Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 7, July 2019, pg.40 – 44

Security Aspects of MANETs: A Review

Zakki Ul Rehman Khan
zakkikhan12@gmail.com
Research Scholar
Arni University
Kathgarh (Indora) H.P

Ms. Ankita Sharma
ankitagsp@gmail.com
Assistant Professor
Arni University
Kathgarh (Indora) H.P

Abstract: The mobile ad hoc network is the type of network in which mobile nodes can join or leave the network when they want. Due to self configuring nature of the network malicious nodes enter which are responsible to trigger various types of active and passive attacks. The active attacks are those which reduce network performance in terms of certain parameters. In this review paper, various techniques are reviewed and analyzed in terms of certain parameters
KEYWORDS: MANETS, Active and Passive Attacks

Introduction

MANETs are the set of mobile nodes which are mobile in nature and communicate with other nodes packets moving in the multi-hops in which there is no central controller. Within this network, there are large amount of mobile hosts which use wireless links in order to communicate with each other. The movement of the nodes is random in nature in any direction as this is infrastructure less network in which no central control [1]. Due to this attributes all the nodes in this network act as the router in which packets are transferred by the host. There are several cases in which optimal solutions are provide by the MANET such as in wired or wireless infrastructure in which the issue of damaged and overloaded exists much. The other major design issue faced in MANETs is the bandwidth constraint [2]. Hence, it is required to design a routing protocol using which the issue of limited bandwidth can be overcome due to which network overhead can be minimized optimally. Another major issues faced in the wireless sensor network are Collision and congestion. The instant movement of the nodes within the network leads to cause data and control packets collisions in the process of transmitting packets in MANET. The issue of hidden terminal and exposed terminal is also faced within it [3]. The packets collision at the end of the receiving node is called as hidden terminal problem. This occurs due to the transmission of the nodes simultaneous towards those which are not in direct transmission range of the sender but lies within the receiver transmission range. The routing protocols will help in minimizing the overhead of routing and reduction in bandwidth consumption due to which packets are delivered properly on time. It is required to done the effective and efficient routing in MNAET for which it is required to have various routing protocols throughout the network [4]. An essential role is played by the intermediate nodes in the mobile ad hoc networks as only routing of packets from source to destination depends on it. Therefore, for the MANET so far various routing protocols has been developed which known for effective, secure and dispersed routing of data packets. Protocols, reactive and hybrid protocols are the three categories in which it is classified. In case there is link failure in the MANETs, a different route is

generated from source to destination in order to continue communication process. If there is disconnections occur in the route, then it stops the transmission of data. Therefore, it minimizes the multicasting within the mobile ad hoc networks.. In the process of route discovery, there are some steps that are followed such as searching of the node disjoint, link disjoint or non-disjoint routes [5]. In the condition when link failures occur, the information is send to the source code so that it can take further steps using which data transmission rate can be minimized and any alternate path can be find easily. The issue of the congestion is informed to the source by the congestion control mechanisms in which transmission control protocol are included. In order to maintain and allocate the network resources, it is required to gather all the users in an effective manner. In this process, all the resources such as bandwidth of relation, queues on the routers or switches are shared. All those packets waiting for their transmission turns are queued. If there are large numbers of packets waiting for one same link in order to free than it causes the overflow of the queue [6]. This overflow caused the packets to be dropped due to which overflow of request prevented within the network. The network is considered as congested in case of frequent dropping of packets within the network. This congestion within the network occur the issue of link failure within the network. There are two types of attacks are present in MANET which break the security of the networks. The passive attacks are the security attacks which do not reduce network performance in terms of certain parameters. In the passive attack the malicious nodes can simply sense the network information. The examples of the passive attack are spoofing attack, eves dropping attack which leads to active attack in future [7]. The active attack is the second category of security attacks which affect network information in terms of certain parameters. In the active attack malicious nodes are present in the network which can harm network normal operations. The general active attacks are denial of service attack, modification attack etc. The wormhole attack is the active type of attack which reduces network performance in terms of delay. In the wormhole attack the malicious node receives packets and sends it to another location through the tunnel which is created in the network [8]. The source node when send the control packets, the malicious node route to tunnel to affect network operations. The wormhole attacks the network layer attack. When the network traffic is redirected through the tunnel to increase network delay it is called worm hole.

Literature Review

Sayan Majumder, et.al, (2018) proposed the AD (Absolute Deviation) of statistical approach for the prevention of wormhole attack [9]. The detection of wormhole attack can be done in very less time duration due to the utilization of absolute deviation covariance and correlation. The proposed algorithm does not require any extra conditions for its execution. The wormhole attackers generate a fake tunnel from source to destination. However, there is large amount of time consumed when the original path is followed. Thus, the amount of time consumed to prevent wormhole attacker from entering the network is to be calculated importantly here. Through simulations, it is seen that absolute deviation technique provides better results in comparison to AODV. Further, the Absolute Deviation Correlation Coefficient is utilized to identify the wormholes by measuring the packet drop pattern.

Roshani Verma, et.al, (2017) presented that during the transmission and propagation processes, the identification and elimination of wormhole attack is the major aim of this paper. The security of ad hoc networks is enhanced by this proposed algorithm. Such kinds of attacks are prevented from this network [10]. The packet delivery ratio is increased and the control overhead is minimized through the enhancement of routing protocols in the networks. For identifying the wormhole nodes at high speed, the table entries at destination node are enhanced here. The novel approach also helps in deployment of efficient methods through which the DoS attacks and hybrid attacks can also be prevented from enter the networks such that their security is improved.

Sunil Kumar Jangir, et.al, (2016) provided a detailed study of the wormhole attack occurring in MANET. The false shortest path is presented by wormhole and all the network traffic is attracted towards it. The throughput of the network is also minimized along with delays in the network due to the presence of wormhole attacks. Further, various approaches such as packet leashes, time-based approaches and many more which help in detecting and preventing wormhole attacks are discussed in this paper [11]. Several protocols such as OLSR, DSR, and AODV are also studied in this paper along with their possible attacks. All the wormhole detection techniques are compared on the basis of their quality here. Thus, it is seen that for solving the issue of wormhole attack, huge amount of studies have been proposed. The availability of only one solution to

all the scenarios cannot be said to be applied. However, a stronger detection technique can be identified with the help of the study of various techniques presented in this paper. Thus, a proper solution can be proposed to prevent wormhole attack.

H.Ghayvat, et.al, (2016) presented a study related to the wormhole attack that can be detected and mitigated with the help of proposed security technique [12]. The wormhole attack within MANETs can be efficiently identified with the help of this secured Ad hoc on demand distance vector (AODV) technique. For the prevention of this attack, digital signature is utilized here. The decision whether the given node is genuine of wormhole node can be made on the basis of calculated tunneling time and threshold value. For the mitigation of wormhole node, the digital signature as well as hash chain algorithm is applied.In comparison to the existing approach, the lifetime, and throughput of proposed technique are maximized and the network delay is reduced here. The QoS is enhanced here using proposed approach however, the still concerning issue is the elimination of unwanted errors.

Chitra Gupta, et.al, (2016) studied that it is important for MANET routing protocols to have properties such as reactive, anonymous and stateless as per the results achieved from previous approaches. Several approaches applied for wormhole attack are presented here. With respect to various parameters such as packet delivery ratio, throughput, routing overhead drop, the proposed mechanism that is based on movement or neighbor based approach provides enhanced results [13]. More network parameters are assessed for sudden enhancement in the networks. Various other types of probable network layer attacks are prevented to enter the network as well, with the application of proposed approach. Further, the proposed mechanism can be enhanced in future such that the node mobility and dynamic adjustment of algorithm parameters can be done.

Pratik Gite, et.al (2017) proposed the emerging technology of Mobile Ad-hoc Network in this paper that is utilized widely in the wireless connections. Mobility, wireless connectivity and independence are some properties on which this technology is based. The mobility of the nodes and the shortage of the power are some factors in multi-hop Ad-Hoc network that occur the link failure losses in the network. They proposed a new routing protocol in this paper using which priority is given to the available routes on the basis of their path stability [14]. They utilized the link prediction technique for the illustration which is based on the signal strength. On the AODV routing protocol, they implemented the proposed routing concept. On the basis of the performed experiments, it is concluded that performance of the proposed method is better as compared to existing algorithm. The issues of routing overhead, energy consumption, and the throughput for different number of experiments is improved considerably by this method.

Kavitha T, et.al (2017) presented the major issue of the link failure within the mobile ad hoc network occurred due to the nodes mobility. Therefore, they proposed an Instant Route Migration protocol in this paper using which immediately path is constructed in which path distance and hop count are considered. In order to obtain the shortest path immediately, they implemented partial topology aware mechanism [15]. With the help of this method in which packets to the destination can be easily rerouted in case of link failure as at every node cache maintenance is present. As per obtained results, it is concluded that maximum throughput, less end to end delay, instant route migration is provided by the proposed method as compared to existing systems.

S. B. Geetha, et.al, (2015) proposed, the issues of trade-off are still a major concern in these approaches. The important issues of existing approaches are presented in this paper. Further, to provide enough support to complex cryptographic algorithms such that the security of data transmission can be enhanced, a novel secure routing protocol is proposed [16]. Few simple entities are added to enhance the multicast routing protocols within the proposed routing mechanism. As per the simulation results it is seen that in terms of energy efficiency and packet delivery ratio, the performance of proposed technique is better than previously proposed mechanism.

Table of Comparison

Authors' Names	Year	Description	Outcome
Sayan Majumder,	2018	The detection of wormhole attack can be done in very less time duration due to the utilization of absolute deviation covariance and correlation. The proposed algorithm does not require any extra conditions for its execution.	Through simulations, it is seen that absolute deviation technique provides better results in comparison to AODV.
Roshani Verma	2017	The security of ad hoc networks is enhanced by this proposed algorithm. Such kinds of attacks are prevented from this network.	The novel approach also helps in deployment of efficient methods through which the DoS attacks and hybrid attacks can also be prevented from enter the networks such that their security is improved.
Sunil Kumar Jangir,	2016	Various approaches such as packet leashes, time-based approaches and many more which help in detecting and preventing wormhole attacks are discussed in this paper.	A stronger detection technique can be identified with the help of the study of various techniques presented in this paper. Thus, a proper solution can be proposed to prevent wormhole attack.
H.Ghayvat,	2016	The wormhole attack within MANETs can be efficiently identified with the help of this secured Ad hoc on demand distance vector (AODV) technique. For the prevention of this attack, digital signature is utilized here.	The QoS is enhanced here using proposed approach however, the still concerning issue is the elimination of unwanted errors.
Chitra Gupta,	2016	With respect to various parameters such as packet delivery ratio, throughput, routing overhead drop, the proposed mechanism that is based on movement or neighbor based approach provides enhanced results.	Various other types of probable network layer attacks are prevented to enter the network as well, with the application of proposed approach.
Pratik Gite,	2017	They proposed a new routing protocol in this paper using which priority is given to the available routes on the basis of their path stability.	The issues of routing overhead, energy consumption, and the throughput for different number of experiments is improved considerably by this method.
Kavitha T,	2017	In order to re-route the packets quickly, various methods has been proposed so far in which hop count is considered as the parameter but they do not provide the optimal results for end to end delay.	As per obtained results, it is concluded that maximum throughput, less end to end delay, instant route migration is provided by the proposed method as compared to existing systems.
S. B. Geetha	2015	They proposed, the issues of trade-off are still a major concern in these approaches. The important issues of existing approaches are presented in this paper.	As per the simulation results it is seen that in terms of energy efficiency and packet delivery ratio, the performance of proposed technique is better than previously proposed mechanism.

Conclusion

In this work, it is concluded that mobile adhoc networks is the decentralized type of network in which mobile nodes change its location any time. Due to such nature of the network various type of active and passive attacks are possible which affect network performance. In this paper, various techniques which are proposed to isolate malicious nodes are reviewed in terms of certain parameters.

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] Sayan Majumder, Prof. Dr. Debika Bhattacharyya, "Mitigating Wormhole Attack in MANET Using Absolute Deviation Statistical Approach", 2018, IEEE.

[10] 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.

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

[12] 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.

[13] 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).

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

[15] 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.

[16] 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.

