IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 11, Issue 2 (May. - Jun. 2013), PP 01-09
www.iosrjournals.org

A New Approach for Improving Performance of Intrusion Detection System over MANET

[1]Kusum Nara, [2]Aman Dureja
[1]*Student, Computer Science and Engineering Deptt, PDM College of Engineering, Bahadurgarh, Haryana (India)*
[2]*Asst. Prof, PDM College of Engineering, Bahadurgarh, Haryana (India)*

Abstract: *A Mobile Ad-hoc Network (MANET) is one of the busy and public networks; Because of this the network suffers from the problems of different kind of attacks. In such attacks some malicious nodes are present that falsely claim itself as a valid node. It will accept the information and will not forward the information to next nodes. Intrusion Detection System (IDS) will be used to detect such kind of attacks, but these attacks slows down the performance of IDS. To improve the performance of IDS and to handle these attacks we have presented an attack avoidance scheme. In which a preventive path will be discovered in which not attacker node will be covered. The detected path may be wider than the shortest path but will provide the higher throughput and reduce the data loss over the network. In our present work we record an interconnection table to track the communication information over the network. The INVERTED TABLE APPROACH will be used to maintain this table. Once the table will be defined, the DATA MINING APPROACH will be used to identify the attacker nodes. The work will be implemented in NS2.35 and the result analysis will be driven based on throughput and the loss analysis.*

Keywords*: Mobile Ad-Hoc Network (MANET), routing protocol, Black Hole Attack, AODV.*

I. Introduction

A Mobile ad hoc network is a group of wireless mobile computers (or nodes);in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed.A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile. The network is decentralized, where all network activity, including discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes.

II. System Architecture of MANET:-

In our architecture, one or more pre-defined nodes act as a *group controller* (GC), which is trusted by all the group nodes. A GC has authority to assign resources to the nodes in MANET. This resource allocation is represented as a Key Note style credential (capability) called *policy token*, and it can be used to express the services and the bandwidth a node is allowed to access. They are cryptographically signed by the GC, which can be verified any node in the MANET. When a node (initiator) requests a service from another MANET node (responder) using the policy token assigned to the initiator, the responder can provide a capability back to the initiator. This is called a *network capability*, and it is generated based on the resource policy assigned to the responder and its dynamic conditions. Figure gives a brief overview of our system. All nodes in the path between an initiator to a responder (*i.e.*, nodes relaying the packets) enforce and abide by the resource allocation encoded by the GC in the policy token and the responder in the network capability. The enforcement involves both accessibility and bandwidth allocation. A responder accepts packets (except for the first one) from an initiator only if the initiator has authorization to send, in the form of a valid network capability. It accepts the first packet only if the initiator's policy token is included. An intermediate node will forward the packets from a node only if the packets have an associated policy token or network capability, and if they do not violate the conditions contained therein. Possession of a network capability does not imply resource reservation; they are the maximum limits a node can use. Available resources are allocated by the intermediate nodes in a fair manner, in proportion to the allocations defined in the policy token and network capability.

The capability need not be contained in all packets. The first packet carries the capability, along with a transaction identifier (TXI) and a public key. Subsequent packets contain only the TXI and a packet signature based on that public key. Intermediate nodes cache policy tokens and network capabilities in a *capability database*, treating them as soft state. A capability database entry contains the source and destination addresses, TXI, the capability, public key for the packet signature and packet statistics

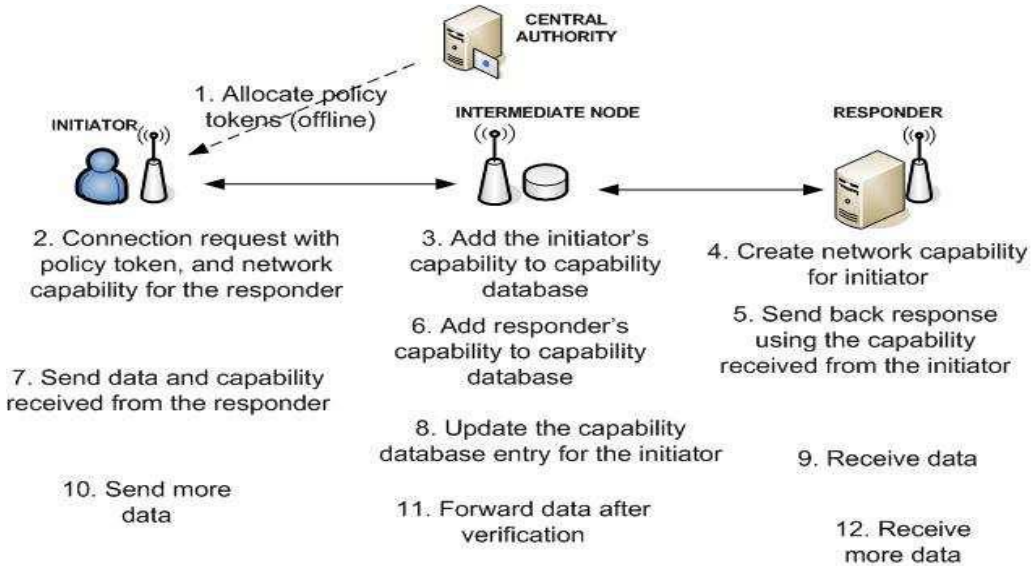


Fig... MANET System Architecture

1.1 Key Issues in MANETs

Many issues can be addressed in the context of MANETs. Here some important issues are presented that have dominated the field of research since the evolution of MANETs.

A. Static Datasets
In MANET, the mining work is generally performed on a static confined datasets. In this the support and confidence values are defined statically.

B. Ineffectiveness
The existing work is ineffective if two malicious nodes will build the path and perform a fake communication.

C. Cooperativeness
MANET routing protocols are usually highly cooperative. This can make them the target of new attacks. For example, a node can pose as a neighbour to the other nodes and participate in decision mechanisms, possibly affecting significant parts of the network.

D. Mobility
MANET nodes can leave and join the network and move independently, so the network topology can change frequently. The highly dynamic operation of a MANET can cause traditional techniques of IDS to be unreliable.

E. Lack of Central Points
MAMANETs do not have any entry points such as routers, gateways, etc. These are typically present in wired networks and can be used to monitor all network traffic that passes through them. A node of a mobile ad hoc network can see only a portion of a network: the packets it sends or receives together with other packets within its radio range. Since wireless ad hoc networks are distributed and cooperative, the intrusion detection and response systems in MANETs may also need to be distributed and cooperative and this leads to some difficulties.

2. Related Work

Xiao Yang Zhang performed a work," Proposal of a Method to Detect Black Hole Attack in MANET". Author propose a new detection method based on checking the sequence number in the Route Reply message by making use of a new message originated by the destination node and also by monitoring the messages relayed by the intermediate nodes in the route. Computer simulation results demonstrate that Presented method has a feature of much lower false positive and negative rates in detecting any number of malicious nodes than the conventional methods.

After Xiao Yang Zhang , Satoshi Kurosawa performed a work," Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" in 2007. The Author analyzes the black hole attack which is one of the possible attacks in ad hoc networks. In this paper, Author proposes an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals. The simulation results show the effectiveness of Presented scheme compared with conventional scheme.

In Year 2009, Mehdi Kargar performed a work," Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes". Author study routing in ad hoc and wireless networks from a game theoretic

view point. Based on this view, the network consists of selfish and greedy nodes who accept payments for forwarding data for other nodes if the payments cover their individual costs incurred by forwarding data. In this work, Author considers that the network consists of malicious nodes too.

After Mehdi Kargar,Athira.M.Nambiar performed a work," Wireless Intrusion Detection Based on Different Clustering Approaches" in 2010. The Author finding optimal set of features from collected WLAN data using a Ranking Algorithm technique. Then with the aid of different data mining techniques such as K-Means, self organizing map and decision tree, these features are analyzed and the performance comparison is carried out.

After Athira.M.Nambiar,Rajib Das performed a work," Security Measures for Black Hole Attack in MANET: An Approach" in the year 2011. The Author gives an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Presented aim is on ensuring the security against Black hole attack. The proposed solution is capable of detecting & removing Black hole node(s) in the MANET at the beginning.

In Year 2012, SaurbhGoyalperformed a work," An Improved Inverted table Approach to Detect Selfish Node In Mobile Ad Hoc Network" after Rajib Das. Authors have to find the frequency of different node and group nodes over the network. To perform the frequency analysis the improved Inverted table will be used. As the selfish node will be identified the network throughput will be improved.

III. Approaches Used

A number of different approaches have been used to detect and remove malicious nodes. We will use two major approaches to detect and remove the malicious nodes. One is The Inverted Table based approach and other is Data Mining approach. Inverted Table approach is used to define communication table with improved information management. Data mining approach is used to identify the black hole and to perform communication over the safe path.

3.1 Inverted Table Approach

Inverted matrix is the numerical representation of a string. The rows of the matrix represent the various characters present in the string and are indexed in the order in which they appear in the string. In this proposed we have taken a sequence. The complete work is divided in three steps:-

i. Identification of Node Sequence
ii. Build the Inverted Table for the Specific Node Sequence.
iii. Frequent Pattern Identification

3.2 Data Mining Approach

There are basically three data mining approaches for detecting malicious nodes. They are:

i. Anomaly-based Intrusion Detection approach
ii. Misuse-based Intrusion Detection approach
iii. Specification-based Intrusion Detection approach

The first technique is *anomaly-based intrusion detection approach.* Itprofiles the symptoms of normal behaviors of the system such as usage frequency of commands, CPU usage for programs, and the like. It detects intrusions as anomalies, i.e. deviations from the normal behavior.

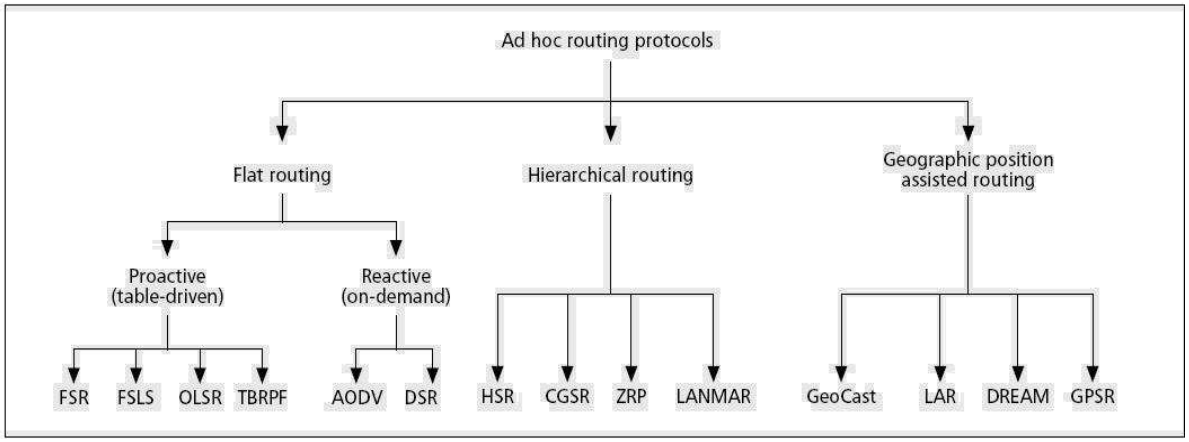
Misuse-based intrusion detection approach compares known attack signatures with current system activities. It is generally preferred by commercial IDSs since it is efficient and has a low false positive rate. The drawback of this approach is that it cannot detect new attacks.

The last technique is *specification-based intrusion detection approach.* In this approach, a set of constraints on a program or a protocol are specified and intrusions are de-tected as runtime violations of these specifications. It is introduced as a promising alternative that combines the strengths of anomaly-based and misuse-based detection techniques and providing detection of known and unknown attacks with a lower false positive rate. It can detect new attacks that do not follow the system specifications.

IV. Routing Protocols

The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile networks.

Classification of routing protocols in mobile ad hoc network can be done in many ways, but most of these are done depending on routing strategy and network structure. The routing protocols can be categorized as flat routing, hierarchical routing and geographic position assisted routing while depending on the network structure. According to the routing strategy routing protocols can be classified as Table-driven and on-demand.



4.1 flat routing protocols

Flat routing protocols are divided mainly into two classes; the first one is proactive routing (table driven) protocols and other is reactive (on-demand) routing protocols. One thing is general for both protocol classes is that every node participating in routing play an equal role. They have further been classified after their design principles; proactive routing is mostly based on LS (link-state) while on-demand routing is based on DV (distance-vector).

4.1.1 Pro-Active/Table Driven routing Protocols

Proactive MANET protocols are also called as table-driven protocols and will actively determine the layout of the network. Through a regular exchange of network topology packets between the nodes of the network, at every single node an absolute picture of the network is maintained. There is hence minimal delay in determining the route to be taken.

4.1.2 Reactive (On Demand) protocols

Portable nodes- Notebooks, palmtops or even mobile phones usually compose wireless ad-hoc networks. This portability also brings a significant issue of mobility. This is a key issue in ad-hoc networks. The mobility of the nodes causes the topology of the network to change constantly. Keeping track of this topology is not an easy task, and too many resources may be consumed in signaling. Reactive routing protocols were intended for these types of environments.

4.2 Hierarchical protocols

These protocols include HSR,ZRP,CGSR,LANMAR protocols.

4.3 Geographic position assisted or Hybrid protocols

Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP), ZHLS etc.

V. An Overview Of AODV Routing Protocol

Ad hoc On Demand Distance Vector Routing (AODV)

Ad hoc On-Demand Distance Vector (AODV) routing is a routing protocol for mobile ad hoc networks and other wireless ad-hoc networks. It is jointly developed in Nokia Research Centre of University of California, Santa Barbara and University of Cincinnati by C. Perkins and S. Das. It is an on-demand and distance-vector routing protocol, meaning that a route is established by AODV from a destination only on demand. AODV is capable of both unicast and multicast routing. It keeps these routes as long as they are desirable by the sources. Additionally, AODV creates trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. The sequence numbers are used by AODV to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes. AODV defines control messages for route maintenance such as:

RREQ- A route request message is transmitted by a node requiring a route to a node. As an optimization AODV uses an expanding ring technique when flooding these messages.

Every RREQ carries a time to live (TTL) value that states for how many hops this message should be forwarded. This value is set to a predefined value at the first transmission and increased at retransmissions. Retransmissions occur if no replies are received. Data packets waiting to be transmitted (i.e. the packets that

initiated the RREQ). Every node maintains two separate counters: a node sequence number and a broadcast_ id. The RREQ contains the following fields
Source Address, Broadcast ID, Source Sequence no., Destination Address, Destination Sequence no., Hop count.

Whenever a node needs to send a packet to a destination for which it has no 'fresh enough' route (i.e., a valid route entry for the destination whose associated sequence number is at least as great as the ones contained in any RREQ that the node has received for that destination) it broadcasts a route request (RREQ) message to its neighbors. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ(unless it has a 'fresher' one).When the intended destination (or an intermediate node that has a 'fresh enough' route to the destination) receives the RREQ, it replies by sending a Route Reply (RREP). It is important to notethat the only mutable information in a RREQ and in a RREP is the hop count (which is being monotonicallyincreased at each hop). The RREP travels back to the originator of the RREQ (this time as a unicast). At eachintermediate node, a route to the destination is set (again, unless the node has a 'fresher' route than the onespecified in the RREP). In the case that the RREQ is replied to by an intermediate node (and if the RREQ hadset this option), the intermediate node also sends a RREP to the destination. In this way, it can be granted that the route path is being set up bi-directionally. In the case that a node receives a new route (by a RREQ or by a RREP) and the node already has a route 'as fresh' as the received one, the shortest one will be up dated. The source node starts routing the data packet to the destination node through the neighboring node that firstresponded with an RREP. The AODV protocol is vulnerable to the well-known black hole attack.

Black Hole Attack

The black hole attack is an active insider attack, it has two
properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.
In other terms, a malicious node uses the routing protocol to advertise as having the shortest path to nodes whose packets it wants to intercept. In the case of AODV protocol, the attacker listens to requests for routes. When the attacker receives a request for a route to the target node, the attacker creates a reply where an extremely short route is advertised, if the reply from malicious node reaches to the requesting node before the reply from the actual node, a fake route has been created. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. It can choose to drop the packets to form a denial-of-service attack.

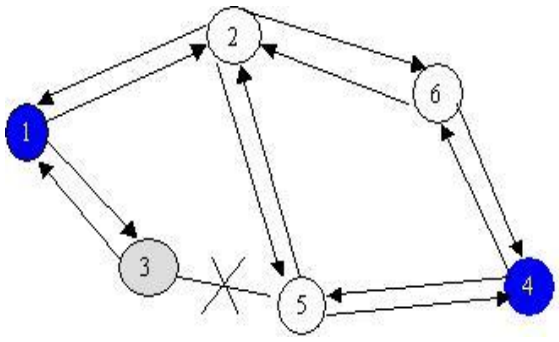


Figure: Black Hole Attack

VI. Performance Evaluation

In this section, we concentrate on describing our simulation
Environment and methodology .To implement the above defined work we have used the NS2.35 as the simulation environment.

A. Network Simulator

NS-2.35 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS-2.35 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithm includes fair queuing, deficit round robin and FIFO. NS-2 started as a variant of the REAL network simulator in 1989. REAL is a network

simulator originally intended for studying the dynamic behavior of flow and congestion control schemes in packet-switched data networks. In 1995 ns development was supported by Defense Advanced Research Projects Agency DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless codes from the UCB Daedelus and CMU Monarch projects and Sun Microsystems have added the wireless capabilities to ns-2.35.

Simulation Parameters

As already outlined, in this proposed system we will observe the actual throughput in shortest path and alternate path. Firstly analyze the network detect if there is some misbehaving node based on the current statistics of receiving packets, forwarding packets and dropping packets. Now the data will be transferred from some compromising node.

The needed Parameters to carry out the simulation and their corresponding values for both protocols are specified below:

Simulation Parameters

Parameter	Value
Number of Nodes	25
Topography Dimension	1051 x 100
Traffic Type	TCP
Radio Propagation Model	Two-Ray Ground Model
MAC Type	802.11.Mac Layer
Routing Protocol	AODV
Antenna Type	Omni directional

Simulation in NS2.35

The ad hoc network comprising of 25 nodes is constructed in the NS-2.35 simulator with the use of ETCL script in the topological boundary area of 1050 m x 100 m. The position of the mobile nodes is defined in terms of X and Y coordinates values. The given scenario showing the packet transmission with shortest path between the nodes starting from the source node 0 to the destination node 9.

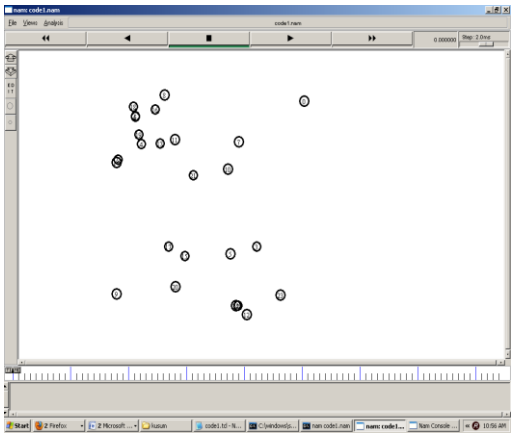


Figure 1: Placement of Nodes

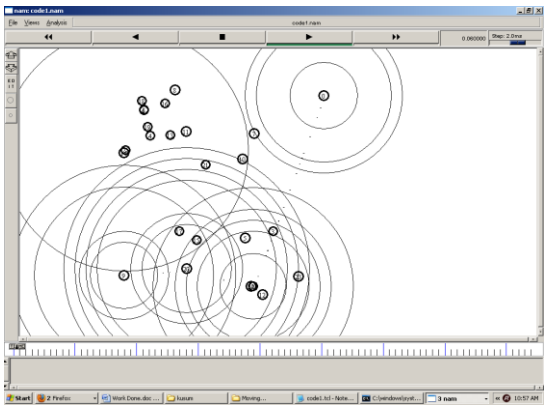


Figure 2: Communication over the network

NS2.35 Overview

The network simulator (NS), which is a discrete event simulator for networks, is a simulated program developed by VINT (Virtual Internetwork Test-bed) project group. It supports simulations of TCP and UDP, some of MAC layer protocols, various routing and multicast protocols over both wired and wireless network etc. Depending on user's requirement the simulation are stored in trace files, which can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called X Graph.

When the simulation is finished, the simulation results are produced in one or more text-based output files that contain detailed simulation data, which can be used to analyze directly or can be used in the graphical user interface Network Animator (NAM). This graphical user interface shows the simulation result in an easy way.

The language that is written in NS-2.35 is not only OTcl but also C++. The event scheduler and the basic network component objects in the data path are written and compiled using C++ to reduce packet and event processing time.These compiled objects need the OTcl linkage to create a matching OTcl object for each of the C++ objects to be able to work with OTcl interpreter.

Tool Command Language (Tcl)

Tool Command Language, Tcl is a powerful interpreted programming language developed by John Ouster out at the University of California, Berkeley. Tcl is a very powerful and dynamic programming language. It has a wide range of usage, including web and desktop applications, networking, administration, testing etc. Tcl is a truly cross platform, easily deployed and highly extensible. The most significant advantage of Tcl language is that it is fully compatible with the C programming language and Tcl libraries can be interoperated directly into C programs.

Network Animator (NAM)

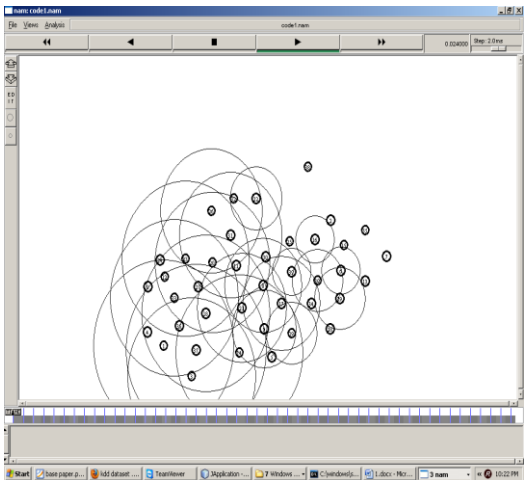
The biggest advantage of network animator (NAM) is that it provides a graphical user interface (GUI) for the different simulation environment according to the parameters specified by the user. The Xgraph utility generates the graphical output of the input data (or trace files).

To animate network traffic in several ways, nam interprets a trace file containing time-indexed network events, as Figure 3(a) shows. Typically, an ns simulation generates this trace, but nam can also use processing data from a live network to produce a trace. Nam usually runs offline using traces stored on disk, but it can also play traces from a running program. The nam trace file contains all information needed for the animation—both on static network layout and on dynamic events such as packet arrivals, departures, and drops and link failures. The input file for wireless networking simulations also includes information on node location and movement.

Network Generation

As the work started at the initial work study the required Simulator NS2.35 to start research on it.This work includes the installation, Environment Setup and basic tutorial study to understand the NS2.35Tcl Script. As the learning stage finish the next work was to setup the network respective to some defined scenario. The scenario parameters are given as

Area	1000x1000
Protocols	AODV
Simulation time	25 seconds
No of nodes	40
Map size	800mx800m
Max speed	20m/s
Mobility model	Random way point
Traffic Type	Constant bit rate (CBR)
Packet Size	512 bytes



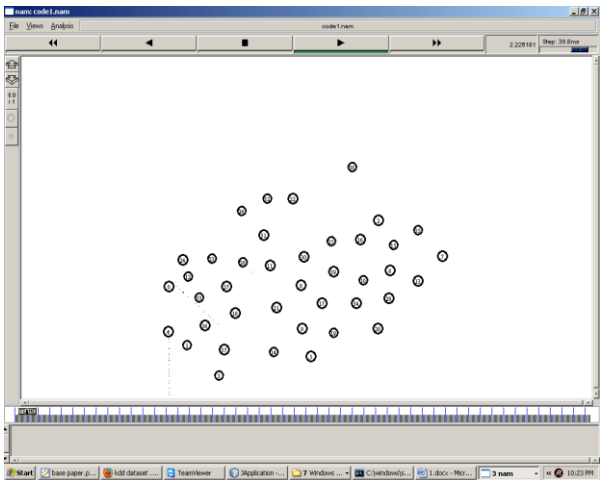


Figure: 3(a)Figure: 3(b)

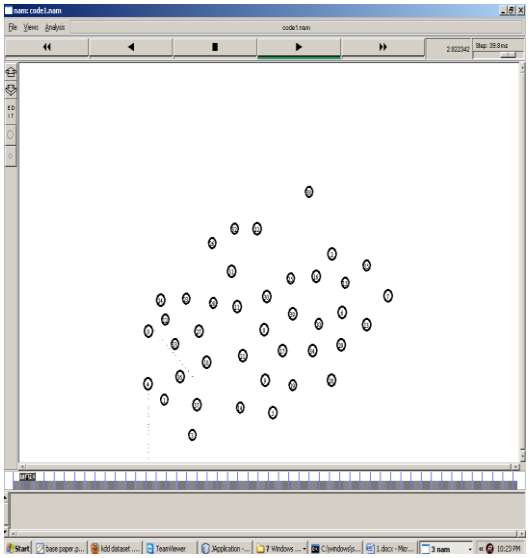


Figure: 3(c)

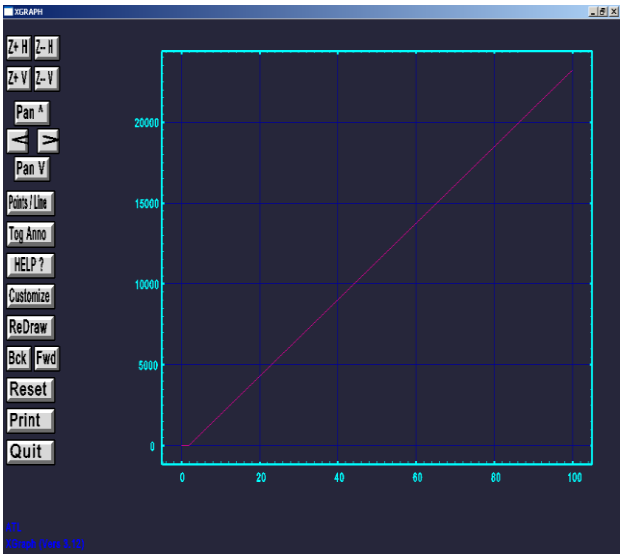


Figure 4: Number of packets Transmitted

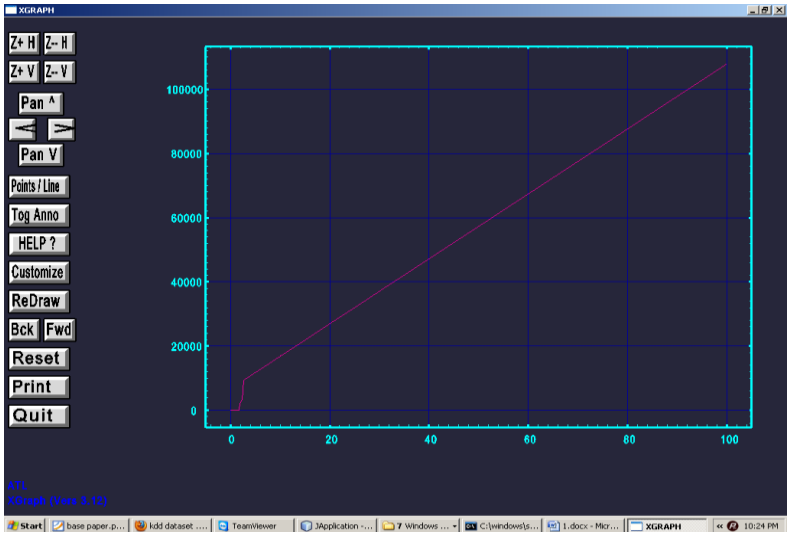


Figure 5: Number of packets lost

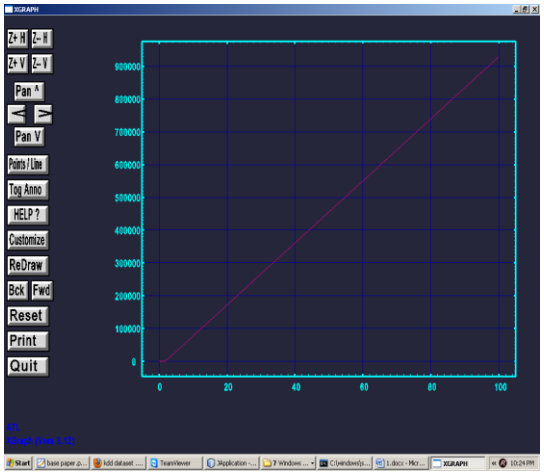


Figure 6: Bytes Transmitted

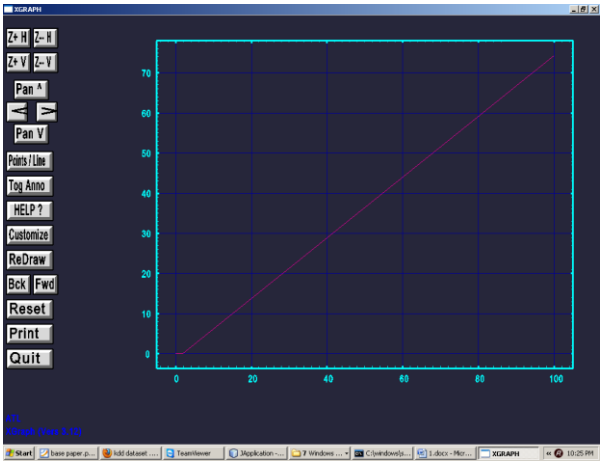


Figure 7: Bit rate

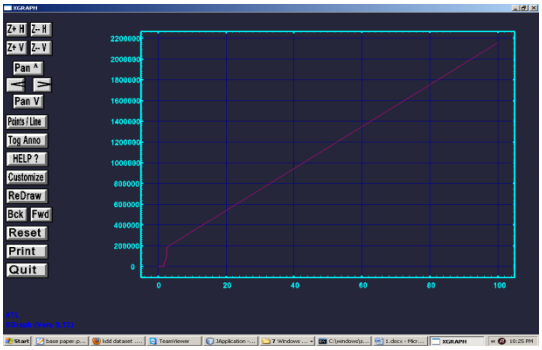


Figure 8: Packet Loss rate

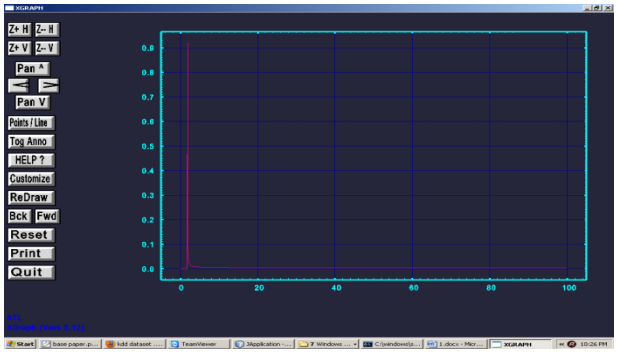


Figure 9: Packet Delay

VII. Conclusion and Future Work

In this paper we have gone through the routing security issues of MANETs, described the black hole attack that can be mounted against a MANET and proposed a feasible solution for increasing performance of Intrusion Detection System (IDS) using the AODV protocol. The proposed solution can be applied to

a) Identify single and multiple black hole nodes cooperating with each other in a MANET

b) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation.

Also we showed the number of packets transferred, number of bytes transferred, packet loss rate and packet delay etc.

In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes. The detection of Black holes in ad hoc networks is still considered to be a challenging task.

We simulated the Black Hole Attack in the Ad-hoc Networks and investigated its affects. In our study, we used AODV routing protocol and NS-2.35, But the other routing protocols could be simulated as well. All routing protocols are expected to present different results. Therefore, the best routing protocol for minimizing the Black Hole Attack may be determined.

References

[1] SaurbhGoyal," An Improved Inverted table Approach to Detect Selfish Node In Mobile Ad Hoc Network", *International Journal of Applied Engineering Research, ISSN 0973-4562 Vol.7 No.11 (2012)*

[2] MonitaWahengbam," Intrusion Detection in MANET using Fuzzy Logic", *978-1-4577-0748-3/12 © 2012 IEEE*

[3] Xiao Yang Zhang," Proposal of a Method to Detect Black Hole Attack in MANET".

[4] Neelam Sharma," Layered Approach for Intrusion Detection Using Naïve Bayes Classifier", *ICACCI'12*, August 3-5, 2012, Chennai, T Nadu, India.Copyright 2012 ACM *978-1-4503-1196-0/12/08 (pp 639-644)*

[5] G.V. Nadiammai," An Evaluation of Clustering Technique over Intrusion Detection System", International Conference on Advances in Computing, Communications and Informatics *(ICACCI-2012) (pp 1054-1060)*

[6] Rajib Das," Security Measures for Black Hole Attack in MANET: An Approach", International Journal of Engineering Science and Technology *(IJEST) ISSN: 0975-5462 Vol. 3 No. 4 Apr 2011 (pp 2832-2838)*

[7] K C Nalavade," Intrusion Prevention Systems: Data Mining Approach", International Conference and Workshop on Emerging Trends in Technology *(ICWET 2010) – TCET*, Mumbai, India ICWET'10, February 26–27, 2010, Mumbai, Maharashtra, India. Copyright 2010 *ACM 978-1-60558-812-4 (pp 211-214)*

[8] Athira.M.Nambiar," Wireless Intrusion Detection Based on Different Clustering Approaches", *A2CWiC 2010*, September 16-17, 2010, India Copyright *© 2010 978-1-4503-0194-7/10/0009*

[9] Mehdi Kargar," Truthful and Secure Routing in Ad Hoc Networks with Malicious and Selfish Nodes", *International Journal of Security and its Applications Vol. 3, No. 1, January, 2009 (pp 117-128)*

[10] Daniela Brauckhoff," Anomaly Extraction in Backbone Networks using Association Rules", *IMC'09, November 4–6, 2009, Chicago, Illinois, USA. ACM 978-1-60558-770-7/09/11 (pp 28-34)*

[11] Satoshi Kurosawa," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007 (pp 338-346*

[12] Vera Marinova-Boncheva," Applying a Data Mining Method for Intrusion Detection", *International Conference on Computer Systems and Technologies - CompSysTech'07*

[13] Zahra Safaei," An Efficient Reputation-Based Mechanism to Enforce Cooperation in MANETs", *LATEST TRENDS on COMMUNICATIONS and INFORMATION TECHNOLOGY ISSN: 1792-4316 ISBN: 978-960-474-207-3 (pp 33-38)*

[14] Tsong Song Hwang," A Three-tier IDS via Data Mining Approach", MineNet'07, June 12, 2007, San Diego, California, USA. *ACM 918-1-59593-792-6/07/0006 (pp 1-6)*

[15] LTC Bruce D. Caulkins," A Dynamic Data Mining Technique for Intrusion Detection Systems", (*pp 148-153)*

[16] Neil Hurley," Statistical Attack Detection", *RecSys'09, October 23–25, 2009, New York, New York, USA. ACM 978-1-60558-435-5/09/10 (pp 149-156)*

[17] Guanhua Yan," Towards a Bayesian Network Game Framework for Evaluating DDoS Attacks and Defense", *CCS'12, October 16–18, 2012, Raleigh, North Carolina, USA.ACM 978-1-4503-1651-4/12/10. (pp 553-566)*

[18] Yu Liu," A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", *GameNets'06, October14, 2006, Pisa, Italy. ACM 1-59593-507-X/06/10*