Indirect communication, Busy vs Idle, Simultaneous vs Non-simultaneous and Insider vs Outsider [10].
- Sinkhole attack – One of the vigorous attacks in the ad hoc network. The attacker node collects the data from the network and advertises a false path towards itself without letting the base station obtain the accurate routing message [11]. This leads to resulting in a serious threat for applications of a higher layer. It attracts all the network traffic to the malicious node by placing it at a distance closer to the base station to enable selective forwarding of the packets [5]. It basically centralizes the data traffic to one node that causes all the trouble in the network. The attack tries to alter the performance parameters of the network like minimizing the hop count or maximizing the sequence number. This way, it provides with the falsified route that possesses to be the best available path for nodes to communicate. The goal of this attack is to lure the traffic from an area through the compromised node, creating a metaphorical sinkhole with the adversary in the middle of the network [5].

Attacks on Transport Layer

- Session Hijacking - A session is referred to as a time set for a particular activity to be held between the users. In ad hoc, this term is known as interactions between the nodes for a given time period. An attacker in this state may take control of the session being held between the two nodes. The adversary node may spoof the address of the victim node, to obtain the correct sequence number of the target node and then launch attacks like denial of service [1]. As a result, the legitimate destination node becomes unavailable, and the attacker acts as an authorized node to collect the data and modify it accordingly [14].
- Flooding attack – A new variation of DoS attack has been introduced in ad hoc networks called Ad-hoc Flooding Attack (AHFA) [18]. In this, the attacker broadcasts the route request packets in bulk to consume/ exhaust the bandwidth of the network to repudiate the legitimate communication message that was issued before. It is caused usually when the packets exchanged weigh down the network or the services provided, thus it initiates connection requests that are incomplete. This attack eventually exhausts the buffer of the server, which results in denial of service. DoS attack when penetrated into the network, consumes the resources, alters the configuration and might end up physically destroying the components of the network.

Attacks on Application Layer

- Denial of Service - Denial in other word means repudiation, which counters the security service that is to be required by the network to function in a secure manner. As the word suggests, it clearly means that the services are denied by the intruder in this situation. It eliminates the capacity of the network to prevent the nodes from performing the expected function.
- Another variant of this attack is Distributed Denial of Service (DDoS) where the adversaries are distributed in the network at different locations to launch the attack so that it prevents the legitimate nodes of the network to function as usual.

CONCLUSION

As it is known that ad hoc networks tend to have characteristics that make the network vulnerable to attacks. This paper concluded the required goals of security that should be present for the network to perform in a secure manner. Also, it discusses the possible categories of the attack that can occur in ad hoc networks solely based on their characteristics. They have a different approach to occur at different layers of the network.

REFERENCES

1. Aarti, Dr. Tyagi S. S., “Study of MANET: Characteristics, Challenges, Application and Security Attacks”, *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.*

2. Tomar P., Suri P. K., Dr. Soni M. K., “A Comparative Study for Secure Routing in MANET”, *International Journal of Computer Applications (0975-8887), Volume 4, Number 5, July 2010.*

3. Sarma S., Devi B., “Secure Routing Protocols in Ad Hoc Wireless Networks”, *International Journal of Modern Engineering Research, Volume 2, Issue 6, Nov-Dec 2012 pp-4502-4509.*

4. Dorri A., Kamel S. R., Kheyrkhah E., “Security Challenges in Mobile Ad Hoc Networks: A Survey”, *International Journal of Computer Science & Engineering Survey, Volume 6, Number 1, February 2015.*

5. Jyotsna, Nandal V., “Comparison of Attacks on Wireless Sensor Networks”, *International Journal of Computer Science and Mobile Computing, Volume 3, Issue 7, July 2014, pg. 208-213.*

6. Bhattacharyya A., Banerjee A., Bose D., Saha H. N., Bhattacharjee D., “Different types of attacks in Mobile ADHOC Network: Prevention and mitigation techniques”, Institute of Engineering & Management, Saltlake.

7. He B., Hägglund J., Gu Q., “Security in Ad Hoc Network”.

8. Faisal M., Kumar M., Admed A., “Attacks in MANET”, *International Journal of Research in Engineering and Technology, eISSN: 2319-1163, pISSN: 2321-7308.*

9. Dr. Mohammadi S., Jadidoleslamy H., “A Comparison of Link Layer Attacks on Wireless Sensor Networks”, *International Journal on Application of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks, Volume 3, Number 1, March 2011.*

10. Gunturu R., “Survey of Sybil Attacks in Social Networks”.

11. Gagandeep, Aashima, “Study on sinkhole Attacks in Wireless Ad Hoc Networks”, *International Journal on Computer science and Engineering.*

12. Bahekmat M., Yaghmee M. H., Yazdi A. S. H., Sadeghi S., “A Novel Algorithm for Detecting Sinkhole Attacks in WSNs”, *Internation Journal of Computer Theory and Engineering, Volume 4, Number 3, June 2012.*

13. Denko M. K., “Detection and Prevention of Denial of Service (DoS) Attacks in Mobile Ad Hoc Networks using Reputation-Based Incentive Scheme”, University of Guelph, Canada.

14. Pawar R. P., “Detect and Prevent Session Hijacking Attacks in MANET”, *Journal of Networking, Computer science and Engineering, Volume 1, Issue 1.*

15. Messai M. L., “Classification of Attacks in Wireless Sensor Networks”, *International Congress on Telecommunication and Application, Algeria, April 2014.*

16. Singh R., Dr. Singh J., Dr. Singh R., “Attacks in Wireless Sensor Networks: A Survey”, *International Journal of Computer Science and Mobile Computing, Volume 5, Issue 5, May 2016, pg. 10-16.*

17. Newsome J., Shi E., Song D., Perrig A., “The Sybil attack in sensor networks: analysis & defenses”, *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on- IEEE, ISBN- 1-58113-846-6.*

18. Ping Y., Yafei H., Yiping Z., Shying Z., Zhoulin D., “Flooding attack and defence in ad hoc networks” *IEEE Journal of System Engineering and Electronics, Volume: 17, Issue: 2, June 2006.*

19. Hu Y.C., Perrig A., Johnson D. B., “Wormhole attack in wireless networks”, *IEEE Journal on Selected Areas in Communications, Volume 24, Issue 2, Feb 2006.*

20. Shahrani A. S. A., “Rushing attack in Mobile Ad Hoc Network”, *Intelligent Networking and Collaborative Systems (INCoS), 2011 Third International Conference on-IEEE, ISBN- 978-1-4577-1908-0.*