# A Model Approach for Detection of Gray and Black Holes in WSN

**Prof. N. V. More[1], Chetana Thombare[2], Prajakta Sutar[3], Rutika Tasgaonkar[4], Komal Joshi[5]**
Department of Computer Engineering
[1]Assistant Professor,, PVPIT, Pune, India
[2, 3, 4, 5]UG Students,, PVPIT, Pune, India

***Abstract-****There are so many systems in WSN which are working on detecting gray hole and black hole and their attacks. The black and gray hole are actually effects on the routing speed in single network. In our concept, we are come with a solution that we are creating clusters in MANET to reduce the workload on nodes and increase the routing speed of the networks. There are so many methodologies are available to detect gray hole and black hole in WSN. Some of them work during route discovery process while others are work when data transmits in network. Most of the techniques having performance issues related to "A Cumulative Study of Gray hole and Black hole detection in MANET" so this paper concentrate on overcoming performance issues by proposing a normal idea for detecting gray hole and black hole in MANET. The previous documents describe the issues related to detect gray hole and black hole in network and we came up with the better solution is forming clusters in MANET which consist of a pool manager of that pool having number of nodes connected to each other wirelessly. This pool manager reduces the workload of nodes by iterative comparison of data hash keys.*

***Keywords****-*Blackhole, Grayhole, Pool Manager, MANETs, Avalance Effects, Titlemapping

## I. INTRODUCTION

MANET is mobile Ad-hoc network which don't have fix infrastructure. In MANET multiple nodes are connected to each other wirelessly for better communication. MANET provides more secure communication than others. In MANET nodes communicates with each other by sending packets. If there are any mediator node in between source and destination node, the mediator node responsible for route the packet in network to send it to destination node.

In area of wireless networking there are number of nodes which transmits the packets in same area of communication. We can call it as cluster. The node transmits the packets in the cluster but they give their total control to one selected node is known as cluster head(CH). Cluster head must be present in the same cluster and the selection process takes place in that cluster. In node voting process every node starts advertising for the nodes which they have and the interested node reply them back and likewise transmission process goes on.

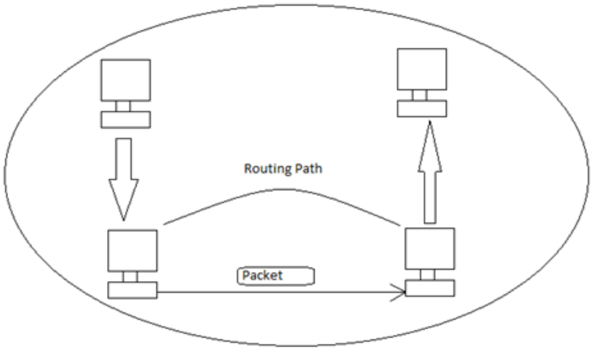


Fig.: MANET

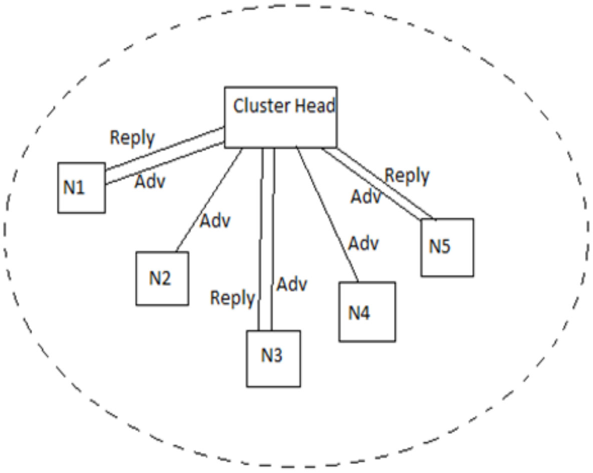


**Fig.:- Cluster**

Pool Manager: The pool is a one type of cluster which contains number of nodes in one network. One node is selected to handle all the data transmission process called as pool manager. The basicoperations of pool manager is to active new arrival node, register its entry and allow him for transmission process.

Detection of gray hole: When the registered node start transmission in network, the sender sends the data packet to the receiver node. After sending data packet in network the path of that packet must be decided by the pool manager. Pool manager always transfer that packet by shortest path of transmission. The hash keys are generated at pool manager record for security and data matching purpose. If in case the mediator node changes the data due to network traffic and send new changed data packet to the receiver, then the hash key will not get match. If hash keys are not match, then mediator node detect as gray hole. After detecting gray hole pool manger remove that node from that path.

Dijkstra Algorithm: We use this algorithm for finding shortest path in network. When sender start sending data packet to the receiver node then pool manager decides the path of routing. That routing path must be shortest so that transmission will much faster than normal.

This paper dedicates section II for Related work, whereas section III describes the proposed techniques in detail. The evolution of proposed technique is done in section IV. In the end the paper is concluded with option for extensions in section V.

## II. RELATED WORK

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 reduces with random mobility and also with mobility of nodes, it has some false detection.

The method proposed by Abdelali Boushaba, Adil Benabbou, Rachid Benabbou, Azeddine Zahi, Mohammed Oumsis [2] makes use of Multipath Optimized Link State Routing Protocol (MP-OLSR) is a multipath extension of OLSR which is proactive routing protocol used in MANET. To integrate Weighted Round-Robin (WRR) scheduling algorithm to MP-OLSR for supporting heterogeneous multiple paths with different hop count. Here, data packets are distributed into different paths by using Round-Robin (RR) scheduling algorithm. RR is incapable to balance load among heterogeneous multiple paths. the cost functions return fixed values without adaptability to network conditions.

The method proposed by Seemita Pal [3], detects gray hole by observing delay in packet arrival by calculating slope of the delay over a given window. Based on difference in slope after a packet loss and the slope of the next coming packet, it decides the reason behind the packet loss. This method exploits the correlation between packet delays and packet loss due to congestion.

The scheme proposed by Xiaoning Ding, Jianchen Shan, and Song Jiang [4] In high-end data processing systems ,a buffer pool management of high scalability plays an important role on system overall performance. The scalability of buffer pool management is largely determined by the data replacement algorithm, which is a major component in buffer pool management. It can seriously degrade the scalability if not designed and implemented properly.

While the method proposed by Parineet D. Shukla [5] works by using the probability for dropping the packets and getting a false reply from the next node, the gray hole can be detected. Probability for getting a false reply from the node, act as a threshold value for deciding the behavior of a node.

The method proposed by K.Thamizhmaran,Akshaya Devi Arivazhagan,M.Anitha,[6] used Dijkstra's Algorithm and to find shortest path, and hence to carrying out the performance analysis on Adhoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) protocols.Protocol tested under realistic conditions such as the transmission of the packets in sensitive transmission range, limited buffer space for storage of messages with several data traffic models, and realistic movement of mobile nodes used Dijkstra's Algorithm.

The method proposed by N. Dharini[7], uses light weight learning based energy prediction algorithm. By comparing consumed energy with predicted energy, gray hole is detected. Less energy consumption means node has not transmitted data. Proposed method achieves energy saving so as it increases network lifetime.

The scheme proposed by Nunzio Marco Torrisi, Ognjen Vukovi´c and Gy¨orgy D´an,Stefan Hagdahl [8] they addressed the vulnerability of SCADA communication to a gray hole attack, in lack of signaling from the outstation to the master, as long as solicited responses are delivered, the master station can not tell if an attacker drops all unsolicited responses.while letting through solicited reports in order to avoid detection.This is possible only if messages are sent through an encrypted tunnel, because due to the strict timing rules used in SCADA protocols for traffic analysis.

The main idea behind the method proposed by Qiang Liu [9] is, it combines downstream assessment and end-to-end assessment to detect gray hol attack. Method uses fast hashing and digital signature techniques to protect packet against manipulation, replay and masquerading attacks at mesh routers.

This theme suggested by Md. Ashraf Uddin,Ashraful Hug Suny [10] main idea behind this is to build a system which assists blind person smoothly. The system finds the shortest path between source and destination using Dij kstra's algorithm. Because Dijktra's algorithm always considers all positive edges. According to the shortest path windows phone gives direction. But for taking advantage of this system user always have to carry out smart phone.

The method proposed by Jiwen CAI [11] deals with network layer and MAC layer. Here they focus on the path of transmission to detect a gray hole by observing the next hop action not all neighbors. This increases system performance. But still there is ῑ problem of false positive probability.

The method proposed by Devu Manikantan Shila [12], uses channel aware detection algorithm. It adopts two strategies for detection, hop-by-hop loss observation by downstream nodes and traffic monitoring by upstream nodes. Here control packets are more which causes overhead in the network.

The scheme proposed by Jaydip Sen [13], First collects the data routing information in a routing table. Then they detect the presence of a gray hole locally. But sometimes there might be chances of declaring an honest node as malicious node. So to avoid the chances of false positive it is once again checked by the nodes in the network cooperatively.

## III. PROPOSED METHODOLOGY

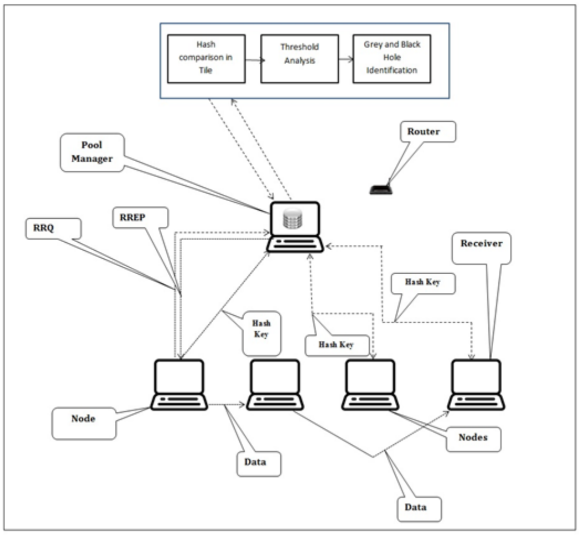


Figure 3: System overview

The proposed methodology of black and grey hole detection can be clearly depicted in figure 3, and it can be explained with the below mentioned steps.

Step 1: This is the initial step of the proposed system where all the nodes have to register with the pool manager by sending their node names and IP address. Once this is done all info is been stored at pool manager for the further transactions.

Step 2: Here in this step source node can view all the registered mobile nodes in the pool to select the destination node. Once the destination node is selected by the source node then a routing path is requested to the pool manager.

Step 3: On receiving the routing path request from the source node, pool manager assigns the random integer values for each of the nodes. Then these random values are feed to the shortest path estimation using Dijkstra algorithm.

Step 4: As soon as shortest path is calculated through the prior step data is start routing based on the route map provided by the pool manager. For every hop a signature of the data in the form of hash code will be generated using MD5algorithm. This data signature will be recorded by the pool manager through the every instance source and destination nodes of the routing sequence.

Step 5:Here in this step a strict analysis of the hash signature is carried out for the pattern of the black hole attack and grey hole attack though avalanche effect for a fixe time slot called as ‘ tile’. If a node is behaving as the grey hole then it partially drops the data or it malfunctions the data, whereas for the black hole it completely drops the data so that only one hash signature will be received by the pool manager.

The whole process of black hole and gray hole detection process can be shown in the below algorithm 1

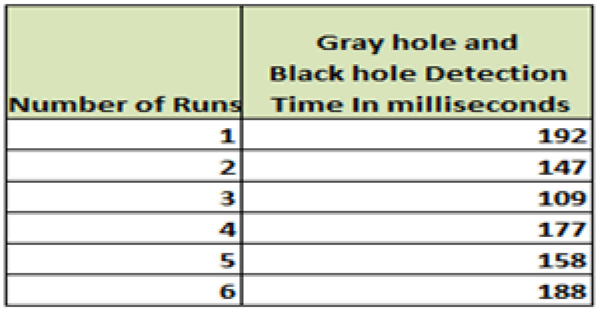
Algorithm 1: Gray & Black & Black Hole Identification Using Pool Tile Method

```
        // Input: Sender Data bytes B
        // Destination Node Dst
        // Output: Successful identification of Gray & Black hole node
Step 0: Start
Step 1: Activate pool managers $\mathbf{P_m}$
Step 2:  Register Node $\mathbf{N_i}$ with pool manager $\mathbf{P_m}$
Step 3: Set Tile T for Pool managers $\mathbf{P_m}$( Where tile is Time in Seconds)
Step 4: Choose Data bytes B by source node $\mathbf{S_{rc}}$
Step 5: Set Destination node $\mathbf{D_{st}}$
Step 6: Identify the shortest path $\mathbf{P_{th}}$
Step 7: WHILE $\mathbf{B \notin B_n}$
Step 8: for each tile T
Step 9: $P_d \rightarrow S_{nt} \in B$ ($P_d$= previous data in Hash and $S_{nt}$= Run time Source node)
Step 10: $C_d \rightarrow D_{nt} \in B$($C_d$ = Current data in hash and $D_{nt}$ = Run time Destination node)
Step 11: check IF$C_d \neq P_d$( Avalanche Effect)
Step 12:  Label Current instance node$C_n$ as Gray hole
Step 13: END IF
Step 14: IF $C_d$ =NULL
Step 15: Label Current instance node $C_n$ as Black hole
Step 16: END IF
Step 17: END WHILE
Step 18: Stop
```

## IV. RESULTS AND DISCUSSIONS

For the deployment process of the proposed system we considered 5 machines having core i3 or greater processor Configuration with 4 GB of RAM. Each machine is equipped with windows operating system enables to support all versions of java.

Table 1: Gray hole and black hole detection time in milliseconds by pool tile method



| Number of Runs | Gray hole and Black hole Detection Time In milliseconds |
|---|---|
| 1 | 192 |
| 2 | 147 |
| 3 | 109 |
| 4 | 177 |
| 5 | 158 |
| 6 | 188 |

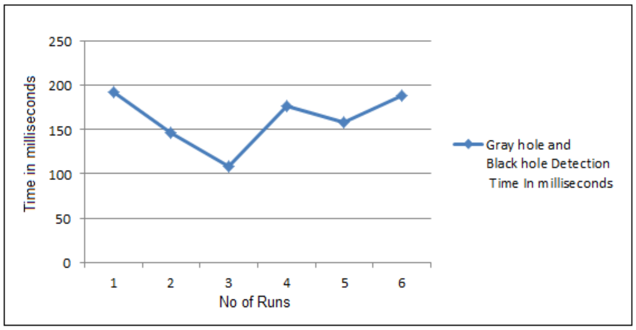


Figure 4: Performance plot for black and gray hole detection

System uses Netbeans 6.9.1 as the standard IDE with MYSQL 5.5 as the databases server. And System uses D-Link DIR -615 Wireless N 300 Router, Which is equipped with two antennas Signal Strength with 802.11n wireless type, which enough to deploy the strengths of the system by considering all advanced scenarios.

An explicit experiment is conducted for the performance evaluation of the system based on the time taken to identify the black hole and gray hole in the wireless network. System is set to detect the black hole and gray hole for much number of runs to record the timings of performance, which are tabled as in table 1.

The plot in figure 4 indicates the time required to find the black hole and gray holes in the wireless network. On an average system takes 161.8 milliseconds of time for detection of gray and black holes. And this performance time can be said as the good in the process of black and gray ho detection.

## V. CONCLUSION AND FUTURESCOPE

Due to increasing usage of wireless networks there is always a huge entry point to the attacker in the network. Black hole and gray hole attacks are most common and highly dangerous form of threats to the wireless network. This paper introduced pool tile method to identify the attacker node which efficiently works than that of most of the other methods. This is because; proposed system eradicates the burden of detection of malicious nodes from the routing nodes which are comes under shortest path sequence. There by assigning the entire detection job to high configured pool manager.

In the future this method can be more efficiently incorporated by assigning the detection of black and grayhole job to the multiple pool manager on increasing of pool size.

## ACKNOWLEDGMENT

The authors would like to thank all the researcher team members as well as publishers for making their resources available and teachers for their valuable guidance.

## 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] Abdelali Boushaba, Adil Benabbou, Rachid Benabbou, Azeddine Zahi, Mohammed Oumsis, “An enhanced MP-OLSR protocol for MANETs” ,2014 Fifth International Conference on Next Generation Networks and Services (NGNS), pp. 73-79.

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

[4] Xiaoning Ding, Jianchen Shan, and Song Jiang,” A General Approach to Scalable Buffer Pool Management”, IEEE International Conference 1045-9219 (c) 2015 IEEE

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

[6] K.Thamizhmaran,Akshaya Devi Arivazhagan,M.Anitha, “Co-operative analysis of Proactive and ReactiveProtocols Using Dijkstra's Algorithm” ,IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO)2015, pp. -----

[7] 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.

[8] Nunzio Marco Torrisi, Ognjen Vukovi´c and Gy¨orgy D´an,Stefan Hagdahl, “Peekaboo: A Gray Hole Attack on Encrypted SCADA Communication using Traffic Analysis” ,2014 IEEE International Conference on Smart Grid Communications, pp.902-907.

[9] 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.

[10] Md. Ashraf Uddin,Ashraful Hug Suny, “Shortest Path Finding and Obstacle Detection forVisually Impaired People Using Smart Phone” ,2nd Int'l Conf. on Electrical Engineering and Information & Communication Technology (ICEEICT) 2015, pp. ------

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

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

[13] 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 IEEE0