International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

Secure Channel and Watch-Dog based technique for Isolation of Wormhole Attack in MANETs

Madhu[1], Dr. Rakesh Kumar[2], Sukhjot Kaur[3]
[1]*Research Scholar,* [2]*Professor and Director,* [3]*Asisstant Professor, Sachdeva Engineering College for Girls, Gharuan, Mohali, India*

***Abstract*- The mobile adhoc networks, is the decentralized type of network in which mobile nodes can join or leave the network when they want. The secure and shortest path from source to destination will be selected on the basis of hop count and sequence number. The selected path must have minimum hop count and maximum sequence number. When the malicious node enters the network it leads to trigger wormhole attack in the network. The wormhole attack increases the delay on the established path. In this paper, technique is proposed which detects and isolates malicious nodes and this proposed technique is based on two steps. The reliability of the proposed technique is tested in NS2 and it is being analyzed that it performs well in terms of various parameters.**

***Keywords*- MANETs, AODV, HYBRID, REACTIVE,PROACTIVE, WORMHOLE, RSA, WATCH-DOG**

I. INTRODUCTION

The network in which the nodes are deployed in such a manner that the nodes that are within the communication range can exchange data is known as a mobile ad hoc network (MANET). In case where the nodes are not in the range for communication, they depend on other nodes for helping them in communicating [1]. The intermediate hosts transfer the packets from source to destination node and this result in generating a multi-hop environment within the network. A self-configuring network which has wireless links connected to each other is called MANET which includes random topology due to combination of variety of links. There is a random arrangement of the routers which can also move within the network in random manner. This results in changing the topology of the network at any duration and at higher speed [2]. There are various emergency applications that utilize the ad hoc networks within them due to its properties such as quick deployment and less setup required for deployment.

A) Routing Protocols in MANETs:

Routing protocols define an arrangement of standards which governs the journey of message packets from source to destination in a network.

In MANET, there are diverse sorts of routing protocols each of them is connected by network circumstances [3].

*a) Proactive Routing Protocols***:** Proactive routing protocols are likewise called as table driven routing protocols.The changes made within the network are updated within the routing table which stores the information of the topology of the network[4].Various actions and further tasks to be performed within the network rely on this routing table's information. There are different understood proactive routing protocols. Example: DSDV, OLSR, WRP etc.

b) Reactive Routing Protocols: Reactive routing convention is otherwise called on demand routing convention. The discovery of a new route is initiated only when required or demanded within the network as per the scenario [5]. In case the route is already available it is provided for the task. If the route is not available only then the route discovery process is initiated.

B) Wormhole Attack in MANETs

An attack caused on the routing protocols of MANETis which the nodes create an illusion that two remote areas are connected using these nodes is known as wormhole attack. These nodes are the ones which seem to be the neighbors to each other and are really far from each other. There are two attackers which are being involved in this network which are connected to the high speed off-channel link. These are placed at various ends across the network. A tunnel is a secret path that is generated within this attack for transmitting the packets in a secret manner [6]. At a certain point within the network, the packets are received and then tunneled to a different point within the network. Further the same packets are replayed within the network from that particular point only so that the attack is difficult to be recognized.

The speed of the packet that is tunneled is higher to reach the destination as compared to the other packets that reach the destination within a multi-hop over larger distances. This is possible due to the increase in hops and also as the speed of the node reduces due to a single long distance hop.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

There is delay introduced within the network due to wormhole attack which can be minimized by transferring bits of packets and not waiting for the whole packet to be transferred across the tunnels [7]. If the tunneling of packets is done in a proper manner within the network, the attacker actually is benefiting the network's efficiency by connecting it reliably.

The organization of this paper is in the following manner: Section 2 contains the review of related literature. In Section 3 the proposed methodology which includes the Pseudo code of proposed technique is explained. Section 4 incorporates the discussion and also demonstrates the results .Section 5 refines the Conclusion of this Research.

II. Literature Review

Vodnala, D.et.al proposed [8] that due to the mobility of devices in MANET, there might result changes in the topology of the network. The changes might occur rapidly and without any specific time prediction. The multicast routing as well as route maintenance is very important tasks in this network. In this paper, multicasting groups are formed which construct a virtual backbone of the network. During the link failure, these groups provide an alternate path on localization and this result in improvement in efficiency and reliability of theMANET. This proposed strategy when compared with the Bach-Bone Group Model (BGM), provides more effective results during the increase in traffic and network size. Dhakad,C.et.al stated [9] that in MANETs, designing the routing protocol is of major concern. Here, a method is proposedthe RSSI value of the neighbor nodes is calculated by the node. If the value is less than the threshold value, then the link failure factor is increased by 1 and the LFF is calculated till the destination node. The link failure factor of every node is calculated using this method the route which has minimum link failure is selected as firstly route between senders and destination. It selects the route for the base of minimum step count. The performance of LFAODV is better than the SEAODV routing protocol, which can be seen in the simulation results. The results are done on the basis of packet delivery ratio, throughput and routing overhead. Aluvala,S.et.al recommended[10] that various routing protocols are introduced in MANETs along with their maintenance which is very difficult. In some scenarios the link failure occurs within the network which further causes loss of data and delay of packet deliveries within the network. For the purpose of maintaining routes an algorithm is proposed in this paper, which is named as DSR-LLF and is based on localization of link failure within the network.

On the basis of the link failure of source route, the decisions are made and thus the route discovery process is enhanced with the help of DSR-LLF technique. Also, the maintenance of the route and the performance of the DSR are enhanced within the help ofthis technique. Hdkelek,I.et.al intended[11] a novel analytic model and simulation studies for node degree and normalized link failure frequency (nlff) in WSNs. A degree of node to increase and nlff to decrease upto certain threshold level is put forth. The random walk model is followed for the movements of nodes. The numerical and simulation results provide the relationship between node degree and nlff along with different node densities. The stability of the virtual backbone is examined with the help of degree of the node. With the help of this modeling framework, the various additional metrics are extended and the connectivity of the network is maintained along with the capacity and the lifetime. Islam,M.et.al, resolted[12] a link failure and congestion-aware reliable data delivery (LCRDD) mechanism. The local packet buffering as well as the multilevel congestion detection is determined together. The data delivery performance is increased using such control approaches. The incoming data packets are buffered at transport layer queue by the LCRDD intermediate node. The transmission mechanism is restarted once the route is repaired locally. This method provides improvement in reliability and throughput and also reduces the end-to-end packet delivery delay as well as routing overhead. The results are to be seen in the performance evaluations made in the network simulator v-2.34. Usturge,S-N.et.al explained in this paper [13] that due to the mobility feature, routing in MANET is a major concerning issue. Link failure is mainly caused due to mobility, interference and congestion. It is seen through various techniques that, the performance of MANETs can be improved. The congestion control however, can be improved by avoiding route failure mainly using cross layer approach and signal strength parameters. AODV is utilized for providing congestion control on the basis of signal strength due to its higher efficiency as compared to other protocols. The link status information is given with the help of the acquired signal strength. The monitoring of state of the route is also performed through this. For highly dense networks the best suitable protocol is the Cross Layer Stability based routing CLS_AODV. Oddi,G.et.al anticipated[14] that the self configuring networks of mobile nodes that communicate through wireless links are known as MANETs. Here, a proactive routing protocol is proposed using the Reinforcement Learning (RL) techniques which chooses the most suitable path dynamically.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

The GPS information is used in this technique and the resiliency is to be increased for link failure. The simulation results depict the effectiveness of the proposed protocol. The comparisons are made with Optimized Link State Routing (OLSR) protocol and numerous propositions are made for the future work. The introduction of new metrics allows the formulation of algorithm.

III. Proposed Methodology

The attack that creates tunnel within the network with the help of malicious node for transferring packets and increases delay in the established path from source to destination is known as a wormhole attack. The mobile ad hoc network has decentralized architecture due to which malicious nodes enter the network and trigger wormhole attack which leads to reduction in network performance. In this paper, technique will be proposed which detects and isolates malicious nodes from the network. The proposed technique is based on two steps.

1. In the first step, the secure channel will be established from source to destination using the RSA algorithm. If the secure channel is not established in a threshold amount of time then there is possibility of the intrusion in the established path.

2. In the second step, the technique of watch-dog is applied which confirms the intrusion. This further identifies the malicious node present within the network. A multipath routing method will be used for isolating the malicious node from the network.

Input: Mobile nodes, malicious node

Output: Malicious node

Define source and destination node in the network

Establish path from source to destination using AODV protocol

Establish shared key using RSA ()

Choose two very large random prime integers:p and q2.

Compute n and φ(n):n = pq and φ(n) = (p-1)(q-1)

Choose an integer e, $1 < e < \varphi(n)$ such that:gcd(e, φ(n)) = 1(where gcd means greatest common denominator)

Compute d, $1 < d < \varphi(n)$ such that:$ed \equiv 1 \pmod{\varphi(n)}$

End

If (Shared key k established in time T)

Start communication on the path

Else

Apply watch-dog technique for the malicious node detection

End if

End if

IV. Results And Discussion

The proposed algorithm is been implemented in Ns2 by taking parameters which are described in table 1

Table 1:
Simulation Parameter

Parameter	Value
Channel	Wireless channel
Link layer	LL
Queue	Priority queue
Anteena Type	Omi-directional
Number of nodes	24
Area	800*800
Range	18 meter
Frequency	2.4 Ghz

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 6, June 2017)

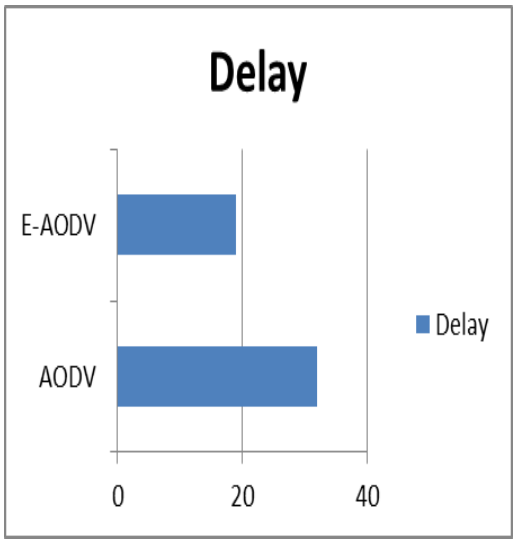

Fig 1: Delay Comparison

As shown in figure 1, the delay of the proposed and existing algorithm is compared in terms of network delay. It is been analyzed that network delay is reduced when the attack is isolated from the network

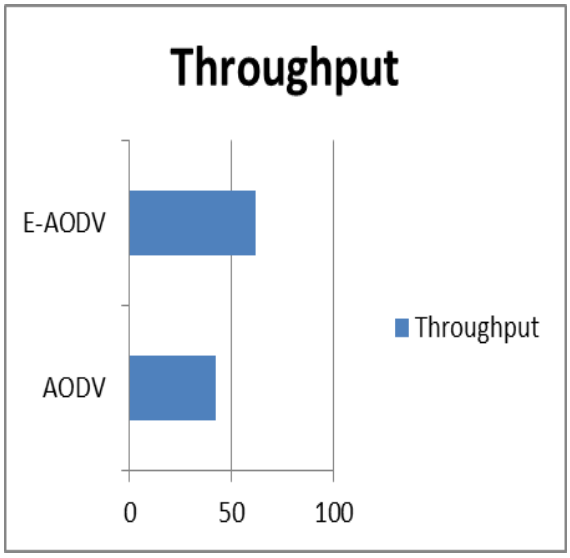

Fig 2: Network throughput

As shown in figure 2, the throughput of the proposed and existing algorithm is compared and it is been analyzed that network throughput is increased at steady rate after attack isolation

V. Conclusion

In this paper, it is being concluded that wormhole is the active type of attack which reduces network performance is terms of network delay. In this paper, two-step technique is being proposed which detects and isolates malicious nodes from the network using multi-path routing. The proposed and existing technique is being implemented in NS2. It is being analyzed that network throughput is increased to 35%, network packetloss is reduced to 23% and network delay is reduced to 18%.

REFERENCES

[1] Lemma, F., Ye, Z. Krishnamurthy, S. V. Tripathi, S.K.., (1996), "Improving TCP Performance in Ad Hoc Networks using Signal Strength based Link Management," ASM, Vol. 1, pp. 98–104.

[2] Perkins, C.E., Royer E.M., and Das S. R.,(2003)"Ad Hoc on Demand Distance Vector Routing Protocol", IETF RFC 3651.

[3] Marina M. and Das, S., (2001), "On-demand multipath distance vector routing in ad hoc networks," Proceedings IEEE International Conference Network Protocols (ICNP), pp. 14–23.

[4] Perkins, C.E., Royer, E.M.B., and Chokers, I., (2003), "Ad Hoc on demand distance vector (AODV) routing," IETF Internet drafts.

[5] Oaken, K., Lertwatechakul M.,(2008),"An improvement of Ad Hoc route maintenance" International Symposium on Communications and Information Technologies (ISCIT).

[6] Wing, L.N., Yang,J., (2010), "A cross-layer stability-based routing mechanism for ultra wideband networks" Computer Communications 33, 2185–2194.

[7] Ramachandran, B.,Shanmugavel, S., (2007), "Impact of Node Density on Cross Layer Design for Reliable Route Discovery in Mobile Ad-hoc Networks" IEEE

[8] Vodnala, D., Kumar, S.,Aluvala,S., (2016), "An Efficient Backbone Based Quick Link Failure Recovery Multicast Routing Protocol", Springer, 8, 135-137

[9] Dhakad, C., Bisen, A.S., (2016), "Efficient Route Selection by Using Link Failure Factor in MANET", IEEE, International Conference on Electrical ,Electronics, and Optimization Techniques (ICEEOT).

[10] Aluvala, S., Vodnala, D., Yamsani, N., Kumar, S.P., (2014), "A Routing Algorithm for Localization of Link Failure in MANET", ISSN: 2393-8374, 2394-0697, VOLUME-1, ISSUE-3.

[11] Hdkelek, I., Uyar, M.U.,Fecko,M., (2006), "Degree and Link Failure Frequency Analysis for MANETs with Different Node Densities", Springer

[12] Islam, M., Razzaque, A., Bosunia, M.R.,Alamri, A., Hassan, M.M., (2012), "Link failure and congestion-awar e reliable data delivery mechanism for mobile ad hoc networks", Springer.

[13] Usturge, S.N., (2012), "Study of congestion control using AODV and signal strength by avoiding link failure in MANET", IEEE.

[14] Oddi, G., Macone, D., Pietrabissa A., and Liberati,F., (2012), "A Proactive Link-Failure Resilient Routing Protocol for MANETs based on Reinforcement Learning", 20th Mediterranean Conference on Control & Automation (MED).