Avoidance of Black Hole and Gray Hole Attack in MANET using Hash Function based

[1]Munish Wadhwa,[2]Ashwani Sethi
Department of Computer Engineering
Guru Kashi University
Talwandi Sabo Bathinda,Punjab(151001) India. *munishwadhwa.cgc@gmail.com*
Department of Computer Engineering
Guru Kashi University
Talwandi Sabo Bathinda,Punjab(151001) India. *ashwani.gku@gmail.com*

ABSTRACT: MANET is mobile ad-hoc network having less number of infrastructural elements. Various mobile nodes inter communicate to each other through wireless links. As there is no central controller which can control the access permission. Any node can be the part of the communication at any time. While doing this there can be any number of malicious nodes. These malicious nodes behaves as they are legitimate node and contributes to the process of building the path. but the path build through them can be wrong. In such situation the packets transmitted through them will be either misrouted and being dropped. In such situation some authentic procedure is required, which can control the access permissions. Timely these nodes should be identified and removed. In current research hash based technique is used. while communicating two nodes shares there keys amongst themselves. If certain node will not be able to share the hash value. Will be declared malicious. That means without malicious node the network performance will be upgraded automatically. Under current research we have checked the performance with different parameters like end to end delay, through put, success rate, packet delivery ratio. All these parameters has shown certain amount of improvement over to the previous technique.

*****

I. INTRODUCTION

As it cost effective solution to the wireless communication in the shorter distance. This type of network due to less infrastructure may prone to various types of attack. This may decrease the usability of the network. Such that may requires higher security for being used in various strategic application such as military. In a MANET, each node not only works as a host as well as relay node. Such that receive the data from one side and switch to the other intermediate node of even final destination. But can also act as a router While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network[2] .

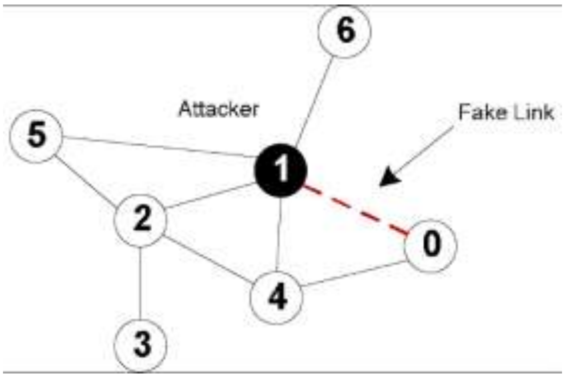

Figure 1 : Black Hole Attack[2]

This environment has also greater threats .As these threats may be of malicious node, whose intention is to destroy the packet rather than forward the packet. They exist in the network for only for dropping the packets. In current time various research works are focus around the security. The main aim is to detect and prevent the attacks. These attacks may become unavoidable when more than one node collectively works as malicious nodes. As lack of the infrastructure also adds to the problem. Where less no of hardware protective measures. Because it will increase the cost of the network. And due to cost it become dis functional. When route request is sent by the source then various nodes check there seq no with the required destination no. If it matches then reply with the route. Else will forward the route request. But malicious node without checking all this falsely reply to the source node for being a shortest route. Under such situations source falsely considers that path as real path for forwarding the data packets. In gray hole attacks, the malicious node is not initially accepted as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. In this paper our main objective is to identify the malicious node which is Black Hole in nature. Such that which sometimes behaves as legitimate node and sometimes behaves as legitimate node. In our case main objective is to detect the identity by checking the packet drop ratio and the

CBDS. With CBDS we can identify the malicious node which is not actually the part of the network. Using packet drop ratio we will identify the Black Hole node. If packet drop ratio is beyond the network efficiency. This is how various types of attack can be detected [3].

BLACK HOLE ATTACK

Black Hole Attack is a type of Denial of Service (DOS) Attack. In this attack, black hole nodes utilize their algorithm in order to market itself for having the greatest path to the destination node or to the packet it wants to interrupt. Under this attack, nasty node absorbs transmitted data from source to destination and drops all this data or forwards it to indefinite address. As a result, the source and the destination nodes become unable to communicate with each other. There two types of black hole attacks such as single black hole attack and collaborative black hole attack. In single black hole attack, the attack caused by individual black hole node in a network. In collaborative black hole attack the attack caused by two or more spiteful nodes. It is very firm to detect and prevent collaborative black hole attack in MANET.

Most of the routing algorithms developed for MANET include AODV, DSR and TORA are based on the statement that each node forwards the packet. But in practice some of the nodes may operate as the selfish nodes[3]

GRAYHOLE ATTACK

Grayhole 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 grayhole Attack a malicious node trashes to precede 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. Grayhole nodes in MANETs are very effective. Every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,when a source node want to route a packet to the destination node , it uses a particular route if such a route is accessible in its routing table. If not, nodes initiate a route discovery process by broadcasting Route Request (RREQ) message to its neighboring nodes. By getting the RREQ message, the intermediate nodes bring up-to-date their routing tables in a reverse route to source node. A Route Reply (RREP) message is sent 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 define the gray hole attackon MANET’S .The gray hole attack has two significant phases[4].

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

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

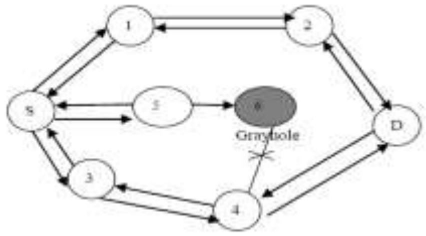

Figure 2 Grayhole Attack in Mobile Ad hoc Network[4]

II. RELATED WORK

Ad Hoc wireless network is a type of wireless network, in which there is no any fixed infrastructure. Devices in Ad Hoc network can move around the network within a given range. Currently most of the transactions are performed through the computer networks so they are more susceptible to many physical security threats. One of the major DOS Attacks that degrade the performance of the whole MANET is Black Hole attack. In the presence of black hole attack, nasty nodes are not forward the packets rather they drop packets. In this work, black hole attack is detected and eliminated through implementing Digital Signature with Two fish Algorithm. We modified on-demand routing protocol Temporally Ordered Routing Algorithm (TORA) and named it as STORA. Our proposed STORA performs well under normal conditions and under black hole attack than original TORA [1].

Delay Tolerant Network (DTN) is developed to cope with intermittent connectivity and long delay in wireless networks. Due to the limited connectivity, DTN is vulnerable to blackhole and greyhole attacks in which malicious nodes drop all or part of the received packets intentionally. Although existing proposals could detect the attack launched by individuals, they fail to tackle malicious nodes cooperating to cheat the defense system. In this paper, we suggest a scheme to address both individual and collusion attacks. Nodes are required to exchange records of previous encounters and evaluate others based on their messages forwarding ratios. Malicious nodes might avoid being detected by colluding to hide misbehaving forwarding ratio metrics. To persistently drop packets and promote the metrics at the same time, attackers need to create forged encounter records at high frequency and with high number of sent messages. This leads to abnormal patterns of fake encounters in contrast ith authentic ones and provides a symptom for collusion detection. Extensive simulation shows that our solution can work with various dropping probabilities and different number of attackers per collusion at high accuracy and low false positive [2].

A review on a various types of coordinated attack is deliberated such as blackhole / grayhole attack which are most serious threats in mobile ad hoc network. In cooperative blackhole attack more than one node collude to each other hence this attack is more challenging to identify. This paper presents a review of different security mechanism to eliminate the blackhole / grayhole attack from the network [3].

The Delay Tolerant Networks (DTNs) are especially useful in providing mission critical services including emergency scenarios and battlefield applications. However, DTNs are vulnerable to wormhole attacks, in which a malicious node records the packets at one location and tunnels them to another colluding node, which replays them locally into the network[4].

They have discussed some attacks that are performed on various layers of TCP/IP model. And we performed a comparative study for a specific network layer attack: grey hole attack. A grey hole attack is often difficult to detect and recover. There are different techniques for its detection which have their advantages and shortcomings [5].

Future VANET Vision: Ubiquitous deployment of VANET/VDTN capable systems from different vendors Can not centralize security infrastructure Big attack surface (even for closed systems) Proposed systems mostly realized using widely available commodity hard- and software WiFi Technology Off-the-shelf operating systems and hardware platforms[6].

A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense. Protecting the network layer of a MANET from malicious attacks is an important and challenging security issue, since most of the routing protocols for MANETs are vulnerable to various types of attacks**[**7].

They have proposed the mechanism to detect and mitigate greyhole attack. We have used trust mechanism to detect the attack. Trust mechanism will calculate the trust value of the node in network which is similar to the concept of trust in human society and then this trust value is use to detect the malicious activity in our case packet dropping. We have used task completion and energy consumption as the parameters for calculating the trust value. There can be a situation where attacker can manipulated its attacking strategies to avoid itself from being detected. Our detection mechanism has also taken care of such situation [8]

According to this paper AODV based on multipath has less pronability to attack. Now days, AODV identify multiple paths from source to destination. If one path fails immediately second path will be adopted without identifying the second path individually. According to this paper intermediate position will be adopted by black hole node which affects more than one paths. Now to cope up this such, such paths will be adopted which has minimum no. of intermediate nodes and has less sequence no. than the total available sequence numbers [9].

III. ALGORITHM

Step1 A network with different mobile nodes is setup. One node will works as source node and one node will works as destination node.

Step2 Send the route request to the neighbor node for identifying the destination.

Step3 Receive the route replies. All those paths will be rejected which has those node which were involved in those communication whose performance was serious less.

Step4 Check the network performance under different parameters like Throughput, End to End delay, Packet Delivery Ratio, Success rate.

Step5 Compare the performance on both with and without the attack.

IV. PSEUDO CODE

```
Step1 Build a network of given number of nodes and bind the nodes with AODV protocol.

Step2 Send the route request packet from source to the destination.

Step3 Share the Has key amongst the node.

Step4 if hash key is correct then goto step 5 else goto step 2.

Step5 Send the packet on to the authentified route.

Step6 Identify the performance.

Step7 end.
```

V. PERFROMNACE PARAMETERS

Throughput: it is the amount of packet sent per unit interval of time. These successful packets that has been arrived at the destination.

End to End delay: it is the difference of end time and start time. Start time is at what time packet has been sent. And received time if the time at which packet has been received.

Packet Delivery Ratio: it is the ration of packet sent versus packet dropped. Packets can be dropped due to the congestion or attacker node or with some other problem.

Success Rate: it is the measure of success rate . that means how many packets has been sent and how many packets has been received.

VI. RESULTS AND DISCUSSIONS

6.1 SIMULATION SETUP

Parameter	**Value**
No. of Nodes	50
Protocol	AODV
Communication protocol	TCP,UDP
Application	CBR,FTP
Delay	1ms.
Simulation time	100

Table 1.1

This simulation setup includes basic network settings. Such that in NS2 the network can function. This network simulation shows the network in simulated way.

6.2 NAM SIMULATION FOR NETWORK WITH ATTACK.

Figure 3

This nam simulation shows the attacker node. When any packet arrives at this node all the packets will be dropped. This will deteriorate the performance of the network.

6.4 NAM SIMULATION FOR NETWORK WITHOUT ATTACK.

Figure 4

This network shows that the attacker node has been identified. Now when in any path these attacker will be encountered the path will be left. That path will be adopted which has no attacker node.

6.5 THROUGHPUT GRAPH FOR NETWORK WITH AND WITHOUT ATTACK

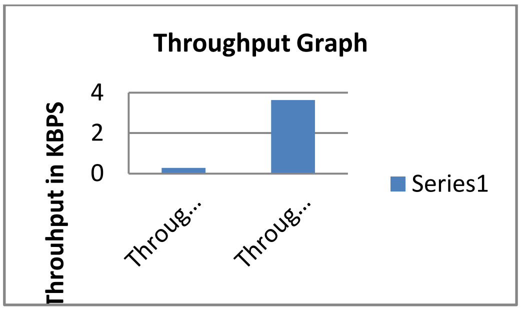

Figure 5

6.6 END TO END DELAY GRAPH FOR NETWORK WITH AND WITHOUT ATTACK

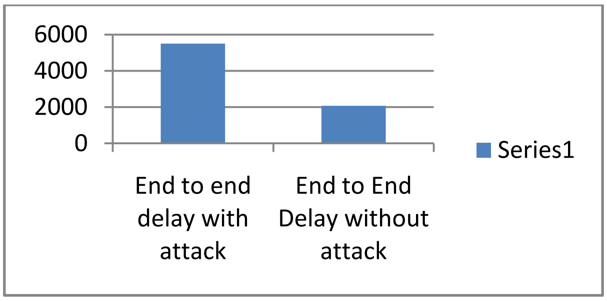

Figure 7

This graph shows the end to end delay for the network with and without attack. In case of situation without attack the end to end delay is less compare to situation when there is attack.

6.7 PACKET DELIVERY RATIO GRAPH FOR NETWORK WITH AND WITHOUT ATTACK.

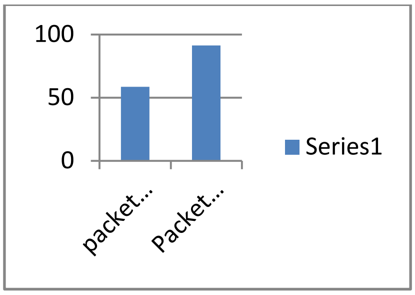

Figure 8

6.8 SUCCESS RATE GRAPH FOR NETWORK WITH ATTACK AND WITHOUT ATTACK

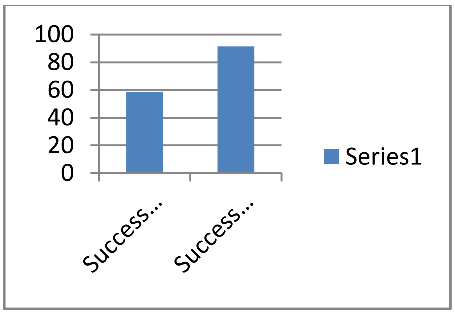

Figure 9

This graph shows the success rate for both the situation. That means under the attack and without the attack.

6.9 PERCENTAGE IMPROVEMENT

Particular	**Percentage**
Throughput	92%
End to End Delay	66%
Packet Delivery ratio	35.88
Success Rate	35.88

Table 3

Above table shows that the network performance on the basis of all the factors has shown the improvement. This means AODV has really improved to SAODV. As secured AODV. Where any attacker node cannot destroy the network performance.

VII. CONCLUSION AND FUTURE WORK

MANET is the mobile ad-hoc network. It is infrastructure less network. There is no central controller which can control the network performance and secure the network from various kinds of attacks. There requires the special arrangement in the protocol so that the attacker node can be identified and removed. It is the special arrangement where any path which has more packet drop rate will be considered as the path having attacker node and while sharing of hash value the two nodes has not correct hash value, will be declared malicious. Any new path which has those attacker nodes in the intermediate list will be avoided. So that network performance can be avoided to be downgraded. In proposed technique all the performance parameters like throughput, end to end delay, success rate and packet Delivery ratio has shown the improvement. In future work further will be extended so that the performance can be further enhanced.

REFERENCES

[1] N.Venkatadri, Reham Abdellatif Abouuhogail and Ahmed Yahya, "Secure TORA: Removal of Black Hole Attack using Twofish Algorithm", International Journal of Software Engineering and its Applications, 2016.

[2] Pham Thi Ngoc Diep, Monika Sachdeva, "Detecting Colluding Blackhole and Greyhole ttack in Delay Tolerant Networks", ICRTEDC-2015, Vol. 1, Special Issue. 2.

[3] Jaydip Sen ," Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks" , Bengal Intelligent Park, Salt Lake Electronic Complex, Kolkata, INDIA,2014

[4] Bansi S. Kantariya1, Dr. Narendra M. Shekokar2," Detection and Mitigation of Greyhole Attack in Wireless Sensors Network Using Trust Mechanism", (2013)

[5] Pham Thi Ngoc Diep," Detecting Colluding Blackhole and Greyhole Attack in Delay Tolerant Networks",2015.

[6] Yanzhi Ren," Detecting Wormhole Attacks in Delay Tolerant Networks",2015

[7] Harsh Pratap Singh," Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", Volume 64– No.3, February 2013

[8] Kanu Geete," A Survey on Grey Hole Attack in Wireless mesh Networks", Volume 95– No.23, June 2014

[9] Akinlemi Olushola O, K. Suresh Babu, "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] Madjid Merabti, David Llewellyn-Joes, and Kashif Kifayat, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.

[11] 11.Ashima Singla and Ratika Sachdeva, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.

[12] R. Kanni Selvam , Mr.C.Karthikeyan, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.