Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 3159-0040
Vol. 2 Issue 7, July - 2015

The Truelink Based Gray Hole Attack Detection In MOBILE AD-HOC NETWORK (MANET)

Mr Parineet D Shukla
Sinhgad Institute of Technology, Lonavala, Pune, India.
Savitribai Phule Pune University, Pune.
sh.neet11@gmail.com

Prof. Ashok M Kanthe
Sinhgad Institute of Technology, Lonavala, Pune, India.
Savitribai Phule Pune University, Pune.
ashokkanthe@gmail.com

***Abstract*—The mobile Ad-hoc network does not have the fixed topology. The nodes are in moving state and participate in the communication. Due to open network it is more prone to the attack. The various attacks can be possible as any malicious node can enter into the communication. The gray hole attack is DoS kind of attack which drops the partial packets passing through them. Due changing behavior of the node from black to honest, it is difficult to detect the malicious node in the network.**

The proposed work implements the TrueLink concept to detect and remove the gray hole attack. The gray hole attack is difficult to detect because of the changing behaviour of the nodes. In gray hole attack, the nodes are always in changing state i.e. from honest node to black hole node and viceversa. In Truelink, the valid node between the two nodes is verified and depending on that the malicious node is detected.

Keywords—gray hole attack, mobile devices, TrueLink, malicious

I. Introduction

A mobile Ad-hoc network is a collection of autonomous systems. The network is independent of infrastructure and hence it reduces the cost and deployment time. The MANET is highly susceptible to various routing attacks. In gray hole attack, the node drops some amount of packets and hence ultimately affects the performance of the network. The node can act in two states as an honest node and as a black hole where all the incoming packets are dropped. The node changes its state from honest to black and vice versa.

The gray hole attack is difficult to detect because some amount of packets may get dropped by the network congestion and some other issues in the network. The partial dropping of packets affects the efficiency of the network hence it's important to detect and remove the gray hole in the established network. The gray hole attack is difficult to detect because some amount of packets may get dropped by the network congestion and some other issues in the network. The partial dropping of packets affects the efficiency of the network hence it is important to detect and remove the gray hole in the established network.

This paper proposes an algorithm based on the TrueLink concept. The TrueLink is used to verify the valid link between the two nodes. Depending on the link between the two nodes, the node can be detected as a malicious node. This paper is organized like section II discusses about related work, section III discusses about MANET and gray hole attack, section IV discusses about TrueLink, Section V discusses about the Gray hole attack detection and removal using TrueLink, Section VI discusses about simulation result and analysis and Section VII describes the conclusion.

II. Related Work

This section gives the information about the previous research work done related to gray hole attack.

J. Hoebeke et al. [1] have given the overview of mobile Ad-hoc network. The applications and challenges of mobile Ad-hoc networks are explained. The authors have explained the evolution and advantages of MANET over wireless network with proper infrastructure as well as applications in the field of tactical networking, emergency services, commercial and civilian environments, home and enterprise networking, education, entertainment, sensor network, context aware services and coverage extension. The various challenges for the MANET are also given.

S. Jain et al. [2] have proposed an algorithm to find the chain of a malicious co-operative node in an Ad-hoc network that disrupts the transmission of data. The algorithm is developed for checking the behavior of a particular node by its neighboring node. When the packets are forwarded from a source to the destination the packet travels through the various nodes, so each node maintains the behavior of a neighbor node. By monitoring the behavior of the node, the malicious node can be detected.

A. Kanthe et al. [3] have proposed a gray hole detection mechanism based on the false replies getting from the node. The counter is used to maintain the count of false replies. The proposed algorithm totally depends on the count of false replies. When the node switches from honest to black and vice versa the node produces the false replies. This information is stored in the local buffer and depending on that the malicious nodes are detected and removed from the network.

G. Wahane et al. [4] have proposed the detection of cooperative black hole and crosschecking it with TrueLink. The TrueLink is used cross check the detection of cooperative black hole attack. The DRI table entries are used to detect the black hole attack.

J. Eriksson, S. V. Krishnamurthy, M. Faloutsos [5] proposed a True-link concept for detecting the gray hole attack. Using True-link, a node can verify the existence of a direct link to an apparent neighbor. Verification of a link operates in two phases. In the rendezvous phase, the nodes exchange nonce. The TrueLink concept is totally based on the timing constraint so that the node does not enter into the network.

III. MANET AND GRAY HOLE ATTACK

Opposed to infrastructure wireless networks, where each user directly communicates with an access point or base station, MANET, does not rely on a fixed infrastructure for its operation. The network is an autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other's send range can communicate directly and handle dynamically discovering each other. Devices are free to join or leave the network and they may move randomly, possibly resulting in rapid and unpredictable topology changes.

Gray hole attack is the attack on the mobile Ad-hoc network. In gray hole attack, a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray hole nodes in MANETs are very effective [6]. Every node maintains a routing table that stores the next hop node information for a route a packet to a destination node, when a source node wants to route a packet to the destination node, it uses a specific route if such a route is available in its routing table. Otherwise, the node initiates a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors. On receiving the RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to a destination. In some other gray hole attacks, the attacker node behaves maliciously for the time until the packets are dropped and then switch to their normal behavior.

The gray hole attack is a kind of denial of service (dos) attack in mobile Ad-hoc networks. It is a specialized type of black hole attack that changes its state from honest to malicious and vice versa. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to congestion.[8] A gray hole attack is an event that degrades the overall network's performance by intentional malicious activity.

IV. TRUELINK [5]

The adjacency of an apparent neighbour can be easily verified with the help of Truelink, using a combination of timing and authentication. Truelink helps to check the authentication of the nodes participating in the communication. The intermediate nodes are checked for the reliability of the communication. TrueLink is used with a secure routing protocol. Authentication is an essential component of such protocols, and TrueLink can use any such mechanism for its authentication needs. TrueLink performs link verification between two nodes i and j in two phases: the rendezvous phase, and the authentication phase. In the rendezvous phase, i and j exchange nonce _j and _i, where the subscript indicates the node that generated the nonce. The time constraint is an important factor to check the adjacency of the neighboring node; only a direct neighbor can respond in time. In the authentication phase, i and j each sign and transmit the message (_j, _i), mutually authenticating themselves as the originator of their respective nonce. The timing constraints of the rendezvous phase makes TrueLink immune to limits the range of attacks based on bit-by-bit or "cut-through" forwarding. TrueLink combines many attractive features, which make it a good candidate for practical deployment:

Deployability with minimal requirements:

TrueLink does not rely on precise clock synchronization, GPS coordinates, overhearing, or geometric or statistical methods.

Backwards compatibility with IEEE 802.11:

TrueLink can be implemented using standard IEEE 802.11 hardware with a minor, backwards compatible, firmware update. TrueLink enabled terminals continued to interoperate with non-enhanced 802.11 hardware, albeit without TrueLink protection.

Compatible with most authentication methods:

TrueLink can be used equally well with asymmetric, symmetric, hash based or other authentication mechanisms.

Widely applicable:

TrueLink is independent of the routing protocol used and improves the security of both proactive and reactive routing protocols.

TrueLink effectively protects the network against such attacks and the cost of protection with TrueLink is small.

TrueLink verifies the adjacency of any neighbour, using a combination of timing and authentication. TrueLink is used as an extension to the IEEE 802.11 MAC layer. TrueLink verification between two nodes i and j operates in two phases. In the rendezvous phase, i and j exchange nonces randomly generated numbers. This phase is completed as a single RTS-CTS-DATA-ACK exchange. The timing constraints in

the IEEE 802.11 standard make it extremely difficult for an attacker to relay these frames successfully. In the authentication phase, i and j each transmit a signed message (_j, _i), mutually authenticating themselves as the originator of their respective nonces.

V. Gray Hole Attack Detection Using Truelink

The proposed work is used to detect the malicious nodes from the network. The TrueLink concept is used to detect the malicious node. The detection of the truelink is based on the number of packets forwarded by the node in particular time frame. The node forwards each and every packet coming to it. When the packet is forwarded from one node to another the forwarding nodes forwards the packet in RTS-CTS-DATA-ACK exchange. This exchange is done in single phase. The TrueLink is implemented in two phases rendezvous and authentication phase. In rendezvous phase the data is exchanged between the neighboring nodes. The authentication phase is validation of the node i.e. the node authenticates itself as a originator of the message. Depending on this the link between the two nodes is verified. When the link between the nodes is valid then the node will not drop the packet. When the link is not TrueLink, the node can drop the packet. To detect the gray hole attack the link is checked multiple times when the link is not TrueLink in multiple check at such times the node can be detected as a malicious node.

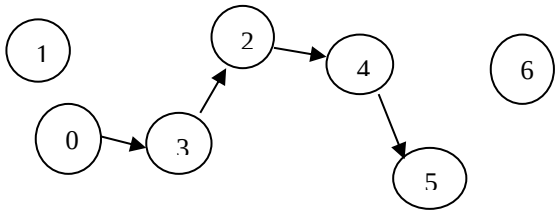

Figure 1: Scenario for Gray hole attack

Figure 1 shows the scenario for detection of gray hole attack. Here node “0” is Source and node “5” is destination. The path established between node “0” and “5” is 0-3-2-4-5. Here node 2 and 4 are acting as a gray hole nodes.

The TrueLink is implemented as follows:

The rendezvous phase is implemented as a single RTS-CTS-DATA-ACK exchange. We describe the operation of the protocol for each of these frames. The rendezvous operation includes following steps:
Request to Send (RTS) : Node i called initiator, calls init ( ). Node i sends an RTS to node j.
Clear to Send (CTS (αj)): After receiving the RTS, node j calls HandleRTS ( ). A locally generated value αj is included in the CTS, which is sent after a delay of one Short Interframe Space (SIFS), is the small time interval between the data frame and its acknowledgment.
DATA (βi): Having received the CTS, i generate value βi. After a SIFS delay, the nonce is sent as the packet payload, together with a header, identifying the packet as a rendezvous packet.

ACK: When node j receives the payload packet containing values βi, the HandleRTS ( ) function sends the ACK frame, after a SIFS delay. The received packet and the locally generated values αj are handed to the upper layer for processing. When node i receives the ACK, the init () function at i returns the pair (αj , βi) to its caller.

Algorithm to detect a gray hole node from the network:

SN: Source node DN: Destination node IN: Intermediate node
α,β: nonce key DRI: Data Routing Information
Step 1: SN broadcasts the RREQ packet
Step 2: SN receives RREP
Step 3: if RREP is from any IN then
Step 4: SN verify the RREP of the node which sends RREP
Step 5: SN verify updates entry of DRI value of the intermediate node that initialized RREP
Step 6.then sendRTS();
Step 7.# recvCTS() times out after ttimeout = SIFS
Step 8.α=recvCTS();
Step 9.if α != nil then
Step 10.β->nonce();
Step 11: # success = true if ACK received
Do reactive Link verification and routing method
Step 12 success=sendPacket([VerifyLink,β]);
Step 13.if success == true then
Step 14: Consider the route to be safe and start routing the data packets
Step 15: else Add node as suspect list
Step 16: check again for number of packets transmitted
Step 17: if SEQUENCE_NUMBERS > max_val and
max_val > MAX_SEQ_TH then
Detect node as malicious node.
Else the node is not malicious.

VI. Simulation Result and Analysis

The proposed algorithm is simulated in Network Simulator (NS-2). NS-2 is open source network simulation tool. The 802.11 MAC layer implemented in ns-2 is used for simulation. The protocol used is AODV. The various parameters are considered to compare the results.

Table 1: Scenario for Mathematical Mode

PARAMETER	USED IN SIMULATION
Channel Type	Channel/Wireless Channel
Antenna type	Omnidirectional
Radio propagation model	Two-ray ground
Link Layer type	LL
MAC type	IEEE 802.11
Protocol for simulation	AODV
Number of packets	50
Number of nodes	30
Simulation time	100 second
Pause time	0.07 second
Area(meter square)	300*300 m2

Table 1 shows the simulation parameters that are used in the simulation. The performance of the network is studied with the help of the graphs plotted with respect to parameters such as throughput, packet delivery ratio, energy, jitter plotted versus the pause time.

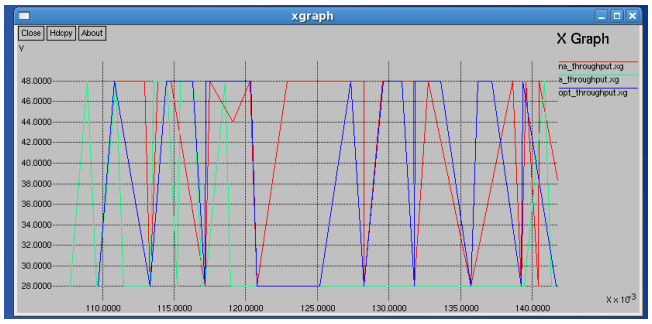

Figure 2 Throughput Vs. Pause time

Figure 2 shows the graphs generated between the throughput and the pause time. Figure 2 shows that when the attack occurs in the network the throughput decreases as compared to the throughput in the normal scenario. After removing the gray hole attack from the network the throughput is improved.

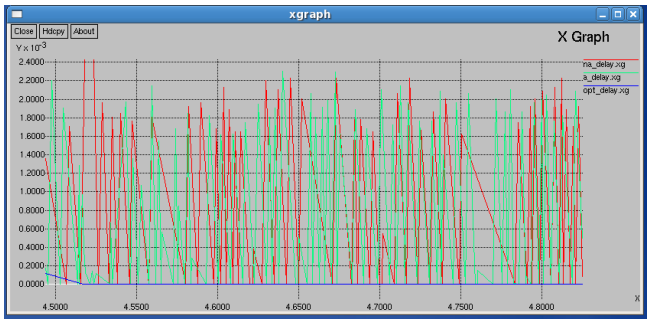

Figure 3 Delay Vs. Pause time (second)

Figure 3 shows the variation in delay with respect to pause time under normal scenario, with attack scenario and attack with solution. Figure 3 shows, when the network is under attack the packet delivery ratio decreses as compared to normal scenario. When the gray hole is detected and removed from the network the delay is minimum.

Figure 4 shows the performance of the network in terms of energy. Figure 4 represents variation of energy with respect to pause time. The figure shows that the energy of the nodes decreases as the network is under attack because the malicious nodes are dropping the packets passing through it and by processing more packets.

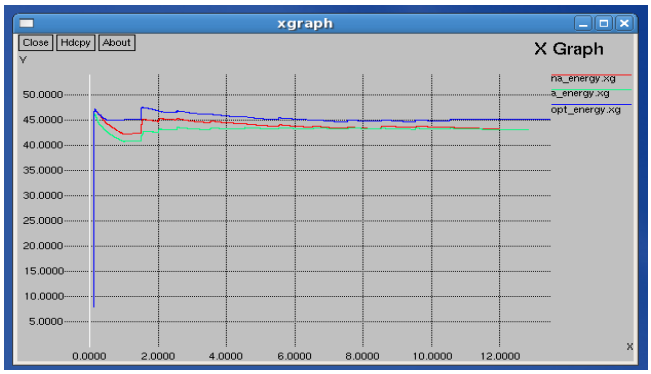

Figure 4 Energy Vs. Pause time

VII. Conclusion

The performance of the network is totally dependent on the behavior of the nodes in the network. For securing the network it is important that each node in the network must be honest node i.e. it must forward all the incoming packets to next node in the path. When a malicious node is present in the path the proper transmission of data is not possible. When a node drops some packets the data which is to be transmitted does not reach to the destination correctly. Detection of gray hole attack is important to ensure proper transmission of data. Because of partial dropping of packets, it is difficult to detect the gray hole in the network.

TrueLink is helpful for verification of the valid link between the neighboring nodes. Depending on how much packets are forwarded by the particular node the node can be detected as the malicious node. The proposed solution reduces the routing overhead by reducing the calculations at each node. Due to continuous changing state of the nodes from honest to black and vice versa the gray hole detection is difficult. So the proposed work will be helpful to keep the nodes with valid link in the network and establish the path through those nodes.

References

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, “An Overview of Mobile Ad-Hoc Networks: Applications and Challenges.” (July 2004). Journal of Communication Network, 3,60-66.0

[2] Shalini Jain, Mohit Jain, Himanshu Kandwal, “Advanced Algorithm for Detection and Prevention of Co-operative Black and Gray Hole Attacks in Mobile Ad-Hoc Networks, International journal of computer Applications (0975-8887) volume 1-No. 7, 2010.

[3] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad, “A Mechanism for Gray Hole Attack Detection in Mobile Ad-Hoc Networks.” International Journal of Computer Application (0975-8887) Volume 53-No 16, September 2012.

[4] G. D. Wahane, A. M. Kanthe, D. Simunic, “Technique for detection of Cooperative black hole attack using Crosschecking with True-Link in MANET ” , IEEE ICCIC 2014, Coimbatore

[5] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, “TrueLink: A practical countermeasure to the wormhole attack in wireless networks”, 2011. The Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program.

[6] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P Balamurlidhar, “A Mechanism for Detection of Gray Hole Attack in Mobile Ad-Hoc Network”, ICICS, IEEE, 1-4244-0983-7/07, 2007.

[7] The network simulator ns 2.35. http://www.isi.edu/nsnam/ns/1997.