Remove the Worm-Hole Attack in Mobile ADHOC Network Using Threshold Based Technique

Poonam Bharitya
M Tech Scholar, Department of CSE
PCST, Bhopal. India
E-mail- poonambhartiya1989@gmail.com

Surendra Vishwakarma
AP, Department of CSE
PCST, Bhopal. India
E-mail- s.wish83@gmail.com

ABSTRACT
In this paper modified the AODV protocol with threshold trust value and increase the security strength of AODV routing protocol. We modified AODV scheme for worm-hole detection protocol in mobile ADHOC network. AODV scheme also provide facility for the detection of weak node and node in sleep mode in ADHOC network. Main ideas of Proposed, consisting of relative trust value. We will apply this idea to AODV as an underlying routing protocol, but it could be applied to some other identification-anonymous routing protocols in an appropriately designed similar way. As mentioned earlier, in Proposed the RREP messages are unified with RREQ messages in appearance since being initiated till a random number of hops from the destination.

Keywords: - MANET, AODV, Worm-Hole, Threshold

INTRODUCTION

The malicious software attack such as worm-hole attack and worm-hole attack degraded the performance of mobile adhoc network and also theft the information of user. The worm-hole attack denied the service of communication during the attacking mode. The detection and prevention of worm-hole attack is various critical tasks. Various authors used various techniques such as threshold based function and reference based model for the detection of worm-hole attack. In this dissertation improved the AODV routing protocol for the secured communication for the prevention of worm hole attack. The prevention of worm hole attack depends on the process of threshold based function. Initially threshold based function estimate the trust value for the request and replay process. The value of trust estimated by differential function. This differential function estimates the individual parameter selection value and reference value. For the detection process used reference selection process model. Threshold is an important part of the proposed technique. In the technique a worm-hole tunnel present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the worm-holeis detected. So accurate value of threshold is necessary for the technique. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the alternate route to its two hop neighbor that is called target node. The shortest path of minimum number of hop count of each and every alternate path is taken by the algorithm. After that the algorithm consider the highest number of hop count which is comes from these various alternate paths in the whole network and consider highest hop count + 2 as a threshold. The proposed protocol focuses on minimizing the routing overhead of the network. The worm of the link is determined by measuring received signal strength of RREQ packet using cross layer design and subtracting it from transmit power. A RREQ packet is only forwarded if the link has sufficient worm. So, the links with high worm i.e. weak links may not participate in formation of route. To decide whether the link has the sufficient worm or not, the worm of link is checked against a predetermined threshold. The threshold to be used can be a fixed value or it could be changing adaptively with changing network condition. Section II discusses about worm hole attack Section III proposed method. Section IV discusses simulation finally, concluded in section V.

II WORM HOLE ATTACK

The worm-hole attack is a serious threat for mobile ad-hoc network. And it cannot be detected easily. For detection of the worm-hole attack in MANET a technique has been proposed. In a worm-hole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network [17]. The worm-hole puts the attacker nodes in a very powerful position compared to other nodes in the network. 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 neighbors 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 worm-hole 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.

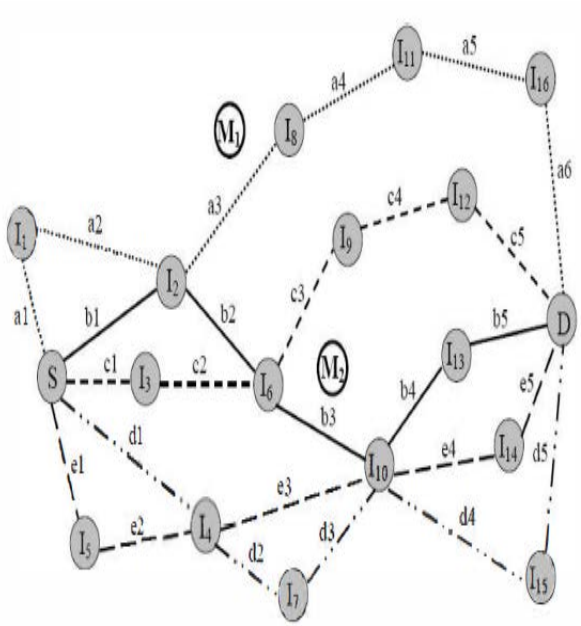

Figure 1: worm-hole Attack scenario M1 and M2 two worm node.

III PROPOSED METHODOLOGY

Threshold is an important part of the proposed technique. In the technique a worm-hole present in the network or not, is decided by the threshold. If the value of alternate path is greater than the threshold, the worm-hole is detected. So accurate value of threshold is necessary for the technique. For deciding the threshold considers a network with n number of nodes. In the network, each and every node finds the alternate route to its two hop neighbor that is called target node. The shortest path of minimum number of hop count of each and every alternate path is taken by the algorithm. After that the algorithm consider the highest number of hop count which is comes from these various alternate paths in the whole network and consider highest hop count + 2 as a threshold.

Assumptions

1. Total number of node in desire network is TN.
2. S_i represent any node among TN, where i = 1,2,3,…….,< TN.
3. $(RS_i)_j$ represent the node that's come in the range of S_i.
4. $((RS_i)_j)_k$ represent the node that's come in the range of $(RS_i)_j$ and assume as a target node T_{jk} for S_i.
5. P_{ST} represent path between S and T.
6. NS_i represent the neighbor node of S_i.
7. $(l_{NSi,Tjk})$ represent number of node in the path $P_{NSi,Tjk}$.

Algorithm

Step 1

If (i<= TN)
Goto step 2
Else
Threshold (T) = max (nH (PS_i,T_{jk})) + 2

Step 2

If (j <= n(RS_i))
Goto step 3
Else
i++, goto step 1

Step 3

Set S_i as a source node and determine $(RS_i)_j$

Step 4

If (k <= (n$(RS_i)_j$))
Goto step 5
Else
J++, goto step 2

Step 5

Determine $((RS_i)_j)_k$ and set $T_{jk} = ((RS_i)_j)_k$ as a target node for S_i.

Step 6

Set (PS_i, T_{jk}) as a path

Step 7

Determine NS_i node and find route to there respective node T_{jk}
$(NS_i, T_{jk}) = l_{NSi,Tjk}$
And reply in term of number of nodes to S_i

Step 8

Source S_i select minimum $l_{NSi,Tjk}$ among all (NS_i, T_{jk}) and set
nH(PS_i, T_{jk}) = min ($l_{NSi,Tjk}$)
k++, goto step 4

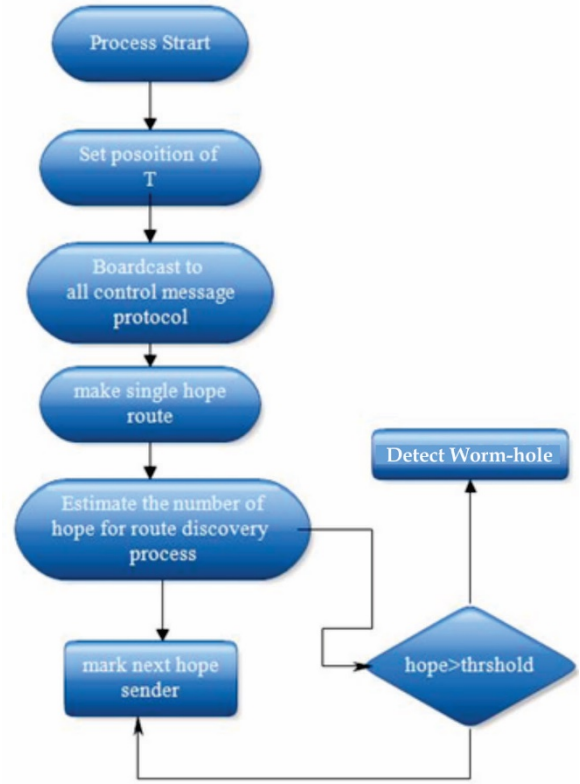

Figure 2: proposed model of worm-hole detection based on threshold based function

IV SIMULATION RESULT

To investigate the effectiveness of the proposed scheme for worm hole detection in mobileadhoc network, the simulation on a simplified topology was carried out using Network Simulator version (ns-2.34)

Parameter	value
Simulation duration	100 sec
Simulation area	1000*1000
Number of mobile node	25
Traffic type	Cbr(udp)
Packet rate	4 packet/sec
Host pause time	10sec

Table-I simulation parameter

The packet delivery ratio can be determined by dividing number of packets received by number of packet sent[24]. This performance metric gives us an idea of how well the protocol is performing in terms of packet delivery at different speeds using different traffic models.

Figure 3 Packet Delivery Ratio v/s Speed of nodes

The normalized routing load is the overhead on the network in order to find and maintain the route [23]. Normalized routing load can be determined by finding number of routing packets sent per number of data packet received, the fraction of all routing control packets sent by all nodes over the number of received data packets at the destination nodes. In other words, it is the ratio between the total numbers of routing packets sent over the network to the total number of data packets received [14].

Figure 4 Normalized Routing Load Vs Speed of Nodes

Both the path loss sensitive variants of AODV does not process the RREQ if it is having large path loss, that will reduce the routing load in both the variants. The AODV does not have stable route which increases the route discovery. Increased route discovery incurs more routing overhead.

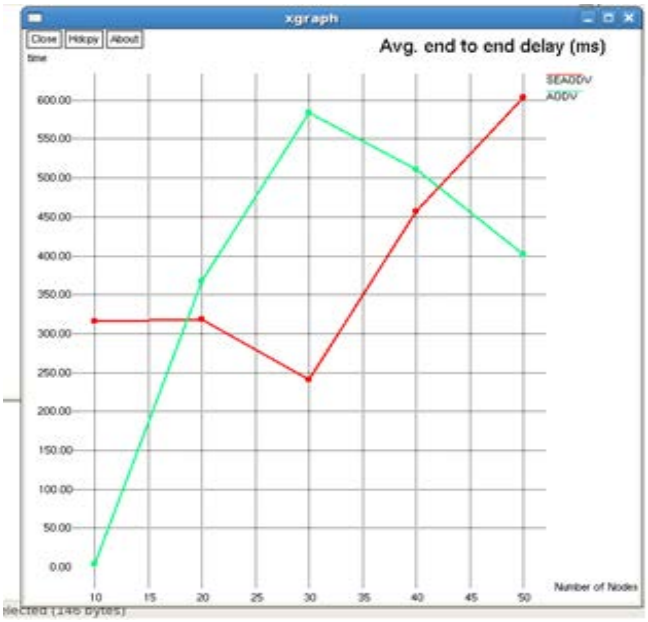

Figure 5 Average End to End Delay Vs Speed of nodes.

AODV has minimum no of hops so, there will be less time spent in processing the data packets. It *is* true that both SEAODV gives stable route but, they finds a route with increased no of hops compared to AODV which will increase the End to End delay compared to AODV. The increased End to End delay of both SEAODV is considered as a trade-off of our proposed work i.e. the price we are paying to achieve the stable path.

V CONCLUSION & FUTURE SCOPE

In this paper modified the AODV routing protocol for the detection of worm-holeattack. 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 worm-hole 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 worm-holes 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.

REFERENCES:-

[1] Sandeep Gupta, Abhishek Mathur "Enhanced Flooding Scheme for AODV Routing Protocol in Mobile Ad hoc Networks" International Conference on Electronic Systems, Signal Processing and Computing Technologies, IEEE, 2014. Pp 316-321.

[2] RanjanDasgupta, Ritwick Mukherjee and Prof DrAmitava Gupta "Congestion Avoidance Topology in Wireless Sensor Network using Karnaugh Map" Applications and Innovations in Mobile Computing (AIMoC), IEEE,2015.Pp 89-96.

[3] Jun Long, Mianxiong Dong, Kaoru Ota, Anfeng Liu, and Songyuan Hai "Reliability Guaranteed Efficient Data Gathering in Wireless Sensor Networks"Reliability Guaranteed Efficient Data Gathering in WSNs, IEEE, 2015. Pp 430-444.

[4] ShabanaMehfuz, Sumit Kumar "Energy Aware Probabilistic Broadcasting for Mobile Adhoc Network" 2nd International Conference on Computingfor Sustainable Global Development (INDIACom), IEEE, 2015. Pp 1028-1033.

[5] Kartikay Garg, Pratibha and Shailender Gupta "A Novel Routing Strategy for Cognitive Radio Adhoc Network" 2nd International Conference on Computing for Sustainable Global Development (INDIACom), IEEE, 2015. Pp 1379-385.

[6] Zhimu Huang, Ryo Yamamoto, Yoshiaki Tanaka "A Multipath Energy-Efficient Probability Routing Protocol in Ad Hoc Networks" ICACT, IEEE, 2015. Pp 244-250.

[7] Akshai Aggarwal, Savita Gandhi, NirbhayChaubey,Keyurbhai A Jani "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs" Fourth International Conference on Advanced Computing & Communication Technologies,IEEE, 2014.Pp 432-438.

[8] Junfeng Wang, Yin Zhang, Jialun Wang, Yujun Ma, and Min Chen "PWDGR: Pair-Wise Directional Geographical Routing Based on Wireless Sensor Network" IEEE internet of things journal, vol. 2, no. 1, February 2015, Pp 14-22.

[9] Cheng chunling, Haojingbo, Zhang dengyin "An Expanding Ring Prediction and Location Aided AODV Routing Algorithm" International Conference of Information Technology, Computer Engineering and Management Sciences, IEEE, 2011. Pp 61-64.

[10] Dinesh Singh, Ashish K. Maurya, Anil K. Sarje "Comparative Performance Analysis of LANMAR, LAR1, DYMO and ZRP Routing Protocols in MANET using Random Waypoint Mobility Model" IEEE, 2011. Pp 62-66.

[11] S.Preethi, B. Ramachandran "Energy Efficient Routing Protocols for Mobile AdHoc Networks" IEEE, 2011. Pp 1136-141.

[12] 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" IEEE, 2011. Pp 1066-1070.

[13] Chaitali Biswas Dutta, Utpal Biswas "A Novel Wormhole Attack for Multipath AODV and its Mitigation" International Conference on Recent Advances and Innovations in Engineering, IEEE, 2014. Pp 1-6.

[14] Bow-Nan Cheng, Scott Moore" A Comparison of MANET Routing Protocols on Airborne Tactical Networks" 978-4673, IEEE 2013, PP 67-89.

[15] M. Goyal, M. Soperi, E. Baccelli, G. Choudhury, A. Shaikh, H. Hosseini, and K. Trivedi " Improving Convergence Speed and Scalability in OSPF: A Survey" IEEE COMMUNICATIONS SURVEYS & TUTORIALS 1553-877, IEEE 2012,PP 86-92.

[16] GihanNagib and Wahied G. Ali" Network Routing Protocol using Genetic Algorithms" International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 10, 2010, PP 56-67.

[17] Joseph Chabarek, Joel Sommers, Paul Barford, Cristian Estan, David Tsiang, Stephen right" Power Awareness in Network Design and Routing" 9781-4244-IEEE 2008,PP 42-53.

[18] Kaixin Xu, Mario Gerla"A Heterogeneous Routing Protocol Based On A New Stable Clustering Scheme" IEEE 2010, PP 36-45.

[19] MuraliKodialam T. V. Lakshman"Minimum Interference Routing with Applications to MPLS Traffic Engineering" IEEE 2010, PP 56-64.

[20]MircoMusolesi, Cecilia Mascolo"A Community Based Mobility Model for Ad Hoc Network Research" 1595933603 ACM 2010, PP 85-94.

[21] Anton Riedl" Optimized Routing Adaptation in IP Networks Utilizing OSPF and PLS"IEEE 2010, PP56-67.