IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

Wormhole Attack Detection and Prevention Based on Threshold Function using SEAODV

Deepali Jamodkar[1], Prof. Kapil Vyas[2], Prof. Deepa Vyas[3]

M.Tech Scholar, Computer Science, BMCT, Indore, India[1]

Assistant Professor, Computer Science, BMCT, Indore, India[2, 3]

Abstract: To manage the ADHOC network is great challenge because it has dynamic infrastructure and mobility of node. Due to mobility of node routing path of network and security of communication suffered. In the process of node mobility and path discovery of routing protocol take huge amount of power and decrease the life of network. For the enhancement of power and protected communication various protocol are designed. A security constraint in mobile adhoc network is very critical task. Some critical security issue such as black hole attack, wormhole attack, sinkhole attack, prevention and detection of attack is major challenge. For the detection of wormhole attack various authors used various techniques such as clock synchronization, nearest neighbour node selection method. In this dissertation modified the AODV routing protocol for the detection of wormhole attack is used. The modified protocol is called secured energy efficient routing protocol (SEE-AODV). The SEEAODV protocol based on two functions one is threshold based function and one is energy based function. The threshold based function measure the distance of normal node and wormhole node and the energy based function is used to measure power consumption in the form of energy. Our proposed algorithm is very efficient as compare to ADOV routing protocol. For the assessment of performance our modified protocol tested in various network situation and tested with different simulations for different distributions of nodes. During this evaluated scenarios, this technique demonstrates excellent detection probabilities with few false alarms that depend on the value of threshold. Our proposed modified scheme "SEAODV" simulate in NS-2 simulator. In simulation process we used 10, 20, 30, 40 and 50 nodes. The evaluation of performance is measured by packet delivery ratio, Average end to end delay, packet throughputs and Energy Consumption. Our modified scheme is compared with existing AODV and good results in compare with old method.

Keywords: MANET, ADHOC Network, AODV, SEAODV, Wormhole Attack**,** Threshold.

I. INTRODUCTION

Mobile Ad Hoc Network (MANET) is network of mobile nodes where mobile nodes communicate with each other through wireless links and there is no fixed infrastructure and no centralized control. Each mobile node in such a situation acts as both a router and host. Security is an important concern in the MANET environment because of its active topology and limited range of each mobile host's wireless transmissions [1]. It dates back to the seventies, the U.S. Defence Research Agency, DARPA worked off PRNET and SURAN projects. They supported automatic route set up and preservation in a packet radio network with moderate movement. Interest in such networks has recently grown due to the common convenience of wireless communication devices that can connect laptops and palmtops and operate in license unrestricted radio frequency bands (for example the Industrial-Scientific-Military or ISM band in the U.S.). In an interest to run internetworking protocols on ad hoc networks, a new working group for Mobile, Ad hoc Networking (MANET) has been formed within the Internet Engineering Task Force (IETF), whose charter includes developing a framework for running IP based protocols in ad-hoc networks. Interest has also been partly fueled through the recent IEEE standard 802.11 that include the MAC and physical layer specifications for wireless LANs without any fixed infrastructure. Routing protocols in packet-switched networks traditionally use either link-state or distance-vector routing algorithm. Both algorithms allow a host to find the next hop neighbor to reach the target via the "shortest path." The shortest path is usually in terms of the no. of hops; however, other suitable cost procedures for example link utilization or queuing delay can also be used. Such shortest path protocols have been successfully used in many active packet switched networks. Prominent examples include uses link state protocol in OSPF (Open Shortest Path First) [2] and use of distance vector protocol in RIP (Routing Information Protocol) for interior routing in the Internet. Even though, any such protocol would, in principle, working with ad hoc networks, a no. of protocols has been exactly developed for use with ad hoc networks. The primary motivation is the shortest path protocols, any link state or distance vector, take too long to converge and have a high message convolution. On account of the limited bandwidth of wireless links, message convolution must be kept low. Also, possibly quickly changing topology makes it important to find routes quickly, even if the route may be sub optimal. Numerous new ad hoc routing protocols have been developed with this basic philosophy. They, however, vary widely in characteristics. For example, few of these protocols are variations of distance vector routing. Some protocols explicitly keep redundant routing paths so that

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

replacements are available when a route changes. Some recently proposed protocols use a reactive method for route discovery and preservation, instead of the more traditional, proactive method [3].

Figure 1: ADHOC network

II. AODV PROTOCOL

Ad hoc On-Demand Distance Vector, AODV, is a distance vector routing protocol that is reactive. The reactive property of the routing indicates that it has only a requested route when it needs one and does not require that the mobile nodes keeps routes to ends that are not communicating [3,5]. The AODV protocol is one of the reactive routing protocols for mobile ad-hoc networks which is established through the IETF Mobile Ad-hoc Networks (MANET) working group. In AODV, every node keeps a local routing table that holds the information of neighbors and forward a data packet so that it reaches eventually the chosen end. It is required to use routes which have minimal length according to hop-count as a distance metric [2,8]. However, AODV provides the functionality like DSR, namely to transport data packets from one node to alternative through discovery of routes and taking advantage of multiple hop communication. AODV is based on UDP as an unordered transportation protocol to send packets within the ad-hoc network. Moreover, it requires that every node can be addressed through network wide-ranging single IP address and delivered packets appropriately through placing its IP address into the sender field of the IP wallets. This means AODV is expected to run within open network, where security is a minor concern. It must be declared that some attempts to spread AODV to prevent malicious nodes from attacking the integrity of network through digital signatures for Safe routing control packets [10]. AODV requires each node keeps a routing table that contain one route entry for each target for node is communicating with.

The route entry keeps certain fields. Around of these fields are the following:

- **Target IP Address**: The IP address of the target for which a route is established
- **Target Sequence No.**: The target sequence no. associated to the route.
- **Next Hop**: It is the target itself or an intermediary node designated to forward packets to the target
- **Hop Count**: The no. of hops from the Initiator IP Address to the Target IP Address.
- **Lifetime**: The time in milliseconds for nodes on which nodes getting the RREP for the identification of route.
- **Routing Flags**: The state of the route; up (valid), down (not valid) or in repair.

In AODV, communication step classified into three procedures, which are discovering, creating and keeping routing paths. For run the algorithm, AODV uses 3 types of control messages. They are Route-Request (RREQ), Route-Reply (RREP) and Route-Error (RERR) messages. When source nodes want to establish communication with target nodes, it will dispute Route Discovery procedure. Source node announcement Route Request announcement packets (RREQ) for its all available neighbors. The intermediary node that receive request will check the request if intermediary node is target, will replay with route-replay message. If not target, request from source will forwarding to further neighbor nodes. Previously progressing the packet, each node will store the announcement identifier and the previous node quantity from which the demand came. Timer used through intermediary nodes to delete the entry when no replay is received for the request. If there is replay, intermediary nodes keep again the announcement identifier and the previous nodes from which replay came.

The basic message set consists of:

- RREQ – Route request
- RREP – Route reply
- RERR – Route error
- HELLO – For link status monitoring

III. PROBLEM STATEMENT

The wormhole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the wormhole attack in MANET a technique has been proposed. In the reactive routing protocols such as AODV, the attackers can tunnel each route request packets to another attacker that is near to destination node. When the neighbours of the destination hear this RREQ, they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process. This type of attack prevents other routes instead of the wormhole from being discovered, and thus creates a permanent Denial-of-Service attack by dropping all the data, or selectively discarding or modifying certain packets as needed.

Wormhole attack is a relay-based attack that can disrupt the routing protocol [7, 8, 9] and therefore disrupt or breakdown a network and due to this reason this attack is serious. We can use 4 steps to explain about a general wormhole attack.

1. An attacker has two trusted nodes in two different locations of a network with a direct link between the two nodes.

DOI 10.17148/IJARCCE.2016.5659

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

2. The attacker records packets at one location of a network.
3. The attacker then tunnels the recorded packets to a different location.
4. The attacker re-transmits those packets back into the network location from step 1.

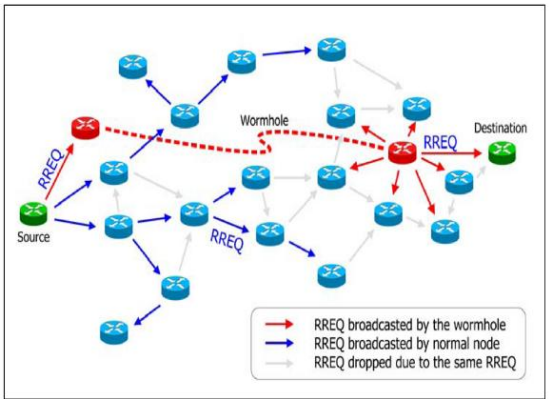

Figure-2: Wormhole attack.

IV. PROPOSED WORK & METHEDOLOGY

SEAODV is described this dissertation proposed a protected AODV routing protocol for the prevention and detection of wormhole.

A. Flowchart of Proposed System

The working of SEAODV is consists of Four modules:

- Local Information Setup
- Calculate Threshold Function
- Route Establishment Process
- Wormhole Detection & Prevention

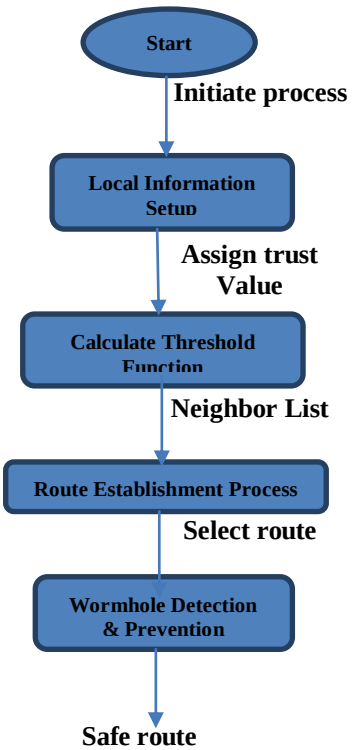

Figure- 4 Flowchart for Proposed System

B. Algorithm for Proposed Method

This proposed method consists of step through step procedure to impove the performance of AODV protocol in the term of SEAODV.

• Local information Setup

1. Generate TN (Total no. of nodes).
2. Select node S (Any random node as a Source).
3. Determine RS (Nodes in the range of S).
4. Set node T (Target node)
5. Set P(S,T) (Path with minimum path length)
6. Assign Trust value to all nodes (No. of hops)

• Calculate Threshold Function

7. Send Hello(Source node announcement a message to all neighbour for Local connectivity)
8. Neighbour node reply to source
9. Each node keep neighbour list
10. Source compare all neighbour list & select common node
11. Assign Tvalue for common nodes

• Route Establishment Process

12. Send RREQ (Source node send a Packet to all neighbour for Local connectivity).
13. Intermediary nodes forward RREQ packet until Target is not found.
14. Target node reply RREP packet to source RREP contains (no. of hops, target neighbour list).
15. For detection of wormhole goto step 18
16. Route established on receiving RREP
17. Source store target neighbour list

• Wormhole Detection & Prevention

18. Check the node location in threshold communication range.
19. Check target neighbour list, if node Tvalue < Threshold
20. Worm hole exist
21. Sent Alert message to all nodes
22. Any node has Wormhole _node_id in there routing table will remove it.
23. Restart the Process from step 12 for route establishment.

V. EXPERIMENTAL RESULT AND ANALYSIS

A. Simulation Parameter

Table-1 Simulation Parameter

Parameter	Value
Simulation duration	50,100.150, 200 sec
Simulation area	1000*1000
No. of mobile node	10,20,30,40,50
Circulation type	Cbr(udp),
Packet rate	4 packet/sec
Abnormal node	Variable
Host pause time	10sec

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

B. Performance Evolution Metrics:

To test and compare the performance of SEAODV against AODV we used NS-2.34 and developed set of tools via TCL script, Mobility files, and AWK programs to process the output trace files.The evolution of SEAODV protocol is measured according to the following metrics.We simulate our method in NS-2 with help of OTCL & TCL simulation script file, now evaluation of performance of these modified scheme we used standard parameter of adhoc network.

- Throughput
- Average end-to-end delay
- Packet Distribution ratio
- Energy Consumption

• Throughput

A network throughput is the average rate at which message is successfully transported between a target node and source node. It is also referred to as the proportion of the quantity of data received from its source to the time the last packet reaches its target. Throughput is measured in bits / sec (bps), packets / sec or packet / time slot.

Throughput =Amount of data received / Time

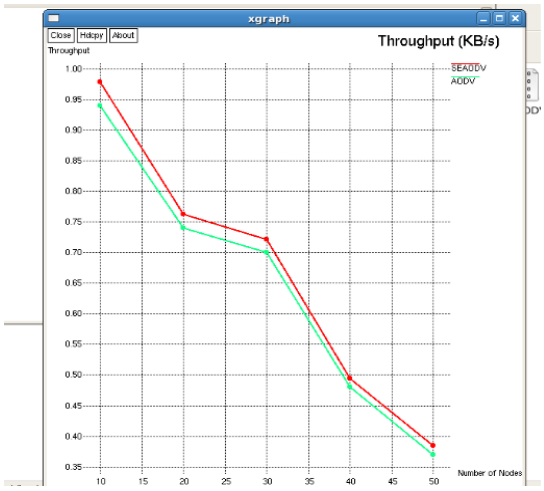

Figure-4: Throughput Vs Speed of Nodes

• Average end-to-end delay

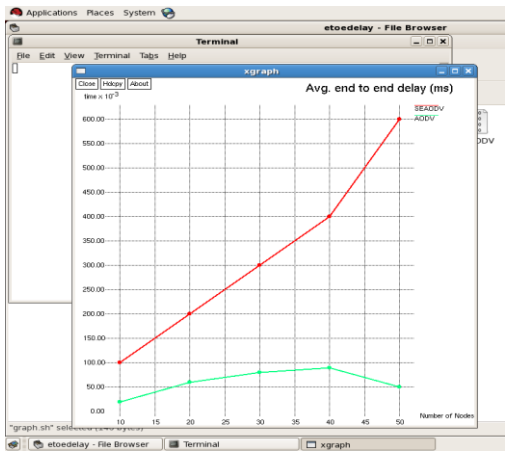

Figure-5 Average End to End Delay Vs Speed of nodes.

This is the average time involved in Distribution of data packets from the source node to the target node. In other word the average end to end delay of the route can be determined through discovery the total delay and dividing it through hop count.

EED =Total delay / hop count

• Packet Delivery Ratio

The packet delivery ratio can be determined as no. of packets received through receiver and no. of packet sent through source. This performance metric gives us an idea of how well the protocol is performs packet Distribution with different speeds using various circulation models.

PDR = Σ Total no. of packets received through receiver / Σ Total no. of packets sent through source

Figure-6 Packet Distribution fraction v/s no. of nodes speeds

• Energy Consumption

The Energy of route request is no of route request per second.

Energy of Route Request = No of Route Discoveries / Sec.

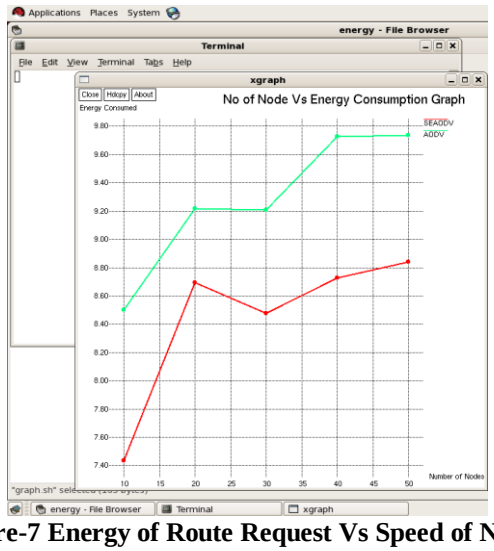

Figure-7 Energy of Route Request Vs Speed of Nodes

DOI 10.17148/IJARCCE.2016.5659

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 6, June 2016

5.3 Comparison of AODV and SEAODV Protocol

Table- 2 Comparison of AODV and SEAODV

Protocol	AODV					SEAODV				
No. of Nodes	10	20	30	40	50	10	20	30	40	50
TH	0.94	0.74	0.70	0.48	0.37	0.98	0.77	0.73	0.50	0.39
PDR	25.00	60.00	70.00	80.00	50.00	100.00	200.00	300.00	400.00	600.00
EED	0.94	0.74	0.70	0.47	0.37	0.98	0.77	0.73	0.50	0.39
EC	8.50	9.22	9.20	9.70	9.71	7.42	8.70	8.50	8.53	8.62

VI. CONCLUSION AND FUTURE WORK

In this dissertation modified the AODV routing protocol for the detection of wormhole attack. The modified protocol is called secured energy efficient routing protocol (SEAODV). The SEAODV protocol based on two functions one is threshold based function and one is energy based function. The threshold based function measure the distance of normal node and wormhole node. Our proposed algorithm is very efficient in compression in ADOV routing protocol. For the evaluation of performance our modified protocol tested in different network scenario tested through simulations for different distributions of nodes and wormholes and different connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent detection probabilities with few false alarms that depend on the value of threshold. The results of the proposed are batter then the previous approaches in order to detect the worm hole. This work has focused on detecting the wormhole not to remove that wormhole. Future work includes developing a technique for removal of the wormhole when it detected with the help of this proposed approach. The proposed method can also be implemented over other proactive or reactive routing protocols such as Dynamic Source Routing (DSR) and Destination Sequence Distance Vector (DSDV).

REFERENCES

[1] Maha Abdelhaq1, Raed Alsaqour1, Mohammed Al-Hubaishi2,3, Tariq Alahdal2, and Mueen Uddin4,5 (Corresponding Author: Maha Abdelhaq)" The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing" International Journal of Network Security, Vol.16, No.5, PP.376-381, Sept. 2014

[2] Aarfa Khan Prof. Shweta Shrivastava, Prof. Vineet Richariya, "Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA)" 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA.

[3] Jih-ching Chiu1, Chun-Yao Zheng, Yao-Chin Huang and Kai-Ming Yang, "Design and Implementation of Sequential Repair and Backup Routing Protocol for Wireless Mesh Network"

[5] Akshay Aggarwal, Savita Gandhi, Nirbhay Chaubey, Keyurbhai A Jani "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs", 2014 Fourth International Conference on Advanced Computing & Communication Technologies

[6] Neha Shirke, Kishor Patil, Shriram Kulkarni, Shriram Markande, "Energy Efficient Cluster based Routing Protocol for Distributed Cognitive radio network" 978-1-4799-3486-7/14/$31.00_c 2014 IEEE

[7] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011

[8] Satoshi Kurosawa and Hidehisa Nakayama" Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" in International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[9] S.Giordano, I.Stojmenovic et al.,"Position based Routing: Algorithms for Ad Hoc Networks: ATaxonomy"

[10] Jyh Sivalingam, K. Agrawal, and M. Srivastava. Design and analysis of low-power Access protocols for wireless and mobile atm networks. Wireless Networks, 2000.

[11] Tamer A. ElBatt, Srikanth V. Krishnamurthy, Dennis Connors, and Son K. Dao. Power management for throughput enhancement in wireless ad-hoc networks. In ICC (3), 2000.

[11] Jyoti Joshi, Vidhate Amarsinh, "Enhanced 2ACK Scheme to Prevent Routing Misbehavior Using OLSR Protocol." 2014 International Conference on Computer Communication and Informatics (ICCCI -2014), Jan. 03 – 05, 2014, Coimbatore, INDIA

[12] Mallapur Veerayya, Vishal Sharma And Abhay Karandikar "Sq-Aodv: A Novel Energy-Aware Stability-Based Routing Protocol for Enhanced Qos In Wireless Ad-Hoc Networks" IEEE 2012.

[13] Tamer A. ElBatt, Srikanth V. Krishnamurthy, Dennis Connors, and Son K. Dao. Power management for throughput enhancement in wireless ad-hoc networks. In ICC (3), 2000.