SAJET

South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 321–329

ISSN No: 2454-9614

Detection of Gray Hole Attack in AODV for MANETs by using Secure Message Digest

V. Dharman, G. Venkatachalam *

Department Of Computer Science And Engineering, Institute of Road and Transport Technology, Erode, Tamilnadu, India.

*Corresponding Author: V. Dharman,

E-mail: vdharmanv@gmail.com,

Received: 14/11/2015, Revised: 10/12/2015 and Accepted: 04/032016

Abstract

MANET (Mobile Ad Hoc Network) is a type of ad hoc network that can change locations and configure itself, because of moving of nodes. As MANETs are mobile in nature, they use wireless connections to connect various networks without infrastructure or any centralized administration. While the nodes communicate with each other, they assist by forwarding data packets to other nodes in the network. Thus the nodes discover a path to the destination node using routing protocols. Gray Hole attack among the different types of attacks possible in a MANET. Gray Hole attack is one type of active attack which tends to drop the packets during Transmission the routing from source to destination. In this paper, we simulate gray hole attack Detection technique the using second shortest route to destination and message digest based technique gives better performance in terms of AODV routing protocol to implement and compare performance of well know protocols AODV, performance metrics Packet dropped or packet loss, Packet delivery ratio, End to End delay and Average Routing load, the performance analysis has been done by using simulation tool ns-2 which is the main simulator.

Keywords: *MANET, AODV Routing Protocol, Gray Hole Attack, Message Digest*

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

In ad hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. As the range of each host's wireless transmission is limited, so to communicate with hosts outside its transmission range, a host needs to enlist the aid of its nearby hosts in forwarding packets to the destination. So all nodes of these networks behave as routers and take part in discovery and maintenance of routes to other.

Wireless networks use some sort of radio frequencies in air to transmit and receive data. Wireless networks are formed by routers and hosts. Ad -hoc networks are wireless networks where nodes communicate with each other using multi-hop links. Topology MANET are created dynamically and maintained by individual nodes comprising the network. In MANET all communication occurs through a wireless medium. MANETs also possess multi hop routing means packets are allowed to forward to destination through multiple nodes thus creating each node act as terminal as well as router. Routing is task of transferring data from source to destination while maximizing network performance. So it becomes a challenge in MANETs. Because of changing topology and network density, limited resources changes paths which were initially efficient but can quickly become inefficient and infeasible.

In such networks, nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network.

Fig 1 MANET infrastructure

Thus routing protocols play an important role in ad hoc network communications. Since all nodes in an ad hoc network can be connected dynamically in an arbitrary manner it is usually possible to establish more than one path between a source and a destination.

1.1 Characteristics of MANET

1) *Dynamic Topologies:*

The nodes of the network are keeps on moving with different speeds, which results in the variations in the structure of the network.

2) *Energy-constrained Operation*:

The devices in the modern electronic world completely rely on batteries. The design of the network is to be improved to conserve the energy consumed by the mobile nodes.

3*) Limited Bandwidth:*

The bandwidth of the wireless network is very narrow and the networks are to be optimized to perform with the maximum efficiency with in the limited bandwidth.

4) *Security threats:*

When compared to the wired communication with wireless, the wireless communication is more affected for security. The security of the MANET is to be improved so that the information transferred is secured.

2. Routing Protocols of MANET

The Routing Protocols has development of many different Protocols for MANET. We Provide an Overview of a wide range of routing protocols in MANET. The dynamic routing protocols main characteristics are mobility and multi-hop. The Applications of MANET are Military or police exercises, Wireless Sensor networks, Rescue or Disaster relief operations, Mine site operations, Urgent Business meetings or Conferences, Students on campus. The routing protocols of MANET are followed below

Table Driven Routing Protocols On-Demand Routing Protocols
Destination-Sequenced Distance Vector Routing Protocol (DSDV)
Cluster based Routing Protocols (CBRP)
Fisheye State Routing (FSR)
Ad-Hoc On-Demand Distance Vector Routing (AODV)
Wireless Routing Protocol (WRP) Signal Stability Routing (SSR)
Global State Routing (GSR) Dynamic Source Routing Protocol (DSRP)
Hierarchical State Routing (HSR) Associatively Based Routing (ABR),
Zone-based Hierarchical Link State Routing Protocol (ZHLS)

Table 1 – Ad Hoc Networks routing protocols

- *Proactive/ Table-driven Routing Protocols* Proactive protocol, each node in the network has maintains one or more routing tables which are up to date routing information. The routes to all host pairs are maintained by sending periodical control message updated. Proactive routing protocols are not suitable for large networks, high routing overhead and unnecessary bandwidth wastage for sending control packets.

  Ex: DSDV (destination sequenced distance vector).

- *Reactive/ On-demand Routing Protocols* Reactive protocols precede for establishing route(s) based on routes can establish 'on-demand' process, when require to the destination. This protocol does not need periodic up to date transmission of topological information of the network.

  Ex: AODV (Ad-Hoc On-demand Distance Vector).

- *Hybrid Routing Protocols*

  Hybrid Routing Protocol combination features of both reactive and proactive routing protocols information. The recently invented several hybrid protocols are also proposed.

  Ex: ZRP (Zone Routing Protocol).

3. AODV Routing Protocol

3.1 AODV Protocol

The Ad-hoc on demand distance vector routing protocol is one of the widely used routing protocols in MANET. The route is established only when it is desired by the source node for data packets. Whenever node requires a route to the destination, a route discovery process is initiated. The source node floods the Route

Request packet to its neighbours. The Route Request packet contains source identifier, destination identifier, source sequence number, destination sequence number, broadcast ID and TTL (Time to live). The intermediate node either forwards the packet or prepares a Route Reply if it has a fresh or valid route to the destination. This validity is determined by comparing the sequence number of intermediate node with the destination sequence number of Route Request packet. The destination node or the intermediate node that has the freshest route sends the Route Reply message back to the source node in the reverse path. The source node receives many Route Reply packets and the fresher and shorter path is selected to send the data packet.

In this attack, a malicious node sends a forged Route REPLY(RREP) packet to a source node that initiates the route discovery in order to pretend to be a destination node. The malicious node launches this attack by advertising fresh route with least hop count and highest destination sequence number to the node which starts the route discovery.

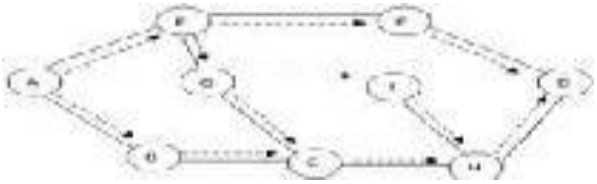

Fig 1: Route discovery process

3.2 Gray Hole attack

Gray Hole attack is a variation of the black hole attack in which the malicious node may behave as an honest node first during the route discovery process and then may change its state to malicious and vice versa. This malicious node may then drop all or some of the data packets. The grayHole attack is difficult to detect due to congestion, overload and. also due to malicious nature and ability of changing states. Instead it behaves as an honest node and when data packets arrive through this path, it drops all the data packets. A condition is added to drop all the data packets if it is not the destination otherwise receive all the data packets. Gray Hole node act honest node during route discovery process but in actual it is an attacker. Dropping all UDP packets while forwarding TCP packets. Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

3.2.1 Routing of MANETs:

In routing user data is send from sender to destination through network. The routing functions are:

- Path Generation
- Path Selection
- Data transmission
- Path Maintenance

1) Path Generation- In this, path is generated from scattered environment of network. There are multiple path generated from sender to destination.

2) Path Selection- In the previous phase, there were multiple path and from them suitable path is chosen for data transmission so that time, memory and overhead will be less and performance is better.

3) Data transmission- In this data is transmitted from sender to destination on the selected path

4) Path Maintenance- The suitable path must have to maintain using control messages like Hello. If the link is broken and not active then using hello messages, maintenance of the route is done.

3.3 Characteristics of Routing Protocols

The Routing protocols should be:

- Adaptable of an grouping data
- Application specific
- Adaptable of improving energy consumption

3.4 Route discovery

When a node wants to communicate with another node in the network a unique communication path is established between the sender and the receiver nodes. The source node scans the neighbourhood vector for the destination. If the destination node is identified to be the single hop neighbour of the source, the source nodes starts transmitting data packets. The transmission of data will be uninterrupted until there is no change in the geographical positions of the source and the destination nodes.

3.5 Problem Statement

Malicious node act as a barrier in the secure path As it will absorb the data and thus reduce packet delivery , degrade the performance ,Decrease end to end delivery , decrease throughput. To secure a network to detect and avoid it very important task.

4. NS-2 Simulation

NS simulator is consists of two languages: one an object oriented simulator in C++ (internally) and OTcl (an Object oriented extension of Tcl) interpreter and execute user's command scripts. NS is an OTcl interpreter with network simulation and object libraries. There are two libraries: the compiled C++ library and the interpreted OTcl, with each other correspondence between them. The interpreted OTcl allows faster interpret and slow to run. The compiled C++ library allows us to achieve efficiency in the simulation, compiled hierarchy and the faster execution times**.**

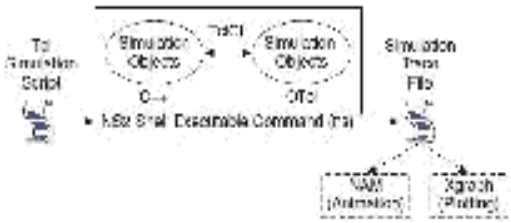

Fig 4.1 Basic architecture

Network Simulator (NS-2) version 2.35 is an open source software, provides simulation results of ad-hoc networks.

A.Tcl and OTcl programming: Tcl (Tool Command Language) **[8, 9]** is used by research people in the real world. It is a very simple language with small sin taxis and it allows easy content with other languages. Tcl provide a graphic interface, compatible with many platforms, flexible for integration, easy to use and also free.

B.NAM: Network Animator (NAM) is an important animator tool for visual aid viewing in real world how packet traces along the network.NAM supports the basic visualization controls, packet level animation, fine tune layout, TCP visualization and generate ns simulation scripts. The NS-NAM interface between node manipulation, link manipulation, topology layout, colour protocol state.

C.AWK Script: The AWK Script is very good, a more capable programming language, which is look like often Perl and Python languages. The AWK script in processing the data from column wise the log.tr or trace files which we get from NS2. The AWK script is to print a specific parameter or fields in output to begin a One Line code, to calculate trace file in all fields and execute output in specific ordered.

To run the awk script in Linux as follows:

awk –f filename.awk filename.tr

4.1 Performance Metrics

4.1.1 End to end delay

It is the total time taken for the packet to reach from source to destination and it is measured in seconds. It includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. Due to node mobility, use of control messages and packet retransmissions due to weak signal strengths between nodes, end to end delay increases. Delay should be less for efficient packet transmission.

4.1.2Packet delivery ratio:

The packet delivery ratio is the ratio of number of packets received at destination node to that of number of packets sent by the source node. It is expressed in percentage. It gives the reliability of the protocol for message deliver. It is affected by node mobility and change in topology. The PDR should be high.

4.1.3 Packet drop rate

It is the ratio of number of packets dropped during transmission to that of number of packets sent by the source node. It is expressed in percentage. It can occur due to node mobility or buffer overflow. It should be less for efficient routing Protocol.

Simulation Parameters

Network Area	1000x1000m
Transmission Range	200m
Number of Nodes	10
Bandwidth	2Mbps
Routing Protocols	AODV
Traffic Type	CBR
Packet size	512 Bytes
Maximum speed	20 m/sec
Simulation time	100 sec

Rutvij H.Jhaveri eTal**.[7]**(2012) proposed a scheme for Ad-hoc On-demand Distance Vector (AODV) protocol, in which an intermediate node detects the malicious node sending false routing information; routing packets were used not only to pass routing information, but also to pass information about malicious nodes. The proposed scheme not only detects but also removes malicious node by isolating it, to make safe and secure communication. Chuanhao Qu, Lei Ju et al. **[9]** (2013) proposed a novel trust model with an intrusion detection system by detecting malicious dropping packet behaviour. As an application of the model, we extended the AOMDV to a light-weight trust based multipath routing protocol called LWT-AOMDV. This new protocol could establish multiple trustworthy paths and launch a route handoff when detecting paths with malicious nodes. This approach could reduce the buffer size and alleviate the computation overhead by using two timers. Three metrics to evaluate the performance of these routing protocols in which the first two metrics especially the delivery ratio are important for the service quality and the third could reflect the scalability of the approach.

5. Existing System

There are some extra nodes-strong nodes, which help source and destination to find black and gray hole attacks. These strong nodes are assumed to be trustful and also capable of turning its antenna to large ranges and short ranges.

Each normal node is inside the range of one of these strong nodes. By using the strong nodes, source and destination starts to check if the data packets have reached the destination or not. If any changes found in number of messages sent from source and received at destination, strong nodes ask the nodes in their areas about the monitoring results of one node's behaviour.

If the checking results show misbehaviour according to the votes, then the network runs a protocol which can detect black or grayHole attack. At last announces malicious node to the network by broadcasting messages.

The disadvantages are,

- There is no limit for detection of malicious node that increases mistakes.
- There is no security.
- Assumes that strong nodes are trustable. There is no limit for detection of maliciousness of one node that increases mistakes.

6. Proposed System

Attack detection using second shortest route to destination and message digest: In this proposed solution **[1]** we have changed our scheme and it contains three parts. In the first part we want to make slight changes in AODV. In this method, we have to use second shortest path for data packets transmission instead of using first path for transmission. Source node transmits the route request packet (RREQ) to the destination, which broadcasts in the whole network. We assume that this message is reached to the destination through many different paths. The first path is the shortest path to the destination due to very less number of nodes. **[1]** There might be chances to present some malicious node in the route. Thus, malicious node can simply become part of the route, through which data can be sent. We desire that the receiver node have to wait for receiving the second route request and sends the route reply (RREP) message on this route back again. The source node can then send data packets successfully on this route to the destination node just because the malicious node will not be able to know that through which route the data will come. It also may happen that malicious node can be a part of second shortest path. **[1]** For this, we desire to apply a hash function on message that has to be sent to get a unique message digest (MD). Source node sends the MD with the first data packets to the receiver and receiver node stores this MD with itself. When the receiver gets all the data packets, it applies a hash function on the message to get a message digest. **[1]** Then it compares this message digest with the stored one message digest. If both the messages are equal, that means the message has been received successfully and there is no attacking node in the route. But if they are not equal, it means some data packets have been dropped in the data transmission and there is presence of malicious node in the network. After detecting the malicious node, the receiver broadcasts Data Packets Received Error (DPRE) message to the source node to re-establishes a new route to the destination**. [1]**

The advantages are,

- This decrease the probability of malicious node present in second route. Message digest provides data integrity.
- To provide node availability and better security for packet delivery in MANET.
- Efficient to improve network security and performance of the network.

7. Conclusion

Misbehaviours of nodes cause the damage to the nodes & packet also. Gray Hole attack cause damage to the network & also it is difficult to detect. In this paper, we proposed a method algorithm for the detection &

prevention of the gray hole attack as well as malicious node behaviour. By implementing a secure hashing algorithm the performance of the network gets increases and also we can secure our network from the gray hole attack. In order to further improve accuracy in the adhoc network, we can go for the some additional features in the simulations parameters of the adhoc network. So that we can achieve the reliability and accuracy in the network & that will be the further direction.

8. Future Enhancement

Many Problems in ad-hoc network remain to be investigated. Method for the detection & prevention of gray hole or malicious node is very efficient for detecting & preventing from the gray hole attack or behaviour of malicious node. Because of the different attacks on the ad-hoc network, the performance of the network gets decreases. Future work will involved some new additional features or parameters using which there is a much more increment in the performance metrics of the network as well as try to avoid the different attacks which occur on the network, with the use of different routing protocols available in MANET. As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the performance metrics and mainly concentrate on one thing that there is a minimum amount of packets loss during the transmission.

References

[1] HizbullahKhattak, Nizamuddin, "A Hybrid Approach for Preventing Black and Gray Hole Attacks in MANET", *Digital Information Management (ICDIM) Eighth International Conference*, pp. 55-57, IEEE September 2013.
[2] M. Kumar, R. Mishra, "An Overview of MANET: History, Challenges and Appln", *IJCSE*, Vol. 3 No. 1, pp. 121-125, Feb-Mar 2012.
[3] Characteristics of MANET available: http://techupdates.in/what-is-manet-characteristics-and-applications-of-manet-in-communication/
[4] C. Siva Ram Murthy, B. S. Manoj, *Ad Hoc Wireless Networks: Archi and Protocols*, Person Educ, ISBN 978-81-317-0688-6, 2004.
[5] K. Vishnu, A. J. Paul, "Detection and removal of cooperative black/gray hole attack in mobile *adhoc*networks", *IJCA(0975-8887)*, Vol. 1 No. 22, pp. 38-42, 2010
[6] Sukla Banerjee, "Detection/Removal of Coperative Black and Gray Hole Attack in Mobile Ad-hoc Networks", *Proceedings of the World Congress on Engineering and Computer Science 2008*, October 22-24, 2008.
[7] Harsh Pratap Singh, Virendra Pal Singh, Rashmi Singh, "Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", *International Journal of Computer Applications (0975 – 8887)*, Volume 64– No.3, pp. 16-22, February 2013.
[8] Onkar V. Chandure, V. T. Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-
[9] Hoc Network using AODV Routing Protocol", *International Journal of Computer Appln(0975-8887)*, Vol 41- No.5, pp. 27-32, Mar 2012.
[10] R. H. Jhaveri, S. J. Patel, D. C. Jinwala, "A novel approach for Grayhole and Blackhole attacks in Mobile Ad-hoc Networks", *Second International Conference on Advanced Computing & Communication Technologies*, IEEE, pp. 556-560, 2012.
[11] Deepali A. Lokare, A.M Kanthe, Dina Simunic, "Cooperative Gray Hole Attack Discovery and Elimination using Credit based Technique in MANET", *International Journal of Computer Applications (0975-8887)*, Volume 88-No.15, pp. 13-22, February 2014.
[12] S. Jain, M. Jain, H. Kandwal, "Advanced algorithm for detection and prevention of cooperative Black and Gray hole attacks in mobile ad hoc networks", *IJCA (0975-8887)*, Vol. 1-No. 7, pp. 37-42, 2010.
[13] Yang, H., Shu, J., Meng, X., and Lu, S., "SCAN: Self-organized network-layer security in mobile ad hoc networks", *IEEE journal*, Vol. 24-No. 2, pp. 261-273, Feb-2006.
[14] P. Agrawal, R. K. Ghosh and S. K. Das, "Cooperative black and gray hole attacks in mobile ad hoc networks", *In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication*,pp.-310-314,January-2008.