IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper **Vol.-6, Issue-11, Nov 2018** **E-ISSN: 2347-2693**

Novel Technique for Detection of Wormhole Attack in MANET

[1*]Sukhwinder Singh, [2]Rajnish Kansal

[1,2]Dept. of Computer Science and Engineering, Asra College of Engineering and Technology, Sangrur Maharaja Ranjit Singh Punjab Technical University, Bathinda, India

Available online at: www.ijcseonline.org

Accepted: 22/Nov/2018, Published: 30/Nov/2018

Abstract- The wireless nature of communication makes mobile ad hoc networks unreliable vulnerable to any attack with intent to steal the data can do so by deploying malicious nodes in the network. Normally the routing protocols are designed to find shortest path length is determined using hop count as metric. Out of many attacks the wormhole attack is pretty dangerous one as it is launched using two pairs of malicious nodes with create a tunnel by skipping few nodes in between source and destination node. The existing scheme considers the wormhole attacks when there are no intermediate nodes present between destinations. This technique is suitable for scenarios where the path length between source and destination is two hops only .this scheme cannot be used for networks with layer hops between source and destination node. In this research work, the novel scheme is proposed which detect and isolation malicious nodes from the MANETs. The malicious nodes are responsible to trigger wormhole attack in MANET. The proposed technique is implemented in NS2 and simulation results shows that proposed technique performs well as compared to other techniques.

Keywords- Wormhole, Delay per hop, Malicious, MANETs

I. 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. The major challenge in the MANET is the maintenance of the route. In the past, various kinds of local link repair mechanisms were proposed in order to minimize the issue of link failure. For instance, the interconnectivity of all the machines coming from the same place such as business meeting at a place in order to form an Ad-Hoc network in condition when network services are available. The mobile nodes will further send the message to their adjacent nodes when receive any message [2]. The message is forwarded by the intermediate nodes and act as a router in the condition when any node wants to send message to a mobile node but it is out of range of transmission of sender node. Due to the movement of nodes randomly, it is not possible to acquire fixed paths to send messages. The major challenges are caused by this wireless network as it has no fixed infrastructure using which the functionality of these networks can performed effectively. The nodes within this network can act as both router and host as it has the capability using which it can route traffic from source to destination. Topology change, unreliable communication and limited energy of nodes are some factors caused as the issue in the design of the network. Therefore, it is required to have more focused due to the constraints of MANET such as limited bandwidth and node mobility. There are various issues faced in the MANET during the routing process due to some factors such as nodes within this network are mobile in nature [3]. The distribution of the nodes randomly and the movement of intermediate nodes in the path causes the breakdown of the path. Therefore, it is required to have the effective mobility management during the process of routing. The other major design issue faced in MANETs is the bandwidth constraint. 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 routing protocols will help in minimizing the overhead of routing and reduction in bandwidth consumption due to which packets are delivered properly on time [4]. 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. 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 [5]. 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. 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. This overflow caused the packets to be dropped due to which overflow of request prevented within the network [6]. 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. 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. 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. When the source node send the control message for the path establishment to the destination, then the control messages are passed through the tunnel. The reply messages are also passed through the tunnel and source analyzed that shortest path is through the tunnel. When the source selects best path to destination then the malicious nodes redirect all the packets through tunnel or through multiple relays. Since these MPRs ahead defective topology information, it results in distribution of inaccurate topology information throughout the network. On receiving this false information, other nodes may send their messages through them for fast delivery. The deployment of wormhole attack is easy. However, within the existing network, huge damage can be caused by it. There are some of the metrics that are calculated for measuring the strength of wormhole. The false link that is being advertised by colluding nodes attracts certain amount of traffic which can be calculated through strength parameter [7]. The difference between the original and the falsely advertised path is calculated to define length. Within the network higher number of malicious nodes can be identified if the difference is also larger. Even when there is very less change in the network topology, the ability that wormhole can still persist is calculated through robustness without reducing the strength of that network. The strength of wormhole attack can be quantified by this metric. The ratio to number of packets being received to the total number of packets being transmitted defines the PDR.

II. LITERATURE REVIEW

Sayan Majumder, et.al, (2018) proposed the AD (Absolute Deviation) of statistical approach for the prevention of wormhole attack [8]. 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. It is assumed here that the distance between source and destination is very less and the time duration taken for transmitting information will be very less. 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 [9]. 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.

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. 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 [10].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. 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. 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 [11]. 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.

Sunil Kumar Jangir, et.al, (2016) presented a detailed study of the wormhole attack occurring in MANET. 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 [12]. 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. 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) proposed security technique through which the detection and mitigation of the wormhole attack can be done [13]. For the prevention of this attack, digital signature is utilized here. The behavior of wormhole is analyzed with the help of calculating tunneling time that is used by tunnel. 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**) presented that 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 [14]. 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.

III. RESEARCH METHODOLOGY

The propose technique is novel in nature as it never used before for the detection and isolation of malicious nodes from the network. The proposed technique is improvement in the existing Delphi Technique. In the existing technique, per hop delay is checked and sensor node which is increasing than per hop is detected as the malicious node. The per-hop delay can be increased in the network due to some other reasons also like congestion, link failure etc. In the proposed technique to calculate threshold formula is applied which calculate threshold value of delay. The malicious node which increase delay above threshold value is detected as malicious node.

Following are the various steps of this algorithm:-

1. The mobile ad hoc network is deployed with the finite number of mobile nodes
2. The source node sends the route request packets in the network to establish path to destination
3. The nodes which are adjacent to destination reply back with the route reply message
4. The path is established from source to destination and maximum delay of each node is stored in the buffer which is kept at the source
5. The source start sending the data packets and node which is increase delay above the threshold value is marked as the malicious node in the network

IV. PROPOSED ALGORITHM

```
Input : Number of Mobile nodes
Output : Detection of Malicious node
1. Deploy network with finite number of mobiles nodes
2. Path Establishment ()
   • Source send route request packets in the network
   • The nodes which are adjacent to destination reply with route reply packets
   • The source selects best path on the basis of hop count and sequence number
3. Calculate Threshold value ()
   • Repeat for all nodes; P = Pb *max_p; Until reach to max_p
4. Detect malicious node ()
   • Repeat loop for all nodes; If node (i) data rate < P; Malicious node =node(i); Return malicious node
5. Apply multipath routing for the selection of new path
```

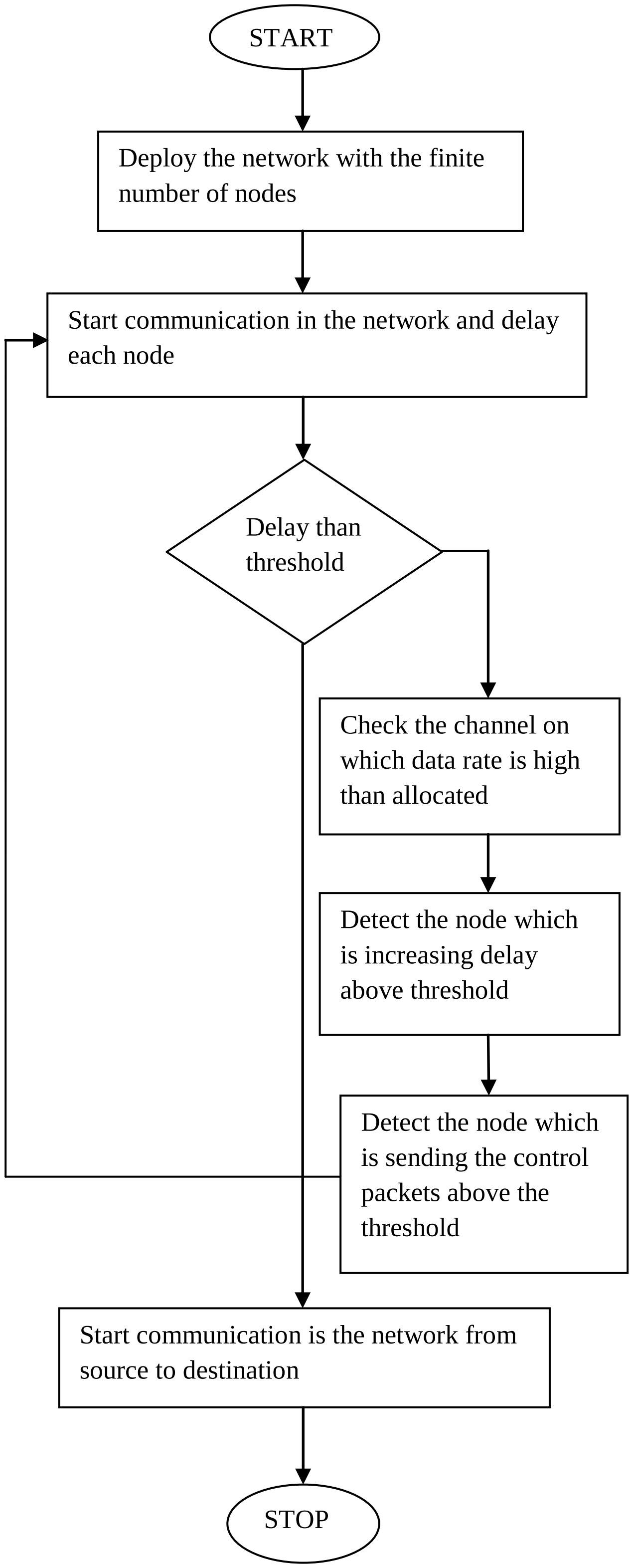
START
Deploy the network with the finite number of nodes
Start communication in the network and delay each node
Delay than threshold
Check the channel on which data rate is high than allocated
Detect the node which is increasing delay above threshold
Detect the node which is sending the control packets above the threshold
Start communication is the network from source to destination
STOP

Figure 1: Flowchart of Proposed Work

V. EXPERIMENTAL RESULTS

The proposed work is implemented in NS2 and the results are analyzed in terms of several parameters.

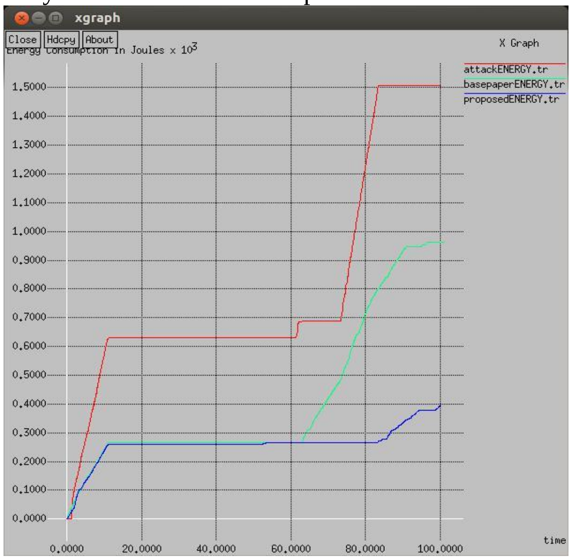

Fig 2: Energy consumption

As shown in figure 2, the energy consumption of the attack scenario, base paper scenario and proposed technique scenario is compared for the performance analysis. It is analyzed that proposed scenario has least energy consumption than other scenarios

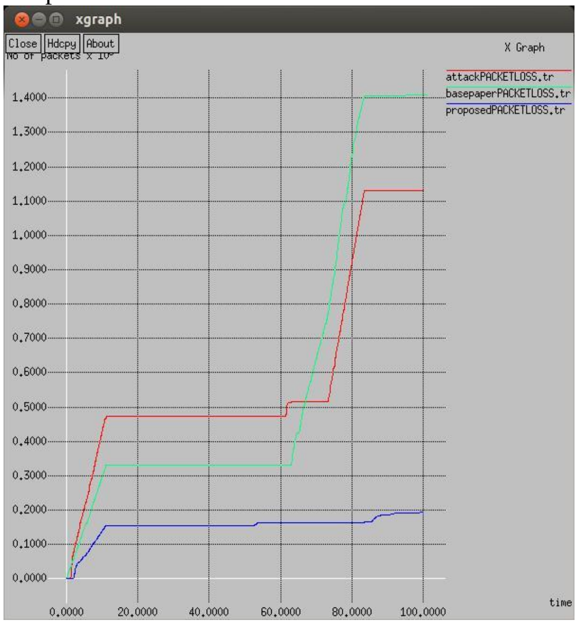

Fig 3: Packet loss Comparison

As shown in figure 3, the packet loss of attack scenario, base paper scenario and proposed scenario is compared for the performance analysis. It is analyzed that packet loss of proposed technique is less as compared to other techniques.

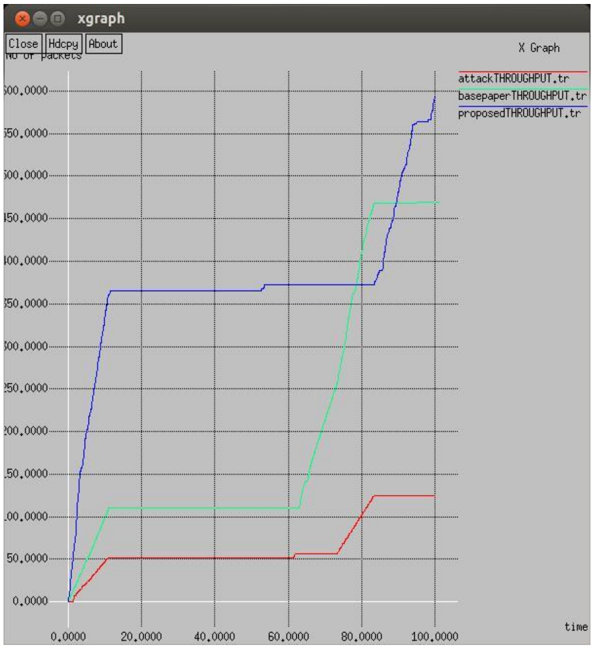

Fig 4: Throughput Comparison

As shown in figure 4, the throughput of the attack scenario, base paper scenario and proposed scenario is compared for the performance analysis. It is analyzed that throughput of proposed scenario is maximum as compared to other scenario's.

VI. Conclusion

The wireless ad hoc network is the decentralized type of network in which mobile nodes can join or leave the network when they want. The wireless ad hoc network is the network in which no central controller is present. Due to self configuring nature of the network security, routing and quality of service are the major issues of this network. The wormhole attack is the active type of attack in which malicious nodes can enter the network and increase delay. The technique is the Delphi technique which is used in the existing work. The Delphi technique has less accuracy and high execution time for the detection of malicious nodes. In this research work, threshold based technique is proposed for the detection of malicious nodes from the network. The proposed and existing techniques are implemented in Ns2 and simulation result shows improvement in energy consumption, throughput and packet loss.

REFERENCES

[1]. M Moharlalpriya and I Krishnamurthi. "Modified DSR protocol for detection and removal of selective black hole attack in MANET", Comput. Electr. Eng., volume 40, issue 55, pp-530-538. 2014.

[2]. VK Sagtani, and SKumar, "Modern Approach to Enhance Routing Recitation in MANET". International Journal of Emerging Technology and Advanced Engineering, volume 4, issue 7, pp.265-270, 2014.

[3]. Y. Hu, A Perrig and D. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on selected areas in communication, Vol. 24, No. 2, pp- 823-836, 2006.

[4]. AC.Yao, "Protocol for Secure Computations," in proceedings of the 23rd annual IEEE symposium on foundation of computer science, volume 5, issue 14, pages 160-164, 1982.

[5]. D. K. Mishra, M. Chandwani, "Extended Protocol for Secure Multiparty Computation using Ambiguous Identity," WSEAS Transaction on Computer Research, Vol. 2, issue 2, pp- 264-275, 2007.

[6]. C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu, "Tools for Privacy-Preserving Distributed Data Mining," J. SIGKDD Explorations, Newsletter, VolA, No.2, ACM Press, pages 28-34, 2002.

[7]. R. Sheikh, B. Kumar and D. K. Mishra, "PrivacyPreserving k-Secure Sum Protocol," in International Journal of Computer Science and Information Security, Vol.6 No.2, pages 184-188,, 2009.

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

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

[11]. 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

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

[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 Tenth International Conference on Sensing Technology

[14]. 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)