Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Manet Routing Protocol Using ID3 Algorithm under Black Hole and Grey Hole Attack

Manpreet Singh*
M-Tech Scholar, S.B.S State
Technical Campus, Ferozepur,
Punjab, India

Chakshu Goel
Asst. Professor, S.B.S State
Technical Campus Ferozepur,
Punjab, India

Abstract— MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.We have two attacks in this Project.Black hole and Greyhole attacks are such attacks that drop significant number of packets by performing packet forwarding misbehaviour and breach the security to cause denial of service in Mobile Ad-hoc Networks (MANETs). In this paper, we discuss our previous work, RAODV, MRAODV, to detect nodes during route discovery process and propose an ID3 modified version to improve the performance of MANET. Here, ID3 is alerting other nodes about the malicious node. We analyse the proposed solution and evaluate its performance using Network Simulator-2 (NS-2) under different network parameters.In this we have various types of parameters like transmission of data,route of discovery process, black hole attack, grayhole attackand on the basis of these parameters we conclude that the performance of our system is better.

Keyword: -Attack;Routing, End-to-end delay,Packet Delivery Ratio, Routing Overhead,Throughput

I. INTRODUCTION

It Stands for "Mobile Ad Hoc Network." A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.Some MANETs are restricted to a local area of wireless devices (such as a group of laptop computers), while others may be connected to the Internet. A **mobile ad hoc network** (**MANET**) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. *Ad hoc* is Latin and means "for this purpose".[1]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.MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network in contrast to a mesh network has a central controller (to determine, optimize, and distribute the routing table). MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).Multi-hop relays date back to at least 500 BC.[2][3] The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale, etc [2].

Security Threats in Ad hoc Network

The current Mobile ad hoc networks allow for many different types of attacks.Although the analogous exploits also exist in wired networks but it is easy to fix by infrastructure in such a network. Current

MANETs are basically vulnerable to two different types of attacks: active attacks and passive attacks. Active attack is an attack when misbehaving node has to bear some energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. Nodes that perform active attacks with the aim of damaging other nodes by causing network outage are considered as malicious while nodes that make passive attacks with the aim of saving battery life for their own communications are considered to be selfish. In this chapter, our focus is onvulnerabilities and exposures in the current ad hoc network. We have classified the attacks as modification, impersonation, fabrication, wormhole and lack of cooperation [3].

Attacks Using Modification

Modification is a type of attack when an unauthorized party not only gains access but tampers with an asset. For example a malicious node can redirect the network traffic and conduct DoS attacks by modifying message fields or by forwarding routing message with false values. In fig. M is a malicious node which can keep traffic from reaching X by continuously advertising to B a shorter route to Xthan the route to Xthat C advertises [14]. In this way, malicious nodes can easily cause traffic subversion and denial of service (DoS)by simply altering protocol fields: such attacks compromise the integrity of routing computations. Through modification, an attacker can cause network traffic to be dropped, redirected to a different destination or to a longer route to reach to destination that causes unnecessary communication delay[5].

Attacks Using Impersonation

As there is no authenticationof data packets in current ad hoc network, a malicious node can launch many attacks in a network by masquerading as another node i.e. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network (such as altering its MAC or IP address in outgoing packets) and alters the target of the network topology that a benign node can gather. As for example, a spoofing attack allows forming loops in routing packets which may also result in partitioning network [4].

Attacks through Fabrication

Fabrication is an attack in which an unauthorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages. Such kind of attacks can be difficult to verify as they come as valid constructs, especially in the case of fabricated error messages that claim a neighbor cannot be contacted [11].

Wormhole Attacks

Wormhole attack is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. This exploit gives the opportunity to a node or nodes to short-circuit the normal flow of messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

Lack of Cooperation

Mobile Ad Hoc Networks (MANETs)rely on the cooperation of all the participating nodes. The more nodes cooperate to transfer traffic, the more powerful a MANETgets. But one of the different kinds of misbehavior a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources. This can endanger the correct network operation by simply not participating to the operation or by not executing the packet forwarding [6].

II. Algorithms Introduction

ID3 (Iterative Dichotomiser 3):-

The ID3 algorithm begins with the original set S as the root node. On each iteration of the algorithm, it iterates through every unused attribute of the set S and calculates the entropy $H(S)$ (or information gain $IG(A)$of that attribute. Then selects the attribute which has the smallest entropy (or largest information gain) value. The set S is then split by the selected attribute (e.g. age < 50, 50 <= age < 100, age >= 100) to produce subsets of the data. The algorithm continues to recourse on each subset, considering only attributes never selected before [8].

Recursion on a subset may stop in one of these cases:

- Every element in the subset belongs to the same class (+ or -), then the node is turned into a leaf and labelled with the class of the examples
- There are no more attributes to be selected, but the examples still do not belong to the same class (some are + and some are -), then the node is turned into a leaf and labelled with the most common class of the examples in the subset
- There are no examples in the subset, this happens when no example in the parent set was found to be matching a specific value of the selected attribute, for example if there was no example with age >= 100. Then a leaf is created, and labelled with the most common class of the examples in the parent set.

Throughout the algorithm, the decision tree is constructed with each non-terminal node representing the selected attribute on which the data was split, and terminal nodes representing the class label of the final subset of this branch.

Ad Hoc On-Demand Distance Vector routing protocol (AODV), defined in, and is a unicast-based reactive routing protocol for mobile nodes in ad-hoc networks. It enables multi-hop routing and the nodes in the network maintain the topology dynamically only when there is traffic. Currently AODV does not define any securityMechanisms what so ever. The authors identify the necessity of having proper confidentiality and authentication services within the routing, but suggest no solutionsfor them. The IPSecis, however, mentioned as one possible solution. Multicast Ad Hoc On-Demand Distance-Vector routing protocol (MAODV), specified in extends the AODV protocol with multicast features [7].

III. Results

a) Scenario 1:-(Generating MANET Environment)

NS-2 is used to simulate the real moving behaviours of the nodes in a mobile ad hoc network. The evaluation will be conducted with some specific number of nodes that will be randomly scattered in a specific region with specific number of connections. Figure 1 shows the MANET Environment generated by using NS-2.

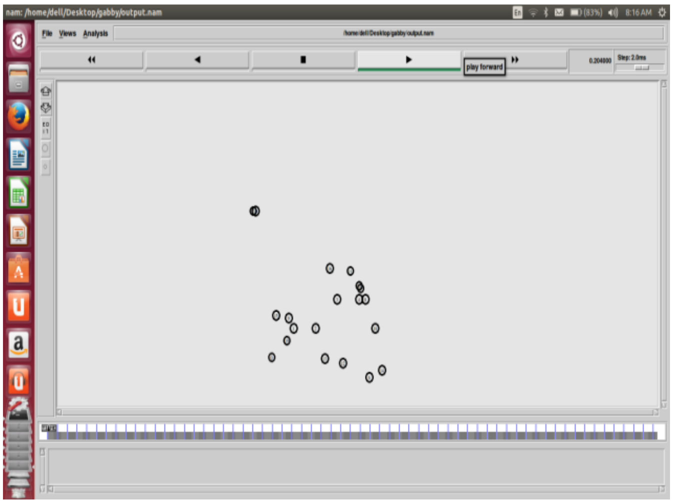

nam: /home/dell/Desktop/gabby/output.nam
File
Views
Analysis
/home/dell/Desktop/gabby/output.nam
play forward
Step: 2.0ms

Figure 1: MANET Environment

In the above figure, initialization of 20 nodes is done.

b) Scenario 2 :-(Route discovery)

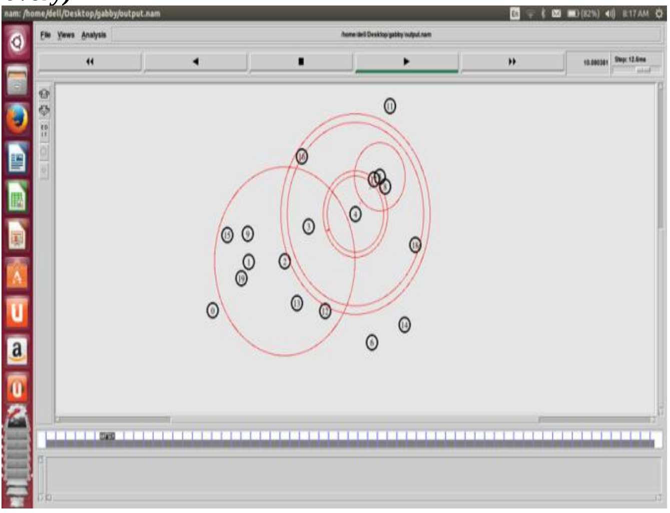

nam: /home/dell/Desktop/gabby/output.nam
File
Views
Analysis
/home/dell/Desktop/gabby/output.nam
Step: 12.6ms

Figure 2: Route Discovery Process in NS-2

In the above figure, route is being discovered. Route discovery process starts only when one node wishes to send packets

c) Scenario 3 :-(Message Transfer)

Figure 3 shows how packet can move or how data can be move from one node to another node by using NS-2.

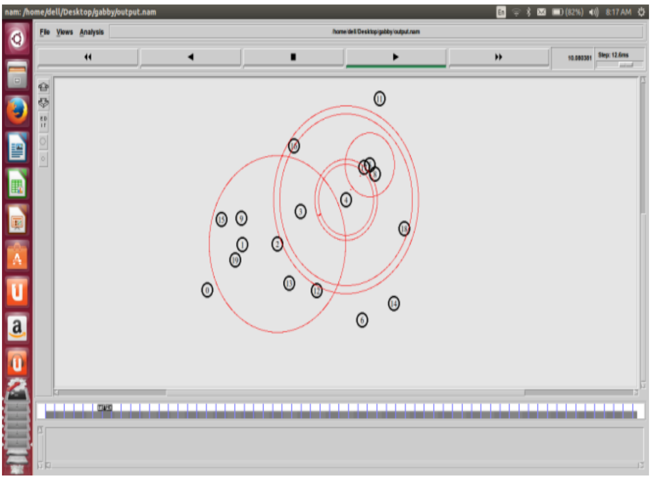

nam: /home/dell/Desktop/gabby/output.nam
File
Views
Analysis
/home/dell/Desktop/gabby/output.nam
Step: 12.6ms

Figure 3: Message Transfer between mobile nodes

In the above figure, red circles around node shows broadcasting process i.e. transferring a message to all recipients simultaneously.

d) Scenario 4- (Attack Detection)

The figures below shows that after receiving the data packets from source, instead of further transmission destination start dropping the data packets. This shows that there is a attack.Here, black hole attack is occurring on the node number 14, when black hole attack occur it start dropping the packet rather than transfer on the route. In this scenario red dots below the node number 6 shows packet drop.

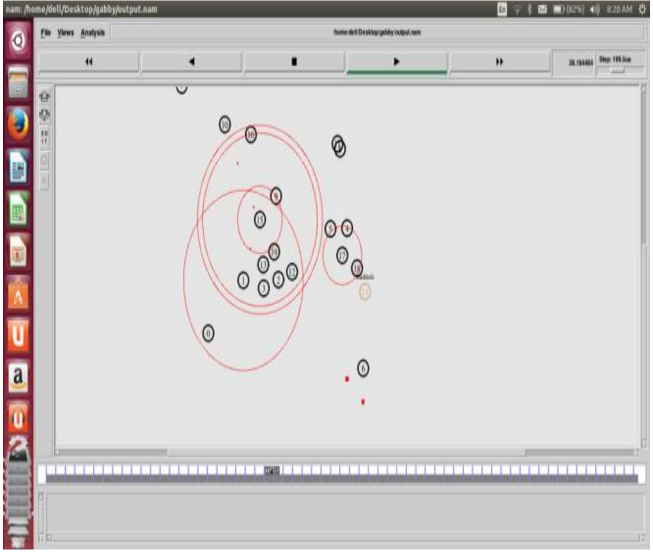

nam: /home/dell/Desktop/gabby/output.nam
File
Views
Analysis
/home/dell/Desktop/gabby/output.nam

Figure 4:- Black hole attack

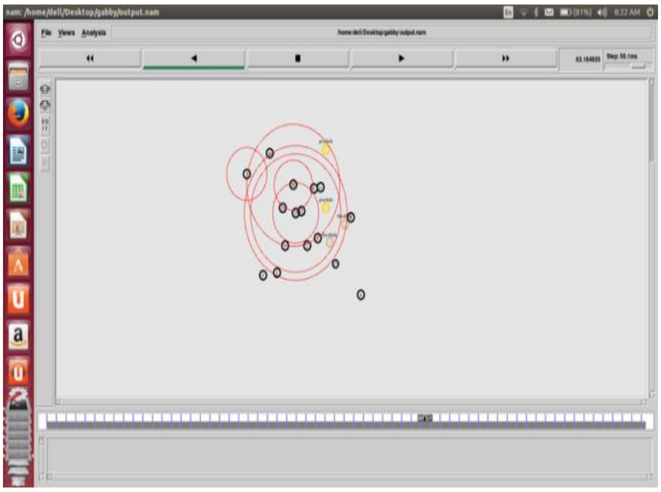
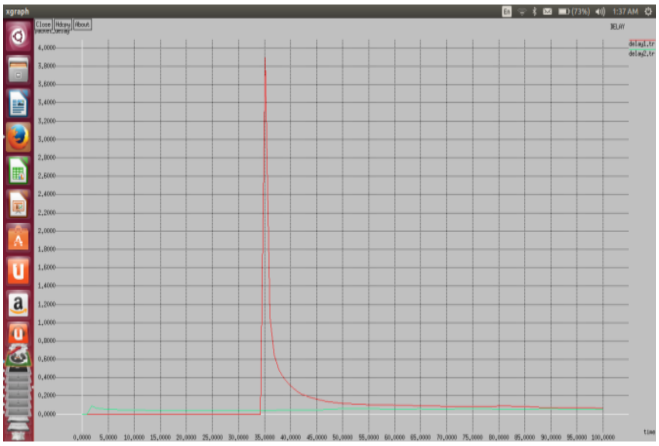

nam: /home/dell/Desktop/gabby/output.nam
File
Views
Analysis
/home/dell/Desktop/gabby/output.nam

Figure 5:-Grayhole attack

In the figure 5, nodes with yellow colour are suffering from grayhole attack. In gray hole attack the node which suffer from the attack alter the message and pass the wrong information in the network which is also called as alteration attack and fabrication attack.

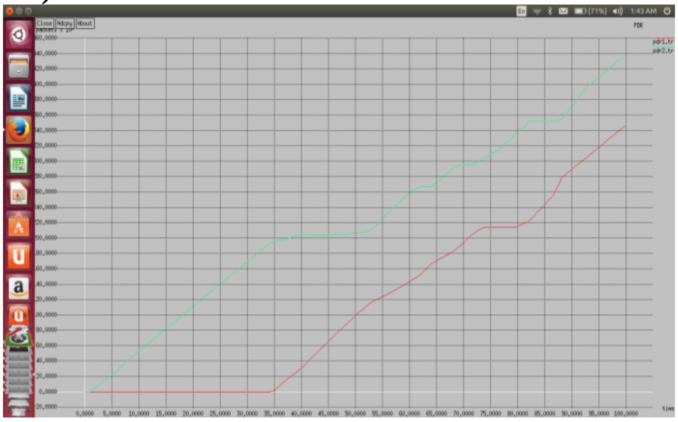
I. Graph Representation

a) End-to-end delay



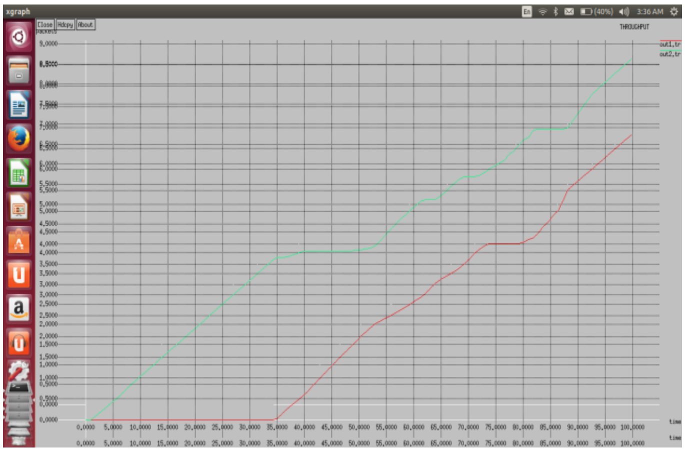
This graph represent end to end delay factor and include end to end factor for MRAODV(most reliable AODV) and ID3(Iterative Dichotomiser 3). This graph shows that red arc is for MRAODV and green arc is for ID3 end to end delay value and this represents the end to end delay factor for ID3 is better because it is having the least value. Lower the end to end delay value higher the efficiency.

a) Packet Delivery Ratio (PDR)



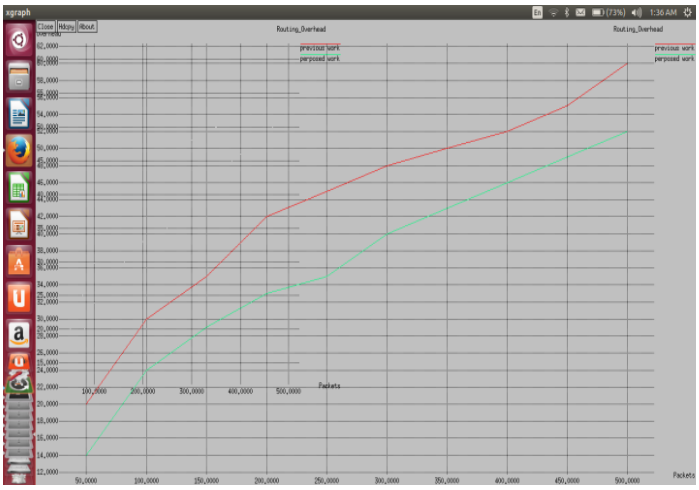
This graph represent PDR factor. It includes PDR factor for MRAODV (Most Reliable AODV) and ID3 (Iterative Dichotomiser 3). This graph shows that red arc is for MRAODV and green arc is for ID3. This represents the PDR factor for ID3 is better because it is having the higher value. Higher the PDR value higher the efficiency.

b) Throughput



This graph represent Throughput factor. It includes Throughput factor for MRAODV (Most Reliable AODV) and ID3 (Iterative Dichotomiser 3). This graph shows that red arc is for MRAODV and green arc is for ID3. This represents the Throughput factor for ID3 is better because it is having the higher value. Higher the Throughput values higher the efficiency.

a) Routing Overhead



This graph represents Normalised Routing Overhead. It includes overhead factor for MRAODV (Most Reliable AODV) and ID3 (Iterative Dichotomiser 3). This graph shows that red arc is for MRAODV and green arc is for ID3 overhead value and this represents the overhead factor for ID3 is better because it is having the least value. Lower the overhead value higher the efficiency.

IV. CONCLUSION

A mobile ad-hoc network (MANET) is composed of a group of mobile, wireless nodes which cooperate in forwarding packets in a multi-hop fashion without any centralized administration.

In this research work is done on the security of MANETs. Firstly scenario is created then nodes are initialised then for the implementation ID3 is used which stands for intrusion detection system and we are using 3rd version of ID3. ID3 is generally used toalert the system about the coming danger. Here, ID3 is alerting other nodes about the malicious node. At the end the comparison is done between RAODV (Reliable AODV), MRAODV (Most Reliable AODV), ID3 .This research concludes that ID3 is better than RAODV and MRAODV. This system can better optimize in future by using some artificial intelligence technique.

REFRENCES

[1] C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance vector routing (DSDV)”. In Proc. of ACM Sigcomm, Vol.8, pp. 234– 244, Sep. 1994.

[2] C. E. Perkins and E. M. Royer, “Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications”, Vol. 3, pp. 90–100, Feb. 1999.

[3] DanaiChasaki and Tilman Wolf, “Evaluation of Path Recording Techniques in Secure MANET” Vol.2, Issue 2, pp. 15-21, 2012.

[4] H. Tian and H. Shen, “Multicast-based inference of network-internal loss performance,” in Proc. of 7th International Symposium on Parallel Architectures Algorithms and Networks (ISPAN 2004), Hong Kong, China, Vol.6 pp. 288–293, May 2004,.

[5] IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501, Vol.2, No6, December 2012.

[6] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Vol. 3, Issue 5, May 2013 ISSN: 2277 128X.

[7] Merin Francis,M. Sangeetha, and Dr. A. Sabari, “A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET” International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE), Vol.3, Issue 1,pp.40-49, 2013

[8] Charles E. Perkins and Pravin Bhagwat, “Highly dynamic destination-sequenced distance vector routing (DSDV) for Mobile Computers”, “Proc. ACM Conf. Communications Architectures and Protocols”, London,UK, pp. 234-244,1944.