A Survey on Secure Cooperative Bait Detection Approach for Detecting Malicious Nodes in MANETs

Mohan.M
Dept of CSE
Vemana IT,Bengaluru
Email:murali.mohan.iyengar@gmail.com

Ramakrishna.M
Dept of CSE
Vemana IT,Bengaluru
Email:Hodcse@vemanait.edu.in

***Abstract*—** In Mobile Ad-hoc Networks (MANETs), the main problem is the security as well as formation of communication amongst nodes is that nodes must work together with each other. Avoiding or sensing malicious nodes initiation grayhole or collaborative blackhole attacks is the main challenge. Cooperative bait detection approach mixes the advantages of both proactive and reactive defense architectures. Here it uses the technique of transposition for implementing security and the CBDA technique outfits a reverse tracing method to help in attaining the specified aim. The demonstration in the occurrence of malicious-node attacks, the CBDA outperforms the DSR, and Best-Effort Fault-Tolerant Routing (BFTR) protocols in relations to packet delivery ratio and routing overhead. In the transposition method we use the key which is the askey value of the character which is encrypted at sender side and decrypted at receiver.

Keywords- *Cooperative Bait Detection Approach (CBDA), collaborative black hole attacks, grey hole, black hole, malicious node*

*****

I. INTRODUCTION

Mobile ad hoc network (MANET) falls in the category of wireless ad hoc network, and is a self-configuring network. Each device is free to move independently in any direction, and hence will change its link with other devices frequently. Each node must forward traffic which is not related to its own use, and therefore be both a router and a receiver. This feature also comes with a serious drawback from the security point of view. Certainly, the above-mentioned applications impose some severe constraints on the security of the network topology, routing, and data traffic. For example, the existence and collaboration of malicious nodes in the network may disturb the routing process, leading to a faulty of the network operations. The security of MANETs deals with prevention and detection methods to struggle individual misbehaving nodes.

With respect to the effectiveness of these methods becomes weak when multiple malicious nodes conspire together to initiate a collaborative attack, which can result to more shocking damages to the network. These networks are highly susceptible to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks).

II. ROUTING PROTOCOLS

1. There are mainly 4 types of routing protocols they are:

    1. Proactive routing
    2. Reactive routing
    3. Hybrid routing
    4. Hierarchical routing

Proactive routing:

It is a table driven protocol and it maintains renewed lists of destinations and the routes by periodically dispensing routing tables through the entire network. The disadvantage of these algorithms is with respective amount of data for maintenance similarly slow response on rearrangement and failures. Examples of proactive algorithms are Optimized Link State Routing Protocol (OLSR),Destination Sequence Distance Vector (DSDV).

Reactive routing:

It is an On-demand routing protocol it finds the route on demand by overflowing the network with Route Request packets. The disadvantage of these algorithm is high inactivity time in route finding, unnecessary flooding which can lead to network blockage. Examples of on-demand algorithms are Ad hoc On-demand Distance Vector(AODV), Dynamic Source Routing(DSR).

Hybrid routing:

It is the combination of both proactive and reactive routing. The routing is originally recognized with the proactively examined routes and then aids the demand from furthermore started nodes over reactive flooding. The optimum of one or the other method needs prearrangement for usual cases. The disadvantage of these algorithms is it depends on number of additional nodes triggered the response to traffic flow demand depends on ramp of traffic volume. Examples of hybrid algorithms is ZRP (Zone Routing Protocol)

Hierarchical routing:

In this protocol the choice of proactive and reactive routing is dependent on the level in which the node is present. The routing process is primarily recognized with some proactively searched routes and then aids the demand from furthermore activated nodes over reactive flooding on the lesser levels. The dis-advantages of this algorithm is that it depends on complexity of nesting and addressing system and response to traffic request depends on interlocking limits. Examples of hierarchical routing are: CBRP (Cluster Based Routing Protocol), FSR (Fisheye State Routing protocol)

III. BACKGROUND

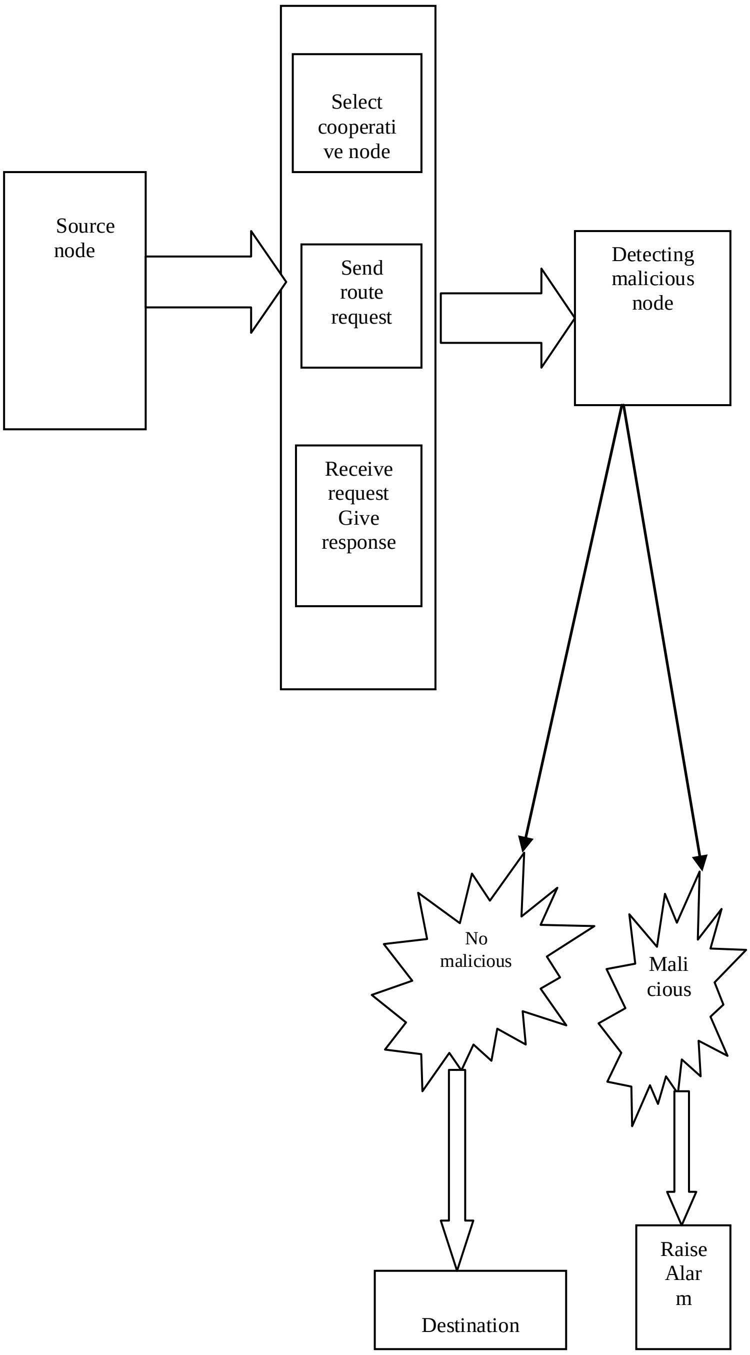
Black hole: A black hole means that the malicious node exploits the routing protocol to claim that it has the shortest path to the destination node, it does not forward packets to its neighbors instead it drops the packets. The main issue is that the PDR decreases.

Gray hole: A Gray hole attack is tougher to detect because nodes can drop packets partially due to its malicious nature or due to overload, congestion and selfish nature of the nodes which are involved in the routing process.

Collaborative Black hole: The malicious nodes cooperate with each other in order to mesmerize the usual into their invented routing information, to hide from the existing detection scheme.

IV. SYSTEM ARCHITECTURE

The source node first identifies all the nodes which forms its neighbors node i.e. which are at particular distance from that node once the neighbor nodes are selected it then sends the destination address to all the neighbor nodes if it is at one hop distance then it has a direct if not then the adjacent node updates the source address by updating it's location in the source address and then it does the same procedure until a route to the destination is found once the path is found then a test packet is sent and the packets is forwarded to the destination.



V. METHODOLOGY

1. Network Model:

It consider a dense multihop static wireless mobile network deployed in the sensing field, it assume that each node has plenty of neighbors. When a node has packets to send to the destination, it launches the on-demand route discovery to find a route if there is not a recent route to a destination and the MAC layer provides the link quality estimation service.

2. Initial Bait:

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, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. First, if the neighbor node had not launched a black hole attack, then after the source node had sent out the RREQ , there would be other nodes' reply RREP in addition to that of the neighbor node. This indicates that the malicious node existed in the reply routing. The reverse tracing program in the next step would be initiated in order to detect this route. If only the neighbor node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDA had initiated the DSR route discovery phase.

3. Initial Reverse Tracing:

The reverse tracing program 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. It should be emphasized that the CBDA is able to detect more than one malicious node simultaneously when these nodes send reply RREPs.

4. Shifted to Reactive Defense Phase:

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. The threshold is a varying value in the range [85%, 95%] that can be adjusted according to the current network efficiency. The initial threshold value is set to 90%. a dynamic threshold algorithm is designed that controls the time when the packet delivery ratio falls under the same threshold. If the descending time is shortened, it means that the malicious nodes are still present in the network. In that case, the threshold should be adjusted upward. Otherwise, the threshold will be lowered.

5. Security Module:

It is going to use the as key value of the message which is going to be sent and then it is added with the public key and sent from the source to destination through the intermediate node and then decrypted in the destination by subtracting the public key from the message obtained and then the original message is obtained from the packets sent.

VI. EXPECTED RESULTS

Packet Delivery Ratio: It is defined as the ratio of the number of the number of packets sent by the source to the packets received at the destination.

Routing Overhead: This metric represents the ratio of the amount of direction finding related control packet transmissions to the amount of data transmissions.

Average End-to-End Delay: It is well-defined as the average time taken for a packet to be transmitted from the source to the destination.

Throughput: It is defined as the total amount of data, that the destination receives them from the source which is divided by the time it takes for the destination to get the final packet.

VII. CONCLUSION

As the transposition security model is applied to the co-operative bait detection approach the data is sent in a secured manner and the packet delivery ratio is also increased and the loss of data packets is reduced.

REFERENCES

[1] Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf.Security, vol. 7,pp 1-5, 2010 .

[2] Patwardhan, J. Parker, A. Joshi, M. Iorga, and T. Karygiannis, "Secure Routing and Intrusion Detection in Ad Hoc Networks," in IEEE International Conference on Pervasive Computing and Communications, pp. 8–12, 2005.

[3] Chang, Y.Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[4] Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002 Book.

[5] P. Agrawal and Q.-A. Zeng, "Introduction to Wireless andMobile Systems", Brooks/Cole Publishing, Aug. 2002 Book.

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

[7] Elizabeth M. Royer, and Chai-KeongToh, "A Review of Current Routing Protocols for AdHoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.

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

[9] H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362–367.

[10] Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, pp. 10, October 2002.

[11] IEEE Standard for Information Technology, IEEE Std 802.11-14997, 1997, Telecommunications and Information

exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY) Specifications, pp. i-445.

[12] Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, “TBONE: A mobile-backbone protocol for ad hoc wireless networks,” in Proc. IEEEAerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[13] J. Lundberg, “Routing Security in Ad Hoc Networks,” Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html

[14] K. Liu, 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.

[15] K. Liu, J. Deng, P. Varshney, K. Balakrishnan, “An Acknowledgment- Based Approach for the Detection of Routing Misbehavior in MANETs,” IEEE Transactions on Mobile Computing, 6(5), pp. 536- 550, 2007.

[16] K. Vishnu and A. J Paul, “Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks,” Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[17] L. Zhou and Z. J. Haas, “Securing Ad Hoc Networks,” IEEE Net., vol. 13, pp. 6-10, Nov./Dec. 1999.

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

[19] P. Michiardi, and R. Molva, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Proceedings of IFIP Joint Working Conference on Communications and Multimedia Security, pp.107-121, 2002.

[20] QualNetSimulaton Tool, Scalable Network Technologies. (Last retrieved March 18, 2013). [Online]. Available: http://www.qualnet.com

[21] Q. He, D. Wu, and P. Khosla, “Sori: A secure and objective reputation based incentive scheme for ad hoc networks,” in IEEE WCNC, 2004 Book.

[22] S. Buchegger and J.-Y. L. Boudec, “Self-policing mobile ad-hoc networks by reputation systems,” IEEE Communications Magazine, pp. 101-107, 2005.

[23] S. Corson 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

[24] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routingmisbehavior in mobile ad hoc networks,” in Proceedings of the 6thAnnual international Conference on Mobile Computing and Networking(MobiCom), pp. 255-265, 2000.

[25] S. Ramaswamy, 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.

[26] W. Kozma and L. Lazos, “REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits,” in Proc.WiSec, 2009, pp.103–110.

[27] W. Wang, B. Bhargava, and M. Linderman, “Defending against collaborative packet drop attacks on MANETs,” in Proc. 28th IEEE Int. Symp.Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[28] Y.-C. Hu, A. Perrig, D.B. Johnson, “Packet leashes: a defense against wormhole attacks in wireless networks,” in IEEE INFOCOM, pp. 1976- 1986, 2003.

[29] Y. Hu, A. Perrig, and D. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Wireless Networks, 11(1):21–38, 2005.

[30] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad hoc routing service in adversarial environments,” Wireless Pers.Commun., vol. 29, pp. 367– 388, 2004.

[31] Fan-Hsun Tseng1, Li-Der Chou1 and Han-Chieh Chao “A survey of black hole attacks in wireless mobile ad hoc networks” Human-centric Computing and Information Sciences 2011, 1:4

[32] Madhusudhananagakumar KS, G. Aghila “A Survey on Black Hole Attacks on AODV Protocol in MANET” International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011.