Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET

Deepali A. Lokare
Sinhgad Institute of Technology,
Lonavala, Pune

A.M Kanthe
Faculty of Electrical
Engineering and Computing,
University of Zagreb, Croatia

Dina Simunic
Faculty of Electrical
Engineering and Computing,
University of Zagreb, Croatia

ABSTRACT

A MANET (Mobile Ad-hoc Network) is a network of mobile devices in a self-configuring and infrastructure less environment. The devices in MANET are linked by wireless medium. There are big chances of attacks in MANET due to its natural features including dynamically changing network topology, open medium, no centralized monitoring and management point. There is no assurance of attack free communication. The malicious node(s) causes dropping and forwarding only selective packets are called as gray hole. So, the security solution must be developed to address the protection of data and route. In this paper we attempted to mitigate the gray hole attack and proposes a credit based approach based on Ad-hoc On Demand Distance Vector (AODV) routing protocol. In the proposed and implemented method, we used credit value measurement for the detection of cooperative gray hole attack. This paper shows the technique which is capable of finding chains of cooperating gray hole nodes which drop a major part of communication. The paper shows the result based on varying density, pause time and mobility.

Keywords

Mobile Ad-hoc Network (MANET), Packet forwarding misbehavior, Cooperative gray hole attack, Security, AODV

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of wireless nodes in infrastructure less networks with no central control. MANET can set up dynamically anytime, anywhere without using any pre-existing infrastructure of a network. The media used for communication is wireless and unreliable. Also, the nodes are free to move at random and they act as router at the same time. Hence the transmission of packets was using multi-hop packet forwarding. This sort of network is well suitable for many applications inclusive of military operations, emergency relief and terrorism response. The mobile ad-hoc networks are vulnerable to different types of attacks because no centralized access control, nodes behavior (nodes are free to leave, join and move inside the network) and partial resources. The attacks are various types of DoS (Denial of Service) attacks [1] [2]. Among these attacks, one of the most important security issues is the safety of network layer from different active and dynamic routing attacks. The attack includes gray hole attack and black hole attack.

The basic description of MANET causes some major issues for MANET including security, mobility management, service discovery, IP addresses, radio interference, protocols of routing, bandwidth constraints and power constraints, Quality of Services (QoS), etc. [3]. Intrusion avoidance techniques such as strong authentication and redundant transmission can be used to improve the security of an ad- hoc network. However, these techniques can deal with only a subset of the threats. Moreover, they are expensive to implement.

The most vital concern in MANET is Security for basic functionality of the network. The basic services like reliability, privacy and network services are achieved by assuring that security issues have been met. Mostly MANET undergoes different security attacks because of its open medium, dynamic changes in topology, no central monitoring and management, and no clear protection mechanism. These factors have changed the conflict zone situation for the MANET beside the security threats [4]

The MANET is vulnerable to many active and passive attacks because of the distinctive and challenging features including no central control, unbounded boundaries (nodes are free to roam) and partial resources. Hence important and the first security issue is protection of network layer from different routing attacks.

Today main threat category in MANET is a DoS attack. Also, the attacks are routing attacks. The routing attacks are classified as a Black hole attack and gray hole attack that show signs of packet forwarding misbehavior.

The malicious node (black hole) replies to the each and every attack route request by incorrectly claiming that it leads to destination and has a fresh enough route to the destination. This is called black hole attack. In this fashion, all traffic is forwarded to the black hole node which then leaves them all. Whereas, there is a change in the case of gray hole attack. In gray hole attack, the malicious node (gray hole) acted honest sometimes and dishonest on the other time. During the route discovery process, this nodes act as honest node then once source believes, it silently drops some of data packets. The packets are dropped partially and not completely. The behavior of the gray hole node is unpredictable. A node behaves as honest node and sometimes malicious. Hence, the gray hole attack is an extension of the black hole attack and its detection tougher than black hole attack. However, both attacks are mainly targeted on route discovery process disturbance and degrading network's performance.

1.1.Black Hole Attack

This is a type of DoS attack. In route discovery, the node (black hole) responds to source's request with implying shortest path to the destination. In reality it is not the case. The source believes and sends the data packet through this black hole node and in turn, this black hole node drops all data packets. Due to this attack, the performance of network humiliate completely since the data to be reached at destination never accomplished.

1.2. Gray Hole Attack

Another version of the black hole attack is a gray hole attack. In this attack, the node (gray hole) acts as honest during the route discovery process and once the source sends data packets it start dropping them all. The behavior of gray hole attack is uncertain and unexpected. For some time it is honest and some other time is behaving like malicious by dropping the data packets. Therefore it is a big challenge to detect gray hole attack compared to black hole attack. Also the data packets are not received at destination because of congestion. This is the other reason why the gray hole attack is more tougher.

2. VARIATIONS OF GRAY HOLE ATTACK

The gray hole attacks working can be studied in two parts. In the first part, the gray hole node does the exploitation of AODV (Ad-Hoc on Demand Distance Vector) protocol. The reason behind doing this is to advertise itself as having route to a destination node even though the route is invalid. The packets are interrupted and false commitments are passed on to the source about the route [5]. In the interesting second part the gray hole node crashes the interrupted packets. It simply drops packets coming from (or going to) certain particular node(s) in the network while forwarding all the packets for some other nodes. There is another category of gray hole attack, the nodes who toggle from normal to malicious and back to normal. The phenomenon happens when the route discovery begins and data packet transmission respectively. The gray hole node advertises itself using a routing protocol for having fresh and a shorter pathway to the destination node. Also such node advertises to the packets they want to interrupt. Mostly during the route discovery process, the gray hole node becomes very aggressive and promotes that availability of fresh and shortest path despite looking into their routing table entries. The malicious and forged route is created through responses received from the malicious node to the source nodes. Once the route is created the gray hole will decide whether to drop data packets or route to the unknown node (address).

2.1 Gray Hole Attack in AODV

This is a kind of active attack. Initially the attacker nodes behave normally and reply true RREP messages to the nodes that initiated RREQ messages. When it receives the packets it begins dropping the packets and start on Denial of Service (DoS) attack. The malicious behavior of gray hole attack is different in different ways. This node drops packets while forwarding them in the network. In some other way, the gray hole node behaves maliciously for the sometime until the packets are dropped and then switch to their normal behavior [6]. Because of this uncertain and unexpected behavior, it’s very difficult for the network to detect such kind of attack. The gray hole attack is also called as a node misbehaving attack [7]. So as to differentiate, there are two types of gray hole attack that can be described in AODV.

2.1.1 Internal gray hole attack

This category is decided depending on the position of the gray hole node. In this category, the internal malicious node exists between the two parties of communication. From the source to the destination, the gray hole is available in between them. The gray hole takes a chance to make this route as active route. Hence there is a great chance of having data packet loss from the beginning of data transmission. This called as internal gray hole attack as the attacker is on the route. Hence it's always a challenge to detect internal gray hole node as it belongs to the route of the data. The attack is carried out in many numbers and happens in two steps.

1) Advertisement step- The node tries to advertise and then attract the other nodes by sending false commitments.

2) Attack step- The node starts attacking and drops as many packets as possible. Hence, this is the simple framework in AODV protocol. Figure 1 shows this type of attack. The attacker has to identify the AODV packets in attack step. Using this, it identifies the route, and then sends RREQ packets. In routing, the attacker manages by sending RREQ packets. During attacker step, the attacker starts increasing its sequence number and publicizes itself that it has the highest sequence number as compared to other nodes in the same network. Thus it encourages attack by sending a false reply to the nodes in the same network.

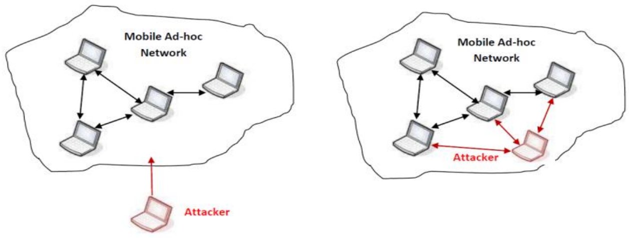

Figure 1 Internal and external gray hole attack

2.1.2 External gray hole attack

This is the reverse side of internal gray hole attack. In this case, the external attacks physically reside outside of the network and refuse access to network traffic. They are capable of doing congestion in the network and also disrupting the whole network. Interesting part of this attack is the external attack can said to be an internal attack when it takes control of internal malicious node and tries to attack other nodes in MANET. In short, the working of external gray hole attack can be easily understood using the following points in sequence.

1. A malicious node first detects the active route and remembers the destination address.

2. A malicious node dispatches a route reply packet (RREP) including the destination address field filled with an unknown destination address. Also, the hop count value is set to minor values and the sequence number is set to the major value.

3. A malicious node sends RREP to the nearest neighbor node which belongs to the mentioned and active route.

4. The neighbor node receives a RREP and replay via the established inverse route to the data of the source node.

5. The source node receives the new information and makes the updating in its routing table

6. For sending data, the new route is selected by the source node

7. The malicious node will drop now all the data to which it belongs in the route.

2.1.3 Active gray hole attack

Active attacks can be an internal or an external attack. The active attacks are meant to destroy the performance of the network in such case the active attack act as an internal node in the network. Being an active part of the network it is easy for the node to make use of and take over any internal node to use it to introduce a false packets injection or denial of service. Figure 2 shows active and passive attack

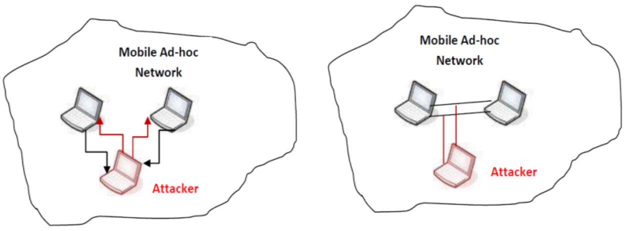

Figure 2 Active and passive gray hole attack

2.1.4 Passive Gray Hole attack

In passive attack, it listens to the network in order to know and understand how they are located in the network, how the nodes are communicating with each other. Before the attacker starts an attack against the network, the attacker has enough information about the network that it can easily capture and introduce attack in the network.

2.1.3 Cooperative gray hole attack

This is another and most recent attack in MANET. It inherits the features of the gray hole attack. In the gray hole attack a malicious node is dropping the packets alone. It doesn't have any cooperation from other nodes in doing malicious activities. However, in cooperative gray hole attack, the attack is made by two or more than gray hole nodes with effective cooperation. The malicious nodes send the false advertisement to other nodes telling fresh and enough routes without looking into their routing table. The malicious nodes work together.

3. RELATED WORK

The AODV protocol is vulnerable to the well-known gray hole attack. A gray hole is a node that occasionally responds positively with a RREP message to every RREQ; in reality it does not have a valid route to the destination node. Since a gray hole node need not to check its routing table always, it responds to the RREQ in most cases. Further, the source tries to route data through the gray hole node, which will drop all the data packets it received rather than forwarding them to the destination. In this fashion, the said malicious node can easily divert a lot of network traffic to itself and could cause an attack to the network with very little effort on it. These gray hole nodes may work as a group. That means more than one gray hole nodes work cooperatively to mislead other nodes. This type of attack is called cooperative gray hole attack. Researchers have proposed solutions for identification and elimination gray hole nodes

S. Banarji et. al. [8] Proposed an algorithm in which before starting the communication source node sends prelude message to the destination the message contain source address, destination address and no. of data packets to be sent. The neighboring node monitors the data traffic and checking whether the next node forward the all data packets or not. At the receiving end after the message is received node sent a postlude message within expire time the message contain no. of data packet received if a data packet received is out of acceptable range then the process of detecting and removing malicious nodes is started by collecting response from the neighbouring node. In this algorithm the overhead is increasing due to additional routing packets. When source node detects black hole node then it broadcasts.

P. Agrawal et. al. [9] In this technique backbone network of strong nodes are established over on an ad - hoc network. In which it assumes that each node in the network is a strong node and trustful node but if it acts as a malicious node then it is detected as a regular node in the network. Source node, send every data block after sending data block it ask the backbone network to carry out end-end checks to destination, whether data packet reached to destination or not. If the data packet never received at destination or destination aware about any kind of attack then it would inform the backbone network. Following this the backbone network starts the detection of the chain of malicious nodes that are cooperating together to drop the packets. On receiving a chain message strong node connected with the destination node initialize a list of gray hole chain to contain the id of the node replied to RREQ. It then initiates all the neighboring nodes to vote for the next node to which it is forwarding packets. If the next id is null then the node is Black hole node. Then the gray hole removal process is stopped and the broadcast to alert the other node in the network. The algorithm will fail if the intruder attacks strong nodes because it violates the assumption that strong node are trusted node.

G. Xiaopang et.al. [10] This technique consists of three algorithms 1) Proof algorithm: - which is based on receiving message source is creating proof of the aggregation signature algorithm. 2) Check up algorithm: - when source are suspect for malicious node then check up algorithm is used.
3) Diagnosis algorithm: -the check up algorithm getting the evidence for diagnosis algorithm for finding the malicious node.

Payal et. al. [11] the DPRAODV is Detection, Prevention and Reactive AODV protocol. That finds threshold value and compares with difference sequence number of reply packet and the route table entry. If it is higher than threshold value then it is added to black listed node. And an alarm packet is generated to inform all other nodes that the node is black hole node. And discard messages from the black listed node. This algorithm increases packet routing overhead due to additional alarm packet.

R. Jhaveri et. al. [12] in this paper author use a technique by which we can detect gray hole node early at the time of the route discovery process. They used sequence number with RREP packet. It compares this sequence number to routing table sequence number if it's greater than one in RREP then the packet is accepted otherwise it is discarded. Source node again re-broadcasts RREQ to their neighbors until a node having a valid route to the destination or destination D itself receives a RREQ.

A. Kanthe et. al. [13] Proposed Algorithm in which checks False_Reply_Count is greater than False_Reply_threshold if it is true then it black list the node. In this method, it stops the detection if the routing table sequence number is less than reply packet sequence number. Also it adds a false reply count if the peak value is greater than route reply packet number. This method uses the static value for the detection of gray hole node.

4. PROPOSED AND IMPLEMENTED APPROACH

The proposed and implemented uses a unique and robust methodology to detect cooperative gray hole nodes. The detected nodes are multiple in number and cooperative in nature. The implemented algorithm is based on AODV protocol with slight modifications. We introduce credit value measurement in AODV protocol. This proposed and implemented an algorithm named as Credit Based AODV (CBAODV). In this approach, initially each and every node assigns a fixed value for its every neighbor node as the neighbor credit value. This credit value is incremented by when it receives a route request packet (RREQ) and decrement when it receives the route reply (RREP) packet. When a node finds credit for one of its neighbors as a negative value, then it identifies the gray hole node. Also it removes all existing paths from its routing table going through that node.

The performance of CBAODV algorithm is tested and observed by changing the number of nodes, mobility and pause time. Based on the study, we simulate the CBAODV protocol using simulation tool Network Simulator (version 2.32) [14]. The simulation area 1000 x 1000 m^2 and results are carried out under different scenario. The CBAODV protocol is described with the help of below three algorithms as in figure 3, 4 and 5.

```
step1: if TTL less than 0 then
    Step 2: discard the packet
Step 3: else
    Step 4: decrement TTL
Step 5: end if
Step 6: if Source ≡ self Address then
    Step 7: discard the packet
Step 8: end if
Step 9: if Seqno⊆ Rseq then
    Step 10: discard the packet
Step 11: end if
Step 12: if Destination ∉RTT then
    Step 13: RTT← RTT∪ Destination
Step 14:  else if (credit<=0)
    Step 15: Malicious node is detected
    Step 16: Don’t forward the RREQ
Step 17: else Credit←  Credit + 1
    Step 18: Rseq← Rseq∪ SSeqno
Step 19: end if
Step 20: if Destination ≡selfAddress then
    Step 21: Send Route Reply Packet
Step 22: else
    Step 23: if Fresh Route Present then
        Step 24: Send Route Reply Packet
    Step 25:   else
        Step 26: Forward route request packet
        Step 27: Assign a credit value (default)
        Step 28: Maintain reverse path
    Step 29: end if
Step 30: end if
```

Figure 3 Route request packet reception

Figure 3 represents the route request packet reception. The algorithm begins by checking TTL (Time To Live) of the packet. The packet is discarded, if TTL is set to zero or less than zero. Also we check the address is self address or not. If it contains self address, packet is discarded. The TTL is decremented by one factor otherwise. It searches destination in its routing table ones the packet is received. If entry is not found then it add an entry and assign default credit value. Whereas if an entry is found, it increments the credit value and adds a sequence number into a cache. Lastly, the route reply packet is sent if destination id found in its routing table else it forwards the route request packet.

```
Step 1: if TTL less than 0 then
Step 2: discard the packet
Step 3: else
Step 4: decrement TTL
Step 5: end if
Step 6: if Destination $\notin$ RTT then
Step 7: RTT $\leftarrow$ RTT $\cup$ Destination
Step 8: else
Step 9: Credit $\leftarrow$ Credit – 1
Step 10: if Credit < 0 then
Step 11: Malicious node is detected
Step 12: Delete its Routing Table Entry
Step 13: Delete from Neighbor's List
Step 14: end if
Step 15: end if
Step 16: if Source≡selfAddress then
Step 17: Update Routing Table
Step 18: else
Step 19: Update routing table
Step 20: forward packet
Step 21: end if
```

Figure 4 Route reply packet reception

Figure 4 represents the phenomenon of route reply packet reception in detail. Initially it checks the TTL of a packet. If the TTL became zero packet is discarded else TTL is decremented. If the source receives reply then it updates the routing table else the intermediate node adds its entry credit value.

Figure 5 represents the data packet reception algorithm stepwise. This is an important algorithm as per detection of the cooperative gray hole is concerned. Here also the packet is discarded if TTL is zero. Now the credit value plays an important role which helps in detection of cooperative gray hole attack. The lookup in the routing table is done when the packet is received by a node. The route discovery starts if entry is not found in the routing table. If an expected entry is found in the table, the respective credit value is checked. If the credit value found to be positive then it forwards the of a time, the routing table entry is deleted. packet. Whereas, if credit value is negative then, for a period

```
Step 1: if TTL less than 0 then
Step 2: discard the packet
Step 3: else
Step 4: decrement TTL
Step 5: end if
Step 6: if Destination $\notin$ RTT then Start Route Discovery
Step 7: else
Step 8: if credit $\leq 0$ then
Step 9: Malicious node is detected
Step 10: RTT $\leftarrow$ RTT$-$ Destination
Step 11: Delete from Neighbor's List
Step 12: else
Step 13: Forward Packet
Step 14: end if
Step 15: end if
```

Figure 5 Data packet reception

5. PERFORMANCE METRICS

To evaluate the performance of our solution, we compare our solution (CBAODV) with AODV without attack and AODV with the attack. We consider several performance metrics. The existence of gray hole nodes in a mobile ad-hoc network directly causes to packet loss in between the source and the destination. This will also have an effect on the throughput between source and destination. Hence, we select the throughput ratio as one performance metric, data packet loss as another and routing overhead as last metric. Since this protocol uses more control packets, we need to find out the control packet overhead that the solution introduced. Then we are also selecting other performance metrics as packet delivery ratio and end to end delay. Next we describe the above five metrics in details.

Throughput ratio

The throughput is defined as the number of bytes received over transmitted per second. Let *T* denotes the throughput ratio and *is* calculated as follows:

$$T = \frac{\sum_{i=1}^{N} T_i^{r}}{\sum_{i=1}^{N} T_i^{S}} X 100$$

Where, T_i^r denotes average received packets and T_i^s denotes average transmitted packets.

Packet loss ratio

Packet loss in MANET is complicated because wireless link are subject to transmission error and network topology changes dynamically. A packet may lose due to transmission error, no route to destination, broken link and congestion.

Let L denotes the loss of data and represented as:

$$L = \frac{\sum_{i=1}^{n} (N_i^{s} - N_i^{r})}{\sum_{i=1}^{n} N_i^{S}} X\ 100$$

Where N_i^r and N_i^s are the number of packets received and sent respectively.

Average end-to-end delay

End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

Let D denotes average end-to-end delay and calculated as:

$$D=\frac{\sum_{i=1}^{n} d_i}{n}$$

Where d_i denotes average end to end delay for n packets.

We are using these mathematical concepts and equation to make performance metrics.

Packet delivery ratio

It is the ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to the destination.

∑ Number of packets receive / ∑ Number of packets send

Normalized routing overhead

It is defined as the total number of routing packets transmitted per data packet.

6. SIMULATION SETTINGS AND RESULTS

Table 1 Simulation parameters

Sr. No.	Parameter	Value
1	Simulator	NS 2.32
2	DoS Attack	Gray hole, Cooperative Gray Hole Attack
3	Channel Type	Wireless channel
4	Antenna Type	Omni directional
5	The protocol used	AODV
6	Underlying MAC Protocol	IEEE 802.11
7	Propagation Model	Two-Ray Ground
8	Queue	PriQueue
9	Area	1000 x 1000 m^2
10	Simulation time	100 Sec
11	Pause time	10 Sec
12	The number of Malicious nodes Detected	Two or more nodes which cooperate each other for dropping packet
13	Traffic type	CBR(UDP)
14	CBR rate	512 byte
15	Speed	1 to 20 m/s
16	Nodes	10 to100

The results were carried out in one propagation model namely two ray ground model with varying the parameters as mobility, pause time and number of nodes. The respective results of each scenario are shown from Figure 6 to Figure 10. NS2 is used as a simulation platform with parameters as shown in Table 1.

Impact of number of nodes

The impact of the number of nodes on different performance metrics is depicted in the Figure 6 to Figure 10 keeping on all parameter shown in Table 1. Moreover, in each graph, the number of nodes varies from 10 to 100 with all other configurations are fixed including pause time and mobility.

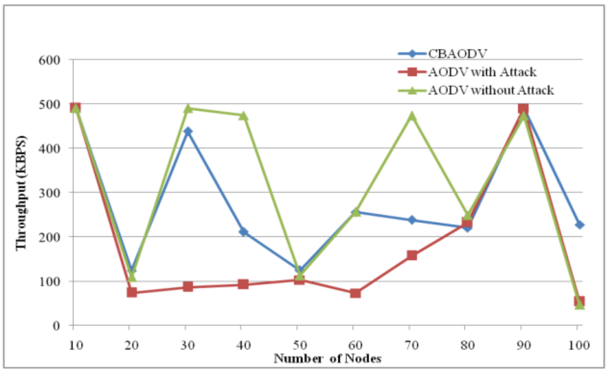

Figure 6 Throughput vs number of nodes

Figure 6 demonstrates the impact of the number of nodes on throughput for protocols AODV and AODV with attack including our solution CBAODV. The first observation of the figure is, AODV with attack protocol suffer a lot from the cooperative gray hole attacks since this protocol doesn't have any provision that prevent cooperative gray hole attacks. Moreover, the throughput of AODV with attack goes down by 55% under regardless of the number of nodes in the network. The second observation is that our protocol CBAODV gives higher and improved throughput than AODV with attack and it's close to the performance of plain AODV (without attacking) protocol. The reason behind the improvement is that the CBAODV strongly prevents gray hole attack because of credit value measurement and in turn, saves packet drops that gray holes does frequently. Furthermore, CBAODV gives higher throughputs compared to other protocols even the number of nodes is more which has more chances of attacks.

Figure 7 demonstrates the impact of the number of nodes on packet loss. The first observation is that, there are heavy packet drops in AODV with attack; we can see prominently that the solution of AODV with attack suffered with approximately 20% increase in packet loss as compared to the CBAODV solution. Therefore, there is a high packet loss percentage in spite of the number of nodes in the network. The second observation is that the packet loss for our solution CBAODV is higher but lower than AODV. Since AODV does not have any type of attack, its plain AODV protocol without attack. Third observation is that protocol gave much lower packet loss percentage than AODV with attack because our protocol put off both individual and cooperative gray hole attacks. Also there is slight increase the in packet loss in our protocol as the number of nodes increases.

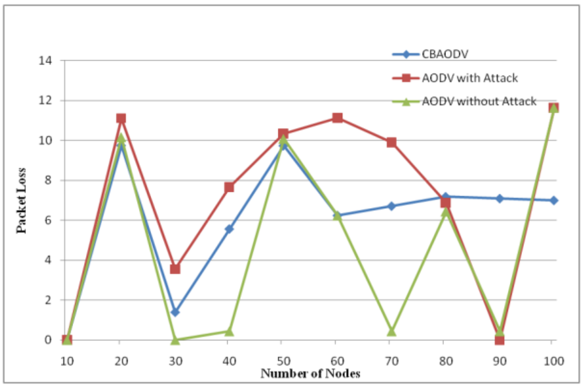

Figure 7 Packet loss vs number of nodes

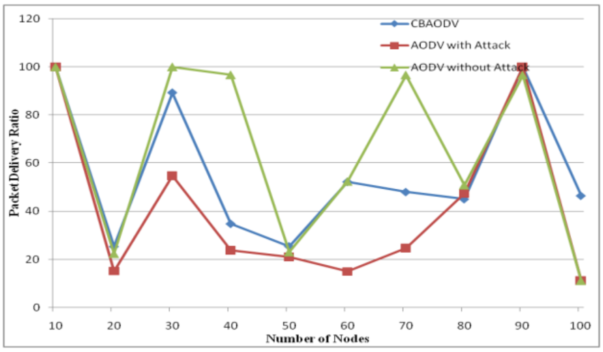

Figure 8 Packet delivery ratio vs number of nodes

Figure 8 demonstrates the impact of the number of nodes on packet delivery ratio. The first observation is that CBAODV protocol has a high packet delivery ratio as compared to others since it takes safer and attack free route for data delivery. The second observation is that, AODV with attack having very less packet delivery ratio i.e. approximately 32% decrease, since it does not have any mechanism to prevent from data loss. Third observation is that the packet delivery ratio is high even though the number of nodes is increasing.

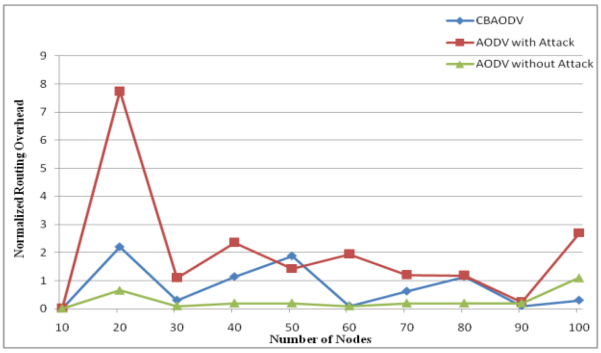

Figure 9 Normalized routing overhead vs number of nodes

Figure 9 demonstrates the impact of the number of nodes on routing overhead. The first observation is that the AODV without attack introduces the least overhead since it does not use any additional requests for deciding secure routes. It also decreases the routing overhead when the number of nodes increases. Second observation is that the solution proposed by us, CBAODV, also introduced the very least amount of overhead with the cooperative gray holes since it checks only the first next hop of intermediate node. Our protocol introduces very less overhead when number of number of nodes increases. Compared to AODV with the attack having an overhead increase as compare to CBAODV is approximately 60%.

Figure 10 demonstrates the impact of the number of nodes on end-to-end delay. The first observation is that our protocol has a little bit of more end-to-end delay compared to others since it takes more time to find out a safe and attack free route. Therefore, this will be the tradeoff between the packet loss and delay. The second observation is that, our solution increases slightly the delay as the number of nodes increases. AODV with attack is having a 5% increase in end- to-end delay as compared to CBAODV.

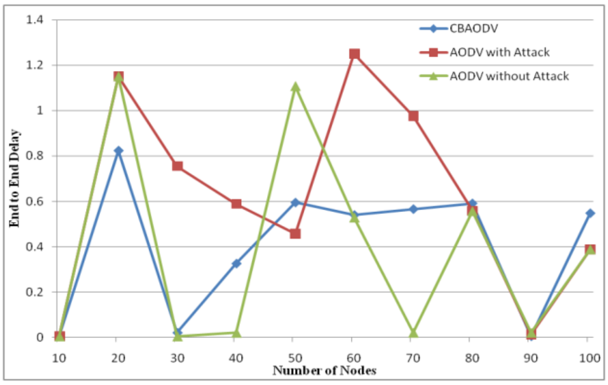

Figure 10 End-to-end delay vs number of nodes

Impact of Mobility

The impact of the mobility on different performance metrics is depicted in the Figure 11 to Figure 15 keeping on all performance metrics discussed above as unchanged. Moreover, in each graph, the mobility varies from 1 to 50 m/s with all other configurations is fixed, including the number of nodes which is 50 and pause time 10 sec.

Figure 11 demonstrate throughput of CBAODV compared to AODV with and AODV without attack Important observation is that the throughput of CBAODV is higher when mobility is less than 30 m/s. This shows the higher performance because of less packet loss prevented using credit value scheme used in CBAODV.

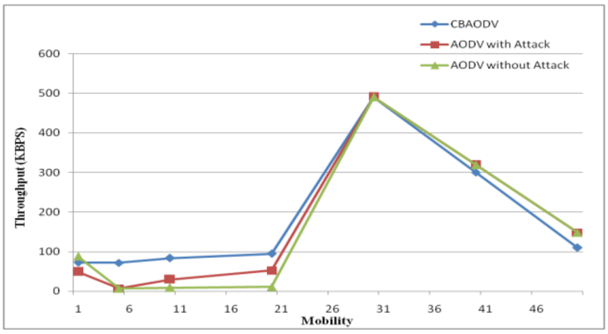

Figure 11 Throughput vs mobility

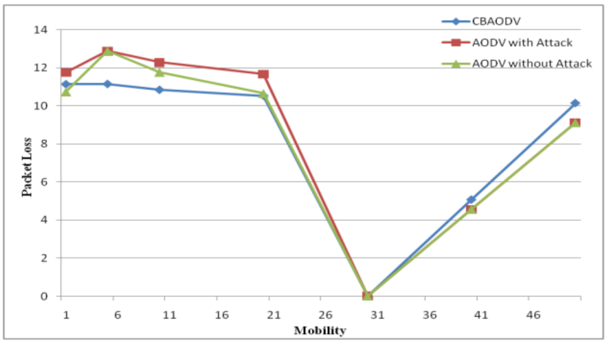

Figure 12 Packet loss vs mobility

Figure 12 demonstrate the impact of mobility on packet loss. The important observation is that CBAODV has lower packet loss compare to other protocols when the mobility is less than 30 m/s. The important reason is CBAODV uses identification of malicious nodes using credit value.

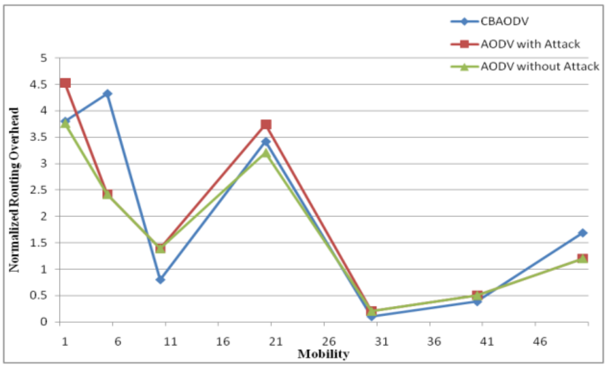

Figure 13 Normalized routing overhead vs mobility

Figure 13 demonstrate the impact of mobility on normalized routing overhead. First observation is AODV without attack has less overhead because it does not use any special requests for making secure routes. However, in some cases, CBAODV produces more overhead since it checks for secure route.

Figure 14 demonstrate the impact of mobility on packet delivery ratio. Important observation is that the packet delivery ratio of CBAODV is higher compare to other protocol and approximately 15% higher than other protocols. Since it decide secure route before data transmission

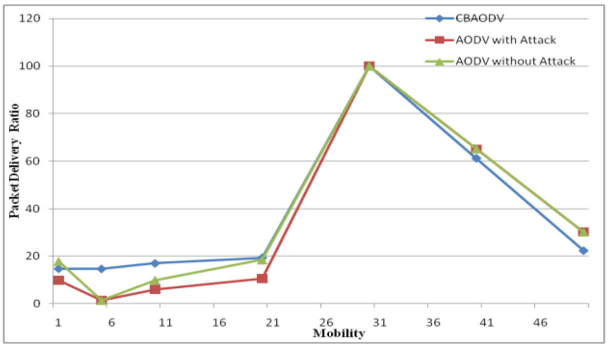

Figure 14 Packet delivery ratio vs mobility

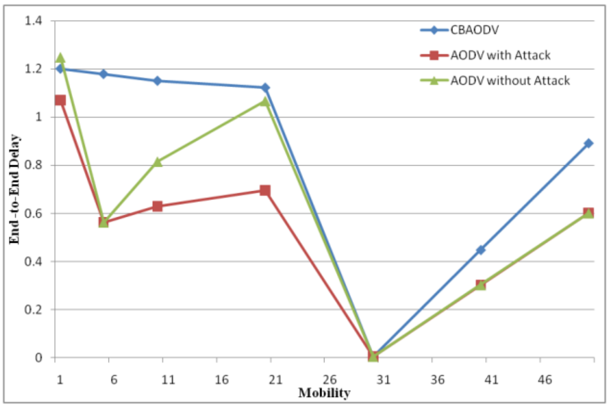

Figure 15 End to end delay vs mobility

Figure 15 demonstrate impact of mobility with end to end delay. Important observation is that CBAODV has more end to end delay compare to other protocols. Because CBAODV takes more time to decide secure and attack free route.

Impact of Pause Time

The impact of the varying pause time on different performance metrics is depicted in Figure 16 to Figure 20 keeping on all performance metrics discussed above as unchanged. Moreover, in each graph, the pause time varies from 1 to 20 sec with all other configurations are fixed, including the number of nodes which is 50 and mobility speed is 1.0 m/s.

The said performance metrics like throughput, packet loss, routing overhead, packet delivery ratio and end to end delay are in figure 16 to figure 20 and observed under the impact of pause time.

In figure 16, the throughput of AODV with attack is decreased as compared to CBAODV by approximately 10%. We strongly propose that the performance of our proposed CBAODV solution shown better performance. Credit value measurement is central reason for less packet loss. Hence there is improvement in throughput.

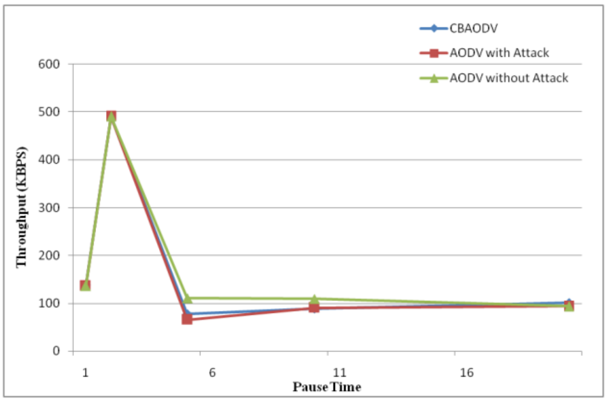

Figure 16 Throughput vs pause time

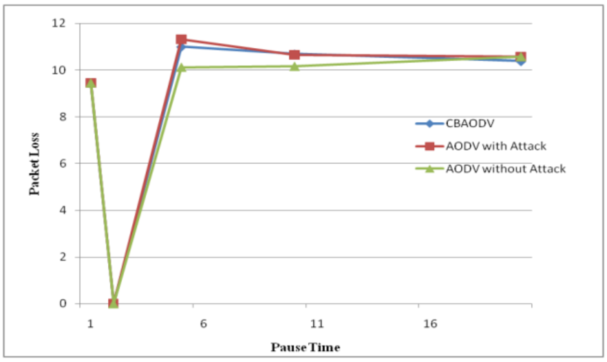

Figure 17 Packet loss vs pause time

In the figure 17 the result of CBAODV has less packet loss compared to AODV with an attack when there are 6 ms and above 16 ms. The packet loss is minimized in CBAODV using unique credit value measurement method. Hence there is less packet loss.

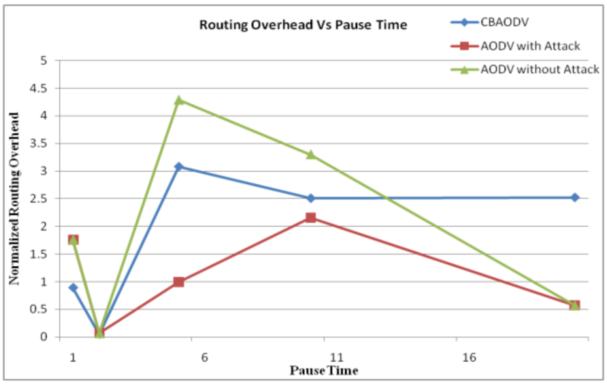

Figure18 Normalized routing overhead vs pause time

Figure 18 shows the impact of pause time over routing overhead. The normalized routing overhead is decreasing in CBAODV with 0.5 to 20%. The CBAODV uses predefined procedure of making secure route

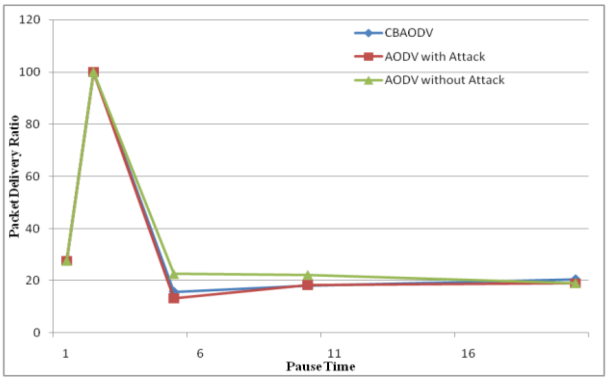

Figure 19 Packet delivery ratio vs pause time

In figure 19, the CBAODV has produced higher packet delivery ratio compared with AODV with attack because it identifies the malicious nodes.

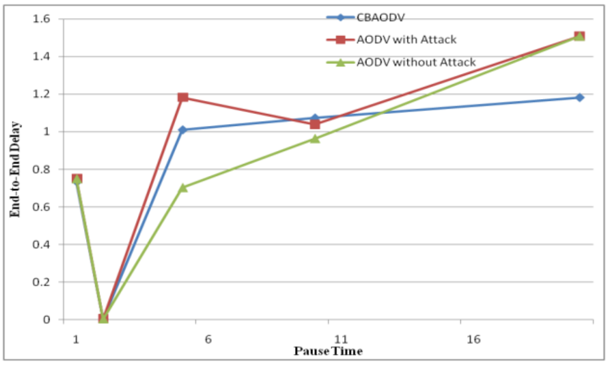

Figure 20 End-to-end delay vs pause time

Figure 20 demonstrate the impact of pause time on end to end delay. The CBAODV solution includes malicious node detection mechanism which increases end to end delay.

7. CONCLUSION

The cooperative gray hole attack is one of the serious attacks on MANET. In proposing CBAODV approach, we use the credit value measurement system that prevents cooperative gray hole attack in MANET. Every node assigns a credit value that we are sending the route request and subtracting the credit value when we got a reply from them. Credit based approach to mitigate the gray hole attack is proposed in this paper, which can detect cooperative or chain of the gray hole node. Proposed idea is implemented by considering two ray ground model. Our proposed solution simulated using the NS2 simulator and compared its performance with the original AODV without attack and with attack in terms of throughput, packet loss rate, normalized routing overhead, packet delivery ratio and end-to-end delay. The results were improved in many cases coming under different scenarios like varying speed, pause time and number of nodes. Simulation results show that the credit based approach improves performance of the network be detecting the cooperative gray hole nodes. This paper presents good performance in terms of better throughput and minimum packet loss percentage over AODV without attack and AODV with attack. In future work this algorithm, static value is used for assigning credit for every node. A dynamic value can also be generated for assigning credit.

8. REFERENCES

[1] R. Prasad, S .Dixit, R. Van Nee, “Globalization of Mobile and Wireless Communication”, March 2011, Springer. ISBN13:9789400701083..

[2] L. Gavrilovska, R. Prasad,” Ad Hoc Networking Towards Seamless Communications”, Springer 2006, ISBN: 1402050658.

[3] A. Kanthe, D. Simunic, M. Djurek , “Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks”, MIPRO 2012, IEEE Conference, Proceedings of the 35th International Convention, ISBN:978-1-4673-2511-6,May21-25,2012, Opatija,Croatia.

[4] A. Kanthe, D. Simunic , R. Prasad, “Effects of Malicious Attacks in Mobile Ad-hoc Networks”, 2012 IEEE International Conference on Computational Intelligence and Computing Research, ISBN:978-1-4673-2481-6,18-20, December 2012, Coimbatore, India.

[5] M. Kumar, R. Mishra, “An Overview of MANET: History, Challenges and Applications”, Indian Journal of Computer Science and Engineering (IJCSE), ISSN: 0976-5166 Vol. 3. No 1. Feb-Mar 2012.

[6] C. E. Perkins and E. M. Royer, “Ad-Hoc on Demand Distance Vector Routing”, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, pp. 90-100, Feb, 1999.

[7] Zhu, C. Lee, M. J. Saadawi, T, “RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing Protocols,” IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.

[8] S. Banerjee “Detection/removal of cooperative black and gray hole attack in mobile ad hoc networks”, In Proceedings of the World Congress on Engineering and Computer Science, October 22 - 24, 2008, San Francisco, USA

[9] P. Agrawal, R. Ghosh, S. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008

[10] G. Xiaopang, C. Wei, "A novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" Network and Parallel Computing Workshops, 2007, NPC Workshops, 2007, IFIP International IEEE Conference.

[11] Raj P , Swades P , “DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV based MANET” In International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp:

[12] R. Jhaveri, S. Patel and D. Jinwala, “A Novel Approach for Gray Hole and Black Hole Attacks in Mobile Ad-hoc Networks” Second International Conference on Advanced Computing& Communication Technologies,2012.

[13] A. Kanthe, D. Simunic, R. 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.

[14] The network simulator-ns 2.35 http://www.isi.edu/nsnam/ns/, 1996-97