© 2016 IJSRSET | Volume 2 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Detection and Prevention of cooperative Attacks on Mobile Ad hoc networks

M. Karmukil, A. Ramasamy, S. Padmavathi

Department of CSE, Park college of Engineering and Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

In Mobile Ad hoc network Preventing or detecting malicious nodes launching Grayhole or collaborative Blackhole attacks is a challenge. In this paper enhanced CBD Scheme is used to detect the worm whole attack and establishes path in between sender and receiver. Dynamic source routing (DSR)-based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that combines the advantages of proactive and reactive defense architectures. CBDS method using a reverse tracing technique to achieving the stated goal.
Keywords: Mobile nodes, Attacks, CBDS, DSR, AODV, Reverse tracing method.

I. INTRODUCTION

Mobile Ad-hoc Networks (MANETs) are wireless network it uses the node as mobile nodes which communicate without base stations. Nodes in networks which generate user and application traffic and carry out network control and routing protocols. Often changing connectivity, network partitions, higher error rates, collision interference, bandwidth and power constraints together create new problems in network control particularly in the design of higher level protocols.

Wireless devices or nodes that communicate by sending packets to one another without having any central network control to controlling data routing. MANET has no limitation of nodes connectivity and mobility to other nodes, each node acts as a router and network manager. It has a secured transmission and communication in MANET is a challenging and energy issue due to the various types of attacks. To secure the communication in order to understanding the wei security attacks to MANET is a great task and concern. MANETs affects from a different types of security attacks and different threats such as Denial of Service (DOS), flooding attack, selfish node misbehaving, routing table overflow attack, wormhole attack, black hole attack, and so forth.

MANET is open to vulnerabilities such as no point of network management, topology changes vigorously, resource restriction, no centralized authority, to mention a few. The types of attacks on MANET such as Passive, Active attacks and Internal, External attacks and the Routing attacks and Packet Forwarding attacks. Some of these attacks are named as single attacks and multiple node attacks and are malicious. Need to find out the consequences of collaborative attacks and their possible mitigation plans. And the effects of these kinds of attacks on MANET have not been well measured since each researcher offers to use different simulators to visualize those attacks and determine the consequences such as impact on packet delivery ratio, throughput, and end-to end delay.

1.1 Organization

In Section 1 Preliminaries of the paper is described. In section 2 System model is described.

Table 1. Notation used in this paper

Acronym	Definition
DOS	Denial of service
CBDS	Cooperative bait detection scheme
RREQ	Routing request
RREP	Routing response

DSR	Dynamic source routing
DSDV	Destination sequenced distance vector routing

1.2 Preliminaries

This section describes the terms used in this document and an overview of algorithms and protocols

In DSR is a network protocol, which forms on demand route when transmitting a data from one node to another node. It based on source routing. DSR which have two main processes which is route maintenance and route discovery.

ADOV is a network protocol which support MANETs, It creates a route between network nodes when the route requested by the source nodes. It give the flexibility to enter and leaves the network when it's want. The path is only active when the period transmission from source to destination, after completion of transmission the path will time out and closed.

II. SYSTEM MODEL

Dynamic Source Routing (DSR)

DSR is a network protocol, which forms on demand route when transmitting a data from one node to another node. It based on source routing. DSR which have two main process which is route maintenance and route discovery. When node A wants to send a packet to node G, but does not know a route to D, node S initiates a route discovery Source node S floods Route Request (RREQ) – RREQ is a control packet Each node appends its own identifier before forwarding RREQ.

Ad hoc On-Demand Distance Vector (AODV)

ADOV is a network protocol which support MANETs, It creates a route between network nodes when the route requested by the source nodes. Can determine multiple routes between a source and a destination, but implements only a single route, because its Difficult to manage multiple routes between same source/destination pair and If one route breaks, its difficult to know whether other route is available. AODV discovers routes as and when necessary , It will not maintain routes from every node to every other, the Routes are maintained just as long as necessary. It will generate a *route request* (RREQ) message and send to destination. A route is found when the RREQ message reaches either the destination or an intermediate node with a valid route entry. For as long as a route exists between two endpoints, AODV remains path create routes in their routing table Packet Forwarding – Not source routing; intermediate nodes determines next-hop nodes for received packets by looking up their routing tables. AODV utilizes routing tables to store routing information.

2.1 Design Goals

2.1.1 Creation of Network Topology

The source nodes in have no prior knowledge about the attack being performed. That is, make no assumption about the attack goals, method of attack, or mobility patterns. The number of attack and their locations are unknown to the network nodes. Instead of relying on direct knowledge of the attack, suppose that the network nodes characterize the attack impact in terms of the empirical packet delivery rate. Network nodes can then relay the relevant information to the source nodes in order to assist in optimal traffic allocation. Each time a new routing path is requested or an existing routing path is updated, the responding nodes along the path will relay the necessary parameters to the source node as part of the reply message for the routing path. Using the information from the routing reply, each source node is thus provided with additional information about the attack impact on the individual nodes.

2.1.2 CBDS

CBDS is DSR-based. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node a reply forged RREP. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a black hole attack. To resolve this issue, the function of HELLO message is added to the CBDS to help each node in identifying which nodes are their adjacent nodes within one hop. This function

assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes. The baiting RREQ packets are similar to the original RREQ packets, except that their destination address is the bait address.

2.1.3 Bait Setup phase

The bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ that it has used to advertise itself as having the shortest path to the node that detains the packets that were covered. To achieve this goal, the following method is designed to generate the destination address of the bait RREQ. The source node stochastically selects an adjacent node, *nr*, within its one-hop neighbourhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. Since each baiting is done stochastically and the adjacent node would be changed if the node moved, the bait would not remain unchanged. The bait phase is activated whenever the bait RREQ_ is sent prior to seeking the initial routing path. The follow-up bait phase analysis procedures are as follows. First, if the *nr* node had not launched a blackhole attack, then after the source node had sent out the RREQ, there would be other nodes' reply RREP in addition to that of the *nr* node. Therefore, the reverse tracing program in the next step would be initiated in order to detect this route. If only the *nr* node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the DSR route discovery phase. Second, if *nr* was the malicious node of the black hole attack, then after the source node had sent the RREQ_, other nodes (in addition to the *nr* node) would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route.

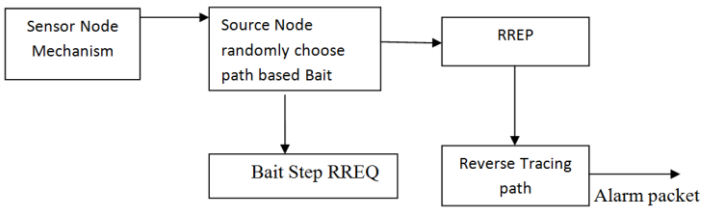
2.1.4 Reverse Tracing Step

The reverse tracing program is used to detect the behaviours of malicious nodes through the route reply to the RREQ_ message. If a malicious node has received the RREQ_, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs. Indeed, when a malicious node, for example, *nm*, replies with a false RREP, an address list $P = \{n1, \ldots nk, \ldots nm, \ldots nr\}$ is recorded in the RREP. If node *nk* receives the RREP, it will separate the *P* list by the destination address *n*1 of the RREP in the IP field and get the address list $Kk = \{n1, \ldots nk\}$, where *Kk* represents the route information from source node *n*1 to destination node *nk*. Then, node *nk* will determine the differences between the address list $P = \{n1, \ldots nk, \ldots nm, \ldots nr\}$ recorded in the RREP and $Kk = \{n1, \ldots nk\}$. Consequently, we get $K\_k = P - Kk = \{nk+1 \ldots nm \ldots nr\}$ (1) where *K_ k* represents the route information to the destination node (recorded after node *nk*). The operation result of *K_ k* is stored in the RREP's "Reserved field" and then reverted to the source node, which would receive the RREP and the address list *K_ k* of the nodes that received the RREP.

2.1.5 Performance Evaluation

Evaluate various aspects of the proposed techniques for detection of attack localization, estimate errors. Simulation setup including parameters such as jammer mobility, errors, detect ratio, packet success rates. Then simulate the process of computing the estimation statistics and for a single link. The effects of the estimation process on the throughput optimization, both in terms of optimization objective functions and the resulting simulated throughput.

System Architecture



III. CONCLUSION

The CBDS mechanism introduced in the existing work for detecting malicious nodes in MANETs under grey/collaborative black hole attacks. The results revealed that the CBDS outperforms the other schemes DSR, 2ACK, and BFTR, in terms of routing overhead and packet delivery ratio. It is necessary to address other types of attacks like worm hole attacks integration of the

CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants.

IV. REFERENCE

[1] Baadache.A and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010

[2] Chang.C, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[3] Corson.S and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). Online]. Available: http://www.elook.org/computing/rfc/rfc2501.html

[4] Deng.H, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[5] Johnson.D and D. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[6] Liu.K, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[7] Marti.S, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[8] Ramaswamy.S, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[9] Rubin.I, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[10] Tsou.C, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5