Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.457 – 465

RESEARCH ARTICLE

PERFORMANCE EVALUATION OF COLLABORATIVE ATTACKS IN MANET

Ajay Dureja
PDM College of Engineering for Women
Bahadurgarh (Haryana)
ajaydureja@gmail.com

Vandna Dahiya
PDM College of Engineering for Women
Bahadurgarh (Haryana)
vandanadahiya2010@gmail.com

Abstract:- Secure communication in MANET is a demanding issue as MANET suffers from different vulnerabilities. Unique characteristics like infrastructure less network, absence of authorization, dynamic-random movement of nodes make these networks prone to various attacks. These attacks become more severe when launched in collaborative manner. Various protocols and secure algorithms have been developed to make the communication hassle free but still there is lack of completely secured protocols due to increasing demand of using of MANET. We present an algorithm for modified AODV against collaborative attacks in this paper.

Keywords: Wireless Networks, MANET, Collaborative Attack, Modified AODV

I. INTRODUCTION

Ad-hoc networks are composed of autonomous nodes which are self-managed and have a dynamic topology such that nodes can easily join or leave the network at any time. They are decentralized that means there is no central authority, self-configuring, self-organizing networks and are capable of forming a communication network without relying on any fixed infrastructure. Nodes in these networks forwards packet to next node, thus they also participate in routing the traffic as well, so each node has to trust one another. Yet another feature of a MANET is, moderate bandwidth, limited battery power. This attribute makes routing in a MANET an additionally more complicated task. Various attacks target the network. There are security protocols to tackle some of the attacks. But if there are two or more attacks synchronized simultaneously in the network, we call them collaborative attacks where 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 (Dynamic Source Routing), DSDV (Destination-Sequenced Distance-Vector), etc. But none of these address security issues satisfactorily. There are two main sources of threats to routing protocols. The first is from nodes that are not part of the network, and the second is from compromised nodes that are part of the network. While an attacker can inject incorrect routing information, reply old information, or cause excessive load to prevent proper routing protocol functioning.

Like most network protocols, MANET routing protocols are often designed for non-adversarial networks and thus forgo security features. This follows the traditional model of first designing a protocol and later (sometimes much later) retrofitting it with security features. Being a popular protocol, DSR has received a lot of attention from the security community. In this paper we present an approach to make AODV more secure to use it in case of collaborative attacks as there is increasing demand of using MANET, we need to consider various approaches of attacks. MANETs have many potential applications, especially, in military and rescue areas, in establishing a new network where existing network collapsed after a disaster like an earthquake. Ad-hoc networks are suitable for areas where it is not possible to set up a fixed infrastructure.

The rest of this paper is organized as follows: section II gives a brief introduction of collaborative attacks. In section III we give simulation of collaborative attack with normal AODV. Section IV describes the implementation of modified AODV. Section V describes Experimental results and analysis. In Section VI, we draw conclusion and give future work.

II. Collaborative Attacks

Collaborative attacks are synchronized attacks where a system is distributed by more than one attacker simultaneously. Collaborative attacks (CA) occur when more than one attacker or running process synchronize their actions to disturb a target network. It is a new generation attack, each individual attacker may have specialized expertise. It is different from multiple attacks where multiple attacks occur when a system is disturbed by more than one attacker, but not necessarily in collaboration. Preventive and secure attacks mechanisms are available only for individual attacks. Like in human body, when various diseases attack simultaneously, like cough, flue, malaria by various viruses, bacteria, immunity of body becomes more down.

III. **SIMULATION OF COLLABORATIVE ATTACK IN NS2**

The network environment, parameters, tools and values and certain assumptions can be described as follows.- TCP/IP Network Transmission, IEEE 802.11b(Media Access Control) MAC, randomly 21 nodes allocated, application of Constant Bit Rate(CBR), node mobility is used, all MANET nodes on the network run on AODV routing protocol.

SIMULATION OF AODV WITH BLACK HOLE AND GRAY HOLE NODE USING NS2

Ad- hoc On-demand Distance Vector (AODV) is a reactive routing protocol in which a path is searched only when a node needs to transmit the data. Using of the destination sequence number for each route entry is the most promising feature of this protocol which is generated by the destination when a link is requested from it. AODV works in two phases: Route discovery and Route maintenance. For route discovery the algorithm uses Route Requests (RREQs) and Route Replies (RREPs) messages. For route maintenance the algorithm uses Route Errors (RERRs) and HELLO messages. When a node wants to communicate with another node it looks for a route in its table. If a legal entry is found, it uses that path else the node broadcasts the RREQ to its neighbors to find the destination. Neighbors again broadcast RREQ to their neighbors. A reverse path for the source is created at every node. This process continues until either the destination or an intermediate node with a fresh route to the destination is located. The node, then builds an RREP packet and sends to the node from which it received RREQ packet. At each intermediate node on the reverse route the RREP packet is inspected and a forward path to the destination is constructed or updated. Path discovery completes when RREP reaches to the originator.

Efficiency of the Network with normal AODV- Efficiency of the network is measured in terms of packet delivery ratio which can be defined as the ratio of total number of data packets delivered to the destination to the total number of data packets generated by the source. It is calculated as: P = (number of packets received) / (number of packets sent) * 100. A drastic decrease in PDR is seen when there is a collaborative attack in the network.

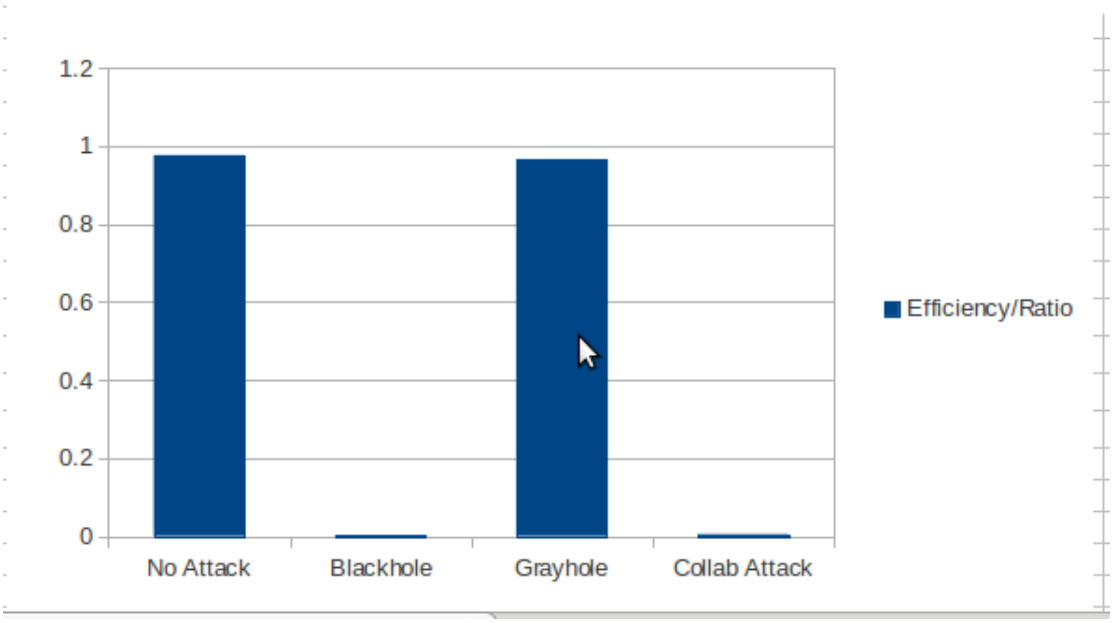

Fig: Efficiency of network with normal AODV

The simulation results are compared on the basis of performance of the network i.e. Packet Delivery Ratio (PDR) or efficiency of the network. On the basis of this parameter the Graphs are drawn for comparing AODV with Collaborative attacks.

IV. Modified AODV

AODV can be extended by adding two types of control packets: Reliable Route Discovery Unit (RRDU) and RRDU Reply (RRDU_REP). RRDU messages are control packets sent by the source node along with RRDU-ID, to the destination at regular intervals and RRDU_REP message is the response of RRDU by the destination to the source node. RRDU_REP can only be generated by the destination. We assume here that there is no impersonation i.e. no node other than the destination, can generate RRDU_REP on behalf of the destination. We also add a field Reliability List (RL) in the routing table entry. The format of this AODV Routing Table entry is same as that of normal AODV except for the additional RL field. Path discovery now can be thought of comprising of two phases. Phase I is same, i.e. when a node needs to communicate with another node it looks for a route in its table. . If it find a valid path to the required destination, it uses that else it forwards RREP to all its neighbors. Neighbors again broadcast RREQ to their neighbors. The process continues until either the destination or an intermediate node with a fresh route to the destination is located.

At each intermediate node, a reverse path is created for the source. It must be noted that several reverse paths may be created in this process. The source receives RREPs from all

these paths. In AODV, it selects the one with minimum hop count and others are discarded. However, with modify approach, at this point Phase II starts.

Algorithm For Modify AODV –

The algorithm for modified AODV to detect and prevent malicious nodes in MANET is given below –

Phase I -When a source node wants to send data to some destination it looks if there is any valid route otherwise it initiates the process of route discovery. When an intermediate node receives an RREQ it does the following steps:

1. If this node has an updated path to the required destination, then it sends RREP to the source else forwards the RREQ to its neighbors with hop count incremented by 1.
2. Sets up a reverse path for the reply message.
    a. If it has an entry in its routing table for the source as the destination but it is not fresh enough it refreshes it. If there is an entry for the destination in RL, delete it.
    b. If there is no entry for the source in the routing table it creates a new entry to the source node by copying the hop-count, source sequence number from the RREQ packet and address of neighbor from which first copy of the broadcast packet is received, as the next hop.

When the destination receives RREQ packet it sends back RREP using the reverse path. RREP may also be sent by some intermediate node which is having an updated path to the destination. While being on reverse route, each node which receives RREP perform the following steps:

1. If that node is having an entry for the destination but not an updated one, it updates the entry, Else creates a new entry.
2. Also appends an entry with IP address of source copied from originator field of RREP packet. FDPC and RRDU-ID are set to zero. Then forwards to next hop on reverse route.

In AODV route discovery is completed when originator receives RREP messages. But in Modify AODV, phase 2 starts from here.

Phase 2-Source node sends RRDU packets to all the nodes from which it got RREPs.

Format of RRDU packet is shown below-

Now every node which receives RRDU does the following-

1. If there is a reverse path entry in its routing table for source, it sets RRDU-ID by copying it from RRDU. Else, creates an entry.
2. Forwards it to all those nodes from where it received RREPs earlier.
3. Each node on the path of RRDU should be having a entry for the destination.

When the destination receives the RRDU packet it replies with RRDU_REP to the neighbor from which it received the first RRDU packet and discards others. The destination sets the reliability flag in the RRDU_REP packet to 1. On the reverse path, each intermediate node receives only one copy of RRDU_REP for the first time (RRDU-ID = 1) does two steps: sets FDPC in RRDU_REP to zero and forwards it to the next hop on the reverse path. Eventually, the source node gets RRDU_REP. Since no intermediate node can generate RRDU_REP, this RRDU_REP is unique and the path is discovered.

V. Simulation Of Modify AODV Using NS2

With the help of NS2, the same network is generated with 21 nodes as for the black hole attack and gray hole attack in conventional AODV. A UDP connection is created between source and destination. Traffic is generated with the help of CBR (constant bit ratio) application which generates constant packets through the UDP connection. CBR packet size is taken as 512 bytes and data rate is set to be 10 Kbps. The same scenario is used for the simulation of UDP connection and traffic generation in modified AODV as in normal AODV. In the next chapter the simulation results of conventional AODV protocol is compared with the modified AODV.

Efficiency of the Network with modified AODV

When modify aodv is used, packet delivery ratio of the network increases thus efficiency of the network is improved.

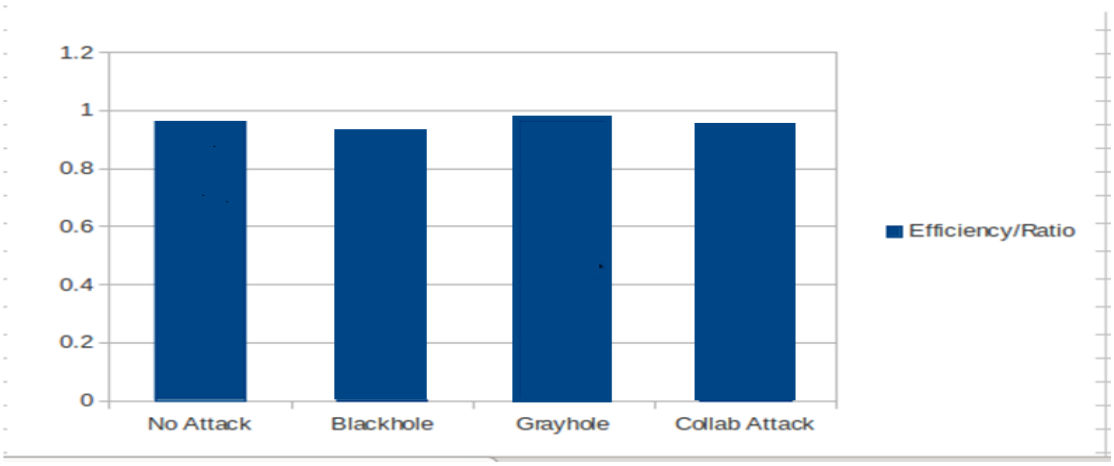

Fig: Efficiency of the network

VI. CONCLUSION AND FUTURE WORK

Collaborative Attacks which are synchronized attacks by more than one attacker are combination of more than one attack which are also compatible to each other. The simulation results here are shown with black hole and gray hole combination and solution is also proposed for collaborative black hole and gray hole attack only in this dissertation in the form of modify aodv. The simulation graphs show various efficiency results in case of single attacks and collaborative attacks, also shows that the proposed algorithm provides better output than the conventional AODV protocol. But there is slight increase in the routing overhead of proposed AODV protocol.

As future work, the simulations can be developed for more combinations of attack that can co relate with others to target a network with each of them having their own expertise.

REFERENCES

[1] L. Venkatraman and D. P. Agrawal, "Strategies for Enhancing Routing Security in Protocols for Mobile Ad Hoc Networks," J. Parallel Distrib. Comp., 2002.
[2] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks" In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.
[3] M. S. Gast, "802.11 Wireless networks-the definitive guide".
[4] 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, Vol.5, No.3, PP.338–346, Nov. 2007.
[5] Djenouri D, Badache N (2008) "Struggling Against Selfishness and Black Hole Attacks in MANETs". Wireless Communications & Mobile Computing 8(6):689–704. doi: 10.1002/wcm.v8:6.

[6] Gagandeep, Aashima, Pawan Kumar, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review".
[7] Mistry N, Jinwala DC, IAENG, Zaveri M (2010) "Improving AODV Protocol Against Attacks", Paper presented at the International MultiConference of Engineers and Computer Scientists, Hong Kong, 17-19 March, 2010.
[8] http://narentada.com/what-is-black-hole-attack-in-manets-my-code-for-adding-malicious-node-as-blackhole-in-aodv-protocol/, Nov. 2012
[9] Pradeep K. Mani, thesis on "Development and Performance characterization of Enhanced AODV Routing for CBR and TCP Traffic", 2001.
[10] Pooja Jaiswal, Rakesh Kumar, International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501Vol.2, No5, October 2012, "Prevention of Black Hole Attack in MANET".
[11] S. Marti, T. J. Giuli, K. Lai, and M. Baker Mitigating routing misbehavior in mobile ad hoc networks. in mobile Computing and Networking (MOBICOM), pages 255–265, 2000. Available on: citeseer.ist.psu.edu/marti00mitigating.html.
[12] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA.
[13] S. A. Razak, S. M. Furnell, P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols",2004.
[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255–265, 2000. Available on: citeseer.ist.psu.edu/marti00mitigating.html.
[15] Sweta Jain, Jyoti Singhai, Meenu Chawla, International journal of Ad hoc, Sensor & Ubiquitous Computing Vol. 2, No. 3, 2011, "A Review Paper on Cooperative Blackhole and Grayhole Attacks in MANETs".
[16]Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur and Prashant Khurana , "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs" 27th International Conference on Advanced Information Networking and Applications Workshops.. IEEE, DOI 10.1109/WAINA.2013.168
[17] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561 (Experimental), Jul. 2003. [Online].
[18] T. Franklin, "Wireless Local Area Networks", Technical Report http://www.jisc.ac.uk/uploaded_documents/WirelessLANTechRep.pdf. 25 July 2005.
[19] Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L (2011) Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs. Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011
[20] Ujjwal Agarwal, K.P Yadav, Upendra Tiwari, International Journal of Research in Science and Technology, 2012, vol. no. 1, issue no. IV, Jan-Mar, "Security Threats in Mobile Ad hoc Networks".
[21] Teerawat Issariyakul, Ekram Hossain, Introduction_to_network_Simulator_NS2.
[22]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 2013: IEEE ICC'13 - Fifth Workshop on Cooperative and Cognitive Networks (CoCoNet5)
[23] Khanh Viet, Brajendra Panda, Yi Hu Korea, "Detecting Collaborative Insider Attacks in Information Systems", 2012 IEEE International Conference on Systems, Man, and Cybernetics October 14-17, 2012, COEX, Seoul, Korea

[24] Tao Gong1 and Bharat Bhargava, "Immunizing mobile ad hoc networks against collaborative attacks using cooperative immune model", SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks 2013; 6:58–68 Published online 26 April 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.530

[25]Amitabh Mishra et al. "INTRUSION DETECTION IN WIRELESS AD HOC NETWORKS",1536-1284/04/$20.00 © 2004 IEEE IEEE Wireless Communications • February 2004

[26]Abhay Kumar Rai , Rajiv Ranjan Tewari ,Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication", International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 265.

