IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

Impact Factor: 6.252

Volume 2, Issue 2, July 2022

A Review on Network Security in Ad-hoc Networks

Mr. Jayanth Kumar Rathod, Nisha Tellis, Pawan J Acharya, Prasad M Patil, Poornachandra
Department of Information Science and Engineering
Alvas Institute of Engineering and Technology, Mijar, Moodbidri, Karnataka, India
jayantkumarrathod@gmail.com, tellisnisha@gmail.com, pawanachar20@gmail.com,
prasadpatil91640@gmail.com, mailmetothis1@gmail.com

Abstract: *Ad hoc network nodes cannot be viewed as trustworthy as dedicated infrastructure nodes due to the lack of a maintained infrastructure. As a result, wireless ad hoc networks are subject to a variety of threats that threaten core network functions including routing and packet forwarding. This paper examines the security challenges faced by ad hoc networks and describes the important concerns that must be addressed to achieve ad hoc security. It also provides an overview of major challenges faced by Ad-hoc networks. We discuss the various security attacks and explore approaches to secure the communication.*

Keywords: Wireless Network, Ad hoc Network, Security Service, Routing Protocols, Key management

I. INTRODUCTION

Ad hoc Networks are being adopted in more and more applications in our daily life. They have been an essential part of communication systems since radio systems .Ad hoc networks are a new type of network that provides mobility without the need for any underlying infrastructure. It is a collection of autonomous nodes or terminals that communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. There is no fixed infrastructure such as base stations. The nodes must deal with the impacts of radio transmission, like noise and interference, because they communicate across wireless networks. Also, the links have less bandwidth than in a wired network. Each node in a wireless ad hoc network acts both as a host and a router. The control of the network is distributed among the nodes. The network topology is in a general dynamic, because the connectivity among the nodes may vary with time due to node departures, new node arrivals, and the possibility of having mobile nodes. There are various classes in which wireless ad hoc networks are classified. These include VANET (vehicular ad hoc network), MANET(mobile ad hoc network), SPAN (Smart phone ad hoc network), Wireless mesh network(WMN) and Wireless sensor networks(WSN).

The network architecture may vary fast over time since the nodes are mobile. All network tasks, including detecting the topology and delivering messages, must be performed by the nodes themselves because the network is decentralized. A smart sensor network consists of several sensors spread across a geographical area. Each sensor has a wireless communication capability for signal processing and networking. Military sensor networks are used to detect enemy movements and the presence of hazardous material. Environmental sensor networks are used to detect environmental changes. Wireless traffic sensor networks keep track of vehicle traffic on highways and in congested areas of cities. In a shopping mall, parking garage, or another facility, wireless surveillance sensor networks are used to provide security. Wireless parking lot sensor networks are used to assess which parking spaces are occupied and which parking spaces are available.

One of the most important criteria in the successful implementation of these ad hoc networks is security. Systems may become involved in cybercrime behaviour. It has the potential to ruin and harm any physical system directly. For many years, several businesses and researchers have been attempting to secure systems from attackers and to reduce network security attacks. Because of the fundamental distinction between ad hoc and fixed networks, security in ad hoc networks should be re-examined. This paper provides an overview of ad hoc security, analyses its challenges and requirements, and explores its vulnerabilities and technologies.

DOI: 10.48175/IJARSCT-5836

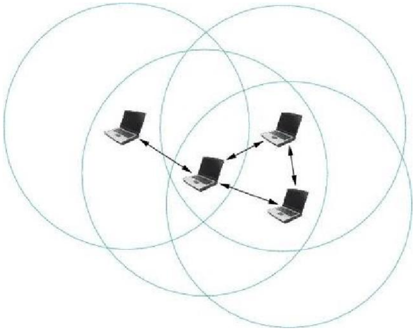

Fig 1. Ad hoc network

II. LITERATURE SURVEY

Ad-hoc is a most promising and rapidly growing technology which is based on a self-organized and rapidly deployed network. Due to its great features, Ad-hoc networks attracts different real world application areas where the networks topology changes very quickly. Many researchers are working to eliminate major Ad-hoc flaws, including restricted bandwidth, battery capacity, processing power, and security. Although there is a lot of research being done on this topic, particularly routing attacks and their existing countermeasures, there is still a lot of work to be done. The existing security solutions of wired networks cannot be applied directly to ad-hoc, which makes it much more vulnerable to security attacks. Some cryptography and key management methods appear promising, but they are too expensive for resource-constrained Ad- hoc networks. In addition, some may require special hardware such as a GPS or a modification to the existing protocol. Attacks on ad hoc networks can be classified as passive and active attacks or internal attack and external attacks. The malicious node(s) can attacks in Ad-hoc using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsections, we review security threats and challenges and solutions in wireless ad-hoc networks.

III. SECURITY GOALS OF AD-HOC NETWORKS

Security is an important issue for ad hoc networks, especially for security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, nonrepudiation and access and usage control.

- **Availability** means ensuring that, despite denial-of-service attacks, the node's service will be available to its users when expected. At any tier of ad hoc networking, a denial- of-service attack can occur. The attacker can change the routing protocol at the network layer. e.g. to be able to divert the traffic to invalid addresses or shut down networks. At the application level, the availability of essential services such as key management services may be threatened.
- **Confidentiality** ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. The leakage of such information to enemies can have devastating consequences. Routing information must also remain confidential in certain cases because the information might be valuable for enemies to identify and locate their targets on a battlefield.
- **Integrity** guarantees that a message being transferred is not corrupted. Communication could be corrupted because of certain failures, similar as radio propagation impairment, or because of vicious attacks on the network
- **Authentication** enables a node to ensure the identity of the peer node with which it is communicating. Without authentication, an adversary could pretend as a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes.
- **Nonrepudiation** ensures that the origin of a message cannot deny having sent the message. Nonrepudiation is useful for the detection and isolation of compromised nodes. When node A receives an erroneous message from node B, nonrepudiation allows A to accuse B of using this message and to convince other nodes that B is compromised.

DOI: 10.48175/IJARSCT-5836

- **Access and usage control** Access control makes sure that access to information resources is controlled by the ad hoc networks. Usage control ensures the information resource is used correctly by the authorized nodes having the corresponding rights. This mechanism provides the ability to control information after it is transmitted.

IV. CHALLENGES IN AD-HOC NETWORK SECURITY

Physical security of the network elements forms the basis for the security architecture. From passive eavesdropping to active impersonation, message replay, and message distortion, wireless networks are vulnerable to a variety of attacks. Active attacks could include removing messages, injecting false messages, and so on. We need to consider attacks from not only the outside but from within the network as well as these nodes may be in hostile environments with low physical protection. The following are vulnerabilities due to which security can be breached:

- **Vulnerability of channels:** Messages can be intercepted and fraudulent messages can be injected into a wireless network without the need for physical access to network components.
- **Absence of Infrastructure:** The traditional security solutions based on certification authorities and on- line servers are inapplicable since ad hoc networks do not operate on established infrastructure.
- **Vulnerability of nodes:** Because nodes are not located in physically secure locations, they can be readily captured and taken over by an attacker.
- **Dynamically changing topology:** It's difficult to tell whether a topology change or false routing information generated by a compromised node caused the change in routing information.

Ad hoc networks should have a distributed architecture with no central entities for high survivability, as centralization increases vulnerabilities. Security methods that are dynamic and scalable are required.

V. SECURITY ATTACKS IN AD-HOC NETWORKS

There are various types of attacks on ad hoc network

- **Location Disclosure:** A location disclosure attack is one that targets an ad hoc network's privacy requirements. Traffic analysis techniques, as well as simpler probing and monitoring approaches, can be used. An attacker can find out where a node is located, or even the network's overall structure.
- **Replay:** When an attacker launches a replay attack, he or she injects previously captured traffic into the network. This attack is commonly used to weaken poorly built security measures, although it can also be used to target the freshness of routes.
- **Denial of Service:** Denial of service attacks try to completely disable the routing function and, as a result, the ad hoc network's whole operation. The routing table overflow and sleep deprivation torture are two examples of denial of service attacks. In a routing table overflow attack, a hostile node floods the network with false route creation packets in order to drain the resources of other nodes and prevent valid routes from being established. The sleep deprivation torture attack seeks to drain a specific node's batteries by keeping it constantly engaged in routing decisions.
- **Black Hole:** A malicious node injects false route replies to route requests it receives, promoting itself as having the fastest path to a destination in a black hole attack. These forged responses can be used to funnel network traffic via the malicious node for eavesdropping, or simply to draw all traffic to it in order to launch a denial-of-service attack by dropping the received packets.
- **Wormhole:** The wormhole attack is one of the most powerful attacks mentioned here since it includes two hostile nodes cooperating in the network. One attacker, such as node A, captures routing traffic at one point in the network and tunnels it to another, such as node B, which has a private communication link with A. The tunnelled traffic is then selectively injected back into the network by Node B. The two conspiring attackers have complete control over the connection of the nodes that have established routes across the wormhole link. Packet leashes are the solution to the wormhole attack.
- **Sinkhole:** In a sinkhole attack, a compromised node tries to attract the data to itself from all neighboring nodes. So, practically, the node eavesdrops on all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be implemented on Adhoc networks such as AODV by using flaws such as maximizing

the sequence number or minimizing the hop count, so that the path presented through the malicious node appears to be the best available route for the nodes to communicate.

- **Flooding attack:** is basically made with the intension to degrade the network performance. In this attack the attacker either aims to squander the resources such as battery power and computational unit, or it aims to exhausts the resources such as bandwidth by flooding the network with useless packets. For example, a malicious node can repetitively broadcast a route request packet for the node which actually doesn't exist in the network. Since, the destination node does not exist the packet will be aimlessly flooded within the network, increasing the network traffic as well as consuming the bandwidth and battery power. Flooding attack may also lead to Denial of Service if they are not timely-checked.
- **Routing Table Poisoning:** Routing protocols keep tables that include information about the network's paths. To construct false entries in the tables of the participating nodes, hostile nodes manufacture and send fabricated signalling traffic, or change valid signals from other nodes, in poisoning attacks.
- **Rushing Attack:** When employed against all prior on-demand ad hoc network routing systems, the rushing attack results in denial of service. For example, DSR, AODV, and secure protocols based on them, such as Ariadne, ARAN, and SAODV, are unable to discover routes longer than two hops when subject to this attack. Rushing Attack Prevention (RAP), general rushing assault protection for on- demand protocols that can be implemented to any existing on-demand routing protocol to allow it to withstand the rushing attack.
- **Fabrication:** The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted.
- **Masquerading:** During the neighbor acquisition procedure, an outside attacker could connect itself to a communication link and join the routing protocol domain illegally by compromising the authentication system, masquerading as a non existent or existing IS. Masquerading poses a threat similar to that of a compromised IS.

VI. SOLUTIONS

Authentication and encryption can be used as a first line of defence to decrease the possibility of attacks. The proposed preventive strategies differ in a number of ways, based on their assumptions about the intended Ad hoc applications.

6.1. Key and Trust Management : Preventing External Attacks

To protect against external (outsider) threats, encryption, authentication, and key management are commonly utilized. In ad- hoc networks, however, they encounter numerous obstacles. To begin, we must deal with dynamic topologies in both communications and trust relationships; whether or not to trust a wireless node can alter over time. Second, we must address Ad hoc's lack of infrastructure support.

Key management consists of various services, of which each is vital for the security of the networking systems. The services must provide solutions to be able to answer the following questions:

Trust model: It must be determined how much different network elements can trust one another.

Cryptosystems: For key management, cryptosystems are available: in certain circumstances, only public- or symmetric key techniques can be used, while in other cases, Elliptic Curve Cryptosystems (ECC) can be used. While public-key cryptography is more convenient (as seen by well-known digital signature algorithms), when the same level of security is required, public-key cryptosystems are much slower than their secret-key counterparts. Secret key systems, on the other hand, provide less functionality and are more prone to issues such as key distribution. In terms of implementations, ECC cryptosystems are a newer branch of cryptography, although they are already widely used, for example in smart card systems.

Key generation: Which parties are authorized to generate keys for themselves or other parties, and what kind of keys are allowed to be generated, must be determined.

Key storage: There may not be centralized key storage in ad-hoc networks. For fault tolerance, there may not be any mirrored storage accessible. In ad-hoc networks, each network element may be required to store its own key, as well as the keys of other network elements.

DOI: 10.48175/IJARSCT-5836

Key distribution: The key management service must ensure that the created keys are transmitted to their owners in a secure manner. Any key that needs to be kept secret must be delivered in such a way that confidentiality, authenticity, and integrity are maintained.

6.2. Secure Routing Protocols: Preventing Internal Attacks

In ad hoc networks, routing protocol should be robust against topology updates and any kinds of attacks. Routing protocols for ad hoc networks are still under active research. In most routing protocols, routers exchange information on the topology of the network to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down. There are two sources of hazards to routing protocols. The first comes from external attackers. By fitting incorrect routing information, or distorting routing information, an attacker could successfully introduce inordinate traffic load into the network by causing retransmission and ineffective routing.

The second danger comes from infected nodes, which may communicate harmful routing information to other nodes. To create a secure route to transport data, a proper routing protocol in Ad-Hoc networks must create a route accurately and maintain it. Let's review a few protocols below.

6.3. DSR (Dynamic Source Routing)

In this protocol, the source node creates a package called RREQ in which the source and target nodes are determined. These packages are sent by flooding. If a node receives an RREQ package but is unaware of the target route, it adds its name to the package list and broadcasts the message. As a result, when the package arrives at its destination, the target node will be able to see information about route nodes and their configurations. The target node generates RREP and returns it to the RREQ package header via the available list .The middle nodes know the target and do it according to the available list. As a result, in order to reach the source node, the package traverses the path in reverse. Although it is a good strategy that is absolutely applicable, it increases network load and consumes high bandwidth, resulting in the network transmitting huge headers. This strategy may not work correctly if the rate of header volumes increases, resulting in increased distance between links.

OLSR works in a totally distributed manner, e.g. the MPR approach does not require the use of centralized resources. The OLSR protocol specification does not include any actual suggestions for the preferred security architecture to be applied with the protocol. The protocol is, however, adaptable to protocols such as the Internet MANET Encapsulation Protocol (IMEP), as it has been designed to work totally independently of other protocols. source and target nodes. This volume increase is due to the name of network middle elements name in the package header. Then, the data sender can put the target route in the sent data header to inform middle nodes through this route to whom they send the package. When a node can't deliver a data package to the next one, it produces a package called RERR (Route Error) and returns it back to the route. So, RERR receiving nodes acknowledge about these two nodes' disconnection and routing operation will be started again.

6.4. AODV (Advanced On-demand Distance Vector)

In contrast to DSR protocol, this protocol doesn't put the route in the package header. But, each node controls it while receiving PREQ according to tables it had before. If the route has the final node in its table, RREP will be sent. Otherwise, it broadcasts RREQ messages. Certainly, RREPs can be returned back to RREQ. It is used consecutive numbers in RREQ messages that a middle node gets informed whether the route is a new one. So, if the number of RREQ consecutive is smaller than the route consecutive number, the RREP message will be sent by the middle node.

6.5. SAODV (Secure AODV)

As it is clear from its name, it is provided to create more security in AODV. In this protocol, it uses Hash functions as it is shown in equation (1)

$$h\,n\text{-}1 = H(h\,n) \qquad (1)$$

In equation (1), H is the function of Hash and h is related to the hop. In this protocol, it is used hop count to measure the number of hops in which the packages go through. If the hop count becomes more than the amount of Max Count, the package will be ignored. To prevent the changes of hop count amount and make sure about the accuracy of its amount, it is used the noted Hash functions.

Due to equation (1), each node can be sure about its authenticity by receiving a message and controlling the equation (1) on it. Number n also indicates the maximum hop that a package can go through.

6.6. OLSR

Optimized Link State Routing protocol (OLSR), is a proactive and table driven protocol that applies a multi-tiered approach with multi-point relays (MPR). MPRs allow the network to apply scoped flooding, instead of full node-to-node flooding, with which the amount of exchanged control data can substantially be minimized. This is achieved by propagating the link state information about only the chosen MPR nodes.

Since the MPR approach is most suitable for large and dense ad hoc networks, in which the traffic is random and sporadic, also the OLSR protocol as such works best in these kind of environments. The MPRs are chosen so that only nodes with one-hop symmetric(bi-directional) link to another node can provide the services. Thus in very dynamic networks where there exists constantly a substantial amount of uni- directional links this approach may not work properly. OLSR works in a totally distributed manner, e.g. the MPR approach does not require the use of centralized resources. The OLSR protocol specification does not include any actual suggestions for the preferred security architecture to be applied with the protocol. The protocol is, however, adaptable to protocols such as the Internet MANET Encapsulation Protocol (IMEP), as it has been designed to work totally independently of other protocols.

Attacks	Brief Explanation	Methods Recommended	Routing Protocol
Black-hole Attack	In this attack ,attacker drops all forwarded packets	1. Path based techniques to detect and prevent the attack . 2. Two stage approach, in first stage detection of suspected nodes and in second stage isolation of malicious nodes. 3. Verification of control message sent by malicious node and detection of attacks	1.DSR Ad-Hoc Routing Protocol 2.AODV, DSR Ad-Hoc Routing Protocol 3. OLSR Ad Hoc Routing Protocol
Wormhole Attack	The attacker replays the packet	1. Cooperative approach Among the multiple nodes to detect & Prevent. 2. Detection & prevention by Digital Signature.	1. Any Ad-Hoc routing protocol(AODV, DSR, OLSR) 2. Combined with Ad-Hoc, OLSR
Sink-hole Attack	Malicious node attracts the hole network traffic towards itself after that it can modify or altered the received packets	1. To prevent attack there are three variables (Image Ratio, Sequence Number and Route Add Ratio) implementation. 2. Trust based algorithm to detect and prevent sinkhole attack	1. DSR protocol. 2. On-demand multipart routing protocol.
Flooding Attack	In this attack, attacker floods the network with fake traffic to	1. To controls the attack by introducing a variable RREQ_RATELIMIT ,it limit the number of packets sent into the Network	1. AODV Ad Hoc Routing Protocol.

Table 1: Summary of Various Attacks and Proposed Mechanism

VII. CONCLUSION

The need for security mechanisms that cope with the threats that are specific to the ad hoc environment has recently gained attention among the research community. The ad hoc network's security- sensitive applications demand a high level of security; ad hoc networks, on the other hand, are naturally vulnerable to security threats.

The security concerns in ad hoc networks were examined in this paper. We listed important challenges that must be addressed initially to achieve ad hoc security.

In addition, we provided an overview of the status of solutions in the areas of secure routing, and key management services. In an ad hoc networking context, this paper focuses on how to protect routing and how to set up a secure key management service.

We mentioned that the security research in ad hoc networks is still in its early stages. There are certain flaws in the current achievement. There is no such thing as a truly practical answer.

REFERENCES

[1]. Security for Ad Hoc Networks, Hang Zhao.

[2]. A Literature Survey on Challenges and Issues on Mobile Ad Hoc Networks Rajneesh Singla / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 7 (1), 2016

[3]. Securing Ad Hoc Networks, Lidong Zhou, Department of Computer Science, Zygmunt J. Haas, School of Electrical Engineering

[4]. A Review of Security Challenges in Ad-Hoc Network , International Journal of Applied Engineering Research ISSN 0973- 4562 Volume 13, Number 22 (2018)

[5]. S. Mäki, M. Hietalahti, and T. Aura, A Survey of Ad Hoc Network Security, Interim report of project 007 - Security of Mobile Agents and Ad Hoc Societies, Helsinki University of Technology, Sep. 2000.]]

[6]. A REVIEW ON AD HOC NETWORK SECURITY , International Journal of Mathematics and Computational Methods in Science & Technology, Vol. 1, No.6, 2011

[7]. Ad Hoc Networks (Published by the IEEE Computer Society -2004)

[8]. Security Issues in Mobile Ad Hoc Networks, Procedia Computer Science Volume 92, 2016

[9]. Security in Ad Hoc Networks Refik Molva and Pietro Michiardi , Information Society Technologies program of the European Commission 2003

[10]. Security in ad hoc networks, Sanjana Lakkadi, Amit Mishra, Manish Bhardwaj, American Journal of Networks and Communications 2015

[11]. Security Issues and Challenges in MANET-VANET-FANET: A Survey Article in EAI Endorsed Transactions on Energy Web · April 2018

[12]. R. Nandakumar K. Nirmala “Security Challenges in mobile Ad Hoc Networks - A Survey” Australian Journal of Basic and Applied Sciences, Vol. 10(1), pp. 654-659, January 2016.

[13]. Security in Ad Hoc Networks, Vesa Kärpijoki, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory,

DOI: 10.48175/IJARSCT-5836