Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

An Improved Approach of Wormhole Attack Prevention and Performance Improvement

Sameeksha Jain
Computer Science and Engineering
AITR Indore, India

Dr. Abhay Kothari
Computer Science and Engineering
AITR Indore, India

***Abstract*— The wireless communication networks frequently replace the traditional wired networks. Due to its low cost of installation and easy maintenance. The wireless networks allow a user to join the network and consume the network services. Additionally that also allows moving the node in any direction randomly. Mobile ad hoc network is similar kind of network where the devices working as both sender and receiver. In this network the device to device communication is possible by the relaying communication therefore an intermediate host always becomes a part of communication. If the intermediate host is not trusted then it can be alter or modify the messages transmitted towards the designation host. Therefore a mechanism is required to enhance the current communication technique in mobile ad hoc network. Therefore in this presented work the security in ad hoc networks is investigated, the investigation leads to find a solution for wormhole attack. In this attacker a group of attackers are deployed in network and harm the privacy and security of network. Therefore a solution with the cryptographic manner to prevent the information forwarded to the destination is proposed. The second contribution of the work is to prepare a technique by which the wormhole nodes are prevented in network. In this approach the watch dog method is used for identifying the malicious host in network and tries to boycott using the presented method during the route discovery. The implementation of the proposed work is performed on the basis of the NS2 network simulator and the generated trace files are used for performance evaluation of the work. The performance of the proposed routing protocol is evaluated in terms of end to end delay, throughput, packet delivery ratio, and packet drop ratio. Additionally to justify the solution the proposed routing protocol's performance is compared with the traditional EAAK and the AODV routing protocol during the attack conditions. According to the experimental results the performance of the proposed routing protocol is found optimum and adoptable for both security and performance issues in network.**

Keywords*— MANET(Mobile Adhoc Network), *IDS*(Intrusion Detection System), AODV(Ad Hoc On Demand Distance Vector), EAAK(Enhanced Adaptive Acknowledgment).

I. INTRODUCTION

In wormhole attack a malicious device receives packets at one place in the network and transfer to another location in the network, where these packets are retransmitted to the network. This channel between two secret agreement attackers is referred to as a wormhole. It could be established through wired links between two secret agreement attackers or using a single long-range wireless connection. In this type of attack the attacker may construct a wormhole for packets not addressed to itself, for the reason that the broadcast property of the radio channel [1].

For example in Figure 1 , X and Y are two malicious devices that wrap data packets and fake the route lengths.

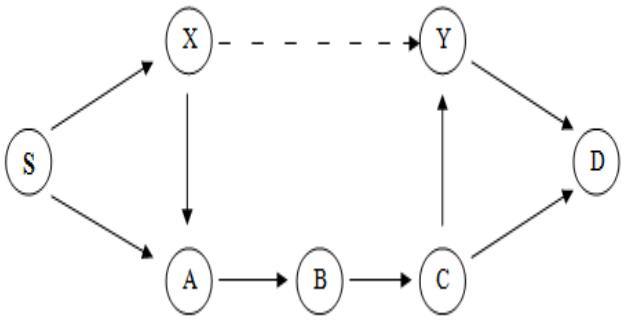

Fig. 1. Wormhole Attack

Assume that node S wants to create a route to D and initiate route detection. When X receives a route request from S, X encapsulates the route appeal and tunnels it to Y over an obtainable route, in this situation {X → A → B → C → Y}. When Y receives the encapsulated route request for D then it will demonstrate that it had only traversed {S → X → Y → D}. Neither X nor Y update the packet header. After route detection, the destination finds two different routes of unequal length from S: one is about 4 and another is about 3. If Y channels the route reply to X, S would falsely consider the pathway to D via X is better than the pathway to D via A. Thus, tunneling can prevent honest intermediary devices from properly increasing the metric used to calculate path lengths.
While no harm is done if the wormhole is used for efficient routing, it puts the attacker in a strong position as compared to other device in the network, by which attacker can utilize in a way that could compromise with the security of network.
The wormhole attack is principally unsecure for various ad hoc network routing techniques by which the device that listen a packet transmission openly from some node consider themselves to be in the range of (and thus a neighbor of) that node. As an instance, while used against an on-demand routing protocol such as DSR, a strong application of wormhole attack can be ridded by tunneling each RREQ packets directly to the target node of the request. When end node's neighbors find this request packet, they will pursue normal routing protocol processing to rebroadcast that copy of the request and then reject without handling all other received RREQ packets originating from this same route detection. This attack prevents routes other than through the wormhole actually detected, and if the malicious user is near source of the route detection. This attack can prevent routes more than two hops from being discovered. The attacker in the wormhole will

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

discard packet rather than forwarding all data packets, thus deploying a permanent DoS attack or selectively discarding or modifying certain data packets. So, if proper mechanisms are not in a job to protect the network from wormhole attacks, most of the active routing protocols for ad hoc wireless networks may fail to find valid routes.

II. RELATED WORK

A Mobile Ad-Hoc Network (MANET) is a self-configuring, infrastructure less network of mobile devices connected by wireless links. Loopholes like wireless medium, lack of a fixed infrastructure, dynamic topology, rapid deployment practices, and the hostile environments in which they may be deployed, make MANET vulnerable to a wide range of security attacks and Wormhole attack is one of them. During this attack a malicious node captures packets from one location in the network, and tunnels them to another colluding malicious node at a distant point, which replays them locally. ***Subhashis Banerjee et al [2]*** present a cluster based Wormhole attack avoidance technique. The concept of hierarchical clustering with a novel hierarchical 32-bit node addressing scheme is used for avoiding the attacking path during the route discovery phase of the DSR protocol, which is considered as the under lying routing protocol. Pinpointing the location of the wormhole nodes in the case of exposed attack is also given by using this method.

Wormhole Attack can significantly impede performance of any Mobile Ad hoc Network (MANET) by disrupting its normal routing operations. Such attack can be launched even if the network communication provides confidentiality and authenticity. Wormhole Attack usually involves two or more malicious nodes located at different physical locations which collude by disseminating incorrect routing information in order to attract data traffic to traverse through them. As result, malicious nodes have the option to drop the packets or deliver them. ***Ali Hassan et al [3]***,an efficient algorithm has been presented for defending against wormhole attacks. The proposed mechanism is called Packet Travel Time (PTT), which enables nodes in the network to monitor how their neighbors behave and thus can detect and avoid forwarding their application traffic to go through suspected wormhole link. Simulation results have been presented to illustrate the effectiveness of the proposed algorithm. For evaluation purposes, AODV protocol has been considered as a routing protocol for MANETs.

Mobile Ad hoc Networks (MANETs) work without any fixed infrastructure and each node in the network behaves as a router in order to transmit data towards the destination. Due to the lack of central point of control, MANETs are more vulnerable to routing attacks as compared to other networks. Wormhole attack is one of the most severe routing attacks, which is easy to implement but hard to detect. Normally, it works in two steps; in the first step, the wormhole nodes attract more and more traffic towards them through the wormhole channel, and in the second step, they start harming the network by modifying or dropping the network traffic. Several authors have proposed different solutions to counter wormhole attacks in MANETs. ***Muhammad Imran et al [4]*** thoroughly analyze these existing techniques on the basis of their limitations as well as features that are vital in detecting wormhole attacks in MANETs.

Security is most critical issue aspects for mobile network. A network in public domain suffers from various internal and external attacks. Worm Hole is one of such attack in which two or more nodes collectively access the bandwidth and disturb the communication. ***Amit Kumar et al [5]*** present, communication parameter based analysis model is presented to provide the safe communication under worm hole attack. The results obtained from work shows that the work has improved the communication and reduced the communication loss.

This paper proposes a method to detect and isolate wormhole attacks in mobile ad hoc networks (MANETs). The main idea of this paper is to create many possible routes when sending Route Request (RREQ) from source to destination and to use those routes as reference of each other, in order to find malicious nodes with suspicious behavior within the network. The proposed method works in three steps, which are using routes redundancy, routes aggregation and calculating round-trip time (RTT) of all listed routes. Routes redundancy is started where source sends RREQ using every possible way to destination. All routes that connect source and destination are listed together with the number of hops from every route. Some routes gathered in the same relay point before destination is aggregated, so all nodes that join the network can be listed and the behavior of malicious nodes in can be detected. The RTT and number of hops of all listed routes are compared in order to detect suspicious route. Nodes with suspicious behavior within network are isolated and will not be considered for transmission. Simulation results shows the ability to prevent the increasing of packets dropped, based on wormhole isolation in our proposed scheme compare to normal AODV protocol and approach of previous time-based calculation, ***Soo-Young Shin et al***[6]

The advancement in wireless technologies and the high availability of wireless equipment in everyday devices is a factor in the success of infrastructure-less networks. MANETs are becoming more and more common due to their ease of deployment. The high availability of such networks and the lack in security measures of their routing protocols are alluring a number of attackers to intrude. A particular type of DoS attack; known as Wormhole is the topic of discussion in this paper. A number of solutions have been proposed catering a wide range of possibilities for detection and prevention of wormholes. Literature review shows that the paths in the routing table have not been used for the detection of the wormhole attack; with a little modification to the structure of the routing table we can be able to detect suspicious links. In this paper we have proposed the use of the modified routing table for detection of the suspicious links, confirmation of wormhole existence, at the end isolating the confirmed wormhole nodes. The approach has been applied to DSDV and the detection of self-sufficient wormhole nodes and attacks. Our future work will involve the use of our own approach for detection and prevention of wormhole attacks in other protocols as well as comparison the technique with other techniques present in literature, ***Zubair Ahmed Khan*** [7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

III. PROPOSED WORK

In order to provide end to end efficient and secure solution for mobile ad hoc network routing the two step solution is introduced. Both the steps are implemented for detecting the wormhole attack and for reducing the network overhead:

A. Step 1

In this step the key management is performed therefore first of all both sender and destination node exchange their keys by using Deffie Hellman key exchange method. That method is a strong solution for secure key exchange over the untrusted network. After securing the key exchange sender node send the dummy packet towards the destination node. The dummy packet contains previous hop field, hop count and timestamp field. This information is gathered during the time of route discovery. This information is secured through the encryption by key which is shared between sender and destination node. Intermediate nodes add a packet which contains hop count and previous hop field.

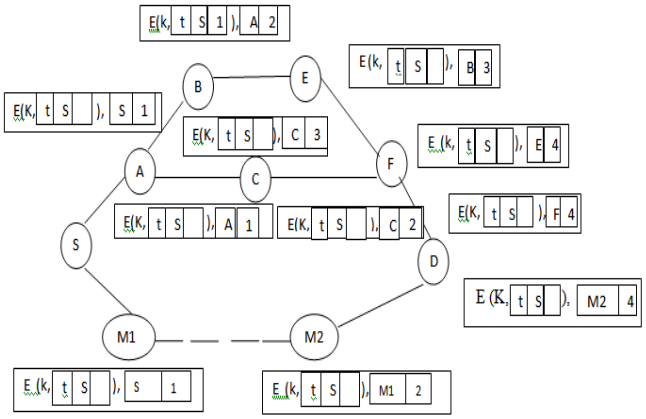

Fig. 2. Request Roadmap

B. Step 2

When destination node get the request packet, than it doesn't immediately reply to requested path, instead firstly it collect the information of each route from source to destination. And start detection processes by comparing the time that is taken for sending the request along with number of hop for each path. If path has larger delay and smaller hop count than another path then this path is under wormhole attack. So destination node reply for only one path that has less delay and least number of hops. At the end this reply is again encrypted by a key that is shared between sender and destination ***Umesh kumar chaurasia [8].***

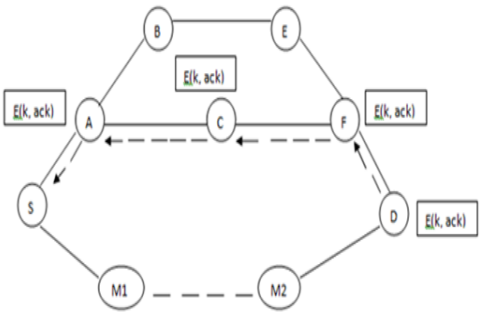

Fig. 3. RREP Roadmap

C. Proposed Algorithm

This section describes the method by which the secure transmission among source and destination is performed.

- Use DH concept for key exchange
- Initiate route discovery using dummy packet transmission
- Packet arrived at the destination node
- For each received packet
- $T_h = \frac{start\ time - end\ time}{number\ of\ hops}$
- if T_h> new T_h
- remove route
- else
- accept the route
- end if
- start transmission using encrypted data

The given summarized steps help to understand the process followed for data exchange during untrusted environment in network.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

IV. RESULTS ANALYSIS

The implementation of the proposed secure routing protocol is performed and simulated in different experimental conditions. After different experimentations, the performance of the protocol is evaluated and compared with the traditional approach discussed previously.

A. End to End delay

End to end delay on network refers to the time taken for a packet to be transmitted across a network from source to destination device.

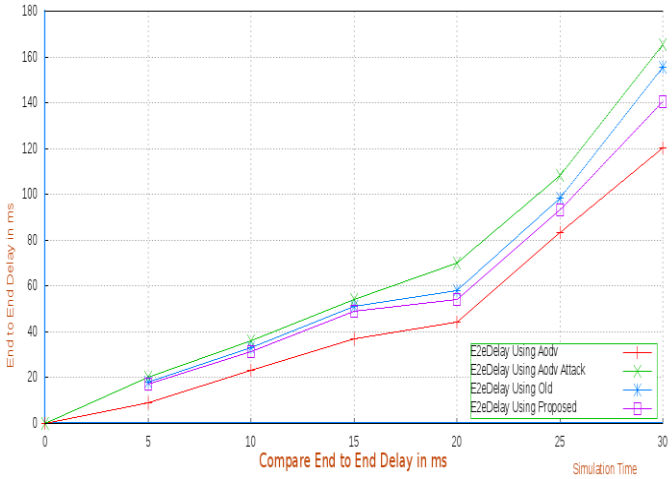

Fig. 4. end to end delay

The end to end delays of the network during the entire implemented scenarios are reported using figure 4. In this figure the X axis contains the number of nodes in network and the Y axis contains the end to end delay of the network in terms of milliseconds. For demonstrating the performance red line shows the performance of traditional AODV routing protocol in normal conditions. That represents the reference line of optimum end to end delay with increasing number of nodes in network. Similarly the AODV protocol under attack condition is simulated using green line. That provides the higher end to end delay in network as the reference. The blue line shows the performance of traditional approach of secure routing and the purple color line shows the proposed routing protocol. The comparative study among both traditional and proposed protocol the proposed routing protocol outperforms as compared to the traditional routing protocol.

B. Packet Drop Ratio(PDR)

The packet drop ratio shows the amount of packets failed to deliver in destination device, thus the percentage amount of data dropped in network is termed as the packet drop ratio.

The packet drop ratio shows the amount of packets failed to deliver in destination device, thus the percentage amount of data dropped in network is termed as the packet drop ratio.

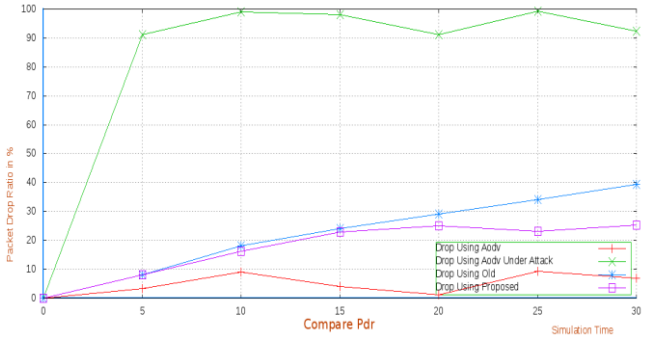

Fig. 5. Packet Drop Ratio

Figure 5 shows the amount of packet dropped during transmission of data in network. In this figure the X axis shows the number of nodes in network and the Y axis shows the percentage dropped packets during transmission. The representation of traditional AODV, AODV under attack, traditional routing protocol and proposed routing protocol is given using red line, green line, blue line and the purple lines. The comparative performance of the protocols shows the effectiveness and efficient performance as compared to the traditional technique of wormhole detection and prevention. The packet drop ratio of the proposed routing protocol is less than the traditional approach.

C Packet Delivery Ratio(PDR)

Provides information about the performance of any routing protocols, where PDR is estimated using the formula given.

Packet delivery ratio= (total delivered packets)/(total sent packets)

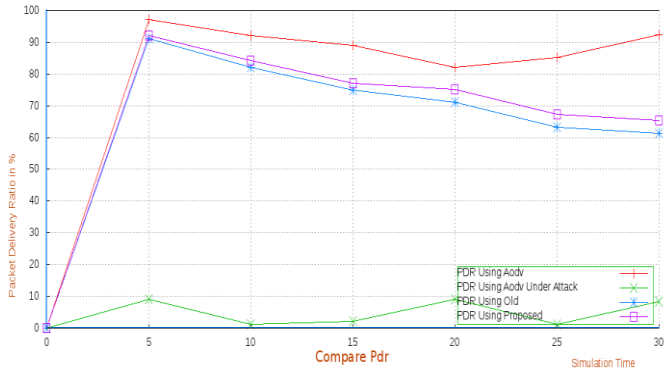

Fig. 6. Packet Delivery Ratio

Figure 6 shows the percentage packet delivery ratio of the network in terms of percentage. The AODV delivers most of the packets in normal scenarios when the attack is not introduced in network as shown by red line. After introducing attack over the network the performance of routing protocol is reduced considerably. Additionally the traditional routing protocol (EAAK) shows improvements on the performance of network as given in blue line. In further the purple line shows the optimal performance for packet delivery ratio. According to the obtained results the performance of the proposed routing protocol performs more effectively as compared to the traditional approach. Additionally improves the performance as compared to the traditional technique during attack conditions. Thus the proposed technique found most optimal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 11, November - 2017

performance of the secure routing protocol. Basically the performance of the network in terms of packet delivery ratio shows the effective performance of network.

D Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.

Received data = (bytes/ time)* 8/1000000

througput_in_mbps=bytes_recv_per_unit_of_time* 8/1000000

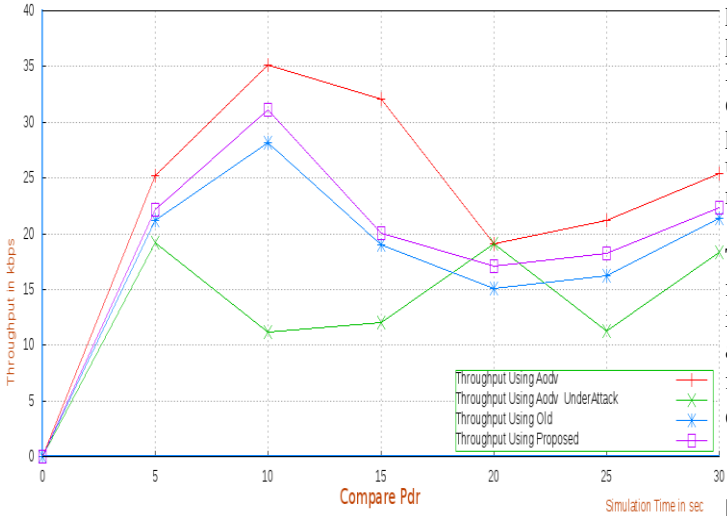

Fig. 7. Throughput

The throughput of the network is given using figure 7, in this diagram the X axis contains the number of nodes in network and the Y axis shows the throughput consumption of the network. The higher throughput consumption shows the effective and efficient network. The red line of the network shows the performance of network during normal scenario and the green line shows the under attack network bandwidth consumption. According to the obtained performance the blue line shows improving performance of the network during the attack conditions and the purple line shows the improved performance of network under the attack conditions. Additionally the bandwidth consumption of the system is much efficient than the older secure routing protocol. Thus proposed routing protocol is more adoptable than the traditional routing performance.

V. CONCLUSION AND FUTURE WORK

The wireless ad hoc network is one of the most demanding network technologies. Therefore a number of different applications are getting advantages of their properties. The mobile ad hoc network is a wireless technology and the topology development is dynamic. Due to this dynamic topology the responsibility of routing protocols are increases in this network. Additionally the security issues are also deployed by attackers using the routing technology. In this presented work the routing based attack deployment is investigated. More specifically the wormhole attack is evaluated. During the study that is observed the wormhole attack is deployed through the more than one attacker. In this attack two attackers are join the network with fully connected high speed network. Due to this most of traffic in network is attracted by this high speed link and causes the network performance loss or congestions.

In order to find the appropriate technique which not only provide security in network that also improves the efficiency of network during the wormhole attacks. Therefore a cryptographic solution achieved by secure key exchange mechanism is observed and modified for enhancing the performance of network and securing the network. The proposed cryptographic solution utilizes the DIFFIE HELLMAN (DH) key exchange technique for secure key exchange. That prevents the intermediate nodes to alter the packet information. Additionally the watch dog technique is used to detect and prevent the attacker's effect in network routing.

The proposed wormhole detection and prevention technique for improving network performance and security is implemented successfully. That is adoptable for both security and performance also, in near future that technique is tested for more than one kinds of attacker and also that technique is extended for improving the geographical networks.

REFERENCES

[1] Athira V Panicker, Jisha G," Network Layer Attacks and Protection in MANET A Survey" Athira V Panicker et al, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3437-3443

[2] Subhashis Banerjee and KoushikMajumder, "Wormhole Attack Mitigation in MANET: a Cluster Based Avoidance Technique", International Journal of Computer Networks & Communications (IJCNC) Vol.6, No.1, January 2014

[3] Ali Hassan, Syed Ahsan, SalehAlshomrani, Adel Alshamrani, "Packet Travel Time based Mechanism for Detection andMitigation against Wormhole Attack in AODV for MANETs", Life Science Journal 2014;11(10s)

[4] Muhammad Imran, FarrukhAslam Khan, Tauseef Jamal, Muhammad HanifDurad, "Analysis of Detection Features for Wormhole Attacks in MANETs", International Workshop on Cyber Security and Digital Investigation (CSDI 2015)

[5] Amit Kumar,Sayar Singh Shekhawat, "A Parameter Estimation Based Model for Worm Hole Preventive Route Optimization", IJCSMC, Vol. 4, Issue 8, August 2015, pg.80 – 85

[6] Soo-Young Shin, Eddy Hartono Halim, "Wormhole Attacks Detection in MANETs using Routes Redundancy and Time-based Hop Calculation" ICTC 2012 978-1-4673-4828-7/12/$31.00 ©2012 IEEE

[7] Zubair Ahmed Khan, M. Hasan Islam "Wormhole Attack: A new detection technique" 978-1-4673-4451-7/12/$31.00 ©2012 IEEE.

[8] Umesh kumar chaurasia, Mrs. Varsha singh "MAODV:Modified Wormhole Detection AODV Protocol" 978-1-4799-0192-0/13/$31.00 ©2013 IEEE.