ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

A Survey on Various Mechanisms to Detect and Remove Collaborative Attacks in MANETs

Supreetha.S, Vinodha.K

M.Tech Student, Dept of ISE, The Oxford College of Engineering Bangalore, India

Associate Professor, Dept of ISE, The Oxford College of Engineering Bangalore, India

ABSTRACT: Mobile Adhoc Network (MANET) are used most commonly all around the world.This is because the mobile nodes has the ability to communicate with each other without any fixed network.The nodes in mobile adhoc network has the tendency to make decisions on its own that is autonomous state.A security solution is very much needed for networks to protect both route and data forwarding operations in the network layer .Security is an essential requirement in MANET.Without any proper security solution ,the attacker node in the network will act as a normal node which causes eavesdropping and selective forwarding attack generally known as Gray hole attack.In this paper a survey about various security mechanisms for Gray Hole attack is proposed to detect and remove collaborative Gray Hole attack that occurs in network layer in MANETs.

.

KEYWORDS: MANETs; GrayholeAttack; Blackhole Attack

I. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a network consisting of a group of mobile nodes that cooperate and forward packets to each other. MANETs extend the limited wireless transmission range of each node by multi-hop packet forwarding, and thus they are ideally suited for scenarios in which pre-deployed infrastructure support is unavailable.

MANETs have some special characteristic features such as unreliable wireless links used for communication between hosts, constantly changing network topologies, limited bandwidth, battery power, low computation power etc. While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are either absent or less severe in wired networks. MANETs are vulnerable to various types of attacks such as passive eavesdropping, active interfering, impersonation, and denial-of-service. Intrusion prevention measures such as strong authentication and redundant transmission should be complemented by detection techniques to monitor security status of these networks and identify malicious behavior present in some of the participating node(s).

One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. A set of nodes may be compromised in such a way that it may not be possible to detect their malicious behavior easily. Such nodes can generate new routing messages to advertise non-existent links, provide incorrect link state information, and flood other nodes with routing traffic, thus inflicting Byzantine failure in the network. In this paper, a discuss on mechanisms to detect and remove one such attack known as gray hole attack is provided and also a mechanism called CBDS used to detect black hole attack is adjusted to detect grayhole attack in MANETs.

II. RELATED WORK

Detection mechanisms proposed so far can be grouped into two broad categories.

1) Proactive detection schemes
2) Reactive detection schemes

Proactive Detection Schemes are schemes in which the nearby nodes will be constantly monitored. In these schemes, regardless of the existence of attacker nodes, the overhead of detection is constantly incurred, and the resource used for detection is constantly wasted. However, one of the advantages of this scheme is that it can help in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

preventing or avoiding an attack in its beginning stage.Reactive detection schemes are triggered only when the destination node detects a significant drop in the packet delivery ratio.

Watchdog: Marti *et al*. [1] proposed a scheme named Watchdog.This approach aims to improve the throughput of network in the presence of attacker nodes. In fact, the Watchdog scheme consists of two parts, namely, Watchdog and Pathrater. Watchdog serves as an IDS for MANETs. It is responsible for detecting attacker node misbehaviors in the network. Watchdog detects malicious misbehaviors by listening to its next hop's transmission promiscously. When a node fails to forward the packet to its adjacent node within a certain period of time, the watchdog node increases the failure counter of that node. Whenever a node's failure counter exceeds a predefined threshold, the Watchdog node reports that node as misbehaving. Finally, the Pathrater avoids the reported nodes in future transmission by cooperating with the routing protocols.

TWOACK:

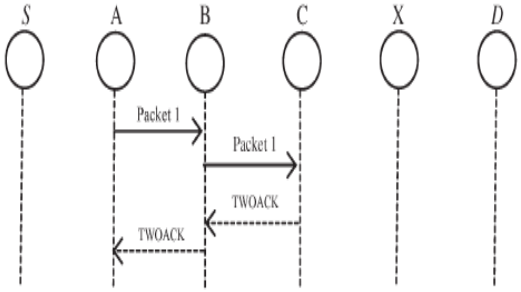

Fig1.TWOACK Scheme

Liu *et al.* [1]proposed a scheme called TWOACK. TWOACK detects misbehaving links by acknowledging every data packet transmitted over every three consecutive nodes along the path from the source to the destination.Uponrecieving a packet, each node along the route is required to send back an acknowledgment packet to the node that is two hops away from it down the route. TWOACK works on routing protocols such as Dynamic Source Routing (DSR)

BFTR :Xue and Nahrstedt[2] proposed a prevention mechanism called best-effort fault-tolerant routing (BFTR). The BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path measured in terms of packet delivery ratio and delay has to be chosen by the destination node. If the behavior of the path changes from a predefined behavior then a set of "good" routes is determined, and the source node uses a new route. One of the drawbacks of BFTR is that attacker nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, leading to significant routing overhead.

JaydipSen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar[3] has proposed a mechanism consisting of four security procedures which are invoked sequentially. The security procedures are: (1) Neighborhood data collection, (2) Local anomaly detection, (3) Cooperative anomaly detection, and (4) Global alarm raiser. The proposed security mechanism increases the reliability of detection by proactively invoking a collaborative and distributed algorithm. Detection decision works on a consensus algorithm based on threshold cryptography.

P. Agrawal et al [4] proposed a technique for detecting chain of cooperating attacker nodes (black and gray hole nodes) in ad hoc network. In this technique initially a backbone network of strong nodes that are capable of tuning its antenna to short (normal) as well as to long ranges are established over the ad hoc network. Each strong node is assumed to be a trustful node. These trustful strong nodes detect the regular nodes having low power antenna if they act maliciously. With the assistance of the backbone network of trustful nodes, an end-to-end checking is carried out at the source and the destination nodes to determine whether the data packets have reached the destination or not. If the checking results indicates a failure then the backbone network initiates a protocol for detecting the attacker nodes. For detecting attacker

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

node strong node associated with source node broadcasts a find chain message to the network containing the id of the node replied to RREQ. On receiving find chain message strong node associated with destination node checks a list ofGrayHole Chain to contain the id of the node that replied to RREQ. It then instructs all the neighbors of that node to vote for the next node to which it is forwarding packets. If the next node id is null then the node is a black hole node. Then the grayhole removal process is terminated and a broadcast message is sent across the network to alert all other nodes about the nodes in GrayHole Chain to be considered as malicious. Else strong node will elect the next node which replied to RREQ is forwarding the packets based on reported reference counts. Then again broadcast the find chain message containing the id of the elected node. The main disadvantages of this algorithm are the difference between the regular node and backbone node in the network in terms of power, antenna range which makes it unsuitable for all types of mobile ad hoc network. Also it is not proved that backbone network is optimal in terms of minimality and coverage. Algorithm will fail if the intruder attacks strong nodes since it violates the assumption that strong nodes are always trusted node.

Madhuri Gupta & Krishna Kumar Joshi[5] proposed a mechanism for detection of Gray Hole attacks in Mobile Adhoc Networks in the paper " An Innovative Approach To Detect Gray Hole attack in AODV based MANET". The algorithm proposed is implemented on a very popular on demand routing protocol known as AODV (Ad hoc On demand Distance Vector) routing protocol. The beauty of this proposed algorithm is that it not only identifies the grayhole attacker node but also confirms it. The algorithm is divided into two phases: Noticing Phase and the Confirmation phase. In the noticing phase, for communicating with the destination nodethe Source node (S) first finds the route for the destination node. For this purpose it prepares a RREQ (Route REQuest) packet, in which it fills the address of the destination node (called as DSTO) and this packet is broadcasted to the neighboring nodes. After that, the source node waits for all the replies sent by the neighbouring nodes in terms of the RREP (Route REPly) packets and after getting all the replies from the replying nodes, it sorts these replies in terms of the Decreasing order of the destination sequence numbers (DSN) into its own Route Record (RR). Means, a RREP containing highest DSN is stored on top of the RR table. Now, the source node compares the DSN of the first entry from the R-R table with the Threshold value (TV), which is average of all the DSNs of the replying nodes. Now, If DSN of the first node is much greater than TV the source node lists this node as attacker node and initiates the second phase. In the Confirmation phase, Source node sends a new RREQ packet for a new destination, known as Virtual Destination (DSTV) and waits for the reply coming from the replying nodes containing the paths from the source node to this virtual node. And stores the replies in terms of their DSNs, and picks the first entry from the RR table and compare it with the TV and if it is much greater than the TV and checks that node is the same which is already considered as the noticing node in the previous phase then confirm it as Grayhole attacker node. And after confirming the grayhole attacker node it broadcasts the information about this node to all other nodes and then they remove the entry of this grayhole node from their route cache.

A detection scheme called the cooperative bait detection scheme was proposed byJian-Ming Chang et al . It aims at detecting and preventing attacker nodes launching black hole andgray hole attacks in MANETs.In this approach , the source node stochastically selects an adjacent node with which to cooperate, that is the address of this node is used as bait destination address to bait the attacker nodes to send a reply RREP message. Attacker nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node to the source node to initiate the detection mechanism again. The CBDS scheme takes the advantage of proactive detection in the first step and the superiority of reactive response at the subsequent steps.The CBDS scheme comprises of three steps: 1)The initial bait step 2)The initial reverse tracing step 3)The shifted to reactive defense step.

III.CONCLUSION

Security is the most important concern in MANETs. The misbehavior of the nodes will cause severe damage to the whole network .The dynamic nature of MANETs make them prone to different limitations &weakness.Due to their Occasional misbehaviour ,gray holes are very difficult to detect .In this paper many mechanisms to detect and remove Gray Hole attacks have been discussed. The aim is to detect &mitigate the false node that acts like a normal node.The main goal of all the mechanism is improvement of security as well as the performance of the network .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

REFERENCES

1. Elhadi M. Shakshuki, *Senior Member, IEEE,* Nan Kang, and Tarek R. Sheltami, *Member, IEEE* "EAACK—A Secure Intrusion-Detection System for MANETs" IEEE Transactions On Industrial Electronics, VOL. 60, NO. 3, March 2013
2. Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," *Wireless Pers.Commun.*, vol. 29, pp. 367– 388, 2004.
3. JaydipSen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar Embedded Systems Research Group, Tata Consultancy Services "A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks" 1-4244-0983-7/07/$25.00 ©2007 IEEE
4. PiyushAgrawal, 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
5. Madhuri Gupta and Krishna Kumar Joshi, " An Innovative Approach to Detect the Gray-Hole Attack in AODV based MANET",International Journal of Computer Applications (0975 – 8887) Volume 84 – No 8, December 2013
6. PrathibhaBhat S, VijayaMurari. T *CSE, NMAM Institute of Technology, Nitte, Karnataka, India,* " Detecting and Removing Cooperative Black or Gray Hole Attacks in MANET**"** International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)
7. V. ShanmuganathanMr.T.Anand M.E,"A Survey on Gray Hole Attack in MANET",IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012
8. 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
9. 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.
10. 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.

BIOGRAPHY

Ms.Supreetha S , a Student of Information Science and Engineering Department at The Oxford College Of Engineering-Bangalore , affiliated to VTU pursuing M.Tech in Computer Networking and Engineering. She Recieved Bachelors of Engineering in Computer Science and Engineering from Govt SKSJTI College of Engineering –Bangalore affiliated to VTU.She is currently a research assistant under the Guidance of Associate Professor VinodhaK.Her research interests are Computer Networks and Information Security.

Mrs.VinodhaK ,an Associate Professor in Information Science and Engineering Department at The Oxford College Of Engineering – Bangalore ,affiliated to VTU. She has an Experience of 10 years in Teaching at The Oxford College Of Engineering.She is pusuingPhd in Computer Science and Engineering.Sherecieved Masters of Engineering in Computer Science and Engineering .She Recieved Bachelors of Engineering in Electronics And Communication .Her research interests are Computer Networks and Distributed Networks.