OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Black Hole Detection in AODV Using Hexagonal Encryption in Manet's

Mr. S. Balamurugan[1], V. Kanmani[2] (MCA), S. Radhika[3] (MCA),
[1]*Assistant Professor, MCA Deptt.*
Sir Manakula Vinayagar Engineering College Madagadipet Pondicherry

ABSTRACT: *In MANETs (mobile ad hoc network), security is common problem and lack of issues in MANET network. When comparing to wired network, MANETs are harmed to security attacks due to the scarcity of a trusted centralized enforce authority and limited resources. This paper proposed a technique to avoid Blackhole node behaviour in AODV (Ad Hoc On-Demand Distance Vector) using Hexagonal Encryption inNS2. Hexagonal Encryption has been chosen for low cost and high computation speed up. Compared to existing blackhole detection technique, this proposed technique obtains better result by stimulating in NS2.*

Keywords: *AODV, Blackhole node behavior, Hexagonal Encryption, MANET's, Security attackss.*

I. Introduction

A **mobile ad hoc network** (**MANET**) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks.

The advantage of wireless networks as opposed to wiredor fixed wireless networks is that they are truly wireless. Most traditional "wireless" access points still need to be wired to the Internet to broadcast their signal. For large wireless networks, Ethernet cables need to be buried in ceilings and walls and throughout public areas. For this mechanism, we are using AODV protocol. This algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an ad hoc network.

AODV allows mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the" counting to infinity" problem offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

II. Black Hole Attack

In a black hole attack, a malicious node can impersonate a destination node by sending a spoofed route packet to a source node that initiates a route discovery. A blackhole has two properties:

1. The node exploits the ad hoc routing protocol to advertise itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets.
2. The node consumes the intercepted packets. In an ad hoc network that uses the AODV protocol, a black hole node absorbs the network traffic and drops all packets. To explain the black hole attack we add a malicious node that exhibits black hole behavior.

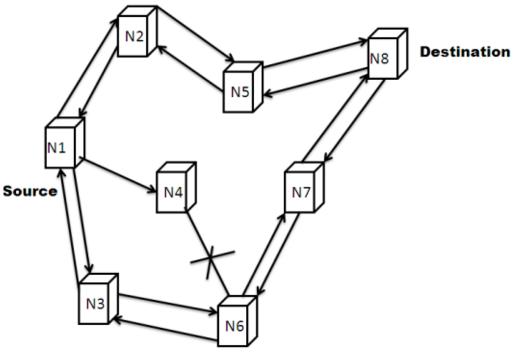

Fig. 1: Black hole attack in AODV

An attacker suppresses or modifies packets originating from some nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrong doing.

NS is a discrete event simulator targeted at networking research. Ns provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

- It should be aligned with the simulation needs of modern networking research.
- It should encourage community contribution, peer review, and validation of the software.

Since the process of creation of a network simulator that contains a sufficient number of high-quality validated, tested and actively maintained models requires a lot of work, ns-2 project spreads this workload over a large community of users and developers

Ns2 is built using C++ and Python with scripting capability. The ns-2 library is wrapped to python thanks to the pybindgen library which delegates the parsing of the ns-2 C++ headers to gccxml and pygccxml to generate automatically the corresponding C++ binding glue. These automatically-generated C++ files are finally compiled into the ns-3 python module to allow users to interact with the C++ ns-2 models and core through python scripts. The ns-2 simulator features an integrated attribute-based system to manage default and per-instance values for simulation parameters. All of the configurable default values for parameters are managed by this system, integrated with command-line argument processing, Doxygen documentation, and an XML-based and optional GTK-based configuration subsystem.

Tcl (Tool Command Language): Tcl gained acceptance on its own. It is commonly used for rapid prototyping, scripted applications, GUIs and testing. Tcl is used on embedded systems platforms, both in its full form and in several other small-footprint versions.

The interpreted class hierarchy is automatically established through methods defined in the class TclClass. user instantiated objects are mirrored through methods defined in the class TclObject. There are other hierarchies in the C++ code and OTcl scripts; these other hierarchies are not mirrored in the manner of TclObject.

III. AODV Protocol

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If such a route is not available in its cache, the node initiates a route discovery process by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ.

A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message is a unicast message to the source node. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. Timers are used to keep the route entries fresh.

3.1 Tradeoff between Delay and Capacity

Increasing transmission power has the side effect of reducing the maximum achievable throughput in a WSN due to increased channel contention and interference. Our focus is on real-time applications in which meeting the deadlines of critical data is more important than the total throughput. For example, in a surveillance application, timely delivery of the location of an intruder is more important to the user than delivering a large amount of non-critical data. It is also important to note that the reduced capacity is a problem only when the workload approaches the network capacity. Recent advances in real-time capacity theory show that the performance degradation may be avoided as long as the amount of high-priority data transmitted in the network is small enough not to trigger capacity bottlenecks.

AODV achieves the desired tradeoff among communication delay, energy consumption, and network capacity by adapting the transmission power based on required communication delays. When deadlines are tight, AODV trades capacity and energy for shorter communication delay by increasing the transmission power. Conversely, when the deadlines are loose, AODV lowers the transmission power to increase throughput and reduce energy consumption. This adaptive approach is a key feature of AODV.

AODV assumes that each packet is assigned a soft deadline by the application, which specifies the desired bound on the end-to-end delay of a packet. The primary goal of AODV is to increase the number of packets that meet their deadlines while minimizing the energy consumed for transmitting packets under their deadline constraints. AODV focuses on minimizing the energy consumed in packet transmissions. In addition, AODV is designed based on the following principles:

MANETs applications have varied communication requirements resulting in workloads with diverse deadlines. A real-time power-aware routing protocol should dynamically adapt its transmission power and routing decisions based on workload and packet deadlines.

The design of AODV should account for the realistic characteristics of MANETs including loss links and extreme resource constraints in terms of memory, bandwidth and energy. AODV should be localized protocol that makes decisions based solely on onehop neighborhood information.

IV. Blackhole Detection Methods

Black hole is nothing but the malicisious node. This node accepts the data from source but does not forward it to the destination. This node used for hacking purpose. There are two detection techniques are involved in the detection of black hole:

- Depending upon how many times that path is used for transmission.
- By updating the routing table and comparing unique sequence number at each time.

Method 1

In this method, the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the network redundancy. Since any packet can be arrived to the destination through many redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sender node will buffer its packets until a safe route is identified. Once a safe route has identified, these buffered packets will be transmitted. When a RREP arrives to the source, it will extract the full paths to the destinations and wait for another RREP. Two or more of these nodes must have some shared hops (in ad hoc networks, the redundant paths in most of the time have some shared hops or nodes). From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This helps for find secure type of communication between the source and destination. But the major disadvantage of the this method is its time consuming. Because here secure intermediate node is find out on the basis how many times that node is used for the data transfer. Now if that node is busy when source wants to transmit data then source have to wait for it. It might be possible that another node which is available for transmissions not black hole. This increase unnecessary delay for transmission of data.

Method 2

Every packet in MANETs has a unique sequence number. This number is an increasing value, i.e., the next packet must have higher value that the current packet sequence number. The node in regular routing protocols keeps the last packet sequence number that it has received and uses it to check if the received packet was received before from the same originating source or not. Packet-sequence-numbers for the last packet received from every node. These tables are updated when any packet arrived or transmitted. The sender broadcasts the RREQ packet to its neighbors. Once this RREQ reach the destination, it will initiate a RREP to the source, and this RREP will contain the last packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives this RREQ, it will reply to the sender with a RREP contains the last packetsequence- numbers received from the source by this intermediate node. This method provides secure type of data transmission and fast transmission of data as compared to the previous method.

V. Black Hole Prevention

Real Time Monitoring

This method first identifies the neighbor of the RREP node creator i.e. suspected node. Neighbor node is instructed to listens the packets send by suspected node. Fcount and rcount are the two counters maintained by neighbor node. When a neighbor node forwards any packet to suspected node it will increase the fcount counter by 1. If suspected node forward a packet it will be overheard by the neighbor node and rcount is increased by 1. After source node receives RREP it sends packets to path to check the node is malicious node or not. Neighbor node forwards packets to suspect node until fcount reaches a threshold; thereafter if rcount is 0. RREP creator will identify as malicious node and blocked.

Overcome Blackhole attack

By modifying an original AODV. To participate in Communication RREP originator must exhibit its honesty. If the node is the first receiver of the RREP packet, it will forward it to Source andcheck forthe honesty of node based on the opinion of the neighbors of RREP originator Node. Neighbors are requested to send an opinion about the RREP originator node. After receiving reply from all neighbor nodes. It checked if RREP originator node has delivered many packets to destination it a an honest node, if RREP originator node as received many packets but do not forward packets further or it has send many RREP packets, it is a misbehaving node. Such nodes are added to the quarantine list and blocked.

Comparing Destination Sequence Number

To prevent Blackhole attack in AODV. In the method source node collects all the RREP from different intermediate node. The first entry received by source is marked first entry in Route reply table (RRT). The destination sequence number (DSN) of first entry is compared with sequence number of source node. If the DSN of first entry is very large as compared to source sequence number, the node is considered as malicious node and removed from the RRT. Path is selected based on the remaining entries in RRT which is arranged according to DSN. The node with highest DSN is selected for path.

VI. Hexagonal Encryption Algorithm

```
1. The sender sends a RREQ packet which contains a plain text.
2.  When a node recieves the RREQ packet
if(not(Reciever)) then
if((has better route to reciever) ||
(has shorter route to reciever) then
Save the reverse route
Forward the packet
fi
else
Encrypt the plaintext in the packet with
the partition and key preagreed upon
Send a RREP towards the sender with the cipher text
fi
3.  When a node node recieves a RREP packet
if(not(Sender)) then //By Sender we mean the
// original source of the RREQ packet
Forward the packet towards sender
else
if(RREP packet contains the required cipher) then
            Forward data packets to the last forwarder
of the RREP packet
else
Drop the RREP packet
fi
fi
```

Fig 2: Algorithm for hexagonal encryption

VII. Experimental Result

The simulation was done with 20,25,30,35,40 nodes. The simulation was done in TCl. With simulations for each in both AODV Black hole Aodv environments, the scenarios for which were created using the stedest command.

In each case the number of packets sent, received, dropped and percentage of packets recieved were recorded by analyzing the trace file. If the nodes are attacked by black hole attack. The hexagonal encryption technique detect the black hole attack node in network and its changes the route path to some other route without any data(packet) drops. From this simulation we are increasing packet delivery ratios and reducing packet end-to-end delay and average packet lengths.The results are shown in the graphs respectively.

Graph 1

It shows the efficient increasing packet delivery ratio when compared to existing one.

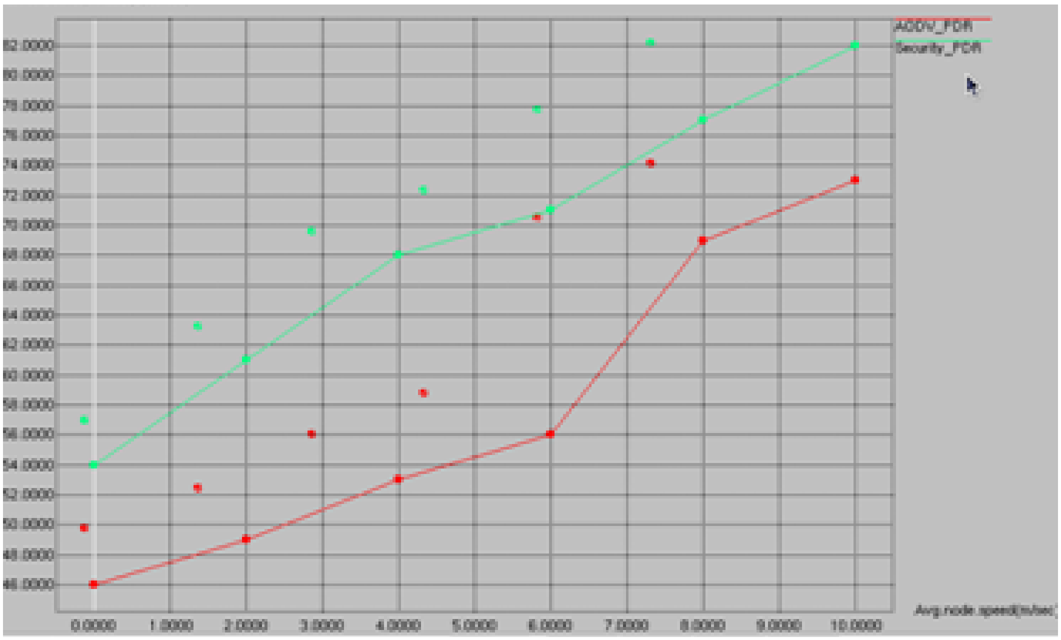

Fig 3: Increasing packet delivery ratio using hexagonal encryption

Graph 2

It shows the decreased average packet length when compared to existing one.

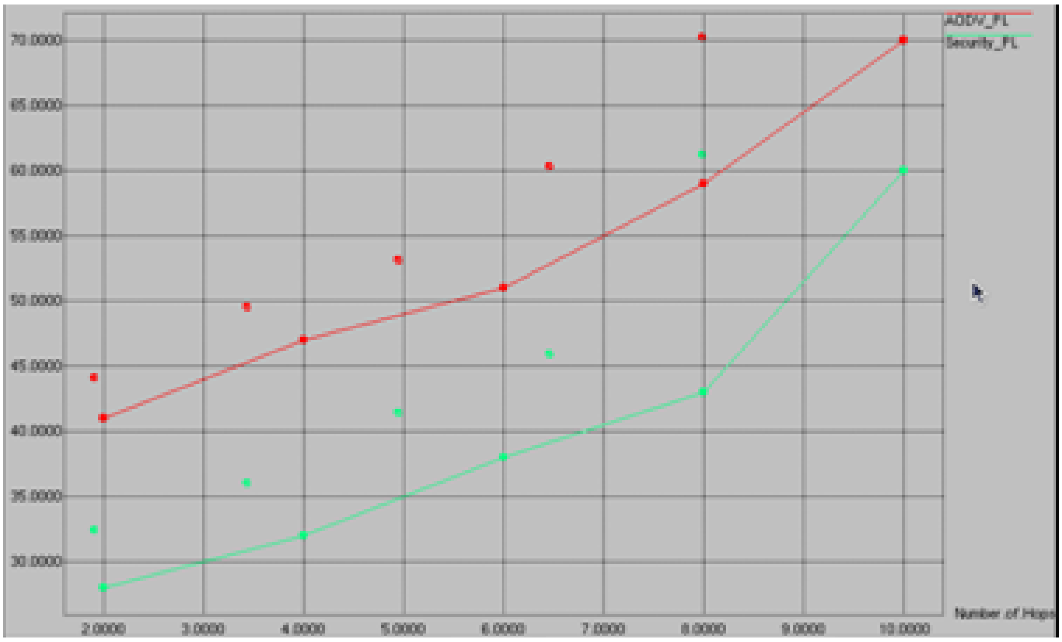

Fig 4: Average packet length

Graph 3

It shows the decreased End-to-End delay when compared to existing one.

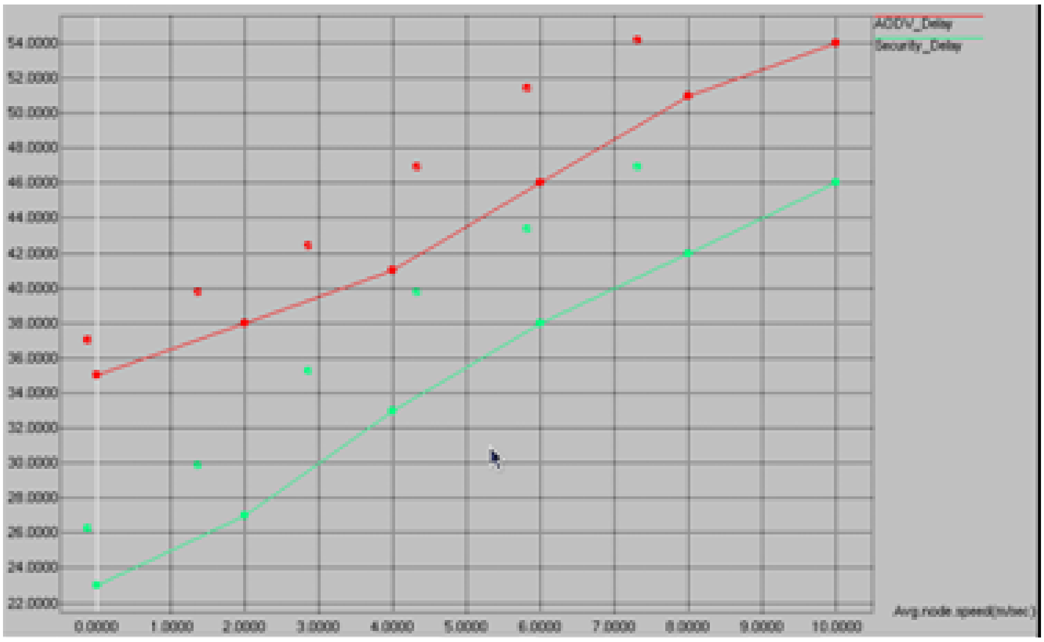

Fig 5: End-to-end delay

VIII. Conclusion

The proposed technique to avoid Blackhole node behaviour in AODV(Ad Hoc On-Demand Distance Vector) using Hexagonal Encryption in NS2. Hexagonal Encryption has been chosen for low cost and high computation speed up. Compared to existing blackhole detection technique, this proposed technique obtain better result by stimulating in NS2.

REFERENCES

[1] L. Raja1, Dr. S. Santhosh Baboo, Dept. of Computer Applications, Pachaiyappa's College, Chennai"Analysis *of Blackhole attacks on AODV Routing Protocol in MANET*" December 2012 | Vol 2, Issue 12, 1522-1526

[2] Shraddha Raut & Sd Chede **"***detection and removal of black hole in mobile Ad-hoc network (manet)"* Electronics & Telecommunication Department.

[3] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park," *Black Hole Attack in Mobile Ad Hoc Networks*"

[4] Vishnu K, Amos J Paul," *Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks*"

[5] AWANDHIYA, P.M., GHONGE, M.M., M.S.ALI, D., DESHPANDE, P.J.. *A Survey of Mobile Ad Hoc Network Attacks. International Journal of Engineering Science and Technology 2010;.*

[6] Perkins, C., Belding-Royer, E., Das, S.. *Ad hoc On-Demand Distance Vector (AODV) Routing. Tech. Rep. RFC 3561; IETF; 2003. URL:https://tools.ietf.org/html/rfc3561*.

[7] Dutta, S.. *An approach towards development of effecient encryption techniques*. Ph.D. thesis; The University of North Bengal; 2004.

[8] The ns Manual (formerly ns Notes and Documentation). UC Berkeley, LBL, USC//ISI, and Xerox PARC; 2011.

[9] Greis, M.. *Tutorial for the Network Simulator "ns". 2004*.

[10] Dokurer, S.. *SIMULATION OF BLACK HOLE ATTACK IN WIRELESS AD-HOC NETWORKS. Master's thesis; Atılım University; 2006*.

[11] Sun, B., et al. *Detecting Black-hole Attack in Mobile Ad Hoc Networks. Personal Mobile Communications Conference, 5th European* 2003;(492).

[12] Berkeley, U., LBL, , USC/ISI, , PARC, X.. *The ns Manual; 2011*.

[13] Ross, F.J., Ruiz, P.M.. *Implementing a New Manet Unicast Routing Protocol in NS2*. Tech. Rep.; Dept. of Information and Communications Engineering University of Murcia; 2004.

[14] Sukla Banerjee, *"Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks"*, Proceedings of the World Congress on Engineering and Computer Science 2008

[15] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , *"A Survey on Attacks and Counterme asures in Mobile Ad Hoc Network,"* Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp, @ 2006 Springer.

[16] Nishu Garg and R.P.Mahapatra, "*MANET Security Issues ,"* IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.8, August 2009.

[17] N.Shanthi, Dr.Lganesan and Dr.K.Ramar, "*Study of Different Attacks on Multicast Mobile Ad hoc Network,"* Journal of Theoretical and Applied Information Technology.