IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Performance Calculation of Adhoc Network under the Impact of Wormhole Attack and Its Prevention Mechanism

Niharika Shrivastava[1], Prof. Tilotma Sharma[2]

M. Tech Student, Department of CSE&IT, Mahakal Institute of Technology, Ujjain[1]

Reader, Department of CSE& IT, Mahakal Institute of Technology, Ujjain[2]

Abstract: Mobile ad hoc network is a new generation communication technology. Now in these days that is adoptable in different manner of small and large range communication. Due to their ad nature of network organization and topology formation the network suffers from various security issues and performance issues. Thus the proposed work is investigation of the security issues ad hoc network. This developed methodology is to identify Worm-hole node. The technique works with slightly modified AODV protocol give the method of preventing WORMHOLE attack by using IDS algorithm. This propose a solution that will increase the basic AODV routing protocol, which will be capable to avoid Wormholes. To reduce the probability of Wormhole, it is proposed IDS based methodology for prevent Wormhole and find safe route to reach the neighbour nodes. A wireless IDS monitor's wireless network traffic and analyzes its wireless networking Protocol to identify suspicious activity.

Keywords: Calculation of Adhoc Network, Wormhole Attack, IDS Algorithm.

1. INTRODUCTION

Mobile Ad-hoc network (MANET) that is a self-configuring network of mobile nodes connected by wireless links is considered as network without infrastructure. Routing protocols will plays a crucial role for effective communication between mobile nodes and operates on the basic assumption that nodes are fully cooperative. There are many routing attacks caused due to lack of security. The routing attack that will be addressed is the worm hole attack. In Worm hole attack a malicious node will advertises itself as it is having the shortest path to the destination. In MANETs, the nodes are free to move randomly and organize themselves randomly.

In MANET, network's wireless topology may change rapidly and unpredictably. MANETs are usually setup in the situations of emergency for temporary operations. These types of networks operate in the absence of any fixed infrastructure, which makes them easy to setup [1].The ability of self-configuration of these nodes makes them more suitable for urgently required network connection.

Extensive research work in this area is progress with major studies on the different routing protocols such as Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and GRP. In An ad-hoc network, Networks are organizing on-the-fly, devices can permit to leave and join the network during its lifetime. Wireless devices communicate directly with the devices inside their radio range in a peer-to-peer network topology. If they wish to communicate with a device which is outside of their range, Ad-hoc network can use a midway device or intermediate devices within their radio range to forward communications. Ad-hoc On- Demand distance vector (AODV) is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. AODV is an on-demand routing protocol that discovers a route only when there is a demand of data transfer exist for mobile nodes.

In AODV routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired target mobile node. If a mobile node discover a fresh enough route, it unicast an RREP (Route Reply) message back along the saved path to the source mobile node or it otherwise re-broadcasts the RREQ message in Ad-Hoc network[2].

A malicious node in the network receiving an RREQ message replies to source nodes by sending a false RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that has actual path to forward data, a malicious node starts to lose all the network traffic it receives from source nodes. Some active attacks that can be easily performed against MANETs are worm hole attack [3].

2. RELATED STUDY

Route Determination Mechanism: NishantSitapara, Prof. Sandeep B. Vanjale [4]: proposed a solution where

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

Worm hole node is detected (assume) and tried to eliminate its effects. Solution tries to eliminate the Worm hole effect at the route determination mechanism of the AODV protocol that is carried out before the nodes begin the packets**.** Furthermore, author used UDP Connection to be able to count the packets at Sending nodes and receiving nodes**.** If we will use the TCP connection between mobile nodes, the Sending node would be the end of the Connection, so ACK packets do not arrive at the sending node. This would be another solution for finding the Worm hole node. This takes place after the route determination mechanism of the ADOV protocol and finds the route in a much longer period. Author solution finds the path in the AODV level.

Verify The Authenticity of The Route: Deng et al. [5] proposed a solution for the Wormhole attack problem in AODV routing protocol. They allowed the intermediate node to send a reply message if it had a fresh enough route to the destination. But the intermediate node could be a malicious node and could send route reply even if it had no fresh enough route to the destination to make a Worm hole attack.

They proposed a solution that the source node would send another route request to the next hop of the intermediate node to verify the authenticity of the route from the intermediate node to the destination node. If the route exists, the intermediate node is trusted; otherwise, the reply message from the intermediate node is discarded.

Adaptive Path-based Technique: Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU [6] proposed a adaptive approach to detect Worm and gray-hole attacks in ad hoc network based on a cross layer design network. In OSI network layer, a path-based technique to monitor the next hop's action.

This method does not throw out extra control packets and saves the network system resources of the detecting mobile node. In network, The Media Access Control Layer a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. They decide to choose DSR protocol to test proposed algorithm and ns-2 as simulation tool.

Issuing Security Certificate Approach: K. Selvavinayaki K. K. Shyam Shankar Dr.E. Karthikeyan [10] proposed solution that the nodes authenticate each other by issuing security certificate in digital form to all the other nodes in the network. The proposed technique is to be modified on DSR protocol and needs to be simulated and analysed for different performance parameters .This method is capable of detecting and removing Worm hole nodes in the MANET.

Using Reliability (fidelity) Table: Latha Tamilselvan, Dr. V Sankaranarayanan [7] proposed a solution with the enhancement of the AODV protocol which avoids multiple Worm holes in group. A method is specified to recognize multiple Worm holes cooperating with each other and discover the safe route by avoiding the WORM HOLE attacks. It was supposed in the solution that mobile nodes are already authenticated and therefore can participate in the mobile network communication. It uses reliability (fidelity) table, where each and every node is participating, is given fidelity level that will give reliability to that node. If any node in the network having '0' value is measured is considered as a malicious node and is discarded. A legitimate valid route is selected between the received RREP based on the threshold value. After getting the acknowledgement the fidelity level of the node is updated proving it safe and reliable.

Comparing Destination Sequence Number: Pooja Jaiswal proposed a method "Sequence Number" [8] that can be used to find the secure routes and prevent the Worm hole nodes in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP packet or is not.

Generally the primary or first route reply (RREP) will be from the malicious node if it contained high destination sequence number, which is saved in Route Request Table (RRT) at the first entry place. Then compare the first destination sequence number with the source node sequence number, if here exists much more difference between them, definitely that mobile node is the malicious node, instantly eliminate that entry from the RRT.

Reliable Nodes Approach: Khamayseh, Mardini, and BaniYasein, proposed "Reliable Route" [9] a new protocol is built on top of the original AODV It extends the AODV to include the following functionalities: source node waits for a reliable route; each node has a table in which it adds the addresses of the reliable nodes; RREP is overloaded with an extra field to indicate the reliability of the replying node. The simulation of the proposed protocol shows significant improvement in the terms of: packet delivery ratio, number of dropped packets, and end to- end delay. The conditions of passing the behavioural analysis filter are not satisfied enough to judge the reliability of the node. Disadvantage of this method i.e. the protocol does not consider the behaviour of two Worm hole nodes working together as a team.

Route Confirmation Approach (RCA): [10] the authors establish the route confirmation request (CREQ) and route confirmation reply (CREP) technique to avoid the Worm hole attack in the ad-hoc network.

In this method, the intermediate node not only sends RREP messages to the source node but also sends CREQ messages to its next-hop node toward the destination node. This is to enquire about the route to the destination node. After receiving a CREQ message, the next-hop node

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

searches its cache for a route to the target node. If it has the route, it transmits the CREP to the starting mobile node. On receiving the CREP message, the source node confirms the validity of the route by comparing the route in RREP message and also in CREP. If individually values of both are the same, the starting node verifies that the route is correct .Disadvantage of this method i.e. this approach cannot avoid the Worm-hole attack in which two consecutive nodes work in agreement with each.

3. PROPOSED METHODOLOGY FOR PREVENTION OF WORMHOLE ATTACK

Mobile Ad-hoc Network consists of some nodes that are standing randomly in operational environment without any predefined infrastructure and mobility which are vulnerable for intrusion and attack. Security is an important field in this type of network. Use IDS (intrusion detection system) based approach to detect and prevent Wormhole. IDS detect and report the malicious activity in ad hoc network. Intrusion detection systems (IDSs) do just that: monitor audit data, look for intrusions to the system, and initiate a proper response. The proposed algorithm is based on the trust values of individual nodes. All the nodes of wireless ad-hoc network have a specific trust value. The algorithm encompasses the following steps:

[A] Initialization:
1. Trust values of all the participating nodes are set to be initialized by specific previously assigned trust value.
2. Initialize the trust value of every node with 100.
3. Assumption: one trust value = 10 packets dropped**.**

[B.] **Upating of trust value:**
1. If the packets are correctly transmitted from one node to another node:

(a)If the correctly transmitted no of packets is between 1 and 10, then trust values of the respective nodes will be incremented by one time.
Update trust value=old trust value+1
(b) If the correctly transmitted no. of packets is greater than 10 ,then the updated trust valuie will be
Update trust value=old trust value+(correctly transmitted/10)

2. If the packets are dropped/delayed :
(a.,) The number of dropped or delayed packets is between 1 and 10,and then trust value of that particular node is decremented by one.
Updated trust value = old trust value – 1;
(b.)The number of dropped or delayed packets are greater than 10, then trust value of that particular node will be,
Updated trust value = old trust value – (Packet dropped or delayed / 10);

3.**If the trust value of particular node is negative, then print "Invalid node".**
[c] Isolating the Packet drop node from the network:
1.If (Updated trust value < Threshold trust value)Then the particular node is treated as malicious node (Worm hole node)
2. If (Updated trust value > Threshold trust value. Then the particular node is treated as legitimate node.
Stop comparing the trust value of nodes with threshold.

WORKING OF TAODV PROTOCOL
This work proposes a solution based on trust detection to detect attacks on AODV. This approach specifying the correct AODV routing behaviour and distributed in the network. Trust Mechanism monitors network for detecting run-time violation of the specifications. Aim of Trust Mechanism is to secure the AODV protocol. Dynamic topologies make it difficult to obtain a global view of the network. Traffic monitoring in wired networks is usually performed at switches, routers and gateways, but an Ad Hoc network does not have these types of network elements so here Trust Mechanism can collect audit data for the entire network.

Trust Value is defined as a sequence of related actions performed by a malicious adversary that results in the compromise of a target network. The existence of a security policy that states which actions are considered malicious should be prevented is a key requisite for an intrusion detection system to work. Trust detection is the process of identifying and responding to malicious activities target at computing and network resources.

Fig.1 Shows the TAODV PROTOCOL FLOW CHART algorithm. At the initial point assign a fix threshold value (assumed) to the Ad-hoc network and start Route discovery process by following STEP-I where source node wait for route reply. If Route is establish so then call TRUST DETECTION step and check the Sequence number of Reply node, if sequence number lie within the threshold value, node is trustworthy and send data packet to the destination ELSE If sequence number is greater than assigned value, detect the Node as a malicious node and now call Trust Value for informing neighbours node about the malicious node.

Source send ICMP packet along the route path for deleting malicious node entry from routing table and then again initialize route discovery process in the Network. Now going to the else part of step-I, If route reply is not come then call STEP-II LREPAIR (local repair). If route is repair with in time to leave period, Route is established and calls STEP-III Trust Detect otherwise node increment sequence number and again start Route discovery. To follow this algorithm TAODV protocol detect malicious node and prevent the network from Worm-hole attack.

For performance analysis following it is important to setup simulation environment to observer protocols behaviour over MANET. Quantitative analysis is conducted to with the help of NS-2 tool. The performance graph are shown in fig

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

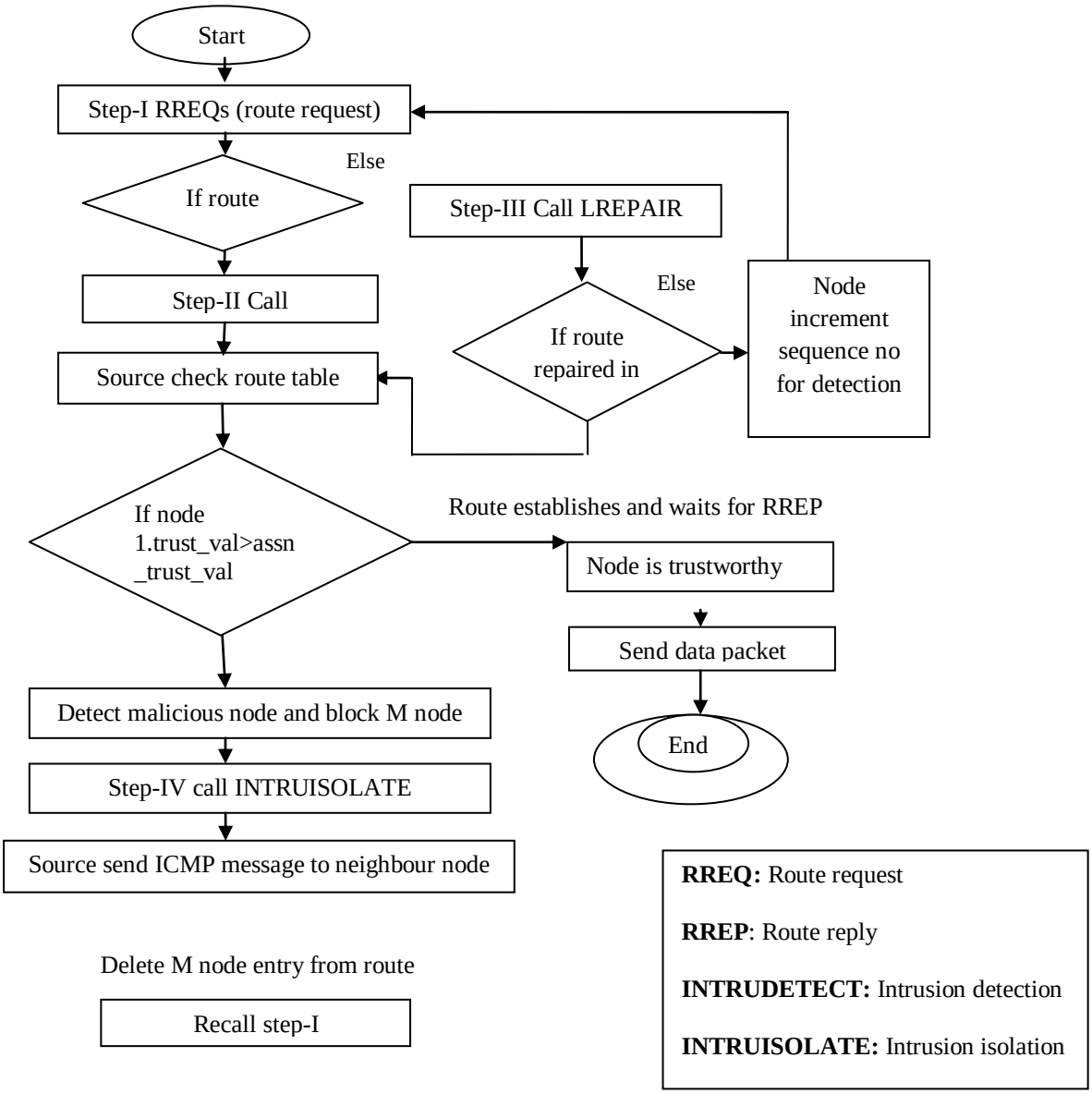

FIG.1

4. SIMULATION SETUP

Simulation tool	Network simulator-2.35
IEEE scenario	MANET(802.11)
Mobility model	Two ray ground
Number of nodes	20,40,60
Node movement speed	10m/sec,28m/sec.
Traffic type	UDP
Antenna	Omni direction antenna
MAC Layer	IEEE 802.11
Routing Protocol	AODV,WAODV,TAODV
Queue limit	50 packet
Simulation area(in meter)	1000*1000
Queue type	Drop-tail
Channel	Wireless channel

DOI 10.17148/IJARCCE.2016.51027

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

5. SIMULATION RESULTS

1. PACKET DELIVERY RATIO-This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Packet delivery ratio under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density**.**

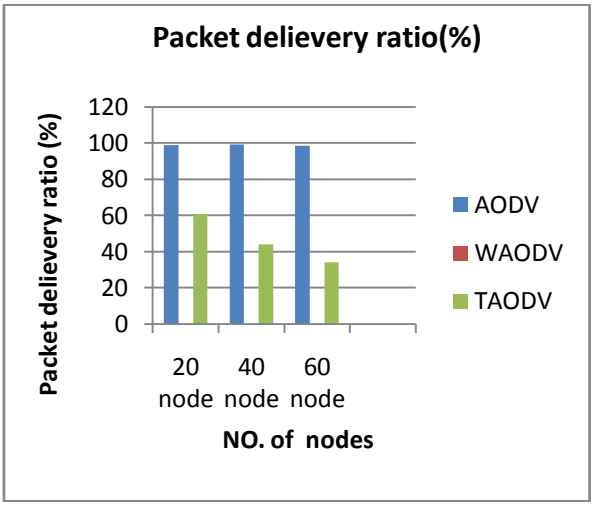

Fig.2

2. **THROUGHPUT**-This is the fraction of the data packets received by the destination to those sent by the source. This classifies the ability of the protocol to discover routes. Figure and table shows the Throughput under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density.

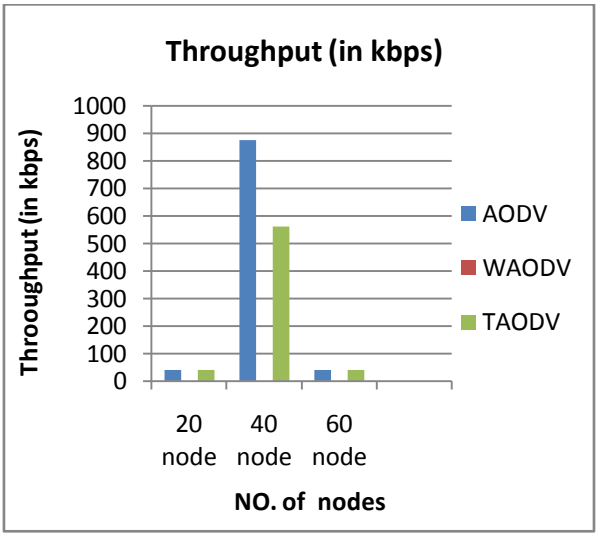

Fig.3

3. END TO END DELAY -This is the average delay between the sending of the data packet by the source and its receipt at the corresponding receiver. This includes all the delays caused during route acquisition, buffering and processing at intermediate nodes. Figure and table shows the End to End Delay under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density.

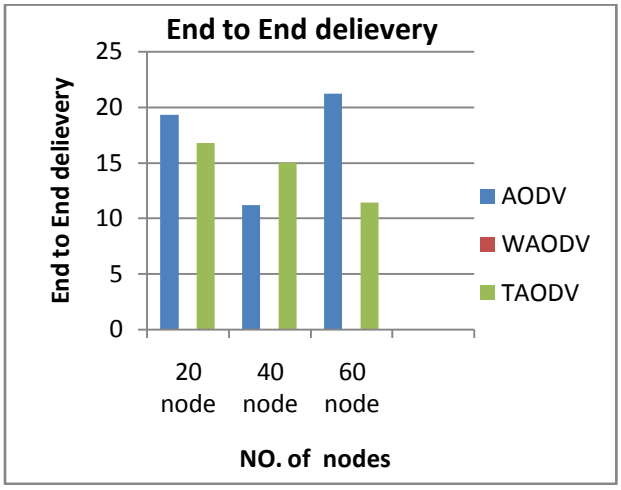

Fig.4

4. RESIDUAL ENERGY

It is the total amount of remaining energy by the nodes after the completion of Communication or simulation. If a node is having 100% energy initially and having 70% energy after the simulation than the energy consumption by that node is 30%.The unit of it will be in Joules. Figure and table shows the Residual Energy under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density.

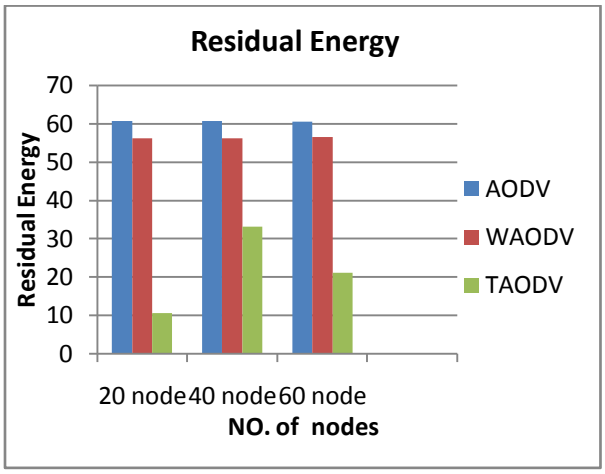

Fig .5

5. ROUTING OVERHEAD -This is the ratio of overhead bytes to the delivered data bytes. The transmission at each hop along the route is counted as one transmission in the calculation of this metric. The routing overhead of a simulation run is calculated as the number of routing bytes generated by the routing agent of all the nodes in the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

simulation run. This metric has a high value in secure protocols due to the hash value or signature stored in the packet. Figure and table shows the Routing Overhead under Worm hole attack detection and its prevention through Trust based mechanism i.e. AODV, WAODV and TAODV for the various node density.

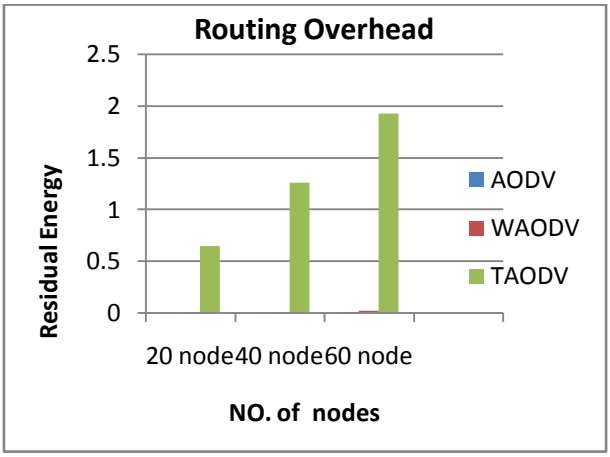

Fig .6

This section describes a detailed functioning of proposed work for Trust based AODV (TAODV). The Results of the work showed performance of network through different parameters during attack and its avoidance. Each Result is clearly pictured and defined with its applicability. Any inexperienced user can also understand.

In according to parameter, each result are represent in graphical form and statistical form. Here, in each, results are compared to existence AODV, AODV under Worm-hole and trusted AODV that is modified of AODV and NS-2 provides users with the simplest way of specifying network protocols and simulating their corresponding behaviours and Result of the simulation is provided within a trace file that contains all occurred events.NS-2 provides extremely modular Platform for wired and wireless simulations supporting totally different network component, protocol (e.g., routing algorithms, TCPUDP, and FTP), traffic, and routing types and follow the application to use it.

6. CONCLUSION

MANET has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. Security of MANET is one of the important features for its deployment, the detection and prevention of worm hole attack in the network exists as a challenging task. In this work analyzed the effect of worm hole attack in the performance of AODV protocol and prevent the network from worm hole attack using TAODV protocol. The simulation has been done using the network simulator (NS-2.35). The performance metrics like packet delivery ratio, throughput and average end to end delay has been measured and analyzed with the variable node density. From the simulation results it is clear that when the worm hole node exists in the network, it can be affected and increases the performance of AODV routing protocol.

Here, we addressed the problem of identifying misbehaving nodes that refuse to forward packets in wireless ad hoc network and give the mechanism to prevent them. The impact of such nodes decreases network performance, lowering the network throughput and increasing the end-to-end delay.

To mitigate the problem of malicious packet dropping, this work proposed a feasible solution for it on the top of AODV protocol to avoid the worm hole attack, and also prevented the network form further malicious behaviour .Proposed method can be used to find the secured routes and prevent the worm hole nodes in the MANET .Our solution presents good performance in terms of packet ratio and throughput.

In this work, we simulated AODV protocol with different density, where each one has 10 nodes, 20 nodes, 40 nodes, 60 nodes and also simulated the same scenarios after introducing single Worm Hole Node into the network. Moreover, we simulated Secure AODV as per algorithm for detection of worm hole attack.
Finally compare the results of solution with High AODV under attack by varying different network parameters using same scenarios in NS-2.Our simulation results are analyzed below:

Analyzing the results of PDR v/s Node Density shows the Packet Delivery Ratio of High AODV, AODV under worm hole attack, Average TAODV under worm hole attack; WAODV is poor in PDR found that there in PDR for Secure AODV. This clearly shows that there AODV is High a significant benefit when the solution against Worm hole attacks is applied.

Analyzing the results of Throughput v/s Node Density shows the Throughput of High AODV, AODV under worm hole attack, Average TAODV under worm hole attack, WAODV is poor under worm hole attack, where worm holes were fixed but number of nodes varied, there was significant rise of 60%-80% in Secure AODV against High AODV under Worm-Hole Attack, which indicates solution work better even though number of nodes increases.

Analyzing the results of End-to-End Delay v/s Node Density shows the End-to-End Delay of High AODV, AODV under worm hole attack, Moderate TAODV under worm hole attack; we found that there is a 60-80% increase in End-to-End Delay for Secure AODV compared to poor WAODV. From the above cases, we can conclude that Secure AODV give significant improvement in End-to-End Delay compared to that of High AODV during worm hole attack.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 10, October 2016

7. COMPARISON TABLE OF PROTOCOLS

Protocol → / Parameter ↓	AODV	WAODV	TAODV
Packet delivery ratio	**High**	Low	Modearet(compared to waodv)
End to end delay	**High**	Low	moderate
Residual energy	**High**	Moderate	Moderate
Routing overhead	**High**	**high**	moderate
Throughput	**High**	Low	Moderate

As described in our table all the performance matrices have been evaluated which reflect that the main quality parameter that are packet delivery ratio and throughput of TAODV protocol is higher when it is compared with WAODV. And vice versa the two negative properties of any network i.e end to end delay and routing overhead are also modified when compared to WAODV protocol.

As future work, research work intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead mobility, increasing number of malicious node, increasing number of nodes and also focusing on resolving the problem of multiple attacks against AODV.

REFERENCES

[1] D. Boneh and M.K. Franklin. Identity-Based Encryption from the Weil Pairing. In Advances in Cryptology CRYPTO, 2010.
[2] J-Y. L. Boudec and M. Vojnovi´c. Perfect Simulation and Stationary of a Class of Moblity Models. In IEEE INFOCOM, 2009.
[3] J.B. Broch, D.A. Maltz, D.B. Johnson, Y-C. Hu, and J.G. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In ACM MobiCom , October 2008.
[4] T. Camp, J. Boleng, and V. Davies. A survey of mobility models for ad hoc network research. Wireless Communication and Mobile Computing (WCMC): Special issue on Mobile Ad Hoc Networking:Research, Trends, and Applications, 2(5):483-502, 2008.
[5] S. ˇCapkun and J.P. Hubaux. Protect Positioning in Wireless Networks. IEEE Journal on Selected Areas in Communications, 24(2):221–232, Fe bruary 2006.
[6] H Choi, S. Zhu, and T.F La Porta. SET: Detecting node clones in Sensor Networks. In IEEE/CreateNet Conference on Security and Privacy for Emerging Areas in Communication Networks (ProtectComm), 2007.
[7] C. Adjih, A. Laouiti, P. Minet, et. al., Optimized link state routing protocol. Work in Progress, IETF draft, MANET Working Group, INRIA Rocquencourt, France, 2003.
[8] C. Perkins and E. Royer. Ad-hoc on-demand distance vector routing. In Workshop on Mobile Computing and Systems Applications, 1999.
[9] D. Johnson and D. Maltz, Dynamic source routing in ad hoc wireless networks. In Mobile computing, T. Imielinski and H. Korth, Eds. Kluwer Academic Publishers, 1996: Ch. 5, p. 153-181.
[10] Shilpa jaiswal , sumeet agrawal , A novel paradigam : detection and prevention of wormhole attack in mobile adhoc network, International journal of engineering trends and technology,vol3 Issue 5,2012
[11] Jyoti thalor, ms.Monika, detection and prevention technique in mobile adhoc network: review, International journal of advanced research in computer science and software engineering, vol 3 Issue 2, february 2013
[12] Vandana c p, Dr. A. francis savior devaraj ,A multilayered detection mechanism for wormhole attack in AODV based MANET ,International journal of security and trust management vol 2 NO.3 , june 2012
[13] K.sivakumar, Dr. g. selvaraj, Analysis of wormhole attack in MANET and avoidance using robust secure routing method, International journal of advanced research in computer science and software engineering vol 3 issue 1, January 2013
[14] Maria Sebastian , Arun raj kumar, A novel solution for discriminating wormhole attack in MANET from congested traffic using RTT and transitory buffer , International journal of computer network and information securityy , 8, 28-38 , aug 2013
[15] Umesh kumar chaurasia, Mrs. varsha singh, MOified wormhole detection AODV protocol
[16] Nishant Sharma, Upinderpal singh, Vrious approaches to detect wormhole attack in wireless sensor networks, international journal of computer science and mobile computing vol 3 issue 2 february 2014