Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

The Security Solutions of MANET

Gagandeep Kaur[1],Dr. Kalpana Midha[2]

[1]Research Scholar, Shri Khushal Das University, Hanumangarh, Rajasthan, India

[2]Assistant Professor, Shri Khushal Das University, Hanumangarh, Rajasthan

Article Info
Page Number: 9009-9017
Publication Issue:
Vol. 71 No. 4 (2022)

Article History
Article Received:
12 September 2022
Revised: 16 October 2022
Accepted: 20 November 2022
Publication: 25 December 2022

Abstract— Mobile Ad Hoc Networks (MANETs) have seen dramatically rising interest, in part because of their potential for use in a wide range of applications. However, because of the dynamic nature of the nodes, the random topology, the constrained wireless range of nodes, and transmission faults, the implementation of such networks presents several difficult problems. The wireless channel is vulnerable to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping, spoofing, etc. because all the nodes in the network work together to forward the data. Since MANET is capable of building temporary networks without the aid of any existing infrastructure or centralized administration, implementing security is therefore of utmost relevance in such networks. Security issues have become a significant priority to ensure secure communication. We concentrate on research results and upcoming projects that might be of interest to researchers. However, in a nutshell, we can say that the prevention, detection, and reaction methods of MANET are necessary for a full security solution.

Keywords— MANET, prevention, detection, reaction.

I. INTRODUCTION

The term "Mobile Ad Hoc Network" (MANET) refers to a network of communication nodes that seek to communicate without the use of a fixed infrastructure and by a predetermined arrangement of accessible links. Dynamically finding other nodes to interact with is done by the MANET nodes themselves. It is a self-configuring system made up of wirelessly linked mobile nodes that can combine to construct any topology. Because the nodes are unrestricted in their movement and organization, the wireless topology of the network may change suddenly and unexpectedly. In emergency scenarios, temporary operations, or just when there aren't enough resources to build extensive networks, MANETs are typically set up. These networks operate without any fixed infrastructure, which makes them simple to deploy but also makes it challenging to use the current routing techniques for network services. This presents several challenges in ensuring the security of the communication, something that is not always easy to do as many of the requirements of network security conflict with the requirements of mobile networks (e.g. low power consumption, low processing load). The operation of any general ad-hoc network is depicted in the flowchart below.

II. MANET History

The first, second, and third-generation ad-hoc network systems can be used to classify the whole life cycle of ad-hoc networks. The systems used in ad-hoc networks today are

regarded as third-generation. The initial generation began in 1972. They were then known as PRNET (Packet Radio Networks). Ad-hoc networks have a long history, dating back to the 1970s military Packet Radio Network (PRNET) research project financed by DoD1, which later developed into the Survivable Adaptive Radio Networks (SURAN) program. Different networking capabilities were tested using methodologies for medium access control and a kind of distance-based routing PRNET in conjunction with ALOHA (Areal Locations of Hazardous Atmospheres) and CSMA (Carrier Sense Medium Access).

In the 1980s, as part of the SURAN (Survivable Adaptive Radio Networks) program, the ad hoc network systems were improved and put into use, giving rise to the second generation of ad hoc networks. In a setting devoid of infrastructure, this gave the mobile battlefield access to a packet-switched network. This initiative succeeded in making the radios more effective by making them more compact, affordable, and resistant to electronic attacks. With the introduction of portable computers and other useful communications technology in the 1990s, the idea of commercial ad hoc networks emerged. At many research conferences, the concept of a group of mobile nodes was put forth at the same time. A lot of work has been done on ad hoc standards since the mid-1990s. The MANET working group was established within the IETF and worked to standardize routing protocols for ad hoc networks. In the meantime, the IEEE 802.11 subcommittee standardized a medium access protocol for creating mobile ad hoc network prototypes using laptops and 802.11 PCMCIA cards. This protocol was based on collision avoidance and supported hidden terminals.

There are currently two kinds of Mobile wireless networks.

Infrastructure networks with fixed and wired gateways are the first type. Wireless local area networks are a few examples of common uses for this kind of "one-hop" wireless network (WLAN).

The infrastructure-less mobile network, or MANET, is the second type of mobile wireless network. MANET typically functions as a "multi-hop" network that may organize itself and configure itself without the aid of a fixed infrastructure. All nodes in such a network are randomly and dynamically situated, and they are obligated to relay packets to other nodes to transmit data across the network.

III. MANET Applications

Ad hoc networking is becoming more important due to the rise in portable devices and advancements in wireless communication, as well as the rising number of widely used applications. Anywhere there is a lack of communication infrastructure, a high cost of using the current infrastructure, or both, ad hoc networking can be used. Ad hoc networking enables the devices to easily add and remove devices from the network as well as retain connections to it. There are many different uses for MANETs, from big, mobile, dynamic networks to tiny, static networks with power source restrictions. Numerous new services can and will be developed for the new environment in addition to the legacy applications that migrate from the conventional infrastructure environment into the ad hoc context. Typical applications include:

A. **Military battlefield** - Nowadays, computers are frequently seen in military equipment. Ad hoc networking enables the military to maintain an information network between the soldiers, vehicles, and military information headquarters while utilizing standard network technology. This discipline gave rise to the fundamental principles of ad hoc networks.

B. **Commercial sector** - Ad hoc can be utilized in rescue and emergencies, such as a fire, flood, or earthquake. Rapid construction of a communication network is required where there is a need for emergency rescue operations due to missing or damaged communications infrastructure. Over a small portable, information is passed from one member of the rescue squad to another. Law enforcement, ship-to-ship ad hoc mobile communication, and other scenarios are examples of other business use cases.

C. **Local level** - To distribute and share information among attendees at a conference or school, for example, ad hoc networks can independently connect a momentary and transient multimedia network using notebook or palmtop computers. Home networks, which allow gadgets to talk directly and exchange information, could be another suitable local-level use. Mobile ad hoc communications will have various uses in the same kinds of everyday settings as a taxi, sports arena, boat, and small aircraft.

D. **Personal Area Network (PAN)** - The communication between different mobile devices can be made simpler via short-range MANET (such as a PDA, a laptop, and a cellular phone). Wireless connections are used instead of laborious wired cords. Through methods like Wireless LAN (WLAN), GPRS, and UMTS, such an Adhoc network can also increase access to the Internet or other networks. In the context of pervasive computing in the future, the PAN is conceivably a possible application area of MANET.

IV. PROPERTIES OF MOBILE ADHOC NETWORKS

MANETs have the following special features that should be considered in designing solutions for this kind of network.

- Dynamic Topology

Mobile multi-hop ad hoc networks' topology is constantly and unpredictably changing as a result of node mobility. Based on how close a node is to another node, the connection connectivity between network terminals varies arbitrarily and dynamically. Additionally, it frequently disconnects while the node is moving. The mobile network nodes' mobility patterns as well as the traffic and propagation conditions should all be taken into account by MANET. As they move around, the mobile nodes in the network dynamically build routing among one another, creating their network on the spot. Additionally, a user in the MANET may need a connection to a public fixed network in addition to operating within the ad hoc network.

- Bandwidth

MANETs' bandwidth capacity is much lower than that of fixed networks. The predicted link

quality is exacerbated by the employed air interface's increased bit error rates. IEEE 802.11 (b, a), which offers a bandwidth of up to 54Mbps, and Bluetooth, which offers a bandwidth of 1Mbps, are currently available technologies that are ideal for the implementation of MANETs. In a MANET, the nature of high bit-error rates of wireless connections may be more severe. Several sessions can share a single end-to-end path. The communication channel between the terminals is less bandwidth-efficient than a wired network and is vulnerable to noise, fading, and interference. In some cases, the route taken by any two users can pass via many wireless links, some of which may even be heterogeneous.

- Energy

Batteries, a finite resource, will be the source of power for all mobile gadgets. Therefore, MANETs place a high priority on energy conservation. This crucial resource needs to be utilized extremely effectively. Energy conservation may be one of the most significant system design criteria for optimization.

- Security

MANETs' nodes and data are subject to the same security risks as traditional networks. In addition to these traditional dangers, MANETs also face unique threats, such as denial-of-service assaults. Additionally, because portable devices may be stolen or their traffic may not be secure via wireless links, mobility implies higher security risks than static operation. Considerations should be given to eavesdropping, spoofing, and denial of service attacks.

- Autonomous

The administration of the various mobile nodes does not require a centralized body. Each mobile terminal in a MANET is an autonomous node with the ability to act as a host and a router. Therefore, in MANET, endpoints and switches are typically indistinguishable.

- Distributed Operation

The administration and control of the network are dispersed among the terminals because there is no background network for the central control of network operations. To accomplish tasks like security and routing, the nodes in a MANET should cooperate and each node acts as a relay as necessary.

- Multi-Hop Routing

Ad hoc routing algorithms can be divided into single-hop and multi-hop categories based on various network layer characteristics and routing protocols. In terms of implementation and structural complexity, single-hop MANET is easier than multi-hop MANET. Data packets should be passed through one or more intermediary nodes when being sent from a source to a destination that is outside of the direct wireless transmission range.

- Light- Weight Terminals

The majority of the time, MANET nodes are portable computers with limited CPU

processing capacity, little memory, and low power storage.

- Infrastructure-Less and Self Operated

The ease of deployment, speed of deployment, and reduced reliance on a fixed infrastructure are just a few benefits that a mobile ad hoc network has over typical wireless networks. Due to its ability to instantly build a network without the need for fixed base stations or system administrators, MANET is appealing.

V. SECURITY GOALS

The Goals of the security mechanism of MANETs are similar to that of other networks. They can be briefly summarized as follow

➢ Availability

Maintaining resources is a matter of availability. Availability may be lost or reduced as a result of many attacks. Some of these assaults can be mitigated automatically with authentication and encryption, but others necessitate human intervention to restore the availability of dispersed system components or pieces. Network services are protected by availability from a variety of threats. An attacker might use jamming on the physical and media access control layers to obstruct communication on physical channels, while on the network layer, it could impair the routing protocol and the continuity of network services. Once more, at higher levels, an enemy may bring down exclusive services like the key management service and the authentication service.

➢ Confidentiality

The confidentiality of information ensures that it can only be viewed or accessed by the appropriate parties. In essence, it defends against passive assaults on data. Confidentiality is required for the transmission of sensitive information, such as military information. Giving such information to adversaries could have disastrous repercussions, such as ENIGMA. To prevent the opponents from ever using the advantages of being able to identify and locate their targets on a battlefield, routing and packet forwarding information must also be kept private. There are many levels of protection when it comes to the dissemination of message content.

➢ Integrity

Integrity ensures that only parties with permission may change the data or communications. It also makes sure that a message is never corrupted while being transferred. Integrity can be applied to a single message, a stream of messages, or certain fields within a message, just like confidentiality. But complete stream protection is the best and most obvious solution. When dealing with a stream of messages, a connection-oriented integrity service ensures that there is no duplicate, insertion, modification, reordering, or replaying of the messages that have already been sent. Integrity service also includes coverage for data erasure. As a result, it covers both denials of service and message stream alteration.

- Authentication

Authentication makes ensuring that only those with permission can access and deliver data. It is focused on ensuring the authenticity of a message. The purpose is to reassure the recipient that the communication is from the source that it claims to be from in the case of a single message, such as an alarm or warning signal. Without authentication, an adversary could impersonate a node, obtaining access to resources and sensitive data without authorization and interfering with other nodes' operations.

- Non-Repudiation

The inability of the sender or the receiver to reject a communicated communication is known as non-repudiation. As a result, when a communication is transmitted, the recipient can demonstrate that the purported sender sent the message. On the other side, the sender of a communication can demonstrate that the message was received by the alleged recipient after it has been sent. To identify and isolate vulnerable nodes, non-repudiation is helpful. Non-repudiation enables node A to accuse node B using an incorrect message it received from B and persuade other nodes that B is hacked.

- Scalability

Although scalability and security are not directly related, it is a critical issue that greatly affects security services. There could be hundreds or even thousands of nodes in an ad hoc network. Scalable security measures are required for such a big network. Otherwise, the attacker may compromise the newly installed node in the network and use it to obtain unauthorized access to the entire system. In a dispersed network, it is fairly simple to launch an island-hopping attack through a single weak spot.

VI. CHALLENGES AND OPPORTUNITIES

Ad hoc networks' distinctive characteristics are both opportunities and problems for accomplishing these security objectives. First of all, a mobile ad hoc network is vulnerable to link attacks, which might range from passive eavesdropping to active interference, due to the use of wireless links. Attacks on a mobile ad hoc network can originate from any direction and can target any node, in contrast to fixed hardwired networks that have a physical defense at firewalls and gateways. Infringing on the fundamental security criteria, damage includes disclosing confidential information, tampering with messages, and impersonating nodes. All of these indicate that each node must be ready for a direct or indirect confrontation with an enemy.

Second, since they lack proper physical security, autonomous nodes in mobile ad hoc networks are more vulnerable to being taken over, corrupted, and hijacked. Attacks with malicious intent may come from both the outside and the inside of the network. Attacks from a compromised node are more harmful and harder to spot because it is challenging to locate a specific mobile node in a large-scale mobile ad hoc network. All of these points out that any node operating in a mode that does not immediately trust any peer must be ready to do so.

Thirdly, due to the networks' changing topology, any security solution with a static setup would be insufficient. A distributed architecture without central entities should be used to achieve high availability. This is so that, if any central entity is introduced into a security system, a fatal attack might be launched on the entire network. In mobile ad hoc networks, decision-making is typically decentralized.

VII. TECHNIQUES USED TO SECURE MOBILE AD-HOC NETWORKS

To provide solutions to the security issues involved in mobile ad-hoc networks, we must elaborate on two of the most commonly used approaches in use today:

- Prevention
- Detection and Reaction

Solutions that are created to stop malicious nodes from actively launching assaults are necessary for prevention. To offer routing information with authentication, confidentiality, integrity, and non-repudiation, prevention measures need to use encryption techniques. Among the current preventive strategies, some suggestions make use of symmetric algorithms, others of asymmetric algorithms, and still, others use one-way hashing, each with a particular set of trade-offs and objectives.

The full cooperation of all network nodes cannot be guaranteed by prevention techniques alone. On the other hand, detection solutions are more focused on finding signs of any malicious behavior in the network and punishing offending nodes. A node may act inappropriately if it agrees to forward packets but then fails to do so due to overload, selfishness, or maliciousness. Insufficient CPU time, buffer space, or available network bandwidth prevent an overloaded node from forwarding packets. Even though it expects others to advance packets on its behalf, a selfish node is unwilling to use up battery life, CPU time, or available network bandwidth to forward packets that are not directly of interest to it. By discarding packets, a rogue node starts a denial of service assault.

Using this as the basis, we describe the following broad classifications:

1. Prevention

- using asymmetric cryptography
- using symmetric cryptography
- using one-way hash chains

2. Detection and Reaction

- Prevention by Asymmetric Cryptography

Asymmetric cryptographic methods define the essential fundamental mode of operation for these protocols. To distribute public keys or digital certificates in the ad-hoc network, a secure wired network or a network with a comparable architecture is needed. A network with n nodes theoretically needs n public keys kept on the network. Two of the protocols

outlined in this category are SAODV (an extension to the AODV routing protocol) and ARAN.

- Prevention using symmetric cryptography

In this part, we prevent attacks on routing protocols by using symmetric cryptographic approaches. We presume that over a secured wired connection, symmetric keys are pre-negotiated. A network of "n" nodes would need to store n * (n + 1) / 2 pair-wise keys, according to a mathematical analysis. The two procedures that fall under this heading are SAR and SRP.

- Prevention by one-way chain

To defend against attacks on routing protocols, this category defines a one-way hash chain. They guard against the alteration of routing data like metric, sequence number, and source route. This includes SEAD and Ariadne.

- Detection and Reaction

On the other hand, detection solutions are more focused on finding signs of any malicious behavior in the network and punishing offending nodes. All protocols in this category are created to be able to recognize malicious activity and respond to threats as necessary. The only protocols listed in this area are Byzantine, CONFIDANT, DSR, CORE, and one that employs Watchdog and Path rater.

VIII. CONCLUSION

Mobile Ad-Hoc Networks can quickly build up networks in challenging environments where the deployment of conventional network infrastructure may not be feasible. Despite the enormous potential of ad hoc networks, there are still numerous obstacles to be solved. An essential component of MANET deployment is security. This paper includes an introduction to MANET, information on the history of these networks, goals of the security mechanism, different sorts of problems in MANET, and different methods for securing these networks. It is abundantly evident that prevention, detection, and reaction methods are necessary for a full security system. Preventive mechanism: The initial line of defense in the preventive mechanism is provided by using traditional methods including authentication, access control, encryption, and digital signature. Additional security measures include the use of tokens or smart cards that can only be accessed with a PIN, a passphrase, or a biometric verification. Detection mechanism: This refers to approaches that focus on finding indicators of any harmful activity as well as the malicious node that is causing the malicious activity in the network. Reaction mechanism: In the Reaction mechanism, it imposes sanctions on the malicious node that is instigating the network's destructive behavior. Therefore, we may argue that the prevention, detection, and reaction methods are necessary for a complete security system.

IX. MANET FUTURE WORK

Although still in its early stages, significant research in MANET has been going on for

many years. Our primary goal in writing this article is to provide researchers with guidance in the field of security in mobile Adhoc Networks. To provide security at various levels, we currently need to use a variety of tools and techniques. To do this, researchers may in the future create tools or strategies to offer security at various levels where there has been a security breach. The functionality of the prevention, detection and reaction mechanisms must all be included in the established technique under a single command line or GUI.

REFERENCES

1. Z. Niu, "Broadband computer networks," Lecture Notes, Tsinghua University, 2003.
2. L. Tao, „Mobile ad-hoc network routing protocols: Methodologies and applications," Ph.D. thesis in Computer Engineering, Virginia Polytechnic Institute and State University, 2004.
3. L. Zhou and Z. Haas, "Securing ad hoc networks," IEEE Network Magazine, vol. 13, 1999.
4. S. Buchegger and J.-Y. Le Boudec, "The selfish node: increasing routing security in mobile ad hoc networks," IBM Research Report RR 3354, 2001.
5. S. Yi, P. Naldurg, and R. Kravets, Security-Aware Ad hoc Routing for Wireless Networks The Second ACM Symposium on Mobile Ad Hoc Networking & [12] Computing (MobiHoc'01), 2001 .(another version Security-Aware Ad Hoc Routing Protocol for Wireless Networks, Report, August, 2001)
6. M. Guerrero Zapata, Secure Ad hoc On-Demand [13] Distance Vector (SAODV) Routing, INTERNET-DRAFT draft-guerrero-manet-saodv- 00.txt, August2002. First published in the IETF MANET Mailing List (October 8th 2001).
7. P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 2002.
8. Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, 2002.
9. S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in distributed ad-hoc networks," in Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, 2002.
10. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on- demand secure routing protocol resilient to byzantine failures," in ACM Workshop on Wireless Security (WiSe), Atlanta, Georgia, 2002.