Volume-4, Issue-5, May-2015 • ISSN No 2277 - 8160

Research Paper Technology

Monitoring and Detection of Gray Hole Attacks in Manet to Achive Minimum Packet Drop Rate

Sushma B. Akhade Department of CSE ,TPCT, COE,Osmanabad

Prof. Dr. S.M Jagade TPCT, COE, Osmanabad, Dr..BAMU, Aurangabad

ABSTRACT

Information Technology is one of the fast growing area. Users of Information Technology devices such as computer, handled devices are from students to Researchers. To fetch the information or to exchange the information from one another devices, these devices can communicate with each other using some protocols. These devices may be connected with wired network or by wireless network. The medium of communication may be unsecure and the transmitted data can be prone to malicious activity. Wireless networks are more prone to malicious activity than wired network.AD hoc networks is special kind of interconnection of wireless network. The network is created temporary as per requirement area . In this each node itself acts as router in MANET. Any device can join or leave network at any time so, malicious devices can join the network any time without any detection.

Ad hoc network are established where there is absence of interconnection backbone and mostly use in emergency needs. There are various types of attacks such as Wormhole attack, Misdirection, Flooding attack, Packet drop attack, black hole attack, gray hole attack. Among them most destructive attacks are gray hole and black hole attack who's intention is to degrade the overall performance of network. Gray hole is similar to black hole attack but it switches from black to normal and vice versa, Hence detection of gray hole attack is difficult. In this report an innovative approach is proposed to detect gray hole attack.

KEYWORDS : MANET , Gray Hole, Black Hole, AODV, DSR

I INTRODUCTION

ADHOC Networks

Computer Network or internet is the interconnection between the computers or devices. Wired networks are the networks which have the network backbone or infrastructure using fixed wires their distance among each node is fixed with respect to one another, nodes are not mobile hence static topology is maintained. While ad hoc networks are temporary in nature. They are established for specific time being, for specific use where the backbone for communication is absent. It is especially useful in any place where the deployment of base stations or access points is impossible or expensive such as disaster rescues, battlefields, dangerous environment, etc. MANET is the internet among the mobile computers or communication devices, mobile node can join or leave network anytime, and the nodes at any instance may change their position with respect speed and mobility pause time, hence the network topology is dynamic and multi hop in nature.

Each device/node not only act as acts as host but also as router ,to route a packets from source to destination as per route request. Reliability ,security and availability of ad hoc networks are less than wired networks because of the constraints like individual node's battery power, Range of communication, speed, pause time, adaptation in changing environment. The devices in the network have different architecture, Operating System and characteristics. E.g. Mobiles with android OS and IOS, Mac-Book, Windows machine. _[1]

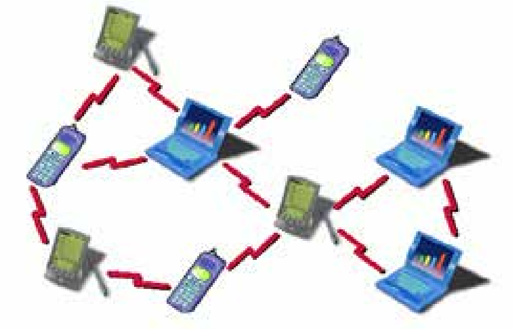


Figure 1.1:Heterogeneous network of having different hardware, platform.

Devices in the network have same hardware architecture, Operating System.

E.g. All devices are Windows machine.

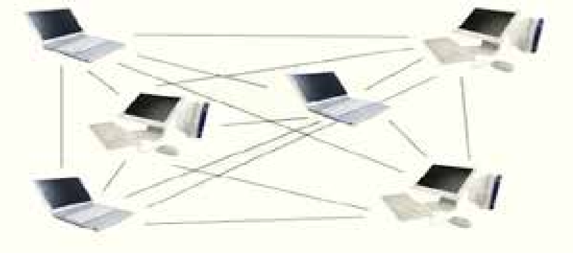


Figure 1.2:Homogeneous Network of only computer/ laptops.

Characteristics of Ad hoc Networks

- Ad hoc networks are self organizing and adaptive.
- Each mobile host acts as a router as well as host.
- Each node acts as server as well as client.
- Supports peer-to-remote communications.
- No centralized server for administration.
- Can be easily deployed like plug and play.

Challenges

- Due to mobility network topology is dynamic.
- Frequent network partitions and grouping of nodes.
- Every node can be mobile or static to some position for certain period of time.
- Limited power capacity(battery)
- Limited wireless bandwidth Presence of varying channel quality(some node configuration may be good some may not).
- Sensitive to malicious attacks.[2]

II LITERACTURE SURVEY

Shalini Jain[3] proposed the technique of detection using defragmenting data.

Processes performed at Source node. Packets are divided into n number equal parts this parts sent to destination in the form of messages. When the destination receives count of number of messages, then sources starts sending actual data. A timer is set until all packets are not received by destination. If number of data packets at destination is less than a limit, initiates removing process of black/gray hole attack as it is assumed that some packets has been dropped. After ending of timer, if it did not get any message from destination, starts removing function of black hole attack. Detection process at destination node. After a timeout, number of data packet is sent to source node. Source will send monitoring message, after getting this each node starts a counter for counting number of data packets of its neighbors. Source node gets the information malicious node with the help of neighbour monitoring. And select the node as malicious which have been set malicious by neighbours (like a vote).If votes of neighbors about malicious activity of node exceeds from a limit, source enters that node in blacklist and finds (selects)a new route to destination.

S.Marti [4] proposed a technique, in which watchdog timer is used. Each node in the network monitors its next hop node in the route. If it finds any packet forwarding misbehaviour, it will mark the next node as a malicious node to the source. Source node should believe on the other node's information about one node's maliciousness. This technique is not so effective as it is not using proper required data for detection of next hop node.

Abderrahmane Baadache[5] proposed technique in which he used Merkle tree concept. Merkle tree is a binary tree in which each leaf node has a hash value and intermediate nodes use that hash values for detecting black hole attack, this hash value is combination of node's id and a secure value that only the node knows. Source node save concatenation of all hash values of nodes on one route to destination in its memory. Each node sends combination of its hash and previous nodes in route with RREP packet from destination to source. Source node compares this value with saved concatenation of hash value of this route in its memory and if any differences found, then it will informs to other nodes about maliciousness of this route. Difference result shows that one node may drops RREQ packets and does not send packets to destination. This technique may create calculation overhead.

Ramaswamy's[6] approach Data Routing Information (DRI) table is maintain at each node that has two fields named from bit and through bit. Consider a node. For a node. FROM means I have accepted or routed packet from so and so node. THROUGH means I have routed or forwarded my packets through so and so node. During route discovery source initiates by sending RREQ packets. If destination sends back RREP, source trusts to its answer as it may it next hop. If an intermediate node returns RREP, that node should also send its DRI table and ID of next neighbor in the route to source. If source previously sent a message to that node, it is a trustable node for source and starts sending data packets through that to destination. If source does not know that node, it sends a packet to next node of marked node and asks it for DRI table and also ID of its next node. In cross-checking the data provided by DRI table is checked whether its correct or not.

Y.Hu[7] proposed a Secure Efficient Ad hoc Distance Vector routing protocol (SEAD) based on the structure of Destination Sequenced Distance Vector (DSDV). It uses the reply protection of routing update messages. It is uses the one way hash function. This protocol is examined against DSR protocol. This protocol can protect from external attack only. It will not protect from internal attack. Hence it is not possible to detect eavesdropping. Because of hashing technique there is calculation overhead.

Payal Raj[8],DPRAODV technique uses packet sequence number(R-REP) of replying node and threshold value. It uses the concept of dynamic learning method, in which threshold value is dynamically updated through at instance of time when RREP packet is received. If RREP packet sequence number is greater than the threshold value, then the node is considered to be malicious and it will add in blocked list. It sends ALARM packet to the neighbors informing about malicious node. This protocol takes higher routing overhead due to ALARM packets. This modified protocol does not detect gray hole attack.

III ROUTING IN MANET

If the nodes/devices are within the range of each other, then routing is not necessary as they can directly communicate with each other directly (neighboring nodes are source and destination). If a node (either source or destination) moves out of range, and they are not able to communicate with each other directly (within single hop), intermediate nodes are needed to establish communication between them. The purpose of a routing algorithm is to define a scheme for transferring a packet from one node to another. This algorithm takes decision to choose their next hop for communication based on criteria such as number of hops to communicate to destination, latency, transmission power, bandwidth, etc.

Ad hoc routing protocols can be classified as either proactive or reactive, depending on the method used to discover and maintain routes [9].

Proactive routing algorithms are table driven using link state routing in which the algorithm maintains the partially copy of network and cost of communication needed to communicate with nodes in network, basically proactive algorithmic are used where the network topology is known or may not change by enough period of time. They can be optimized.eg Destination Sequenced Distance Vector (DSDV) [10].

Reactive routing algorithms does not maintain any predetermined information of network, this algorithms are runtime in nature. Information are collected only when routes are to establish that is on demand, routes are discovered on when needed.

They can be optimized up to certain limit. Proactive is more reliable than reactive.

E.g. Ad hoc On-demand Distance Vector (AODV),Dynamic Source Routing(DSR) .

Routing challenges

- Routers are moving i.e. Intermediate node are mobile.
- Link changes as neighboring node are changing positions.
- Packet losses due to transmission errors.
- Flooding of Control message increasing routing overhead.
- Routing loop may exist even using sequence numbers.[11]

IV TYPES OF ATTACKS

There can be two kinds of attacks:

1. passive attack and
2. active attack

Active attacks can be further divided in two types

1. Internal Attacks And
2. External Attacks

External attacks are divided in following types

1. Attacks Using Impersonation,
2. Attacks Using Modification,
3. Attacks Using Fabrication

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) may disturb the network operations or consume node resources. Some well-known fabrication attacks are[12]

1. Gray Hole Attacks
2. Black Hole Attacks

BLACK HOLE ATTACKS:

In Black hole attack, the malicious node generates and sends fabricated routing information and advertises itself as having a valid shortest path to the destined node. If the malicious node replies to the requesting node before the correct node replies, a false route will be created. Therefore, packets will not reach to the specified destination node. A black hole is a malicious node that replies for route requests without having an active route to the destination. Then the routing protocol advertise malicious node as having a good and valid path to a destination node. It tries to become an member of an active route, if there is a chance. It has bad intention of disturbing data packets being sent to the destination node. Cooperative black hole attack is caused by many neighbor black holes cooperating each other. Black hole attack may be internal or external.

GRAY HOLE ATTACKS:

Gray hole attack is an extension of Black hole attack in which a malicious node's behavior is unpredictable. A node behave maliciously for a sometime, but after that it behaves just like other normal nodes. Both Black hole and Gray hole attacks create a problem in the network by disturbing route discovery process and minimises network's performance. A gray hole may forward all packets to destination nodes but may drop packets coming from source destined to specific nodes. Sometimes, a node may combine the behavior of attacks discussed above. Due to this uncertainty in behavior of gray hole, this type of attacks are more difficult compared to black hole attack. Like black holes, cooperative gray hole attacks may be possible against AODV.

These two types of attacks disturb process of route discovery, which is done by the routing protocol.

Ad hoc networks are more prone to attacks because :

- **Open Medium**

Any one can join. Hence, internal attack is easier than in wired network.

Any node can steal a confidential data as the malicious node can be intermediate node.

- **Dynamically Topology due to mobility**

Nodes can join and leave the network at any instance of time, changing their position hence the network has changing topology. This allows any malicious node to join the network.

- **Mutual trust among nodes**

In ad hoc networks every node trust other node , hence a normal node can trust a malicious node and try to route the packet through it.

- **Centralized Monitoring is absent**

There is no centralized infrastructure that prohibits any monitoring agent in the system, every nodes target is sent packet to destination and not keeping audit of any nodes and to become coordinator.

V PRAPOSED WORK

The new technique is presented here for detection of malicious nodes .

Algorithm for Gray Hole/Black Hole Attack Detection

1. Start (for each node which receives RREP).

2. Check if a replying node has generated

False_Reply_Count greater than False_Reply_Threshold

if yes goto step 3,

no goto step 4

3. Black list the node, don't accept any RREP packet (discard) from this node further.

4. Check if routing table sequence number is less than reply packet sequence number.

if yes goto step 6

no goto step 5

5. Skip detection engine and goto step10.

6. Calculate

- Difference between routing table sequence number and route reply sequence (Diff.).

RFR- Reply Forward Ratio

- Peak = ([((Diff) × RFR) + No. of replies received by replying node + Current Simulation Time])/3

7. Check if peak < route reply sequence number

If yes goto 8

No goto 10

8. Add/Increment the false reply count to corresponding replying node.

9. Free the packet (RREP)

10. Follow the remaining aodv recvreply() function.

VI RESULTS

Platform for implementation

Network simulator is an open source Unix based object oriented simulator. It is used for simulating the network protocols. Object Oriented Tool Command Language(OTCL) is scripting language used for configuring the nodes and setup the scenario. While the protocol algorithms are written in C++.

Output of simulation are two files, NAM file and TRACE file ,both are used for analysis purpose.NAM file is visual Animation file while TRACE file are used for calculating the performance metrics using AWK files.

Below are few performance metrics which can be compared for three cases i.e. for normal AODV , AODV with Gray hole , AODV with solution for attacks

- Total Packet sent
- Total Packet Received
- No. of Dropped Packets
- Packet Drop Rate:

Packet drop Rate is the ratio of total lost packets to generated packets by the sources. We are calculating values for all these parameters in two cases :

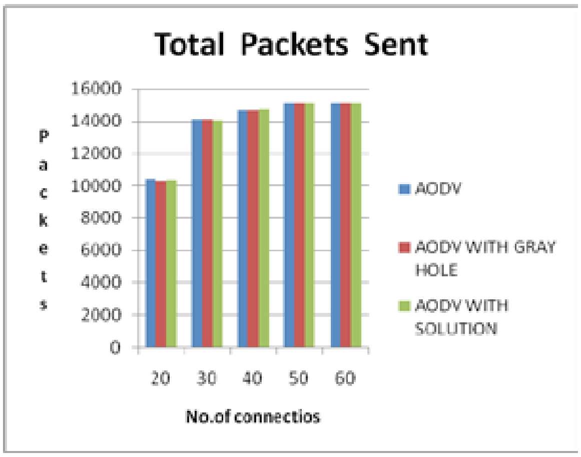
1. No. of nodes fixed and No. of connections are variable

2. No. of connections is fixed and No. of nodes are variable

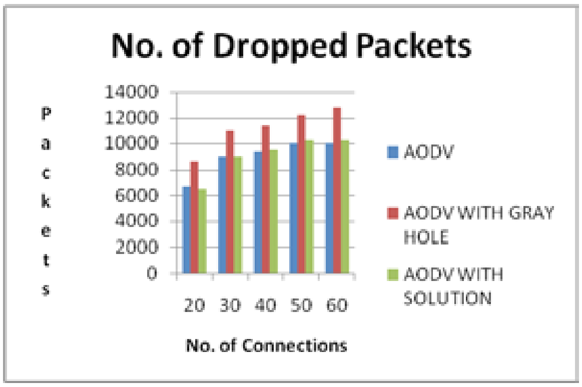
Result Tables are as follow,

When the no. of Nodes = 60

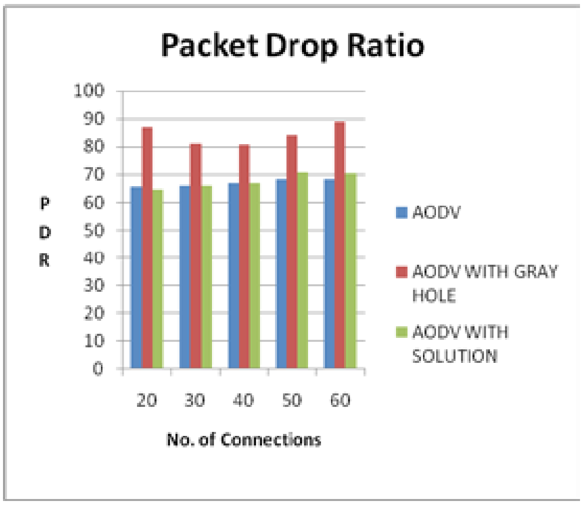
Total Packet Sent			
No.of connections	AODV	AODV WITH GRAY HOLE	AODV WITH SOLUTION
20	10418	10335	10361
30	14089	14083	14057
40	14703	14660	14716
50	15098	15058	15058
60	15098	15083	15111



No. Of dropped Packets			
No.of connections	AODV	AODV WITH GRAY HOLE	AODV WITH SOLUTION
20	6677	8628	6497
30	9014	10956	9038
40	9378	11380	9528
50	9978	12212	10271
60	9978	12814	10230

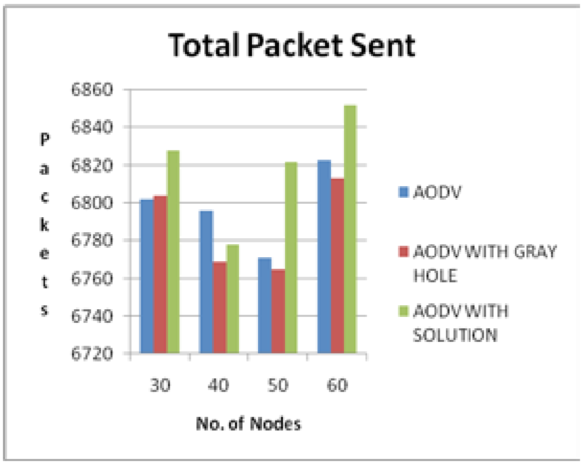


Packet drop ratio			
No.of connections	AODV	AODV WITH GRAY HOLE	AODV WITH SOLUTION
20	65.68	86.84	64.69
30	65.96	81.13	66.09
40	66.86	80.67	67
50	68.45	84.3	70.74
60	68.45	88.94	70.44

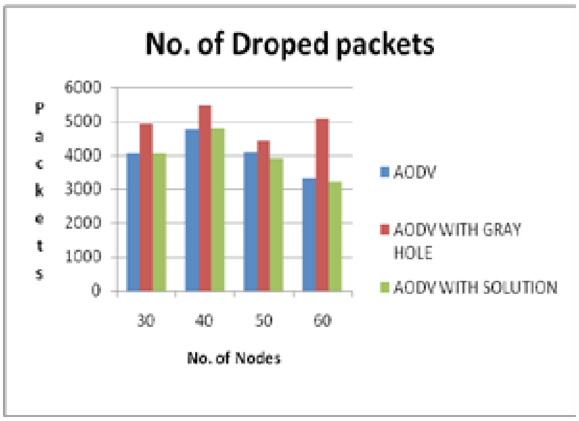


When No. of Connections fixed

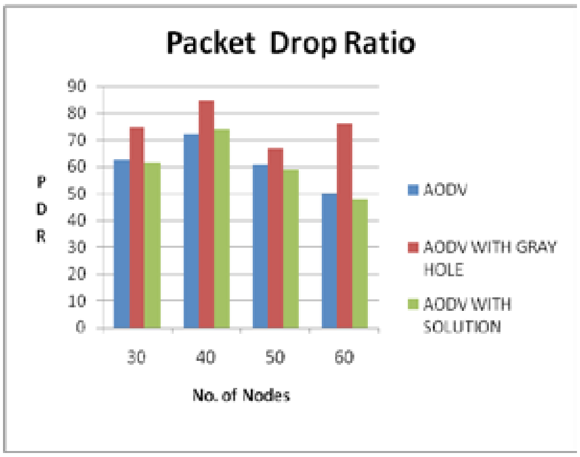
Total Packet Sent			
No. of Nodes	AODV	AODV WITH GRAY HOLE	AODV WITH SOLUTION
30	6802	6804	6828
40	6796	6769	6778
50	6771	6765	6822
60	6823	6813	6852



No. Of dropped Packets			
No. of Nodes	AODV	AODV WITH GRAY HOLE	AODV WITH SOLUTION
30	4050	4925	4041
40	4767	5450	4786
50	4086	4433	3918
60	3322	5091	3204



Packet drop ratio			
No. of Nodes	AODV	AODV WITH GRAY HOLE	AODV WITH SOLUTION
30	62.2	74.51	61.3
40	72.19	84.46	73.81
50	60.71	66.54	59.04
60	49.83	76.22	47.85



VII CONCLUSION & FUTURE WORK

Ad hoc networks are more prone to attacks Major destructive attacks are black hole attack and gray hole attack. Various methods to detect has been studied, disadvantages are observed in DPRAODV, Kurosawa's and Jhavari's approach. In which normal node with higher sequence number than threshold value may get in black list. Alarm packets are sent to neighboring nodes which creates routing overhead. It detects only black hole not gray hole nodes

Proposed algorithm is to detect gray hole nodes and removes the normal nodes with higher sequence number to enter in black list. Proposed approach dynamically calculates peak value like in DPRAODV, but it uses some more parameters than DPRAODV. Proposed Approach uses false reply, black list, and reputation concept.

Future work is to implement the proposed approach in network simulator and obtain the results for various metrics like

- Total Packets Received.
- Average end to end delay.
- Packet delivery Ratio.

VIII ACKNOWEDEMENT

I would like to say thanks to my guide for their valuable suggestions to improvise the content and quality of this paper. The author is grateful to our principal for providing necessary facilities towards carrying out this work. We acknowledge the diligent efforts of our Head of the Department to guide us towards implementation of this review paper.

REFERENCES

1. Charles E_ Perkins , Elizabeth M_ Royer "Ad_hoc On_Demand Distance Vector Routing" Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop | | 2. P.W.Yau,S.Hu and C.J.Mitchell, "Malicious attacks on ad hoc network routing protocol," International Journal of Computer research ,15 no.1 (2007) 73-100. | 3. Shalini Jain,"Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks", 2010 International Journal of Computer Applications (0975 – 8887). | | 4. S.Marti,"Mitigating Routing Misbehavior in Mobile adhoc networks",Stanford University. | | 5. Abderrahmane Baadache," Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks", International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010. | | 6. Sanjay Ramaswamy," Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", North Dakota State University. | 7. Yih-Chun Hu,David B.Jhonson,Adrion Perrig,"SEAD:Secure Efficient Distance Vector Routing for Mobile Ad hoc Networks,"2002 | 8. Raj P N,Swades P B, "DPRAODV:A Dynamic Learning System Against Blackhole Attack in AODV based MANET,"International Journal of Computer Science 2:54-59,doi:abs/0909.2371. | 9. S.Dokurer,"-Simulation of black hole attack in wireless ad-hoc networks", Atılım university. | 10. Akanksha Saini, Harish Kumar,Comparision Between Various Black Hole Detection Techniques in Manet", NCCI 2010 -National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 19-20 March 2010. | 11. Marjan Kuchaki Rafsanjani,"Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV based MANET",IJCA Special Issue on "Network Security and Cryptography" NSC, 2011. | 12. Dr.S.S.Dhenakaran, A.Parvathavarthini "An Overview of Routing Protocols in Mobile Ad -Hoc Network" International Journal of Advanced Research in Computer Science and Software Engineering © 2013. |