IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

A Cumulative Study on Gray and Black Hole Detection in MANET

Prof. N. V. More[1], Chetana Thombare[2], Prajakta Sutar[3], Rutika Tasgaonkar[4], Komal Joshi[5]

Assistant Professor, Computer Engineering, PVPIT, Pune, India[1]

Student, Computer Engineering, PVPIT, Pune, India[2,3,4,5]

Abstract: Mobile Ad-hoc Network is a network in which multiple mobile nodes are interconnected and they communicate which other without fixed infrastructure. Such network invites multiple threats in network which affects the routing speed and decreases performance level of the network. In all these threats gray hole is silent but more vulnerable attack which attacks the network in repetition mode. There are so many techniques invented in order to detect and remove these gray hole in which all the actions need to be taken by the nodes themselves to find out malicious node. It is hard to detect gray hole node in pool if the neighbour node of gray hole node is malicious or does not work properly due to some technical reasons. So a pool manager of the pool keeps the record of routing history and detects gray hole node by iterative comparison of the data hash keys.

Keywords: Gray hole, Wireless Sensor Network, MANET.

I. INTRODUCTION

Now a Days MANET is widely in use. MANET is basically a Type of ad-hoc network in which multiple mobile nodes are connected wirelessly. MANET is collection of different nodes that communicates with other nodes and other adjacent nodes. MANET works without any fixed infrastructure. It make the topology dynamical. So that , that MANET having high risk of security.

MANET is more secure than the other network infrastructures with are currently in use. In MANET if source and destination node are within the communication range of each other than source node can send the packet to destination node directly otherwise intermediate nodes are responsible to route the packet from source to destination node [3].

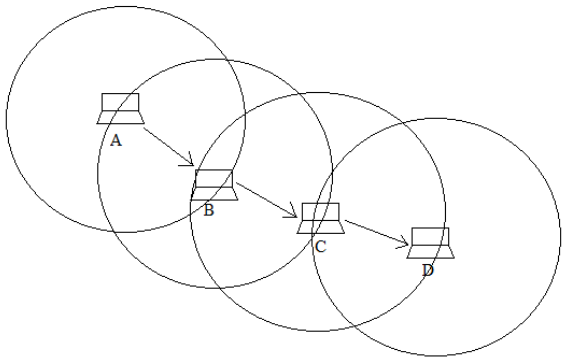

Fig: Ad hoc Network

In the rest of this paper, Section 2 summarizes the basic of gray hole attacks with more details. In Section 3, we summarizes the basic operation of pool manager. In Section 4, we describe some methods that have proposed for detecting or preventing these attacks of gray hole and finally, we conclude the paper.

II. LITERATURE SURVEY

Various techniques are introduced to detect gray hole node in the wireless network. In this section, we review eight different approaches for detection and removal of gray hole attacks.

The method proposed by **S D Khatawkar[1**], makes benefit of mobile agents (MA) to detect gray hole using the code migration facility. MA consists of program code and program execution state. Here the performance reduce with random mobility and also with mobility of nodes, it has some false detection.

This method introduced by N. **Dharini[2],** uses light weight learning based energy prediction algorithm. By comparing consumed energy with concluded energy, gray hole is detected. Less energy consumption means node has not transmitted data. Proposed method accomplishes energy saving so as it increases network lifetime.

While the another method planned by **Parineet D. Shukla [3]** slog by using the probability for dropping the packets and getting a deceitful feedback from the next node, the gray hole can be catched. Probability for getting a false reply from the node, act as a threshold amount for deciding the nature of a node.

The method proposed by **Seemita Pal [4**], detects gray hole by observing suspension in packet arrival by calculating slope of the delay over a given window. Based

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

on contrast in slope after a packet damage and the slope of the adjacent coming packet, it establish the reason behind the packet loss. This method feat the correlation between packet delays and packet loss due to congestion.

The main idea behind the design proposed by **Qiang Liu [5]** is, it combines downstream assessment and end-to-end assessment to detect gray hole intervention. Method uses fast hashing and digital signature capabilities to protect packet against handling, replay and masquerading attacks at mesh routers.

The method explained by **Jiwen CAI [6]** deals with network layer and MAC layer. Here they spotlight on the path of conveyance to detect a gray hole by awaring the next hop action not all neighbours. This increases system performance. But still there is ī problem of false positive probability.

The method emphasised by **Devu Manikantan Shila [7],** needs channel aware detection algorithm. It adopts two strategies for detection, hop-by-hop loss observation by more recent nodes and traffic monitoring by upstream nodes. Here control packets are more which causes overhead in the network.

The scheme narrated by **Jaydip Sen [8],** First collects the data routing information in a routing table. Then they detect the existence of a gray hole locally. But sometimes there might be chances of declaring an honest node as vengeful node. So to avoid the chances of false positive it is once again checked by the nodes in the network cooperatively.

III.CLUSTER FORMATION

In data transmission infrastructure the number of nodes are sometimes in same area. That area of transmission is called as cluster. These nodes are transmitting the packets in the same cluster but they require the observer for the operations. That observer is known as cluster head in networking world. The cluster head is one of the node in same transmission area. The cluster head selection process is done in the cluster. The node starts advertising for its data packets and those who are interested they replied and transmission is going on.

IV.GRAY HOLE ATTACK

Social Gray hole is a packet drop attack in which malicious node misconducts the start node to forward the packets to destination nodes and drop or changing packets coming from the source node or intermediate nodes. It is difficult to detect gray hole attack because nodes can drop packet partially and behaves like normal node. If M forward data completely or partially to the destination. It may send some selective packets drops an important data[4][6][8]. Whenever a node has a data to transfer in order to communicate among the nodes, it checks in route cache for existing route table, whether destination node is available or not. If it is available then node will transfer the data over the path. But if it is not available then, it initiate route discovery process opinions.

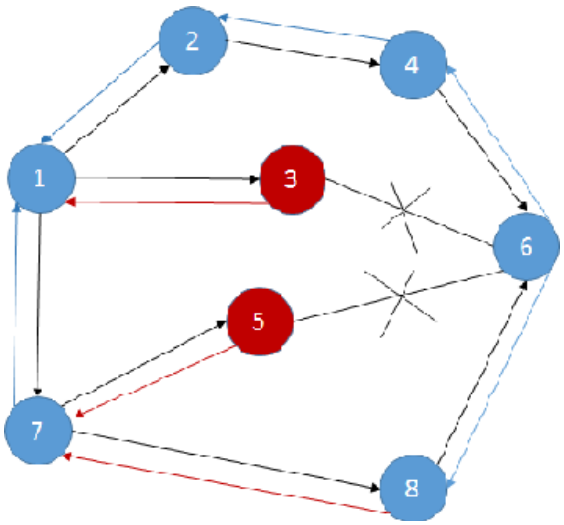

Fig: Gray Hole Attack

In Route Discovery process, the node who initiates the process becomes source node. When source node wants to route a packet to destination node first, it sends Route Request RREQ packets in network. Each node broadcast this packet to its neighbour's until it receives all RREQ. Every node preserve a routing table that stores the next hop node information for a route the packet to destination node. After that source node wait for period of time until receive all Route Reply RREP. Then source node checks and selects route with the capital sequence number. If there are more than one RREP with the same sequence number then, source node selects least hop count to destination[6][8].

V. POOL MANGER WORKING

Pool is a number of nodes which are connected to each other. In this pool there is a pool manager which secures the data from the attack of gray hole by identify the gray hole. Pool manager takes the input as the source and destination nodes and identify the available paths for routing.

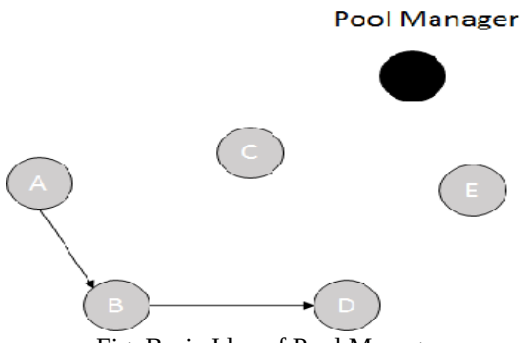

Fig: Basic Idea of Pool Manager

DOI 10.17148/IJARCCE.2017.6358

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Pool manger detects gray hole by the iterative comparison of the data hash keys. So we come out with an idea in which we are creating a pool which actually comprises many number of mobile nodes and this pool also contains a pool manager which actually a system which identifies the gray hole node and removes it too. Node is characterized by the concept of sending the hash key of the received data created by the MD5 Algorithm to the pool manager. As soon as pool manager receives both the hash keys for the verification, it checks the data.

The two phase commit protocol is a distributed algorithm which is type of atomic commitment protocol and allows all distributed devices to commit a transaction. This protocol results in the transaction or aborting by all node, even in the case of site failures and message losses. The protocol achieves its goal even in many cases of temporary system collapse, and is thus widely utilized. However, it is not resilient to all possible failure configurations, and in unusual cases, user intervention is needed to remedy an outcome. To accommodate recovery from decline the protocol's participants use logging of the protocol's states. Log records, which are typically slow to generate but survive declines, are used by the protocol's recovery procedures. Many protocol variants exist that primarily differ in logging strategies and reconstruction mechanisms. Though usually intended to be used infrequently, recovery procedures constitute a substantial portion of the protocol, due to many possible failure scenarios to be considered and supported by the protocol.
Main assumption is node is designated the pool manager, which is the master node, and the rest of the nodes in the network are called devices. Assumptions of the protocol include storage at each node and use of a write tag by each node. Also, the protocol assumes that no node crashes forever, and eventually any two nodes can connect with each other. The latter is not a big deal since network conversation can typically be rerouted

VI. SYSTEM OVERVIEW

Pool manager takes the input as the source (first node) and destination node and identify the possible shortest path for traverse the nodes. Once the possible paths of traversing is been identified then the time delay is calculated for all the recognized paths.

Data Transmission in Cluster:

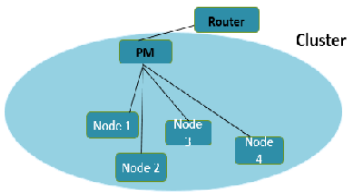

Fig: Data Transmission in Cluster

So the path which finally yields the least time delay for recognized nodes is considered as the shortest path. This shortest path will be returned to the request source node as Route reply .In our case of narration the path will be Node 1 to Node 2 after that Node 4.

In First step nodes sends the hash key of the data which is been generated by the Dijkstra Scholten Algorithm to the pool manager. Then by comparing both the hash keys from the source node and the destination node of the occurrence, pool manager will check for the avalanche effect of the hash keys. If any effect is identified then this is considered as the gray hole.

VII. CONCLUSION

The Wireless networks are often suffered by the gray and black holes which causes severe vulnerability for the routing of the data. Most of the routing protocols like AODV and DSR are suffer from this kind of black and gray hole seriously due to infectious nodes. So there is always an urge for effective detection of black and gray holes to fasten the process of routing.

So this paper collectively study various methods elaborated by the different authors for the detection of the black and gray holes. And after thoroughly analysing the prior work this paper come to a conclusion that individual nodes in the shortest path spend much more time for detection of these kinds of infectious nodes. So an idea of decreasing the burden on nodes to identify black and gray holes will be proposed in our future edition to increase the performance of the MANET.

ACKNOWLEDGMENT

We take this golden opportunity to owe our deep sense of gratitude to our project guide **Prof. N. V .More,** for his instinct help and valuable guidance with a lot of encouragement throughout this paper work, right from selection of topic work up to its completion. Our sincere thanks to Head of the Department of Computer Engineering and Information Technology **Prof. B, K. Sarkar** who continuously motivated and guided us for completion of this paper. I am also thankful to all teaching and non-teaching staff members, for their valuable suggestions and valuable co-operation for partially completion of this work. We specially thank to those who helped us directly-indirectly in completion of this work successfully.

REFERENCES

[1] S D Khatawkar, NitinTrivedi, "Detection of Gray hole in MANET through Cluster Analysis", IEEE 2015 2nd International Conference on Computing for Sustainable Global Development(INDIACom), pp.1752-1757.
[2] N.Dharini, Ranjith Balakrishnan and A. Pravin Renold,"Distributed Detection of Flooding and Gray Hole Attacks in Wireless Sensor Network" ,IEEE 2015 International Conference on Smart

Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), pp.178-184.

[3] Parineet D. Shukla, Ashok M. Kanthe,Dina Simunic, "An Analytical Approach for Detection of Gray Hole Attack in Mobile Ad-hoc Network (MANET)" ,IEEE International Conference on Computational Intelligence and Computing Research 2014.

[4] Smita Pal, Huijiang Li, BiplabSikdar and Joe Chow,"A Mechanism for Detecting Gray Hole Attacks on Synchrophasor Data", IEEE ICC - Selected Areas in Communications Symposium, pp.4131-4136, 2014.

[5] Qiang Liu, Jianping Yin, Victor C. M. Leung,and ZhipingCai,"FADE: Forwarding Assessment Based Detection of Collaborative Grey Hole At- tacks in WMNs", IEEE Transactions on Wireless Communications, Vol. 12, No. 10, October 2013, pp.5124-5137.

[6] Jiwen CAI, Ping YI, Jialin CHEN, Zhiyang WANG, Ning LIU,"An Adaptive Approach to Detesting Black and Gray Hole Attacks in Ad Hoc Network",24th IEEE International Conference on Advanced Information Networking and Applications, 2010, pp.775-780.

[7] Devu Manikantan Shila, Yu Cheng and Tricha Anjali,"Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks", IEEE, GLOBECOM 2009.

[8] Jaydip Sen, M. Girish Chandra, Harihara S.G., Harish Reddy, P. Balamuralidhar,"A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks", ICICS 2007 IEEE