Analysis of Various techniques of MANET

Amanpreet Kaur[1], Er. Kiranpreet kaur[2]
[1]Research Scholar, CSE Department, Rayat Bahara University, Mohali Campus, India
[2]Assistant Professor, CSE Department, Rayat Bahara University, Mohali Campus, India

Abstract- The mobile ad hoc network is the self configuring type of network in security and routing are the major issues of the network. The security issues are raised in the network because malicious nodes join the network which triggers various active and passive attacks. In the previous years, various security enhancement for mobile ad hoc network are designed. The security techniques which are designed in the previous years are based on data encryption and trust mechanism. In this paper, various security techniques for mobile ad hoc network are reviewed in terms of certain parameters

Keywords- MANET, Data encryption, Trust mechanism

I. INTRODUCTION

Mobile ad hoc Networks are also identified as wireless ad hoc network or ad hoc wireless network. These networks generally contain a routable networking topology over a Link Layer ad hoc network. These networks are made up of mobile sensor nodes. These nodes are connected to each other through a wireless link. These networks are considered as self arranged and self healing network. This is due to the fact that these networks do not have a permanent infrastructure [1]. Due to the frequent changes in network topology, the nodes within these networks can move freely in random manner. Every node plays the role of both router as well as host in this network. Each node within network transfers traffic to other particular node. MANET can work separately or as a component of bigger internet. These networks generate extremely dynamic independent topology by employing single or various transceivers amid mobile devices. The major challenge for this network is to deploy nodes to constantly preserve the information needed for the proper routing of data traffic. These networks are used to serve different purposes. The important applications include road safety, home, health, disaster rescue operations, air/land/navy defense, weapons, robots, and so on.

Security within MANET is a very challenging task. Its open peer-to-peer design causes a basic vulnerability in this network [2]. Each sensor node in this network can act as a router and sends packets to other nodes. Both legal network users and malevolent intruders can get the access of wireless channel. This means that MANET does not have any definite protection from the viewpoint of security. The edge separating the inner network from the outer world becomes indistinct. These networks do not have any clear infrastructure for the deployment of a particular security approach. In addition, movable nodes and the information stored by them are susceptible to compromise. Particularly, this issue occurs in low-end nodes due to their feeble security. These weaken nodes may be used by intruders for sneaking into the network. The inflexible resource limitations present one more important challenge to security of these networks [3]. The wireless medium has limited bandwidth. This medium is shared between many networking objects. A mobile node has also limited calculation potential. In contrast to wired networks, the wireless channel and node mobility cause more dynamics in these networks [4]. The topology in MANET is extremely dynamic in nature. The wireless channel also suffers from intrusions and faults. These dynamics exhibit unstable features in terms of bandwidth and delay. Security services may be demanded by mobile users with change in their location in spite of these dynamics. In MANET, one of the biggest challenges occurring due to the unavailability of fixed infrastructure is termed as routing. The process of choosing routes within a network for delivering data packets is known as routing. Routing protocols are generally divided into three categories. These are pro-active protocols, reactive protocols and hybrid protocols. Table-driven routing protocols are the other name given to pro-active routing protocols. In these protocols, an individual routing table is maintained by every mobile node [5]. The route to all the probable destination mobile devices is included in this table. The routing table is updated once in a while with the change in network topology because of the dynamicity of this network. A good example of pro-active routing protocol is Destination Sequenced Distance Vector Routing Protocol (DSDV). This protocol is based on the concept of Bellman-ford routing protocol. The addition of a Destination sequence number is done with each routing entry within the routing table. It is essential for every node to maintain this table. A node will include the new update in the table only if the entry consists of the new updated route to the destination with higher sequence number. The entry containing the novel updated route with greater destination sequence number will be included as the novel update by the node. Reactive routing protocols are also named as on-demand routing protocol. The route is generated as per the demand in this sort of routing. The route request packets are flooded all over the mobile network in the route discovery process. Dynamic Source Routing protocol (DSR) is an example of a reactive routing protocol. This routing protocol has two main stages [6]. These stages are known as route discovery and route maintenance. In the first stage, the best route for the transferring of data packets among the source and

the destination mobile nodes is determined. The third category is of hybrid routing protocols. These protocols mainly merge the benefits of both, reactive as well as pro-active routing protocols. These protocols are quite flexible. These protocols adjust themselves as per the zone and location of the source and destination nodes. Zone Routing Protocol (ZRP) is a very common example of hybrid routing protocols. In this type of routing, the division of entire network is done into several zones. Afterward, the location of source and destination node is detected [7]. Proactive routing is utilized for transferring data packets between source and destination nodes if they occur in the similar zone. On the other hand, reactive routing is used for the transferring of data packets if the source and destination nodes do not occur in the same zone. MANET faces different types of routing attacks. These attacks include black hole attack, wormhole attack, eavesdropping attack, link spoofing attack etc. A malevolent node transmits false routing message declaring to have an optimum route in a black hole intrusion. This node convinces other normal nodes to route data packets via the malevolent node. The main motive of flooding attack is to wear out the network resources e.g. bandwidth. This attack causes disruption in the routing operation and degrades the performance of the network to a large extent [8]. A malevolent node promotes bogus links with distant nodes for causing disruption in routing during the link spoofing attack. In eavesdropping attack, the malicious node tries to get the access of secret information. The secrecy of this information is essential during the information sharing. This information can contain the location, open key, private key or even passwords of the nodes.

II. LITERATURE REVIEW

Houda Moudni, et.al (2019) recommended a new technique based on ANFIS algorithm. The recommended algorithm was merged with PSO approach for optimization purpose [9]. Detection and prevention of black hole attack was the main aim of this approach. A database from MANET had been retrieved for computing the input metrics. For this purpose, a routing table had been created. The behaviors of the all neighboring nodes were recorded using this table. The tested results depicted that the recommended approach showed good performance in terms of detection rate and a false alarm rate. The recommended approach would be compared with other existing approaches in nearby future for the detection of black hole intrusion.

Qussai M. Yaseen, et.al (2018) recommended an improved AODV Protocol to prevent black holes within MANET [10]. The new algorithm developed a universal reputation system. This algorithm helped AODV protocol in the selection of optimum path among various available routes to the destination. The recommended algorithm improved the use of regulators in AODV. For this purpose, this algorithm used a less expensive approach for gathering the observations and later transferred them to all nodes with the network. In addition, the recommended algorithm considered the detection issues during the continuous movement of a black hole.

Gurveen Vaseer, et.al (2018) recommended a novel distributed trust-based security approach for preventing different types of concurrently occurring intrusions [11]. It was analyzed that the recommended approach showed accuracy rate of more than 95% in data transferring and receiving. In an AODV routing algorithm scenario, a simulation tool called NS2 had been utilized for carrying out simulation. This was the first ever attempt that reported a distributed trust-based attack avoidance approach to prevent different types of intrusions. In MANET, variable node densities had been used for checking the scalability of the recommended approach.

Vidya Kumari Saurabh, et.al (2017) suggested the use of a clustering approach in AODV routing algorithm [12]. The main aim of this clustering approach was to detect and prevent the black-hole intrusion within mobile ad hoc network. Each candidate of the module on one occasion contacted to the cluster head, for detecting the unique difference among the received number of data packets and data packets delivered by an individual node. All nodes eliminated the compromised node after detecting fault. The performance of recommended approach had been evaluated in terms of some performance metrics. These metrics included throughput, end to end delay (ETD), packet delivery ratio (PDR). A simulation tool called NS2 had been used in this work to record the conclusions based on energy simulation.

H. Ghayvat, et.al (2016) recommended a new security scheme for detecting and mitigating the wormhole intrusion [13]. The recommended approach was identified as secured Ad hoc on demand distance vector (AODV) routing protocol. This protocol successfully detected wormhole intrusion occurring within mobile ad hoc network. This approach made use of digital signature for preventing this attack. The tunneling time consumed by tunnel was computed in this work for analyzing the activities of launched attack. After that, a stationary threshold value had been decided. The specified node was distinguished as wormhole node or reliable node on the basis of these two factors. In order to isolate the contagious node, two approaches called digital signature and hash chain were implemented in this work.

Sandeep Dhende, et.al (2017) realized that security was one of the most challenging issues within MANET [14]. Its dynamicity and impermanent configuration were the two main factors behind this issue. Moreover, security concerns were

raised due to the mobility and selfishness of malevolent devices. MANET was vulnerable to different types of security attacks. However, the detection of black hole intrusion was a very difficult task. A secure AODV protocol called SAODV had been recommended in this work. The main aim of this approach was to identify and isolate different types of intrusions. A simulation tool called NS-2 was used in this work for simulating the recommended approach. The simulation results revealed that the recommended approach proved safer in contrast to the available approach.

Shabina Parbin, et.al (2017) stated that MANETs were prone to different types of routing attacks. The main aim of this work was to analyze and prevent wormhole intrusion [15]. This attack was usually launched in two stages. In the initial stag, wormhole nodes tried to generate large number of traffic routes. In the next stage, these nodes caused breakdown within the network by changing or plunging the traffic of the network. Over the years, a lot of approaches were recommended by researchers for preventing different types of routing attacks. A trust and reputation management approach had been introduced in this work. The main aim of this approach was to discover trusted location within network.

Author	Year	Description	Outcome
Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi	2019	Recommended a new technique based on ANFIS algorithm. The recommended algorithm was merged with PSO approach for optimization purpose	The tested results depicted that the recommended approach showed good performance in terms of detection rate and a false alarm rate.
Qussai M. Yaseen, Monther Aldwairi	2018	Recommended an improved AODV Protocol to prevent black holes within MANET. The new algorithm developed a universal reputation system.	The recommended algorithm considered the detection issues during the continuous movement of a black hole.
Gurveen Vaseer, Garima Ghai, Dhruva Ghai	2018	recommended a novel distributed trust-based security approach for preventing different types of concurrently occurring intrusions	This was the first ever attempt that reported a distributed trust-based attack avoidance approach to prevent different types of intrusions.
Vidya Kumari Saurabh, Roopesh Sharma, Ravikant Itare, Upendra Singh	2017	Suggested the use of a clustering approach in AODV routing algorithm. The main aim of this clustering approach was to detect and prevent the black-hole intrusion within mobile ad hoc network.	A simulation tool called NS2 had been used in this work to record the conclusions based on energy simulation.
H. Ghayvat, S. Pandya, S. Shah, S. C. Mukhopadhyay, M. H. Yap, K. H. Wandra	2016	Recommended a new security scheme for detecting and mitigating the wormhole intrusion. The recommended approach was identified as secured Ad hoc on demand distance vector (AODV) routing protocol.	This protocol successfully detected wormhole intrusion occurring within mobile ad hoc network.
Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar, Anand Najan	2017	A secure AODV protocol called SAODV had been recommended in this work. The main aim of this approach was to identify and isolate different types of intrusions.	A simulation tool called NS-2 was used in this work for simulating the recommended approach. The simulation results revealed that the recommended approach proved safer in contrast to the available approach.
Shabina Parbin, Leeladhar Mahor	2016	A trust and reputation management approach had been introduced in this work. The main aim of this approach was to discover trusted location within network.	The recommended approach efficiently detected and prevented different types of routing attacks.

III. CONCLUSION

In this work, it is concluded that mobile ad hoc network is the decentralized nature of network. The security attacks are possible in the network which is broadly classified into active and passive. The active attacks are those which affect network performance. In this work various techniques are reviewed and analyzed in terms of certain parameters. In future, novel technique needs to be designed to improve network security

IV. REFERENCES

[1]. Mr. L Raja, 2Capt. Dr. S Santhosh Baboo, "An Overview of MANET: Applications, Attacks and Challenges", IJCSMC, Vol. 3, Issue. 1, January 2014, pg.408 – 417

[2]. Mohit Kumar, Rashmi Mishra, "An Overview of MANET: History, Challenges and Applications", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 3 No. 1 Feb-Mar 2012

[3]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer 2006

[4]. Priyanka goyal, vinit, Rishi, " MANET- A valunarable, challenge, attacks and application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011

[5]. Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[6]. Payal N. Raj and PrashantB.Swadas, "DPRAODV: A Dynamic learning system against black hole attack in AODV based MANET", International Journal of Computer Science Issues (IJCSI), Volume 2, Number 3, 2009, pp 54-59.

[7]. E.A. Mary Anita, V. Vasudevan, "Black Hole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", IJCA, Volume 1, 2011

[8]. N.Mistry, D.C.Jinwala and M.Zaveri, "Improving AODV protocol against black hole attacks", international multiconference of engineers and computer scientists 2010, vol 2, IMECS 2010, march 17-19 2010, Hong Kong

[9]. Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Black Hole attack Detection using Fuzzy based Intrusion Detection Systems in MANET", Procedia Computer Science, Volume 151, 2019, Pages 1176-1181

[10]. Qussai M. Yaseen, Monther Aldwairi, "An Enhanced AODV Protocol for Avoiding Black Holes in MANET", Procedia Computer Science, Volume 134, 2018, Pages 371-376

[11]. Gurveen Vaseer, Garima Ghai, Dhruva Ghai, "Distributed Trust-Based Multiple Attack Prevention for Secure MANETs", 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS)

[12]. Vidya Kumari Saurabh, Roopesh Sharma, Ravikant Itare, Upendra Singh, "Cluster-based technique for detection and prevention of black-hole attack in MANETs", 2017, International conference of Electronics, Communication and Aerospace Technology (ICECA)

[13]. 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, 10th International Conference on Sensing Technology (ICST)

[14]. Sandeep Dhende, Sandeep Musale, Suresh Shirbahadurkar, Anand Najan, "SAODV: Black hole and gray hole attack detection protocol in MANETs", 2017, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)

[15]. Shabina Parbin, Leeladhar Mahor, "Analysis and prevention of wormhole attack using trust and reputation management scheme in MANET", 2016, 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT)