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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

A Probabilistic Black hole & gray hole attacks Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks-Review

Yogita Avinash Chaudhari

Student, Master of Engineering, Department of Computer, North Maharashtra University, Jalgaon, Maharashtra, India

ABSTRACT: Malicious and selfish nature displays a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). Due to the unique characteristics of network, designing a misbehavior detection scheme in DTN is regarded as a great research. In this paper, we propose iTrust, misbehavior detection scheme that uses a probability, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a regularly available Trusted Authority (TA) to judge the node's behavior based on the routing evidences collected and probabilistically checking.

KEYWORDS: Greyhole attack; Blackhole attack; Networking; Multiple attack detection; Mobile Ad hoc Network.

I. INTRODUCTION

Mobile Ad hoc Networks Mobile ad hoc network is an autonomous system, where nodes/stations are connected with each other through wireless links. There is zero restriction on the nodes to join or leave the network, there as the nodes join or leave freely. Mobile ad hoc network topology is dynamic which can change randomly because the nodes move very freely and can re-organize themselves dynamically. This property of the nodes makes the mobile ad hoc networks much unpredictable from the point of view of getting scalability and topology.

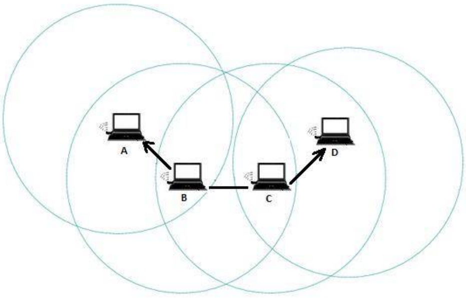


Fig. 2.2 Mobile Ad Hoc Network

DOI: 10.15680/IJIRCCE.2017. 0502003

Characteristics of MANETs

When a node wants to connect with another node, the destination node must lies within the radio range of the base node that wants to initiate the communication. The intermediate nodes within the network helps in routing the packets for the source node to the destination node. These networks are fully self organized, having the capacity to work anywhere without any added infrastructure. Nodes are highly autonomous and play the role of packet router and host at the same time. MANET is self governing network, where there is no centralized control and the communication is carried out with mutual trust on each other amongst the nodes. The network can be set up anywhere without any geographical restrictions. One of the drawbacks of the MANET is the limited energy resources of the nodes.

Types of Mobile Ad Hoc Network:
1. Vehicular Ad Hoc Networks (VANET's)
2. Intelligent Vehicular Ad Hoc Networks (InVANET's)
3. Internet Based Mobile Ad Hoc Networks (iMANET's)

1 Vehicular Ad Hoc Networks (VANET's)

VANET is a type of Mobile ad hoc network where vehicles are equipped with wireless and form a network without help of any additional infrastructure. The equipment is placed inside vehicles as well as on the road for providing access to other vehicles in order to form a network and communicate.

2 Intelligent Vehicular Ad Hoc Networks (InVANET's)

Vehicles that form Mobile Ad Hoc Network for connect using WiMax IEEE 802.16 and WiFi 802.11. The main aim of designing InVANET's is to avoid vehicle collision so as to keep passengers as safe as possible. This also help drivers to keep safe distance between the vehicles as well as help them at knowing how much other vehicles speed are approaching. InVANET's applications are also employed for military purposes to connect with each other.

3 Internet Based Mobile Ad Hoc Networks (iMANET's)

These are used for linking up the mobile nodes and fixed internet gateways. In these networks the normal routing algorithms does not apply [2].

Applications of MANETs

The properties of MANET make it so much favorable that would bring so many benefits. There are so many research areas in MANET which is under studies now. The most important area is vehicle to vehicle communication. Where the vehicle would connect with each other, keeping a secure distance between them as well as collisions warning to the drivers. MANET can be used for fully automated battlefield and war games. One of the most important areas where MANETs are applied is emergency services such as relief activities and disaster recovery, where traditional wired network is already destroyed. There are so many other application areas such as entertainment, education and commercial where MANETs are playing their role for connecting people.

Short comings of Mobile Ad Hoc Networks

Some of the disadvantages of MANETs are as follows.

- Limited Resources.
- Scalability problems.
- No central check on the network.
- Dynamic topology, where it is hard to find out malicious nodes.

MANETs Routing Protocols

Mobile Ad hoc Network is the fast growing technology from the past 20 years. The gain in their popularity is because of the easily deployed, infrastructure less and their dynamic nature. MANETs created a new set of demands to be implemented and to provide better end to end communication. MANETs works on TCP/IP structure to provide the means of communication between connecting work stations. Work stations are generally mobile and they have limited resources, therefore the traditional TCP/IP model needs to be modified, in order to support the MANETs mobility to provide efficient functionality. Therefore the key research area for the researchers is Routing. Routing protocols in

MANETs is a difficult yet challenging and attractive tasks, researchers are giving tremendous amount of attention to this key area.

Attacks:

Gray Hole Attack

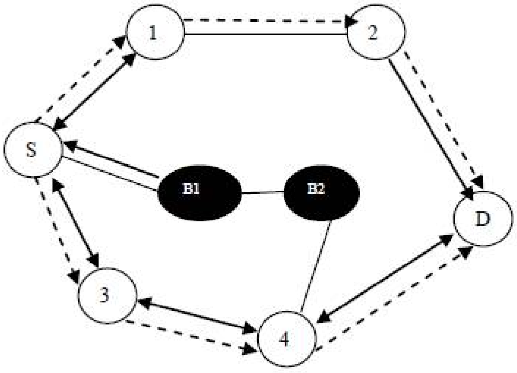
In this kind of attack the attacker misleads the network by agreeing to forward the packets in the preferred mentioned network. As soon as it receive the packets from the neighboring node, the attacker drop the packets without forwarding it. This is a type of active attack. In the beginning the attacker nodes behaves as usual and reply true RREP messages to the nodes that started RREQ messages. When it receives the packets it starts dropping the packets and launch Denial of Service (DoS) attack. This malicious behavior of gray hole attack is different in different ways. It drops packets while forwarding them in the network. In some other gray hole attacks the attacker node behaves highly maliciously for the time until the packets are dropped and then switch to their previous normal behavior [14]. Due this behavior it's very difficult for the network to figure out such kind of attack. Gray hole attack is also termed as node misbehaving attack in network [15].

Black Hole

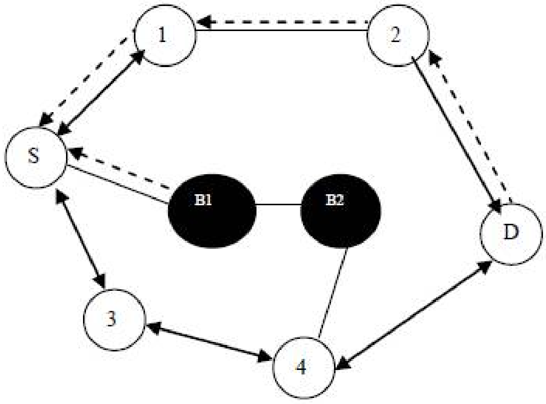
The black hole [2] node passes two things. First, the node of the network uses the routing protocol, such as AODV, which advertise itself as having a valid or shortest route to a destination node, whereas the route is forged by attacker node, with the intent of intercepting packets. Second, the malicious node consumes the seized packets.

Cooperative Black Hole Attack

In AODV routing protocol, the source node S wants to communicate with the destination node D, then the source node S sends broadcasts requests to the route request (RREQ) packet to their adjacent active nodes and update their routing table with an entry for the source node S, and check if it is the destination node or has a shortest route to the destination node. If does not have, shortest distance then the intermediate node updates the RREQ (by increasing the hop count) and passes the RREQ to the destination node D till it find their destination or any other intermediate node which has a fresh enough route to D, as described by example in Figure 2. The destination node D or the intermediate node with a fresh enough route to D, initiates a route reply (RREP) in the reverse path, as described in Figure 3. The source node S starts sending the information packets to their adjacent node which answered before, and rejects the other replies. This works is satisfactory when the network has no mischievous nodes.



Flooding of RREQ



Propagation of RREP

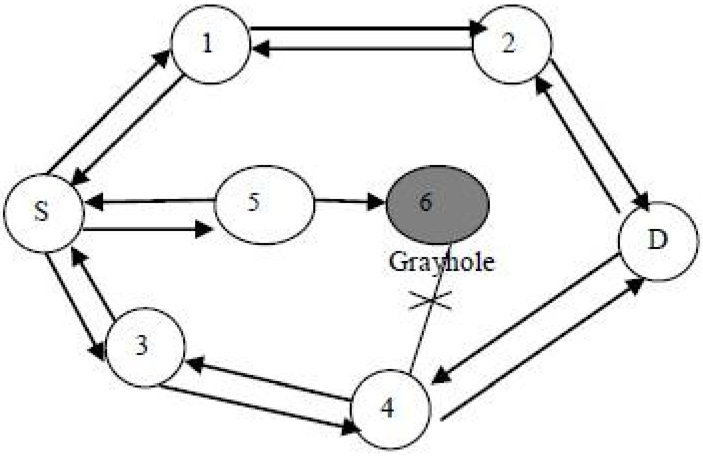
Several authors have projected an protocols and techniques to distinguish and eliminate a single black hole node [2]. Nevertheless, In case of multiple black hole nodes intermediate in coordination has not been addressed. For example, when composite black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its associative black hole B2 as the next hop, as described in the figure 3. According to [2], the source node S sends a "Further Request (FRq)" to B2 through some different route (S-3-4-B2) other than via B1. Node S asks B2 if it has a new route to node B1 and some route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "OK" to both the enquiries. Now as per the explanation suggested in [2], node S starts forwarding the data packets supposing that the route S-B1-B2 is assumed to be secure. Though, in reality, the packets are consumed by node B1 and the security of the network is breached.

Grayhole Attack

Gray hole is one of the attacks found in ad hoc network. Which act as a slow poison in the network side, it means we cannot suppose how much data can be lost. In gray hole Attack [3] a malicious node pretends to certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address of node or a range of IP addresses in network and forwards the remaining packets. Gray hole nodes in MANETs are very effective and erroneous. Every node maintain a vector routing table that stores the next hop node information for a route a packet to destination node ,and when a source node want to route a packet to the destination node , it uses a particular route from table if such a route is accessible in its routing table. If not, nodes initiate a new route discovery process by broadcasting Route Request (RREQ) message as discovery packets to its neighboring nodes. By getting the RREQ message, the intermediate nodes bring up-to-date to their routing tables in a opposite route to source node. A Route Reply (RREP) message is sent in backward direction of the source node after the RREQ query reaches either the destination node itself or any other intermediate node that has a recent route to destination. Now we explain the gray hole attack[4] on MANET'S .The gray hole attack has two significant phases.

In first phases, a malicious node exploits the secured AODV protocol to announce itself as having a valid route to destination node, with the concept of disturbing or humiliating packets, even though route is wrong.

In second phases, the malicious nodes drop the intermediate packets with a certain purpose. The process of finding gray hole is very difficult and challenging task. In certain new gray hole attacks the attacker node acts far maliciously for the duration until the packets are dropped and then switch to their ordinary nodes behavior. By this behavior it's very challenging for the network to distinguish between such kinds of attack. In some cases gray hole attack is also called as node misbehaving attack. The discrepancy of black hole attacks is the gray hole attack, in which the attack affected nodes either drop packets selectively. Both categories of gray hole attacks look to unsettle the network without being detected by the security measures in place provided for network.



Grayhole Attack in Mobile Ad hoc Network

II. PREVENTION TECHNIQUES

Design Considerations:

- Initialize the network.
- Plot the number of nodes in x and y locations where x location has the width and y location has height.
- Discover the path in that vary network only.
- Initialize the source and destination to find the simplest and shortest path, which is a simple process.
- Initialize the Gray hole attack to discover the path.
- Implement the process by using Genetic Algorithm with new fitness function.
- Evaluate the parameters that are Throughput, Bit Error rate, end to end delay, packet overhead, packet delivery ratio.

Description of the Proposed Algorithm

The *Genetic Algorithm (GA)* is a method for solving both constrained and unconstrained optimization problems in network that is based on natural selection of steps, the process that drives biological evolution. The genetic algorithm repeatedly modifies a population of individual solutions.

Step 1: Create Initial population of individuals
Step 2: Evaluate fitness of individuals
Step 3: Select the individuals
Step 4: Apply Genetic Operators
Step 5: Finished generations in genetic algorithm

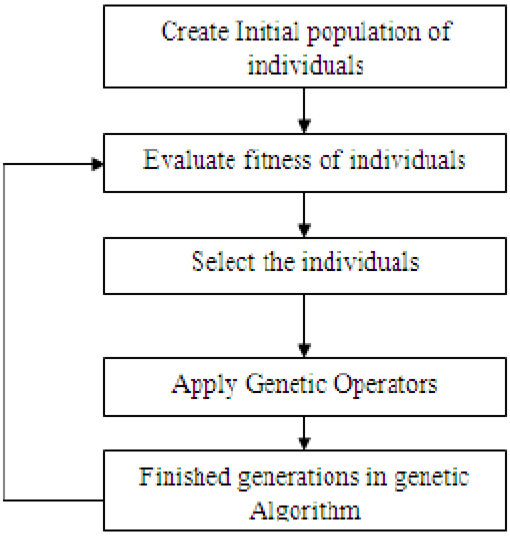
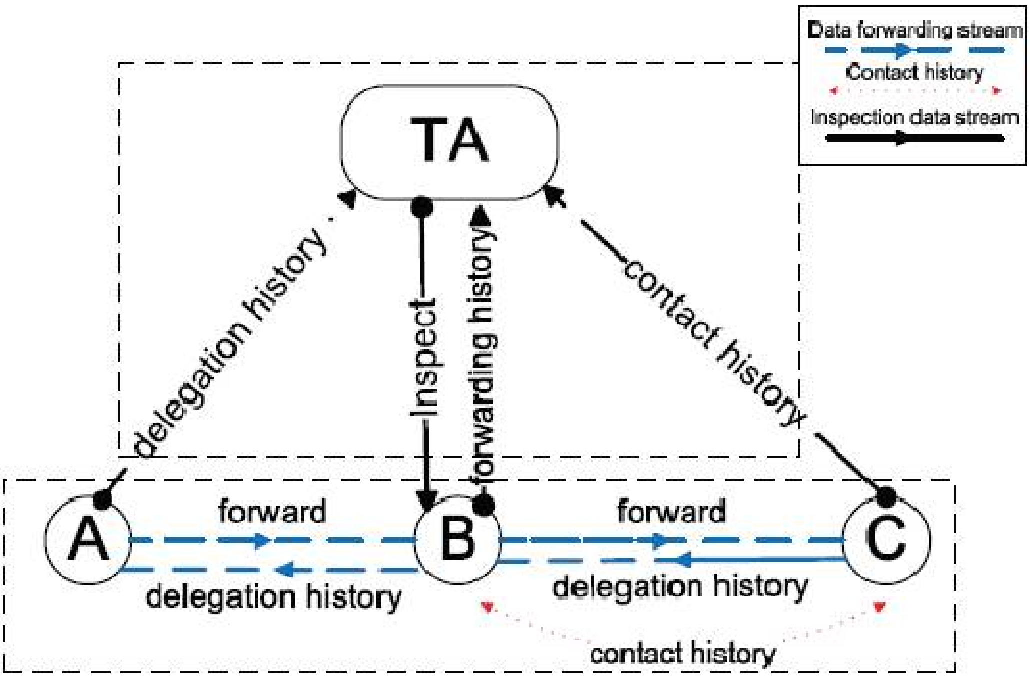

Create Initial population of individuals
Evaluate fitness of individuals
Select the individuals
Apply Genetic Operators
Finished generations in genetic Algorithm

Fig: Algorithm for Prevention



III. CONCLUSION

Thus We studied various problems and characteristic of gray hole and black hole attacks amd hot to distinguish between both of them. As it is major concern of detecting this both kind of attacks with hugh accuracy is again challenging. Thus we will propose itrust algorithm to improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users.

REFERENCES

[1] K. Fall, "A delay-tolerant network architecture for challenged internets," in Proc. Conf. Appl., Technol., Archit. Protocols Comput.Commun., 2003, pp. 27–34.
[2] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, "Disruption-tolerant networking: A comprehensive survey on recent developments and persisting challenges," in Proc. IEEE Commun. Surveys Tuts., 2012, vol. 14, pp. 607–640.
[3] Delay-tolerant networking research group [Online]. Available: http://www.dtnrg.org/wiki
[4] S. Burleigh, V. Cerf, R. Durst, K. Fall, A. Hooke, K. Scott, and H. Weiss, "The interplanetary internet: A communication infrastructure for Mars exploration," in Proc. Committee Space Res. Sci. Assem., 2002, 365–37.
[5] J. Partan, J. Kurose, and B. N. Levine, "A survey of practical issues in underwater networks," in Proc. 1st ACM Int. workshop Underwater Netw., Sep. 2006, pp. 17–24.
[6] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet," in Proc.
10th Int. Conf. Archit. Support Program. Lang. Oper. Syst., Dec. 2002, pp. 96–107.
[7] S. Guo, M. H. Falaki, E. A. Oliver, S. Ur Rahman, A. Seth, M. A. Zaharia, and S. Keshav, "Very low-cost Internet access using KioskNet," in Proc. ACM SIGCOMM Comput. Commun. Rev., Oct. 2007, vol. 37, no. 5, pp. 95–100.
[8] J. Ott and D. Kutscher, "A disconnection-tolerant transport for drive-thru internet environments," in Proc. IEEE 24th Annu. Joint Conf. Comput. Commun. Soc., Mar. 2005, pp. 1849–1862.
[9] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in Proc. 4th Annu. Int. Conf. Workshop Security Emerging Ubiquitous Comput., 2007, pp. 1–8.
[10] Y. Ren, M. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2010, pp. 1–6.
[11] Z. Gao, H. Zhu, S. Du, C. Xiao, and R. Lu, "PMDS: A probabilistic misbehavior detection scheme toward efficient trust establishment in Delay-tolerant networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.
[12] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," Elsevier J. Ad Hoc Netw., vol. 14, pp. 1497–1509, 2013.
[13] F. Li, J. Wu, and A. Srinivasan,, "Thwarting blackhole attacks in disrupt-tolerant networks using encounter tickets," in Proc. INFOCOMM, 2009, pp. 2428–2436.
[14] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in Proc. IEEE 5th Int. Conf. Commun. Syst. Netw., Jan. 2013, pp. 1–7.
[15] Q. Li and G. Cao, "Mitigating routing misbehaviors in disruption tolerant networks," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 664–675, Apr. 2012.
[16] A. Keranen, J. Ott, and T. Karkkainen, "The one simulator for dtn protocol evaluation," in Proc. 2nd Int. Conf. Simul. Tools Tech., Rome, Italy, Mar. 2009, pp. 55:1–55:10.
[17] A. Lindgren, A. Doria, and O Schelen, "Probabilistic routing in intermittently connected networks," SIGMOBILE Mobile Comput. Commun. Rev., vol. 7, pp. 19–20, 2003.
[18] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc. IEEE Int. Conf. Comput. Commun., Barcelona, Spain, Apr. 2006, pp. 1–11.