ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 6 Issue 2 March 2018

International Manuscript ID : 23482001V6I2032021-116

(Approved and Registered with Govt. of India)

=

A Review on Security Features of MANETs

Sakshi Gaur
Research Scholar,
Singhania University, Jhunjhnu
sakshigaur3793@gmail.com

Dr. Amit Sanghi
Associate Professor, CSE Department
Marudhara Engineering College, Bikaner
dr.amitsanghi@gmail.com

Abstract: The mobile ad hoc network is a sort of network in which mobile nodes can join and depart at any time. Because of the network's self-configuring nature, hostile nodes infiltrate, triggering a variety of active and passive assaults. Active attacks are those that have a negative impact on network performance in terms of certain characteristics. Various approaches are evaluated and analyzed in terms of key parameters in this review study

KEYWORDS: MANETS, Active and Passive Attacks

Introduction

MANETs are a collection of mobile nodes that communicate with one another via packets going over multi-hops and without the use of a central controller. There are a significant number of mobile hosts in this network who connect with one another via wireless networks. Because this is an infrastructure-free network with no central control, the movement of the nodes is random in any direction. Because of this property, all nodes in this network operate as routers, allowing the host to send packets. The MANET provides ideal solutions in a variety of situations, such as when there is a problem with broken or overburdened wired or wireless infrastructure. The bandwidth restriction is another key design concern in MANETs [2]. As a result, it is necessary to develop a routing system that can solve the problem of restricted bandwidth while also minimising network overhead. Collision and congestion are two more key issues in wireless sensor networks. In the process of transmitting packets in MANET, the instantaneous movement of nodes inside the network causes data and control packet collisions. It also has to deal with the issue of concealed and exposed terminals [3]. A concealed terminal problem occurs when packets collide at the receiving node's end. This happens because the nodes transmit at the same time to those who are not in the sender's direct transmission range but are within the receiver's transmission range. The routing protocols will assist to reduce routing overhead and bandwidth usage, ensuring that packets are delivered correctly and on time. In MNAET, effective and efficient routing is essential, which necessitates the use of several routing protocols throughout the network [4]. The intermediate nodes play a crucial role in mobile ad hoc networks since it is only through them that packets are routed from source to destination. As a result, for the MANET, numerous routing protocols have been created that are known for effective, secure, and dispersed data packet routing. It is grouped into three categories: protocols, reactive protocols, and hybrid protocols. In the event that a link in a MANET fails, a new route from source to destination is established to keep the communication going. The transmission of data is halted if there are disconnections in the route. As a result, multicasting inside mobile ad hoc networks is reduced. Some phases are taken in the route discovery process, such as looking for

=

node disjoint, link disjoint, or non-disjoint routes [5]. When a link fails, the information is transmitted to the source code, which may then take further measures to reduce the data transfer rate and quickly find an other way. The source is alerted of the congestion issue via the congestion management techniques, which include transmission control protocol. It is necessary to gather all users in an efficient manner in order to maintain and allocate network resources. All resources, such as connection bandwidth and queues on routers or switches, are shared in this process. All of the packets that are waiting for their transmission turns are stacked in a queue. When a high number of packets are waiting for the same link to become available, the queue will overflow [6]. The packets were lost as a result of the overflow, which avoided a request overflow inside the network. When packets drop often inside the network, the network is termed crowded. As a result of the network congestion, there is a problem with connection failure. In MANET, there are two sorts of assaults that compromise the network's security. Passive attacks are security assaults that have no effect on network performance in terms of certain characteristics. Malicious nodes can simply detect network information in a passive assault. Spoofing attack and eves dropping assault are examples of passive attacks that lead to active attacks in the future [7]. The active attack is the second type of security assault that modifies network data in terms of certain characteristics. Malicious nodes are present in the network during an active attack, which can disrupt network operations. Denial of service assaults, modification attacks, and other active attacks are common. The wormhole attack is a sort of active assault that lowers network performance in terms of latency. The malicious node accepts packets and transmits them to another site through the network tunnel produced by the wormhole attack [8]. When the source node sends the control packets, the malicious node takes the path of least resistance in order to disrupt network operations. The wormhole is an assault on the network layer. Worm holes are created when network traffic is diverted through a tunnel to increase network latency.

Literature Review

The discovery and eradication of wormhole attacks throughout the transmission and propagation processes is the primary goal of this work, according to Roshani Verma et al. (2017). This suggested technique improves the security of ad hoc networks. Such assaults are not possible on this network [9]. Through the strengthening of routing protocols in networks, the packet delivery ratio is enhanced and control overhead is reduced. The table entries at the destination node are increased here in order to detect the wormhole nodes quickly. The unique methodology also aids in the implementation of effective strategies for preventing DoS and hybrid assaults from entering networks, hence improving network security.

Sunil Kumar Jangir et al. (2016) conducted a thorough investigation of the wormhole attack that occurred in MANET. The wormhole presents the fake shortest path, and all network traffic is drawn to it. Due to the prevalence of wormhole assaults, the network's throughput is also decreased, as are network delays. This document [10] also discusses several ways for detecting and blocking wormhole attacks, such as packet leashes, time-based approaches, and many more. This work also examines a number of protocols, including OLSR, DSR, and AODV, as well as various attacks against them. The quality of all wormhole detecting approaches is compared in this article. As can be observed, a large number of research have been offered to address the issue of wormhole assault. There can't be considered to be application if there's only one answer for all of the cases. However, by examining the numerous strategies described in this research, a more powerful detection strategy

=

may be discovered. As a result, an appropriate solution to wormhole attack may be offered.

H.Ghayvat et al. (2016) published a paper on a wormhole attack that may be identified and mitigated using a suggested security approach [11]. With the use of this safe Ad hoc on demand distance vector (AODV) technology, the wormhole attack within MANETs may be quickly discovered. The use of a digital signature is used to avoid this attack. The determined tunnelling duration and threshold value can be used to determine whether a particular node is a real wormhole node. The digital signature as well as the hash chain method are used to mitigate the wormhole node. The lifespan and throughput of the suggested technology are maximised in contrast to the previous approach, and the network latency is decreased. The proposed technique improves the quality of service, but the removal of unnecessary mistakes remains a worry.

According to the results of earlier techniques, Chitra Gupta et al. (2016) found that reactive, anonymous, and stateless features are critical for MANET routing protocols. Here, we'll look at a few different wormhole attack methods. The suggested technique, which is based on movement or neighbour based approach, gives improved outcomes in terms of several characteristics such as packet delivery ratio, throughput, and routing overhead decrease [12]. For sudden network improvement, more network parameters are evaluated. With the suggested strategy, several additional sorts of possible network layer assaults are also blocked from entering the network. Furthermore, the suggested technique can be improved in the future to allow for node mobility and dynamic algorithm parameter change.

In this research, Pratik Gite, et al. (2017) suggested the new technology of Mobile Ad-hoc Network, which is widely used in wireless communications. This technology is built on the principles of mobility, wireless communication, and freedom. In a multi-hop Ad-Hoc network, the mobility of the nodes and a lack of power are two reasons that cause network link failure losses. In this study, they introduced a novel routing system in which accessible routes are prioritised based on their path stability [13]. For the illustration, they used the link prediction approach, which is based on signal strength. On the AODV routing protocol, they implemented the recommended routing idea.

The primary issue of connection failure inside the mobile ad hoc network caused by node mobility was presented by Kavitha T, et al. (2017). As a result, they presented an Instant Route Migration technique in this study, which involves constructing an instantaneous path that takes into account path distance and hop count. They built a partly topology aware technique [14] to quickly find the shortest path. With the aid of this technology, packets to the destination may be readily diverted in the event of a link failure, as cache maintenance is present at every node. In comparison to existing systems, the suggested technique provides maximum throughput, decreased end-to-end latency, and rapid route migration, according to the obtained data.

According to S. B. Geetha et al. (2015), trade-off concerns are still a prominent worry in these techniques. This paper discusses the major challenges with existing techniques. A unique safe routing protocol is also presented [15] to give enough support for complicated cryptographic algorithms so that data transmission security can be improved. A few basic entities are added to the proposed routing mechanism to improve the multicast routing protocols. According to the simulation findings, the new approach outperforms the previously described mechanism in terms of energy efficiency and packet delivery ratio.

=

Table of Comparison

Authors' Names	**Year**	**Description**	**Outcome**
Roshani Verma	2017	This suggested technique improves the security of ad hoc networks. Such assaults are not possible on this network.	The unique methodology also aids in the implementation of effective strategies for preventing DoS and hybrid assaults from entering networks, hence improving network security.
Sunil Kumar Jangir,	2016	This article discusses a variety of ways for detecting and blocking wormhole attacks, including packet leashes, time-based approaches, and others.	The research of numerous strategies described in this work can be used to identify a more powerful detection strategy. As a result, an appropriate solution to wormhole attack may be offered.
H.Ghayvat,	2016	With the use of this safe Ad hoc on demand distance vector (AODV) technology, the wormhole attack within MANETs may be quickly discovered. The use of a digital signature is used to avoid this attack.	The proposed technique improves the quality of service, but the removal of unnecessary mistakes remains a worry.
Chitra Gupta,	2016	The suggested method, which is based on movement or Neighbour based approach, gives improved outcomes in terms of many characteristics such as packet delivery ratio, throughput, and routing overhead decrease.	With the suggested strategy, several additional sorts of possible network layer assaults are also blocked from entering the network.
Pratik Gite,	2017	In this research, they offer a novel routing system in which accessible routes are prioritized based on their path stability.	This strategy significantly improves the concerns of routing overhead, energy usage, and throughput for various numbers of tests.
Kavitha T,	2017	Various approaches have been presented so far to re-route packets fast, with hop count as a parameter, however they do not deliver the best end-to-end outcomes in terms of end-to-end latency.	In comparison to existing systems, the suggested technique provides maximum throughput, decreased end-to-end latency, and rapid route migration, according to the obtained data.
S. B. Geetha	2015	They claimed that trade-off concerns remain a prominent concern in these techniques. This paper discusses the major challenges with existing techniques.	According to the simulation findings, the new approach outperforms the previously described mechanism in terms of energy efficiency and packet delivery ratio.

Conclusion

The conclusion of this study is that mobile adhoc networks are a decentralized network in which mobile nodes

=

can change their location at any moment. Due to such design of the network many sorts of active and passive assaults are available which impair network performance. Various strategies for isolating malicious nodes are reviewed in terms of specific parameters in this study.

References

[1] R C Poonia, D. Bhargava, and B.Suresh Kumar. "CDRA:Cluster-based dynamic routing approach as a development of the AODV in vehicular ad-hoc networks." In Signal Processing and Communication Engineering Systems (SPACES), International Conferenceon, vol. 6, issue 3, pp.397-401, IEEE, 2015.

[2] S.Umang, BVR Reddy, MN Hoda, “Enhanced intrusion Detection System for Malicious Node detection in ADHoc Routing Protocols using Minimal energy Consumption”, IET Communications volume 4, issue 17, pp-2084-2094. 2010.

[3] B Wu, J Chen, J Wu, M Cardei, “A survey of attacks and counter measures in mobile adhoc networks”, Wireless network security, volume 15, issue 7, pp-103-135, 2007.

[4] A. Shastri, R. Dadhich, and R.C. Poonia, “Performance analysis of on-demand Routing protocols for vehicular ad-hoc Networks”, International Journal of Wireless & Mobile Networks (IJWMN) Vol 3, issue 6, pp-103-111, 2011.

[5] R A R Mahmood, A L Khan, “A Survey on Detecting Black Hole Attack in AODV-based Mobile AdHoc networks” In High Capacity Optical Networks and Enabling Technologies, 2007. HONET, International Symposium, volume 5, issue 4, pp.1-6. IEEE, 2007.

[6] MS Alkatheiri J Liu, A R Sangi, “AODV Routing Protocol under several Routing Attacks in MANETs” In Communication Technology (ICCT), 2011 IEEE 13th International Conferenceon, volume 6, issue 19, pp.614-618, IEEE, 2011.

[7] S Corson and J Macker, “Mobile adhoc networking (MANET): Routing protocol performance issues and evaluation considerations,” IETFRFC 2501, volume 18, isse 14, pp- 624-633, 1999.

[8] S. Hazra, and S.K. Setua. “Black Hole Attack Defending Trusted On-Demand Routing in Ad-Hoc Network.” In Advanced Computing, Networking and Informatics-Volume 2, issue 9, pp.59-66, Springer International Publishing, 2014.

[9] Roshani Verma, PROF. Roopesh Sharma, Upendra Singh, “New Approach through Detection and Prevention of Wormhole Attack in MANET”, International Conference on Electronics, Communication and Aerospace Technology ICECA 2017.

[10] Sunil Kumar Jangir, Naveen Hemrajani, “A Comprehensive Review On Detection Of Wormhole Attack In MANET”, 2016, IEEE.

[11] H.Ghayvat, S.Pandya, S.Shah, S.C.Mukhopadhyay, M.H.Yap, K.H.Wandra, “Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET”, 2016 Tenth International Conference on Sensing Technology.

[12] Chitra Gupta, Priya Pathak, “Movement Based or Neighbor Based Tehnique For Preventing Wormhole Attack in MANET”, 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[13] Pratik Gite, “Link Stability Prediction for Mobile Ad-hoc Network Route Stability”, International Conference on Inventive Systems and Control, 2017.

[14] Kavitha T, Muthaiah R, “ INSTANT ROUTE MIGRATION DURING LINK FAILURE IN MANETS”, International Journal of Mechanical Engineering and Technology (IJMET) Volume 8, Issue 8, August 2017.

[15] S. B. Geetha, Dr. Venkanangouda C. Patil, “Elimination of Energy and Communication Tradeoff to Resist Wormhole Attack in MANET”, International Conference on Emerging Research in Electronics, Computer Science and Technology – 2015.