Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 70 (2015) 137 – 145

Procedia Computer Science

4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS 2015

EMAODV: TECHNIQUE TO PREVENT COLLABORATIVE ATTACKS IN MANETs

Anuj Rana[a,]*, Vinay Rana[b] , Sandeep Gupta[c]

[a]*Hindu College Of Engineering, Sonipat, Haryana-131001, India*
[b]*International Institute Of Technology And Business, Sonipat, Haryana-131023, India*

Abstract

Most demanding issue in MANETs is Security or Secure communication due to its various vulnerabilities. Vulnerabilities or exclusive characteristics that make MANETs prone to various attacks are as non appearance of authorization functionality, infrastructure less network environment, dynamically-randomized movement of nodes. Collaborative attacks have more harsh affects on MANETs than single particular attacks. Due to increasing demand of using MANETs various type of protocols and secure algorithms have been developed one after other but still there is lack of completely secured protocols which makes communication bother free. Now, in this paper an algorithm to prevent collaborative attacks on MANETs is presented.

Peer-review under responsibility of the Organizing Committee of ICECCS 2015

Keywords: Wireless Networks; MANETs; Collaborative Attack; Enhanced Modified AODV

1. Introduction

Ad-hoc networks are collectively composed of autonomous nodes, which are self managed and hold a dynamic topology such that nodes can easily join or leave the network at any instant time. Without relying on any fixed infrastructure, they are organized in decentralized manner means no central authority, self-configuring, self-managing networks and also capable of modeling a communication network. Packets forwarded from one node to another that means each Node in the network have to trust one another because they participate in routing the traffic or acts like a mediator for routing. Some attributes in mobile ad-hoc networks makes routing additionally more

* Corresponding author. Tel.: +0-903-495-8089
E-mail address: it07407.sbit@gmail.com

Peer-review under responsibility of the Organizing Committee of ICECCS 2015
doi:10.1016/j.procs.2015.10.060

complicated are moderate bandwidth and limited battery power. Various types of attack target the network, therefore requirement of security protocols truly demanded. Many security protocols were already developed to tackle some of the attacks. But if talk about two or more attacks synchronized simultaneously in the network, knows as collaborative attacks where each and every attack is launched by a specialized expertise.

Since the nodes have the ability to forward the data packets themselves, they support this connectivity with the help of various routing protocols that have been developed by Internet Engineering Task Force's MANET working group such as AODV (Ad-hoc On-demand Distance Vector), DSR, DSDV, etc. In spite of, no one of all these security protocols are satisfactorily to security issues. Mainly two main sources of threats act on routing protocols. One is from the nodes that are not part of the network and other from inner or compromised nodes that are part of the network. While an attacker can reply old information, also modify routing information and also cause excessive load to prevent the proper routing protocol functioning.

Routing protocols are required for exchanging routing information between nodes or select routes between nodes within the network. Similarly, MANETs routing protocols are also designed for non-antagonistic networks to provide security aspects. This follows the traditional approach like first design a protocol and later on back fit it with security aspects. In this paper, we present an approach that enhanced the routing protocol AODV more secure to use it in case of collaborative attacks as demand of using MANETs increase with the past of each day. Now we consider various approaches to handle attacks.

For example- Blackhole and Grayhole attacks compatible with each other while Wormhole attack is incompatible with DoM attack because Wormhole attacks need fast connections but DoM attacks need lower bandwidth.

The remaining part of this paper is well organized as follows: In Section II gives a brief about related works.

In Section III, Introduction and implementation of proposed method EMAODV(Enhanced Modified AODV).

In Section IV, We discussed about Simulation environment and Graphical result analysis.

In Section V, Last section of the paper provides Conclusion and future scope.

2. Related Work

Threat of collaborative attacks on MANETs is noticed by so many researchers. Hence, research in various defending mechanisms, preventive approaches are going on and result design of several mechanisms to defend against collaborative attacks done.

- In [1] the author used a data routing information (DRI) table at each node and cross checking method to identify the cooperative black hole nodes in the network. The modified AODV routing protocol was used to achieve this methodology. The experiment results show that this solution performs better than other solutions.
- In [25] the author presents the most important forms of attacks, discuss possible collaboration among various attackers and show how various signal processing and neural learning can help in detection and defense of collaborative attacks in such environments. They also showed how collaborative attacks can cause a worse effect on wireless than on a wired network. Experimental results demonstrate the validation and effectiveness of the model proposed by minimizing the collaborative attacks and immunizing the mobile ad hoc networks.
- In [3] the author addresses the problem of collaborative insider attacks where critical data within the information systems is compromised by two or more insiders working together. Author first discussed about various relations among illegal information flow diagram and information system components. Then after, various characteristics of data accesses summarized by the mutual-access-record's probability value and the transaction distance to data item are presented. Afterwards the algorithm is introduced for detecting collaborative insider attacks.
- In [5] the authors analyze MANETs under single and collaborative Black Hole attack and proposed a technique to prevent it by diverting traffic from the Black Hole nodes. The MANETs so discussed make use of the AODV routing protocol and the method so proposed is based on sending confirmation packets that are verified by the destination to check for the Black Hole presence in the GAODV routing protocol so proposed.
- In [20] the author proposed a theory that balanced Collaborative attackers can pass trusted nodes assistance methods which are very often used in existing secure schemes. On the basis of theoretical analysis, the reports so formed between BC attackers have the highest similarities ratio. They proposed an algorithm to check abnormality detection and to detect BC attackers. The bit error probability of secondary users is the only

information they required to know of reporting channel. The Numerical simulation results show that the proposed technique can easily identify and find out BC attackers clearly.

In this paper, a new technique is proposed for preventing and detecting collaborative attacks in a MANET by focusing on detecting and preventive malicious nodes through bridge data items.

3. Proposed Method EMAODV(Enhanced Modified AODV)

AODV can be extended by adding two types of control packets and threshold value: Secure Reliable Route Discovery Request (SRRD_REQ) and Secure Reliable Route Discovery Reply (SRRD_REP). SRRD_REQ messages are also known as control packets sent by the source node along with SRRD-ID as destination sequence number of destination node over the MANET on regular intervals and SRRD_REP message in response of SRRD_REQ by the destination to the source node after matching SRRD_ID. SRRD_REP can only be generated by the destination node as assumption which means there is no role of other nodes i.e. no node other than the destination, can generate SRRD_REP on behalf of the destination node. In addition, Routing table also contains new fields called Reliability List (RL) and Threshold Value (TV) as routing table entry. But no change in the format of EMAODV Routing Table entry compare to normal AODV routing table entry except two additional fields RL and TV. RL (Reliability list) contains nodes that are trustworthy and TV contains average of all destination sequence number of reliable nodes. Path discovery compose of two phases: Phase I & Phase II discussed below.

3.1 Algorithm For Enhanced Modify AODV

The algorithm for EMAODV to detect and prevent attacker nodes in MANET given below –
Phase I **-**When a source node in MANET wish to send data packets to any destination node within the network then firstly check whether there is any update route present in the routing table. If reliable route found then transfer data packet through it else initiate the route discovery process. In this process, the source forward SRRD_REQ to its neighbor nodes with SRRD_ID for creation of new route. When an intermediate node receives an SRRD_REQ it does the following steps:

- If this node has an updated route to the required destination, then it sends SRRD_REP to the source else broadcast the SRRD_REQ to its neighboring nodes with hop count incremented by 1.
- Sets up a reverse path discovery for the reply message.
  - If the node having an entry in its routing table towards the source as destination but it is not updated enough, hence it refreshes it. If there founds an entry in RL (Reliable list) for the destination, then delete and update it also.
  - If no entry found for the source in the routing table entries then creates new entry during reverse path technique. More than one reliable route found and arranges these routes according to minimum hop count. Then Compare first node destination sequence number of top reliable route with minimum hop count with TV (threshold value). If its value greater than average of DSNs of route nodes then it must be an attacker node so discard this route and check for another till no reliable route found having less DSN value then TV.
  - Most Reliable route with minimum hop count is selected for new entry to the source node by copying the hop count, source sequence number from the SRRD_REQ packet and address of neighbor from which first received copy of broadcasting request or message packet, take as the next hop.

When the destination receives SRRD_REQ packet it sends back SRRD_REP using the reverse path. SRRD_REP may also be sent by some intermediate node which is having an updated path to the destination. During reverse route technique, each node that receives SRRD_REP performs the following steps:

- If that node contains an entry for the destination but not currently updated one, it updates that entry, else creates a new entry to its routing table.
- Also must appends an entry with IP address of source copied from originator field of SRRD_REP packet. FDPC and SRRD_ID are set to zero. Also forwards it to next hop on reverse route.

In AODV route discovery process done when originator receives Route REP messages. But in Enhanced Modified AODV, phase 2 starts from this point.
Phase 2-Source node sends SRRD packets to all the nodes from which it got RREPs. Now every node which receives SRRD does the following-

- If there is a reverse path entry in its routing table for source, it sets SRR_ID by copying it from SRRD. Else, creates new entry.
- Now Forwards packets to all those nodes from where it received SRRD_REPs earlier.
- Each node on the path of SRRD should be having an entry for the destination.

When the destination receives the SRRD packet it replies with SRRD_REP to its neighbour node from which it received the first SRRD packet and else discards others. The destination sets the reliability value in the SRRD_REP packet to 1. During reverse path technique, each intermediate node receives only one copy of SRRD_REP for the first time (SRRD_ID = 1) do two steps: sets FDPC to zero in SRRD_REP and then forwards it to the next hop on the reverse path. Finally, the source node gets SRRD_REP. After all no intermediate node can generate SRRD_REP, this SRRD_REP is unique and the path is discovered.

4. Simulation Environment and Graphical Results Analysis

In this section, we discussed about various simulation parameters, operations of proposed method EMAODV and lastly graphical results to be analysed.

4.1. Simulation Parameters

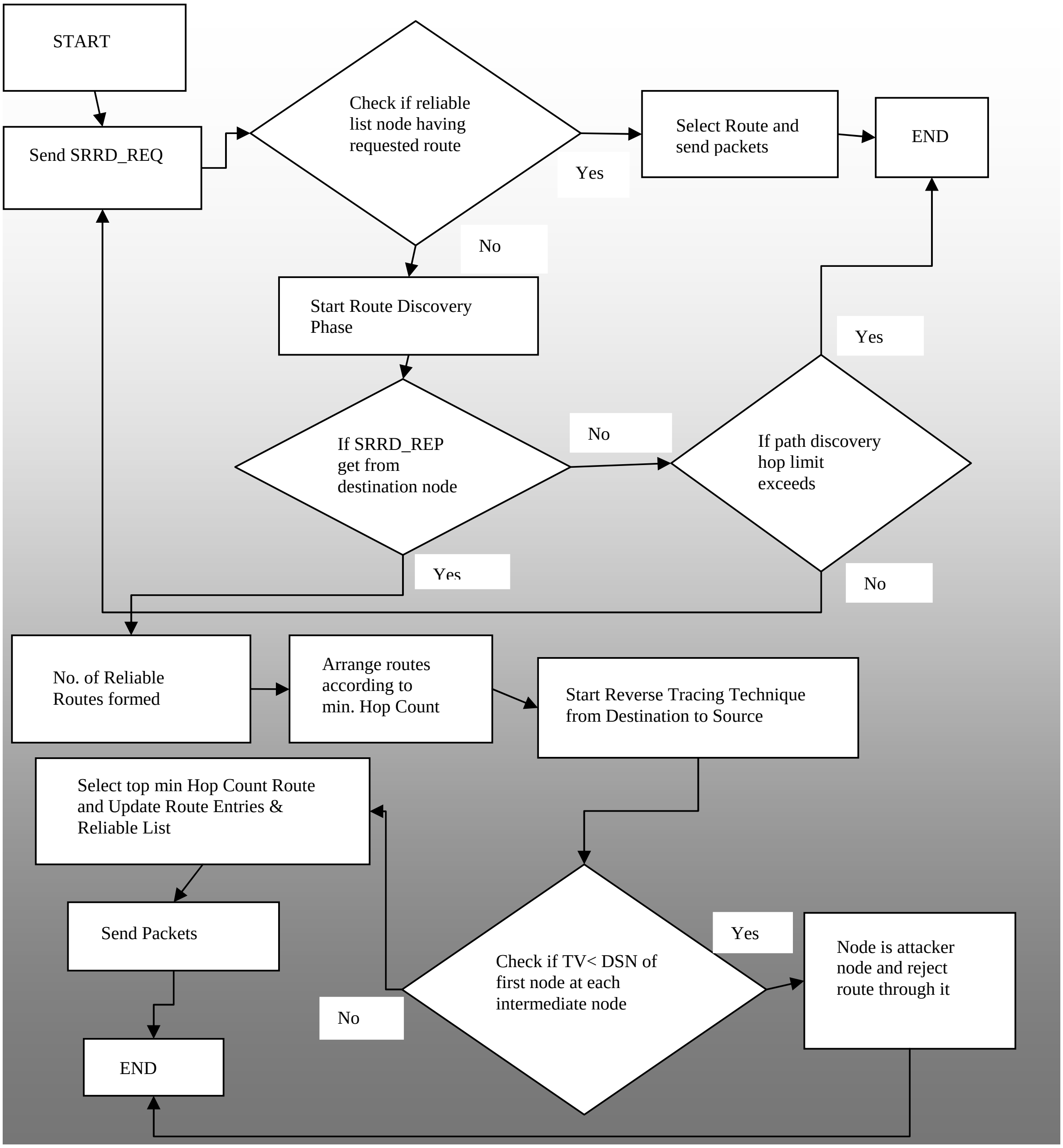
The first phase of Simulation is to design a mobile Ad hoc network scenario which provides the workspace where the desired MANET is modelled. Predetermined parameters of NS2 and required attributes of node are configured. The entire system is built on some values and settings that we hope would enable us to provide more stable simulation results than before.

Table 1. Parameter setting of research simulation with NS2

Parameter name	Initial value
Simulation time	90 (s)
Sum of mobile nodes	23
Sum of static nodes	3
Sum of base-station node	1
Sum of blackhole nodes	3
Sum of grayhole node	2
Normal routing protocol	AODV
Blackhole and Grayhole attack protocol	blackholeAODV,grayholeAODV
Traffic	CBR
Normal packet size	512 bytes
Abnormal packet size	1024 bytes
Data rates	10 Kbits

By using NS2, same network is generated with 23 nodes having some nodes act as the Blackhole attack and Grayhole attack similar to normal AODV. The Connection so creates between source and destination is UDP. With the help of CBR (Constant Bit Ratio) application, Traffic is generated with constant packets through the UDP connection. Packet size of CBR seized to 512 bytes and set data rate to 10 Kbps. Similar scheme used for the simulation of UDP connection and traffic generation in EMAODV as in normal AODV.

4.2. Operations of Proposed Method EMAODV


START
Send SRRD_REQ
Check if reliable list node having requested route
Yes
Select Route and send packets
END
No
Start Route Discovery Phase
If SRRD_REP get from destination node
No
If path discovery hop limit exceeds
Yes
No
Yes
No. of Reliable Routes formed
Arrange routes according to min. Hop Count
Start Reverse Tracing Technique from Destination to Source
Select top min Hop Count Route and Update Route Entries & Reliable List
Send Packets
END
Check if TV< DSN of first node at each intermediate node
Yes
No
Node is attacker node and reject route through it

4.3. Observations with changing Malicious Nodes ratio and fixed mobility

In Fig. 1, we clearly observed that Normal AODV radically experience from Blackhole attacks and Grayhole attacks when malicious node percentage increases. This recognized the fact that Normal AODV doesn't have any secure method to detect or prevent Blackhole and Grayhole attacks. The Proposed EMAODV scheme illustrates high packet delivery ratio compared with that of Normal AODV in different conditions (with no attacks, with Blackhole attacks only, with Grayhole attacks only and with collaboration of both Blackhole and Grayhole attacks). Also during the case where 50% of the total nodes in the network are malicious, the EMAODV proposed method still prevents or detects those malicious nodes successfully while keeping the packet delivery ratio above 85%.

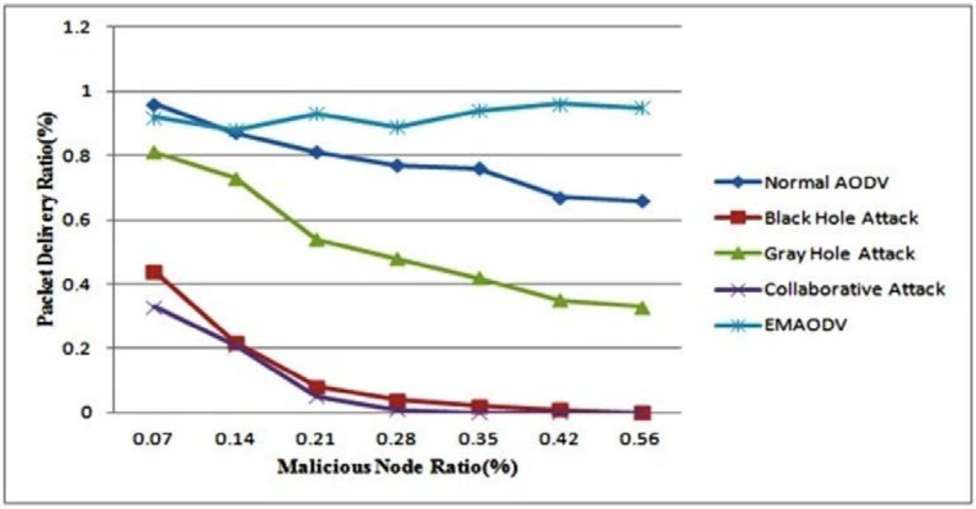


Fig. 1.Packet delivery ratio of Normal AODV during different conditions and the EMAODV w.r.t. MNR

In fig 2, we study about routing overhead of the EMAODV and Normal AODV with respect to MNR(malicious node ratio). The results show that when the total no. of malicious nodes increases, Normal AODV generates the lowest routing overhead contrast with the EMAODV. This recognized the fact that Normal AODV doesn't have any secure method to detect or prevent Blackhole and Grayhole attacks.

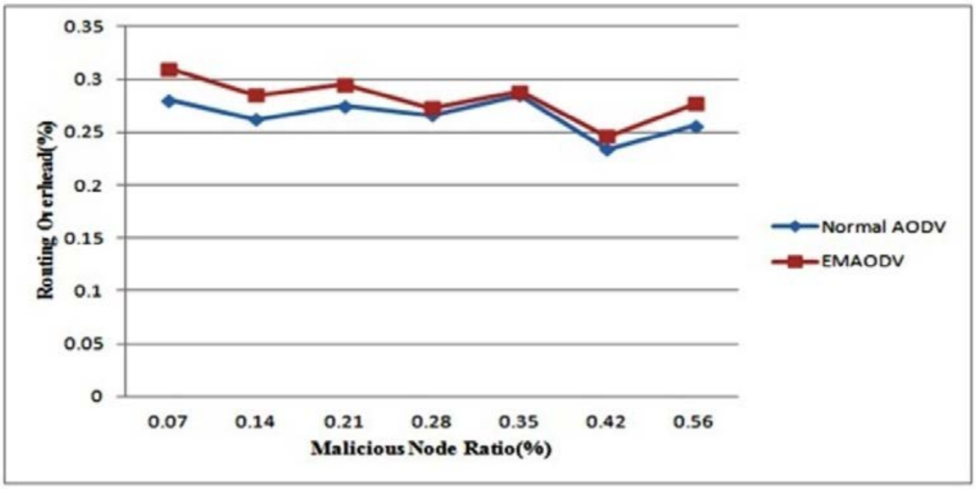


Fig. 2.Routing Overhead of Normal AODV and the EMAODV w.r.t. MNR

In fig 3, the results are captured about average end-to-end delay of the proposed EMAODV and Normal AODV with respect to MNR(malicious node ratio). The results show that the EMAODV gains a little bit more avg. end-to-end delay as compared with Normal AODV. This recognized that the EMAODV requires more time to detect malicious nodes. Therefore, end-to-end delay and packet delivery ratio are inversely proportional to each other.

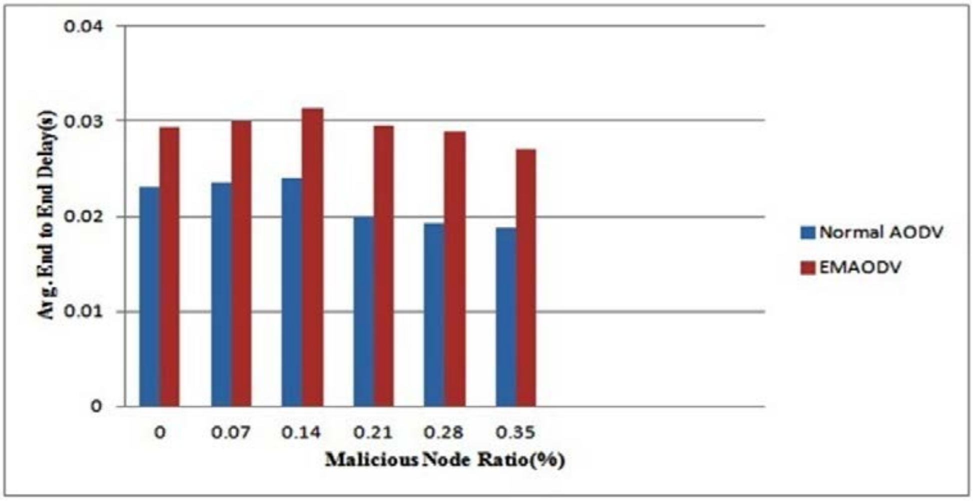


Fig.3.Avg. END to END Delay(s) of Normal AODV and the EMAODV w.r.t. MNR

In fig 4, we examined the throughput of proposed EMAODV and the Normal AODV with respect to MNR(malicious node ratio). The results show that Normal AODV experiences the most from malicious-node attacks compared with the EMAODV. Also during the case where the total number of malicious nodes in the network is comparatively high (up to 40%) the EMAODV can still detect malicious nodes successfully while keeping the throughput above 14 000 bit/s.

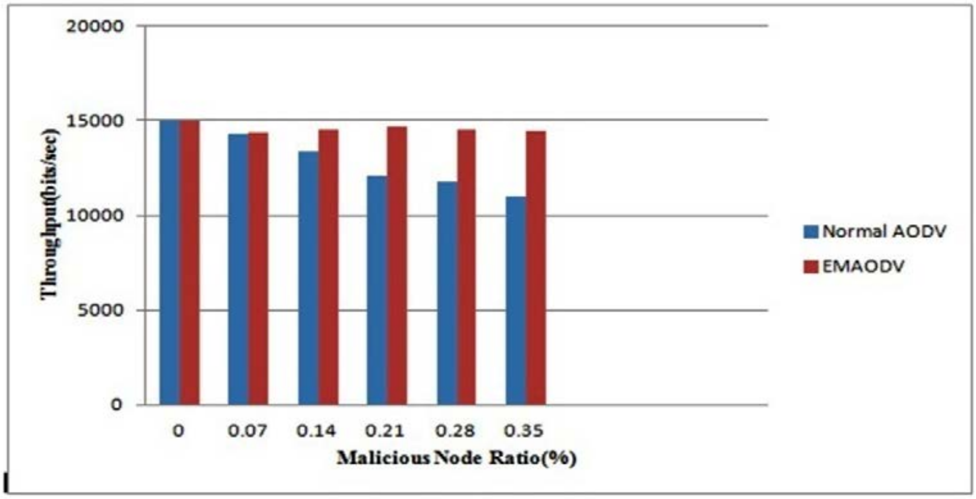


Fig. 4.Throughput (bit/sec) of Normal AODV and the EMAODV w.r.t. MNR

5. Conclusion and Future Work

In this paper, we proposed a new technique called EMAODV(Enhanced Modified AODV) for preventing and detecting malicious nodes in MANETs during conditions of single individual attacks or collaborative Blackhole and Grayhole attacks Collaborative Attacks are combinational synchronized attacks by two or more attacker on MANETs which are also compatible to each other. The simulation results in form of graphs shows various routing overhead, packet delivery ratio and throughput evaluation results in case of individual attacks and collaborative attacks, also demonstrates that the proposed algorithm EMAODV provides better output than the normal or traditional AODV protocol. This algorithm is very much suitable for 15-45 nodes MANETs for preventing and detecting collaborative attacks black hole and gray hole. But little routing overhead in proposed EMAODV prevents full efficiency utilization of MANET which is not in case of normal AODV. Therefore routing overhead increases with increase in MANETs size.

In future work, the simulations can be developed for other combinations of attacks that are compatible to each other having their own specification to target the MANETs. Also find out different compatible collaborative attacks having own expertise that targets MANETs.

References

1. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks", *International Conference on Wireless Networks (ICWN)*, 2003.p.1-7.
2. S. A. Razak, S. M. Furnell, P. J. Brooke, "Attacks against Mobile Ad-hoc Networks Routing Protocols", In *Proceedings of 5th Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking & Broadcasting (PGNET)*, England: Plymouth; 2004.
3. Khanh Viet, Brajendra Panda, Yi Hu Korea, "Detecting Collaborative Insider Attacks in Information Systems", *IEEE International Conference on Systems, Man, and Cybernetics*, Seoul; 2012.p.502-507.
4. Sweta Jain, Jyoti Singhai, Meenu Chawla, "A Review Paper on Cooperative Blackhole and Grayhole Attacks in MANETs", *International journal of Ad-hoc Sensor & Ubiquitous Computing*, 2011.p.71-80.
5. Sanjay K. Dhurandher, I. Woungang, R. Mathur, P. Khurana, "GAODV: A Modified AODV against single and collaborative Blackhole attacks in MANETs", *IEEE 27th International Conference on AINA Workshops*, Barcelona; 2013.p.357-362.
6. C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," *RFC3561 (Experimental)*, 2003.p.1-37.
7. *http://narentada.com/what-is-black-hole-attack-in-manets-my-code-for-adding- malicious-node-as-blackhole-in-aodv-protocol/*, Nov. 2012
8. P. Mani, D.W. Petr, "Development and Performance characterization of Enhanced AODV Routing for CBR and TCP Traffic", *Wireless Telecommunications Symposium*, USA: IEEE; 2004.p.44-51.
9. Pooja Jaiswal, Rakesh Kumar, "Prevention of Blackhole Attack in MANET", *International Journal of Computer Networks and Wireless Communications (IJCNWC)*, 2012.p.599-606.
10. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad-hoc networks", *MobiCom '00 Proceedings of the 6th annual international conference on Mobile computing and networking*, USA: New York; 2000.p.255-265.
11. L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad-hoc Networks", *Journal of Parallel and Distributed Computing*, USA: Elsevier Science; 2003.p.214-227.
12. Piyush Agrawal, R. K. Ghosh, Sajal K. Das, "Cooperative Black and Grayhole Attacks in Mobile Ad-hoc Networks", *2nd international conference on Ubiquitous information management and* communication, Korea; 2008.p.310-314.
13. M. S. Gast, "*802.11 Wireless networks-the definitive guide*", 2nd edition, US: O'Reilly Media; 2011.
14. S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad-hoc Networks by Dynamic Learning Method", *International Journal of Network Security*; 2007.p.338–346.
15. Amitabh Mishra et al. "Intrusion Detection in Wireless Ad-hoc Networks", *IEEE Wireless Communications*; 2004.p.48-60.
16. Jian-Ming Chang et al., "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach", *IEEE Systems Journal*; 2015.p.65-75.
17. Djenouri D, Badache N, "Struggling Against Selfishness and Blackhole Attacks in MANETs", *Wireless Communications and Mobile Computing*, UK: Wiley Online Library; 2008. p.689–704.
18. Neha Kaushik, Ajay Dureja, "Performance Evaluation of modified AODV against Black Hole Attack in MANET", *European Scientific Journal*, Portugal: University of the Azores; 2013.p.182-193.
19. Mistry N, Jinwala DC, IAENG, Zaveri M.,"Improving AODV Protocol Against Attacks", *International MultiConference of Engineers and Computer Scientists*, Hong Kong; 2010.
20. Mingchen Wang, Bin Liu and Chi Zhang "Detection of Collaborative SSDF Attacks using Abnormality Detection Algorithm in Cognitive Radio Networks", *IEEE International Conference on Communications*, Budapest; 2013.p.342 – 346.
21. T. Franklin "Wireless Local Area Networks", Tech. Rep. *http://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf.*,UK; 2005.
22. Ujjwal Agarwal, K.P Yadav, Upendra Tiwari, "Security Threats in Mobile Ad hoc Networks", *International Journal of Research in Science and Technology*, 2013.p.53-64.
23. Teerawat Issariyakul, Ekram Hossain, *Introduction to Network Simulator NS2*, US: Springer*; 2009*.
24. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L, "Developing a BDSR Scheme to Avoid Blackhole Attack Based on Proactive and Reactive Architecture in MANETs", *13th International Conference on Adv. Communication Technology(IEEE)*, Seoul; 2011.p.755-760.
25. Tao Gong1 and Bharat Bhargava, "Immunizing mobile ad-hoc networks against collaborative attacks using cooperative immune model", article published in Wiley Online Library (*wileyonlinelibrary.com*), *Issue: Security and Communication Networks*, 2013.p.58-68.
26. M. Amitabh, "*Security and Quality of Service in Ad-hoc Wireless Networks*", Cambridge: University Press; 2008.
27. Su Ming-Ying et al., "Prevention of Selective Balckhole Attacks on MANETs through intrusion detection systems", *Computer Communications (ELSEVIER)*, The Netherlands; 2011.p.107-117.

28. H. Weerasinghe and H. Fu., "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation", Proc. *IEEE ICC*, jeju; 2007.p.362 -367.