isrjournals

International Journal of Advanced Research in Computer Science Engineering and Information Technology

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

Collaborative Attack Detection Of Malicious Node In Manet Using Co-Operative Biat Reduction Approach

Mrs.Jeyaselvi.M[1], Aswathi Devi.N.K[2], Athulya Peethambaran[3]

Sr.Asst. Professor, Dept. of Computer Science and Engineering, Agni College of Technology, Chennai. [1]

Student, Dept. of Computer Science and Engineering, Agni College of Technology,Chennai.

ABSTRACT__ *The primary objective is to establish communication among nodes i.e. the nodes should cooperate with each other. In the presence of malicious nodes, this requirement may lead to serious security problem. To detect and to prevent gray hole and collaborative black hole attacks is the major challenge. This project attempts to resolve this issue by designing a Ad-hoc On-Demand Distance Vector (AODV) based routing mechanism, which is referred to as the Cooperative Bait Detection Scheme (CBDS). CBDS method implements a reverse tracing technique.*

Keywords— Cooperative bait detection scheme (CBDS), Ad-hoc On-Demand Distance Vector(AODV), RREQ, RREP, Gray hole and Black hole, malicious node, mobile adhoc network (MANET).

1. INTRODUCTION

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind speed and direction, pressure, etc. Wireless Ad-hoc networks are rapidly gaining popularity as a mode of communication, especially among highly mobile sectors of society.In mobile Ad-hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malicious nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. In this context, preventing or detecting malicious nodes which launches gray or collaborative black hole attacks is a challenge.

This project attempts to resolve this issue by designing a Ad-hoc On-Demand Distance Vector algorithm with cooperative bait detection scheme (CBDS). The CBDS method implements a reverse tracing technique to help in achieving the stated goal. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route, if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbours, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself.

2. SYSTEM ANALYSIS

EXISTING SYSTEM

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as black hole and gray hole (known as variants of black hole attacks). In black hole attacks, a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages. In this case, a malicious node (so-called black hole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that “fake” shortest route to the destination and then discard these packets without forwarding them to the destination. In gray hole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it.

LIMITATION

- Higher energy consumption
- Routing overhead
- Increase time delay

PROPOSED SYSTEM

We propose a Cooperative Bait Detection Scheme (CBDS) that effectively detects the malicious nodes that attempt to launch gray hole/collaborative black hole attacks. The address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a black hole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list.

3. IMPLEMENTATION

3.1 COOPERATIVE BIAT DETECTION SCHEME

We propose a detection scheme called Cooperative bait detection scheme (CBDS),which aims to detect the gray hole/collaborative black hole attacks in MANET. CBDS method implements a reverse tracing technique to help in achieving the stated goal. The CBDS scheme comprises three steps:

1. the initial bait step;
2. the reverse tracing step; and
3. the reactive defense step.

The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step.

A. Initial Bait Step

The goal of 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 converted. 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, i.e., nr, within its one-hop neighborhood 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. If nr deliberately gave no reply RREP, it would be directly listed on the black hole list by the source node. If only the nr node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that nr had provided; in this case, the route discovery phase of

AODV will be started. The route that nr provides will not be listed in the choices provided to the route discovery phase.

B. Reverse Tracing Step

The reverse tracing step is used to detect the behaviors 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.

C. Reactive Defense Step

After the above initial proactive defense (steps A and B), the AODV route discovery process is activated. When the route is established and if at the destination it is found that the packet delivery ratio significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency.

3.2 ADHOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV routing is an algorithm use for finding a route for peer to peer connection between sensors. AODV relies on a broadcast route discovery mechanism, which is used to dynamically establish route table entries at intermediate nodes. Each senors as router and routes are obtain only when needed. AODV will broadcast route request (RREQ) to all and whoever in the range of the frequency being transmitted and awake, they can receive RREQ. Any sensor which meets the information in the RREQ will answer RREQ with route reply (RREP). After the sender gets the RREP, it now has the peer-to-peer connection and ready to send.

The path discovery process of AODV is initiated whenever the source node needs to transmit data to another node, but for which the source node does not have routing information in its table. Each node in the network maintains its own sequence number. A source issuing an RREQ packet also includes its own sequence number and most recent sequence number it has for the destination. Therefore intermediate nodes reply to an RREQ only if the sequence number of their route to the destination is greater or equal to the destination sequence number specified in RREQ packet.

AODV primary objectives are:

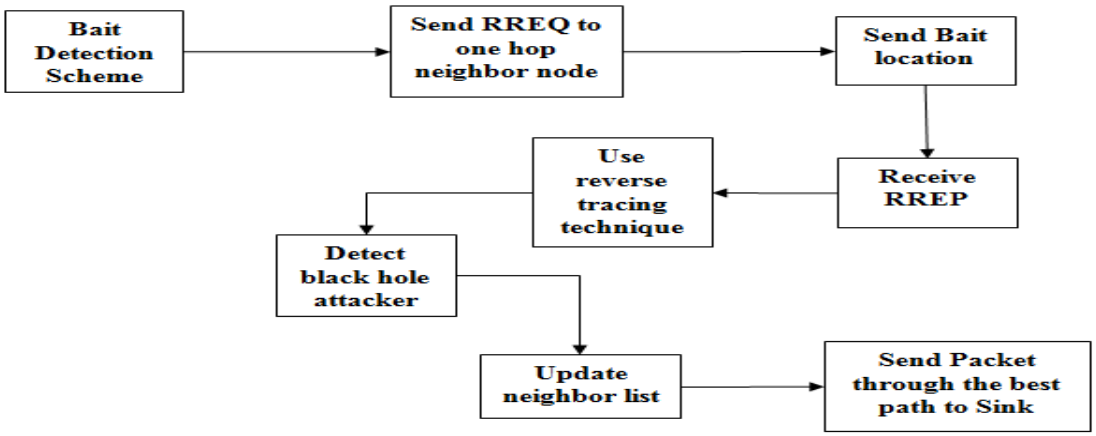
Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

1. To broadcast discovery packets only when necessary.
2. To distinguish between t local connectivity management and general topology maintenance.

Advantage of AODV:

AODV is the simplest and widely used algorithm either for wired or wireless network. The advantages of bandwidth efficiency loop free routing and act as a reactive protocol makes it worth to apply within the network. They provide access to information and services regardless of geographic position. Independence from central network administration. Self-configuring network, nodes are also act as routers. Less expensive as compared to wired network.

4. SYSTEM ARCHITECTURE



5. PERFORMANCE EVALUATION

In this section, we evaluate the performance of simulation. We are using the xgraph for evaluate the performance.

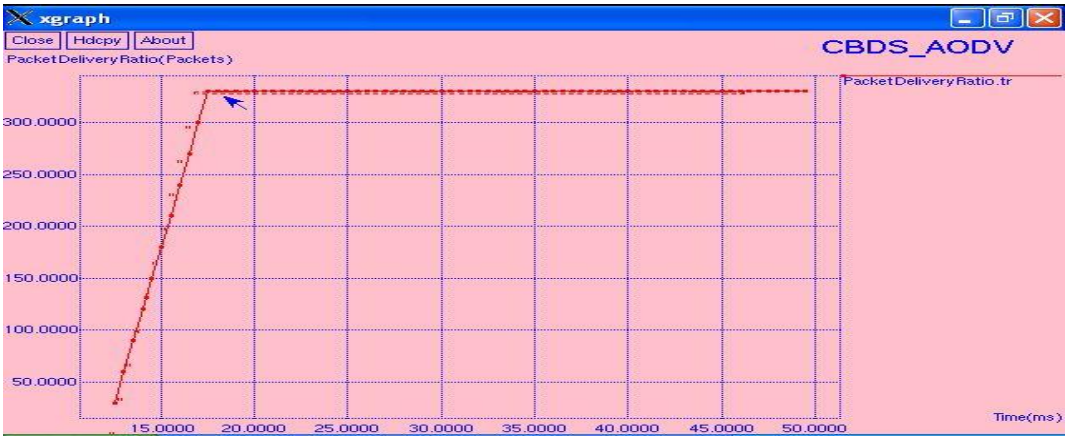
We choose the three evaluation metrics:

1. **Packet delivery ratio** – it is the ratio of the number of packet received at destination and number of packet sent by the source.
2. **End-to-End delay** – the average time taken for a packet to be transmitted from the source to destination,

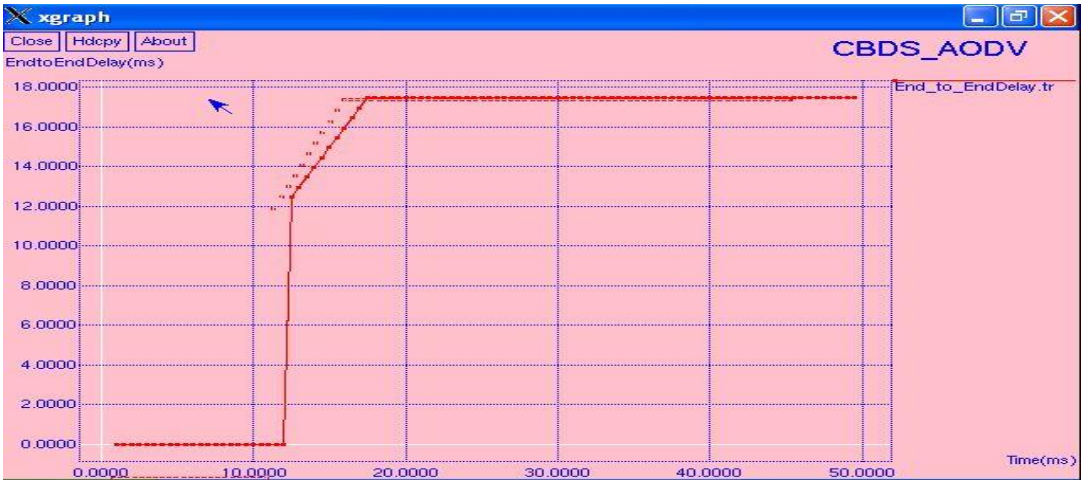
Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337

3. **Throughput** – number of data received by the destination without any losses.

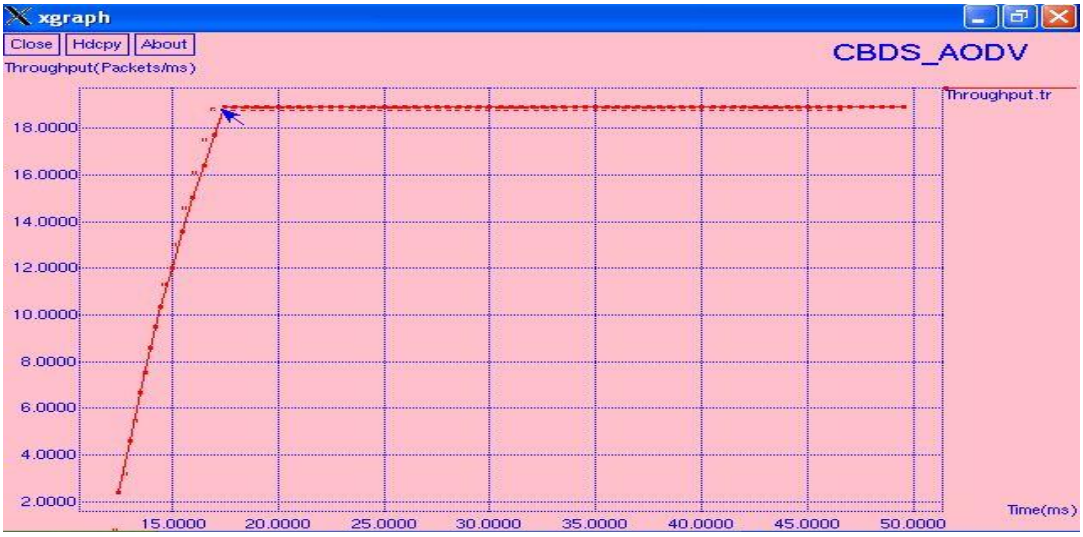
Packet delivery ratio



End-to-End delay



Throughput



6. CONCLUSION AND FUTUREWORK

Conclusion

In this project, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANET's under gray/collaborative black hole attacks. Our simulation results revealed that the CBDS outperforms the AODV, RREQ, RREP and BAIT schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio.

Future Work

Investigate the feasibility of adjusting our CBDS approach to address other types of collaborative attacks on MANETs. Investigate the 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.

REFERENCE:

[1] "Dynamic source routing in Ad-hoc wireless networks," Mobile Comput, 1996, D. Johnson and D. Maltz,.

[2] "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks."Proceedings of the 6th annual international conference on Mobile Computing and Networking, 2000, S. Marti, T. J. Giuli, K. Lai, and M. Baker,.

[3] "Prevention of cooperative black hole attacks in wireless Ad-hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K.Nygard,.

[4]"Prevention of cooperative black hole attack in wireless ad hoc Networks". 570–575, 2003, S. Ramaswamy, H. Fu, M.,Sreekantaradhya, J. Dixon, and K. Nygard.

[5] "A Survey on Intrusion Detection in Mobile Ad Hoc Networks," (Eds.) pp. 170– 196, 2006 Springer, Y. Xiao, X. Shen, and Z. Du,.

[6] "SCAN: Self-organized network-layer security in mobile ad hoc networks," vol. 24, issue 2, pp. 261-273,2006,H. Yang, J. Shu, X. Meng, and S. Lu,.

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

[8] "Preventing cooperative black hole attacks in mobile Ad-hoc networks: Simulation implementation and evaluation" in Proc. IEEE ICC, 2007 H. Weerasinghe and H. Fu, .

[9] "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks,"Pg 310-314,2008, Piyush Agrawal, R. K. Ghosh, Sajal K. Das,.

[10] "Detection and removal of cooperative black/gray hole attack in mobile Ad-hoc networks," Int. J. Comput.Appl., vol. 1, no. 22, 2010, K. Vishnu and A. J Paul,.

[11]"Security Issues in Mobile Ad Hoc Networks- A Survey" Wenjia Li and Anupam Joshi,

Volume: 4, Issue: 3,Special Issue: 1 ,Mar,2016 ,ISSN_NO: 2321-3337