Detection and Prevention of DOS on Mobile Adhoc Networks

[I]Guljar Singh, [II]Jasbir Singh Saini, [III]Gurdeep Singh Hyher
[I]M.Tech Student, Dept. of IT, [II]Dept. of CSE Associate Prof., [III]Dept. of CSE Assistant Prof.
[I,II,III]G.N.D.E.C. Ludhiana, Uniersity: IK Gujral Punjab Technical University Jalandhar, Ludhiana, India

Abstract

A mobile ad-hoc network (MANET) is collection of a group of mobile.Role of ad-hoc networks has become vital in ubiquitous computing. Mobile Ad-hoc is such a routing protocol which is susceptible to a variety of security threats against networks. Black hole and Grey hole 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 RSA AND MD5 modified version to improve the performance of MANET. Here, RSA AND MD5 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.

Keyword

Attack;Routing;

I. Introduction

A MANET is considered a collection of wire-less mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. The mobile hosts are not bound to any centralized control like base stations or mobile switching centers. Existing link level security techniques (e.g. encryption) are often applied within wireless networks to reduce these threats. Absent link-level, at the network layer, the most pressing issue is one of inter-router authentication prior to the exchange of network control information Networking Operations Most important networking operations. Include out in and network management.Routing protocols can be divided in to proactive,reactive and hybrid protocols,depending on the routing.

II. Security Threats in AD- HOC Networks

Types of Attacks:-

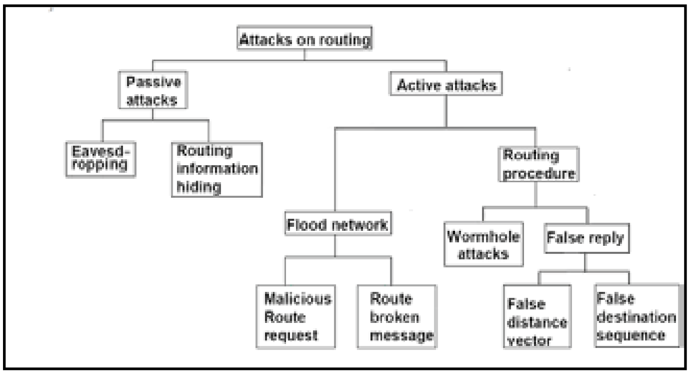

Fig (a): - Types of attack.

a) Passive attack: - Passive attacks typically include only dropping ofd ata.
b) Active attacks: - Active attacktions performedfor replication; modification and deletionofinter data.
c) External attack: retypically active attacks that are targeted e.g. to cause congestion, propagatein correct routing information, preventservices from working properly or shutdown them completely. External attacks can typically be prevented by using standard security mechanismssuc has firewalls, encryption and soon.
d) Internal Attack: - Internal attacks are typically more severe attacks,since malicious insider nodes already belong to the network as anauthorized party and are thus protected with the security mechanisms the network and its services offer.
e) Black Hole Attack**:** In this type of attack, one malicious node uses routing protocol to claim itself of being shortest path to destination node but drops routing packets and doesn't forward packets to its neighbours
f) Gray Hole Attack**:** The gray hole attack is also a kind of DoS attack. Gray hole is an extension of black hole attack in which malicious node behaviours and activities are exceptionally unpredictable.
g) Multiple Black Hole Attack: - The black hole attack is even worse if the multiple Black hole nodes exist in the network. When multiple black hole nodes exist in the network, all the malicious nodes are responsible for triggering the Black hole attack

III. Security Requirements in Manets

1. Availability
2. Authorization and Key Management
3. Data Confidentiality
4. Data Integrity
5. Non-repudiation

IV. Algorithms Introduction:-

RSA AND MD5

The RSA AND MD5 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 recurse on each subset, considering only attributes never selected before.

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 formobile 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 security Mechanisms whatsoever. The authors identify then necessity of having proper confidentiality and authentication services within the routing,but suggest no solutions

For them. TheIPSec is however, mentioned as one possible solution. Multicast AdHoc On-Demand Distance-Vector routing protocol(MAODV),specified in extends

The AODV protocol with multicast features.

V. Discussion Result

Scenario 1

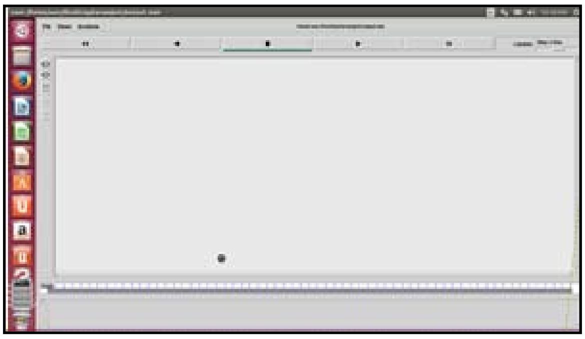

Fig. 1 : Establishment of first node

In this scenario, the black circle here represent establishment of first node.

Scenario 2

In this scenario, 50 nodes are deployed in the simulated area claims that it has the shortest path for further transmission. So source node start sending data packets to destination .

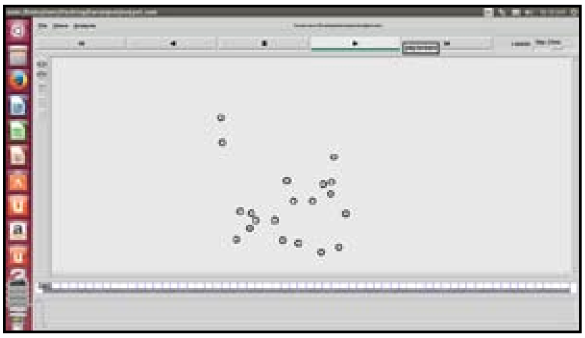

Fig. 2 : Simulation showing 50 deployed nodes

Scenario 3

This scenario shows the packet transfers from the source to destination through the routing. Here circle around nodes represent broadcasting.

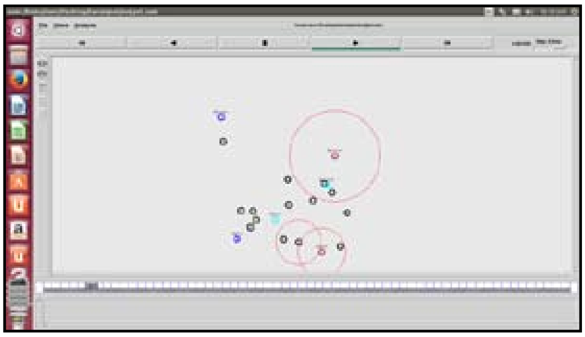

Fig. 3 : Packet transfers between destinations

Here 3 destination and 3 sources are there out of which source1 and destination1 are given with blue colour, source2 and destination2 are given with red colour and source3 and destination3 are given with sky blue colour.

Scenario 4

This scenario 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.

Now our purpose is to detect the attack whether it is a black hole attack or gray hole attack.

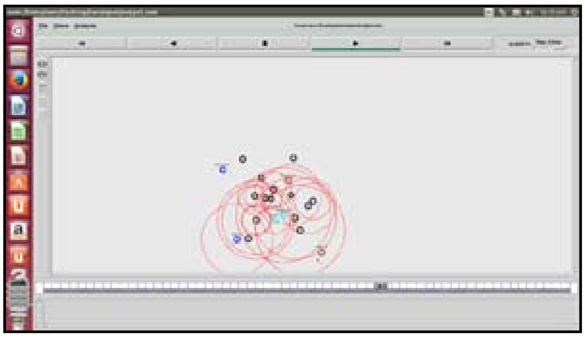

Fig. 4 : Packet drop

Here 3 destination and 3 sources are there out of which source1 and destination1 are given with blue colour, source2 and destination2 are given with red colour and source3 and destination3 are given with sky blue colour. Red dots below reciever2 (which is of red colour) representing packets. These packets are dropping packets.

Scenario 5

This scenario show result using RSA AND MD5 algorithm which is used for the security purpose the packet loss is reduced here.

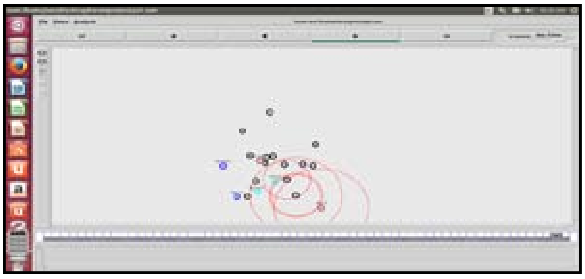

Fig. 5 : RSA AND MD5 algorithm packet loss reduction

This scenario is showing no packets are dropped and this is achieved here after detection of malicious node.

Comparisons Algorithms

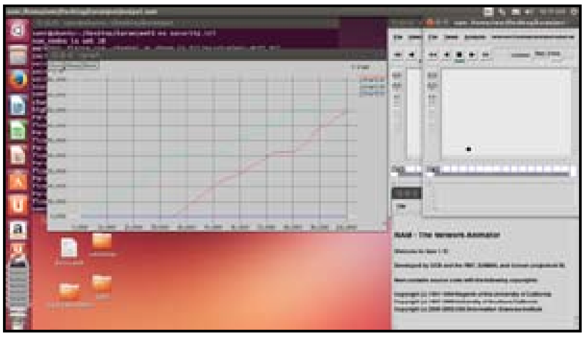

Fig. 6 : Jitter Factor comparison of RAODV, MRAODV and RSA AND MD5

This graph represent jitter factor this graph include jitter factor for RAODV (Reliable AODV)
MRAODV (most reliable AODV) and RSA AND MD5 (intrusion detection). This graph shows that green arc is for RAODV, red arc is for MRAODV and blue arc is for RSA AND MD5 jitter value and this represent the jitter factor for RSA AND MD5 is better because it is having the least value. Lower the jitter value higher the quality.

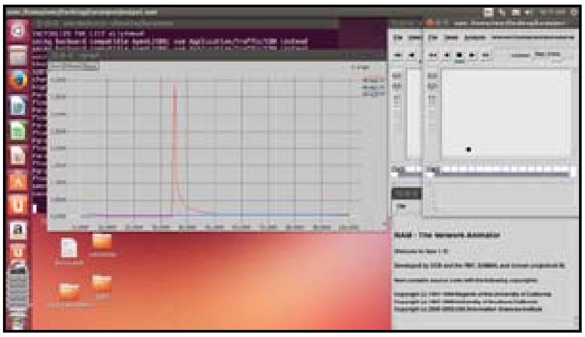

Fig. 7 : E2E delay factor comparison of RAODV,MRAODV and RSA AND MD5

This graph represent end to end delay factor this graph include jitter factor for RAODV(Reliable AODV)
MRAODV (most reliable AODV) and RSA AND MD5(intrusion detection). This graph shows that green arc is for RAODV, red arc is for MRAODV and blue arc is for RSA AND MD5 end to end delay value and this represents the end to end delay factor for RSA AND MD5 is better because it is having the least value. Lower the end to end delay value higher the quality.

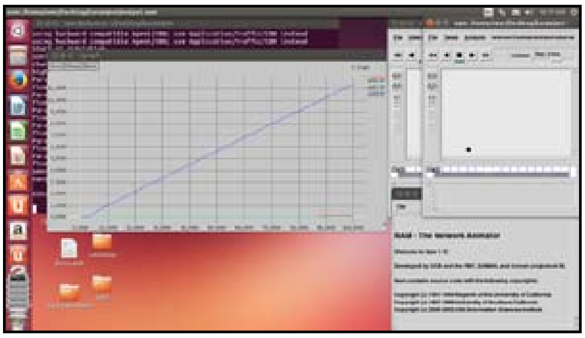

Fig. 8 : Delivery factor comparison of RAODV, MRAODV,RSA AND MD5

This graph represent packet delivery factor this graph include jitter factor for RAODV (Reliable AODV)MRAODV (most reliable AODV) and RSA AND MD5 (intrusion detection). This graph shows that green arc is for RAODV, red arc is for MRAODV and blue arc is for RSA AND MD5 packet delivery value and this represent the packet delivery factor for RSA AND MD5 is better because it is having the highest value Higher the packet delivery value higher the quality.

VI. 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 RSA AND MD5 is used which stands for intrusion detection system and we are using 3rd version of RSA AND MD5. RSA AND MD5 is generally used to alert the system about the coming danger. Here, RSA AND MD5 is alerting other nodes about the malicious node. At the end the comparison is done between RAODV (Reliable AODV), MRAODV (Most Reliable AODV), RSA AND MD5 .
This research concludes that RSA AND MD5 is better than RAODV and MRAODV. This system can better optimize in future by using some artificial intelligence technique.

Referance

[1] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenceddistance 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 vectorrouting. In Proc. 2nd IEEE Workshop on Mobile Computing Systemsand Applications", Vol. 3, pp. 90–100, Feb. 1999.

[3] DanaiChasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in SecureMANET" Vol.2, Issue 2,pp. 15-21, 2012.

[4] H. Tian and H. Shen, "Multicast-based inference of network-internalloss performance," in Proc. of 7th International Symposium on ParallelArchitectures, 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.