RESEARCH ARTICLE OPEN ACCESS

DYNAMIC INTRUSION ANALYSIS AND IMPRECISE INFORMATION BREAKTHROUGH OF MANET

1Mrs. Sandhiya V., 2 Ms. Abarna N.,

*1 M.Phil Research Scholar, PG & Research Department of Computer Science & Information Technology, Arcot Sri Mahalakshmi Women's College, Villapakkam, Vellore, Tamil Nadu, India

*2Assistant Professor, PG & Research Department of Computer Science & Information Technology, Arcot Sri Mahalakshmi Women's College, Villapakkam, Vellore, Tamil Nadu, India

--*************************--

Abstract:

objective is to design and develop an intrusion detection and response model for Mobile Ad hoc Networks (MANET). Mobile ad hoc networks are infrastructure-free, pervasive and ubiquitous in nature, without any centralized authority. These unique MANET characteristics present several changes to secure them. The proposed security model is called the Intrusion Detection and Response for Mobile Ad hoc Networks (IDRMAN). The goal of the proposed model is to provide a security framework that will detect various attacks and take appropriate measures to control the attack automatically. This model is based on identifying critical system parameters of a MANET that are affected by various types of attacks, and continuously monitoring the values of these parameters to detect and respond to attacks. Many number of intrusion detection systems have been discovered to handle the uncertain activity in mobile ad hoc networks. This dissertation emphasized on proposed fuzzy based intrusion detection systems in mobile ad hoc networks and presented their effectiveness to identify the intrusions. This dissertation also examines the drawbacks of fuzzy based intrusion detection systems and discussed the future directions in the field of intrusion detection for mobile ad hoc networks.

Keywords— **Intrusion Detection, Mobile ad hoc Network, Fuzzy Framework, Wireless Sensor Network, clustering, Communication load**

--*************************--

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority. In a MANET, each wireless mobile node operates not only as an end-system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. MANET does not require any fixed infrastructure such as base stations; therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously. For instance, first responders at a disaster site or soldiers in a battlefield must provide their own communications. A MANET is a possible solution for this need to quickly establish communications in a mobile, transient and infrastructure-less environment. This is one of many applications where MANET's can be used. Mobile ad-hoc networks are the future of wireless networks. Nodes in these networks will generate both user and application traffic and perform various network functions

A Personal Area Network (PAN) level firewall as envisioned for the next generation wireless networks can protect only if the users are at home and not when the users are roaming [9]. Even if such a firewall is provided, the communication would get fragmented by these 'check points' on the network, as each firewall needs maintenance of activities like log control, software update etc., creating unnecessary overhead. Thus existing technologies like firewalls and Virtual Private Network (VPN) sandboxes cannot be directly applied to the wireless mobile world. Even if the firewall concept were achieved by creating a private extranet (VPN) which extends the firewall protected domain to wherever the user moves, this would still lead to inefficient routing.

Security is a fundamental concern for mobile network based system. Harrison et al identify security as a "severe concern" and regard it as the primary obstacle to adopting mobile systems. Until recently, the main research focus has been on improving the protocols for multi-hop routing, performance and scalability of the ad hoc networks. Though the performance and scalability have their place in wireless MANET research, the current and future applications of the ad hoc networks has forced the research community to look at dependability and security aspects of ad hoc networks.

Security in mobile ad hoc network is essential even for basic network functions like routing which are carried out by the nodes themselves rather than specialized routers. The intruder in the ad hoc network can come from anywhere, along any direction, and target any communication channel in the network. Compare this with a wired network where the intruder gains physical access to the wired link or can pass through security holes at firewalls and routers.

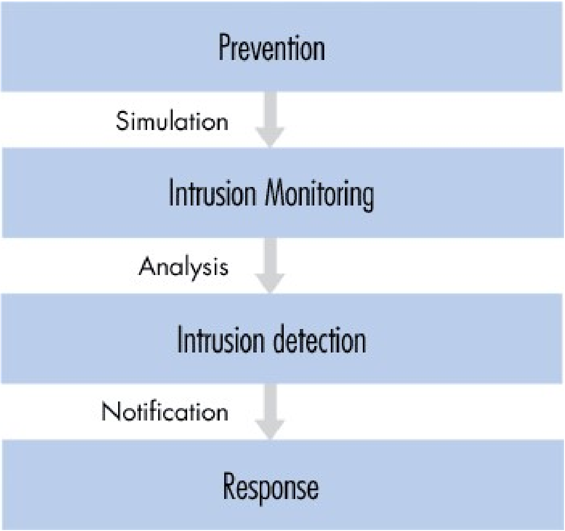


Fig 1.1 : Intrusion detection system activities

1.1 ACTIVE ATTACK IN MANET - ROUTING ATTACK

Routing attack is a significant problem because nodes within the ad hoc network themselves performs routing functions and the security concepts are not incorporated in most of the routing protocols. Also, routing tables form the basis of network operations and any corruption to the routing table may lead to significant adverse consequences. Routing attacks on the mobile ad hoc networks can be reactive routing protocol attacks or proactive routing protocol attacks based on the type of protocol used for routing.

- **Injecting incorrect information in the routing table:** In this type of routing attack, malicious nodes or an intruder would inject incorrect routing information, which in turn would poison the routing tables. These attacks would result in the artificial partitioning of the network, and the hosts residing in one partition would not be able to communicate with hosts residing in the other partition.
- **Routing Loop Attacks:** In this attack, intruder or malicious nodes update the routing table to create a loop, so that packets can traverse in the network without reaching the destination, thereby conserving energy and bandwidth.

1.2 PASSIVE ATTACK IN MANET – SELFISHNESS

Passive attacks could be caused by selfishness, eavesdropping and traffic analysis. In this section we explain selfishness attacks to give an idea of passive attacks. In the selfishness attacks, the selfish node abuses constrained resources, such as battery power, for its own benefit. They do not intend to directly damage other nodes in the network. Attackers may also get hold of a node and modify its behavior to make it malicious, so the node would perform selfish attacks in need of resources.

- **Packet mistreatment or interception:** In this kind of attack, a selfish node does not perform the function of packet forwarding. As mentioned earlier, interruption of packets may reduce the overall throughput of the network. In a specialized form of packet discarding, selfish nodes do not forward the packets to host destination, but to itself. This result in black hole and DoS attacks.
- **Energy consumption:** In this kind of attacks, nodes try to save significant battery power by not performing networking functions such as routing. This is due to the fact that in ad hoc network most of the energy is consumed by routing of packets.

II. RELATED WORK

As discussed in the sections above, security is a fundamental concern for MANET. To address these security related issues, there is a need for an efficient and effective intrusion detection and response framework that could detect and respond to the security related attacks at a node level for MANET. This research work attempts to address this need. So the problem statement for the dissertation can be stated as follows: To design an intrusion detection and response security model, which would detect and control the security related attacks at the node level for mobile ad hoc network in wireless environment.

- The objective of this research is to develop such an efficient and effective intrusion detection and response framework with the following features:
- Identify the attack sensitive network parameters and their threshold values to construct the detection and response models.
- Detect threat at the node level effectively in the MANET environment.
- Identify the intruder that caused the threat.
- Respond to the intruder and attacks, thereby controlling the attack and protecting the MANET.
- Design and construct the MANET intrusion detection and response framework such that it is protocol independent.

The security of these nodes could be compromised by an external attacker or due to the selfish nature of other nodes. This would create a severe threat of Denial of Service (DoS) and routing attacks where malicious nodes combine and deny the services to legitimate nodes. Unlike nodes in a wired network, the nodes of MANET may have less processing power as well as battery life and consequently would try to conserve resources. In this scenario, the usual authentication and encryption methods would not apply to a MANET the same way they would in a wired network. However, both authentication and encryption are even more important in a MANET. Steiner et al have developed a Group key Diffie-Hellman (GDH) model that provides a flexible solution to group key management. Yi et al have developed the MOCA (MObile Certification Authority) protocol that helps manage heterogeneous mobile nodes as part of a MANET. MOCA uses Public Key Infrastructure (PKI) technology

Applications of Mobile Ad Hoc Networks (MANET) are increasing in practice; however, MANET is venerable to attacks due to its mobile and ad hoc natures. The security issue is becoming a major concern and bottle neck in the applications of MANET; therefore, selections of intrusion detection methods are especially important for MANET applications. In the current paper, an overview of existing IDS for MANET is conducted based on reviewing features, security issues and requirements of MANET for intrusion detection systems (ISD). A comparison study is conducted to compare existing intrusion detection methods based on inputs, outputs, processes, advantages and disadvantages. Some guidelines are also proposed in selecting intrusion detection methods. The results of the current research are useful for educational and industrial professionals who are interested in information systems security in the wireless world. This paper also presents a case study of a MIS/CIS/CS curriculum on the first introduction of the new technology for IDS in MANET.

Networks are protected using many firewalls and encryption software's. But many of them are not sufficient and effective. Therefore an intrusion detection system (IDS) is required that monitors the network, detects misbehavior or anomalies and notifies other nodes in the network to avoid or punish the misbehaving nodes. Numerous schemes have been proposed for Intrusion Detection and Response Systems, for Ad hoc networks. The ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users.

Apply local intrusion detection or network intrusion detection for the attack. It will work for both anomaly detection and misuse detection mechanism. By the Observation of the attack signatures, we find that there are some attack signatures dependent on other previous attack signatures. This is due to the new attack is a derivative from the previous attack. To apply the intrusion detection technique this paper introduces a priory known approach known as acknowledgement based approach which is used to detect intrusion in mobile ad hoc network (MANET) and uses intrusion detection technique like matching algorithm. It approaches a technique of developing a network safety by describing network behavior structure that point out offensive use of the network and also look for the occurrence of those patterns while such an approach may be accomplished of detecting different types of known intrusive actions, it would allow new or undocumented types of attacks to go invisible. As a result, this leads to a system which monitors and learns normal network behavior and then detects deviations from the normal network behavior.

III. IDRMAN SECURITY MODEL – DETECTION FRAMEWORK

Intrusion Detection and Response model for Mobile Ad hoc Networks (IDRMAN) detects an attack and responds to the detected attack. An attack is detected by identifying the set of network parameters that will be affected during an attack, identifying the thresholds for these parameters, continuously monitoring these parameters, quantifying the network vulnerability by applying fuzzy logic on the measured values of the network parameters and comparing the quantified values against the reference thresholds of the threat detection metric. The set of network parameters that will be affected during an attack are referred to as significant parameters and are identified using data mining techniques. The thresholds for these significant parameters are identified using Six Sigma methodology. The network vulnerability level is quantified into a numerical value called the Threat Index (TI) computed using Fuzzy logic. Based on the threat level indicated by TI, the response mechanism is invoked (which is explained in Chapter 4) which then identifies the intruder and responds to the attack.

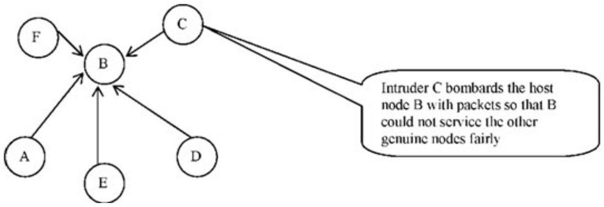

F
B
C
A
E
D
Intruder C bombards the host node B with packets so that B could not service the other genuine nodes fairly

Fig 3.1: DoS Attack

DoS attack is depicted in Figure 3.1, where node B is a host node and C is the intruder. The intruder node C creates a huge traffic resulting in the exhaustion of the node B's resources. This results in the inability of node B to serve genuine nodes A, D, E and F fairly. Thus, DoS attacks on the mobile ad hoc networks can lead to network performance degradation.

- **Packet Drop:** Due to DoS attacks, packets in the link may be dropped due to exhaustion of the hosts' resources.
- **Queue Length:** The inability of the host to service the request from other nodes because of DoS attacks results in increase in queue length on the links between the host and other nodes.
- **Energy consumption**: The bombardment of packets due to traffic and servicing them result in the consumption of significant battery power (a constrained resource in MANET) in the link between intruders and host.

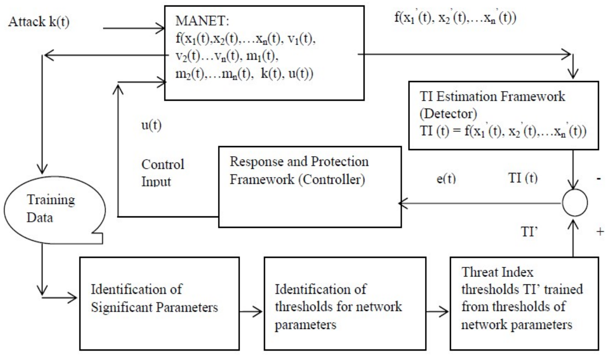

Attack k(t)
MANET:
f(x₁(t),x₂(t),…xₙ(t), v₁(t), v₂(t)…vₙ(t), m₁(t), m₂(t),…mₙ(t), k(t), u(t))
f(x₁'(t), x₂'(t),…xₙ'(t))
TI Estimation Framework (Detector)
TI (t) = f(x₁'(t), x₂'(t),…xₙ'(t))
u(t)
Control Input
Response and Protection Framework (Controller)
e(t)
TI (t)
-
TI'
+
Training Data
Identification of Significant Parameters
Identification of thresholds for network parameters
Threat Index thresholds TI' trained from thresholds of network parameters

Fig 3.2: Feedback Control Model of IDRMAN

$v_2(t)…v_n(t)$, $m_1(t)$, $m_2(t)$,.. .$m_n(t)$, $k(t)$, $u(t)$), where $x_n(t)$ represents the significant attack sensitive network parameters, $vn(t)$ represents the network parameters which are not significant in representing the node vulnerability, $m_n(t)$ represents the mobility parameters, $k(t)$ represents the attack and $u(t)$ represents the control input. x_n (t) represents the modified values of the significant

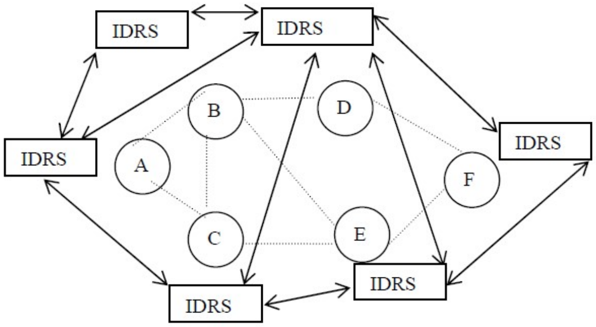


Fig 3.3: Distributed Intrusion Detection and Response System (IDRS)

The need for the cooperative and distributed intrusion detection/response arises because mobile ad hoc networks are dynamic and they typically lack a central entity. Hence, each node responds based on the intrusion reports from other nodes in a distributed manner.

3.1 THE IDRMAN DETECTION FRAMEWORK MECHANISM

The IDRMAN detection framework quantifies an attack or vulnerability with a metric known as Threat Index (TI). Threat Index (TI) is the metric used by the detection framework to detect if the node is under attack or not. Threat Index is a number, which takes values between 1 and 10. When there is no attack, the network is in the normal state (NS) and this is indicated by the TI range from 1 to 4; when there is an attack, the network is in the vulnerable state (VS) and is indicated by the TI range from 7 to 10; the intermediate state of the network between normal and vulnerable state is referred to as the uncertain state (US) which is indicated by the TI range from 4 to 7. The TI thresholds, (4, 7) for the uncertain and vulnerable state are obtained by means of TI threshold training algorithm on the training data.

Steps in Threat Index Computation - Theory and Illustration:

Each step of the threat detection framework, whose objective is to calculate the Threat Index to detect an attack, is explained below with theory and illustration.

Step 1: Log/Data Fetch:

In this step, the raw ad hoc network data is collected from MANET and fed to the detection framework on a real time basis. This step pre-processes the collected data from MANET to make it suitable for threat index evaluation as well as intruder identification. This framework fetches data for both training as well as testing. The training data is used to identify significant parameters and thresholds of those parameters.

Step 2: Identification of Significant parameters/Threat metrics:

This section provides the theoretical foundation of using data mining to identify the significant parameters for the IDRMAN. These significant parameters are used in both the detection and response framework in our model. The measured values of these significant parameters are used to calculate TI in the detection mechanism and to identify the intruder in the response mechanism**.**

Step 3: Classification Tree:

Let Y1,Y2,_Yn, O be random variables where Yi has domain Dom(Yi) and O has domain Dom (O) = {1,...,J}. Here Y1;..., Yn are the predictor attributes and n is the number of predictor attributes. O is the class label. J denotes the number of class labels, which are 1, 2,...,J. i.e, J represents the set of possible values that the class label, O can have in its domain, Dom(O).

Thus, R(C, D2) = | {dj e D2 and C misclassifies dt] | / |D2| = 1/ N x ^ 1{c(d} where 1{A] = {1 if A is True; 0 if A is false].

As an example, let there be 100 records in Testing Dataset D2; whose fields consists of DoS attack sensitive parameters like QL, NC, EC, PL and other network parameters. Let the classifier C, trained using Dataset D1 identify 4 records as Normal when the true label is DoS.

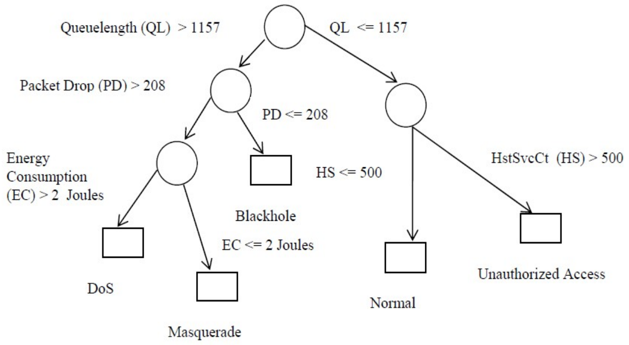


Fig 3.4: Classification Trees

Let us consider the following example to explain the concept of classification trees as used in the thesis. Let us consider a dataset for training that has the records sourced from the network that is subjected to security attack. At the beginning, all of the records in the training set are together in one big box. The algorithm then systematically tries breaking up the records into two parts, examining one variable at a time and splitting the records on the basis of a dividing line in that variable (say, Queue length > 1157 or Queue length <= 1157). The objective is to attain as homogeneous set of labels (say, "DoS", "Masquerade", "black hole" "unauthorized access" or "normal") as possible in each partition. This splitting or partitioning is then applied to each of the new partitions. The process continues until no more useful splits can be found

3.2 Classification Tree Induction Schema Algorithm

Illustrates the classification tree induction schema.

Build Tree (I/P: Node T, dataset D, split selection method, O/P: classification tree T for D).

```
1. Apply V to D to find the split attribute X for node
   T.
2. Let n be the number of children for T.
3. if (T splits)
     Partition D into D1,_, Dn and label node T
   with split attribute X.
   Create children nodes T-i,.. .,Tn of T and label the
   edge(T, Ti) with predicate q(T, Tj)
        for each i €{1,...n]
   BuildTree(Ti, Di, V) end for each
   Else
   Label T with the majority class label of D
```

IV. SYSTEM IMPLEMETNATION

4.1 TI EVALUATION USING FUZZY LOGIC BASED METHODOLOGY

TI is evaluated using fuzzy logic and continuously measured values of the significant network parameters. Fuzzy logic is one of the heuristic approaches for threat evaluation. One of the active areas of fuzzy logic applications is fuzzy expert control system. Fuzzy expert control systems are systems that use common sense rules and natural language statement instead of hard-boundary. Fuzzy control systems have several important characteristics that suit intrusion detection well.

- Fuzzy systems can readily combine inputs from widely varying sources.
- It is easy, flexible, fast and accurate in design and implementation.
- Fuzzy logic is a very natural approach to represent human thinking.
- It is suitable for both linear and nonlinear systems.
- It allows for imprecise mathematical models and measuring sensors

- It is more robust, accurate and flexible than classical controllers. Fuzzy
- Logic may radically affect computer security as a relatively new paradigm.
- It can be used in trusted system analysis and design, in measuring the security of the systems, and in representing the imprecise human world of policies and inference.

4.2 Mamdani Fuzzy Rule Based Model:

Mamdani fuzzy-rule based systems constitute a linguistic description in both the antecedent parts and the consequent parts. Each rule is a description of a condition-action statement that may be clearly interpreted by the users. To describe a mapping from input *U*1× *U*2 × ...× *Un* (where × is the Cartesian product) to output *W*, the linguistic rule structure of Mamdani models is as follows: *Ri*: IF *x*1 is *Ai1* and ... and x_n is *Ain* THEN *y* is *Ci*, *i* = 1, ..., *L*. Where, *L* is the number of fuzzy rules, *xj* € *Uj*, *j* = 1, 2, ..., *n*, are the input variables, *y* is the output variable, and *Aij* and *Ci* are linguistic variables or fuzzy sets for *xj* and *y* respectively. A_{ij} and C_i are characterized by membership functions $\mu_{A_i}(x_j)$ and $\mu_{C_i}(y)$, respectively. Inputs are of the form: x_1 is A'_1, *x*2 is A'_2,..., *xr* is *A'n*. where *A'*1, *A'*2,..., *A'n* are fuzzy subsets of *U*1, *U*2,... *Un*, which are the universe of disclose (or the domain of interest) of inputs.

$$\text{TI} = \frac{\sum_{j=1}^{m} w_j y_j}{\sum_{j=1}^{m} w_j}$$

Here, y_j indicates the output value associated with the particular rule j in the fuzzy set; The output y_j takes its values from the threshold values of TI for normal, uncertain and vulnerable states. Here "m" indicates the number of rules and *wj* indicates the rule strength for rule j in the fuzzy set.

$$W_j = \min(\mu_j(X_i))$$

where i Є {1, 2,...n}, and n is number of network parameters for each rule. If there are k membership values possible for the network parameters and if n is the number of network parameters, then m = kn rules are possible and 1<= j <= m.

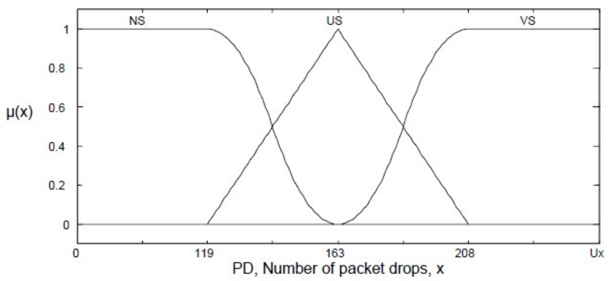


Fig 4.1: Fuzzy Model for Packet Drop Metric

due to the reason that the parametric and functional descriptions of these membership functions are efficient. In these membership functions, the designer needs only to define three parameters; nsx, vsx and usx. Here nsx, usx, and vsx are the normal state, uncertain state and vulnerable state threshold values. It has been proven that triangular MFs can approximate any other membership function. This function is specified by three parameters (a, b, c) as follows:

$$triangle(x_{in}; a, b, c) = \begin{cases} (x_{in} - a)/(b - a) & for\ a \le x_{in} \le b \\ (c - x_{in})/(c - b) & for\ b \le x_{in} \le c \\ 0 & elsewhere \end{cases}$$

The first trapezoid represents the fuzzy set µNS(EC) = {1.0/>=0;<=1.33, 0.0/1.66}. This fuzzy set indicates that membership function µNS of EC is 1 for the value of EC from 0 to 1.33 joules, and the membership function µNS of EC is 0 when the value of EC is 1.66 joules. The second fuzzy set is a triangle and represents the fuzzy set µUS (EC) = {0.0/1.33, 1.0/1.66, 0.0/1.99}. The third fuzzy set is a trapezoid and represents that µVS(EC) = {0.0/1.66, 1.0/>=1.99}.

Rule Number (j)	$\mu_{j\,(PD)}$	$\mu_{j\,(QL)}$	$\mu_j(EC)$	Rule Strength, w_j, $\min(\mu_{i(PD)}\mu_{i(QL)}\ \mu_{i(EC)})$	Output, y_i	$w_j y_j$
1	0	0.25	0	0	1	0
2	0	0.25	0.4	0	1	0
3	0	0.25	0.6	0	1	0
4	0	0.75	0	0	1	0
5	0	0.75	0.4	0	4	0
6	0	0.75	0.6	0	4	0
7	0	0	0	0	1	0
8	0	0	0.4	0	4	0
9	0	0	0.6	0	7	0
10	0.75	0.25	0	0	1	0
11	0.75	0.25	0.4	0.25	4	1
12	0.75	0.25	0.6	0.25	4	1
13	0.75	0.75	0	0	4	0
14	0.75	0.75	0.4	0.4	4	1.6
15	0.75	0.75	0.6	0.6	4	2.4
16	0.75	0	0	0	4	0
17	0.75	0	0.4	0	4	0
18	0.75	0	0.6	0	7	0
19	0.25	0.25	0	0	1	0
20	0.25	0.25	0.4	0.25	4	1
21	0.25	0.25	0.6	0.25	7	1.75
22	0.25	0.75	0	0	4	0
23	0.25	0.75	0.4	0.25	4	1
24	0.25	0.75	0.6	0.25	7	1.75
25	0.25	0	0	0	7	0
26	0.25	0	0.4	0	7	0
27	0.25	0	0.6	0	7	0

Table 4.1 : Calculation of rule strength

Here, $\sum_{j=1}^{m} w_j y_j = 11.5$ and $\sum_{j=1}^{m} w_j = 2.5$ and hence, from equation, TI = 4.6. Comparing the TI calculated with the TI thresholds

4.3 Intrustion Detection Algorithm

- Identify the significant parameters, X= {xi; 1<i<n}, using the CART data mining technique.
- Calculate the threshold values for the significant parameters, X identified in step 1 using six-sigma methodology.
- Set the threshold ranges for the Threat Index, TI using TI threshold training algorithm
- From the MANET, continuously measure the values of these parameters identified in step1, on all the links where the node whose TI is to be evaluated is the destination node. For each parameter, compute their average.
- For each node in the MANET, calculate Threat Index (TI) using the average parameter values obtained in 4 above.
- Compare the calculated TI with the TI threshold to detect if the network is under attack.
- For each node that is under threat (abnormal TI) invoke intruder identification and response algorithm

V EVALUATION RESULT

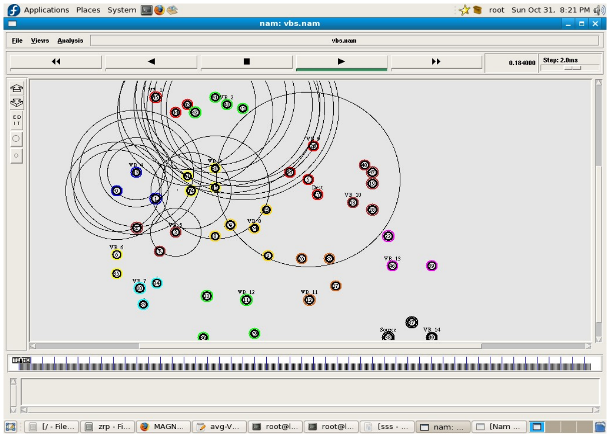
In this section, three experiments were designed to evaluate the performance of the improved clustering algorithm. The simulating program was developed by our team using NS2. In the following experiments, Most of studies only consider that wireless sensor networks are equipped with only Omni-directional antennas, which can cause high collisions. It is shown that the per node throughput in such networks is decreased with the increased number of nodes. Thus, the transmission with multiple short - range hops is preferred to reduce the interference. However, other studies show that the transmission delay increases with the increased number of hops. Found that using directional antennas not only can increase the throughput capacity but also can decrease the delay by reducing the number of hops.

Contains both merits and limitations when people use it to simulate WSNs. To the merits, firstly as a non-specific network simulator, NS-2 can support a considerable range of protocols in all layers. For example, the ad-hoc and WSN specific protocols are provided by NS-2. Secondly, the open source model saves the cost of simulation, and online documents allow the users easily to modify and improve the codes. However, this simulator has some limitations. Firstly, people who want to use this simulator need to familiar with writing scripting language and modeling technique; the Tool Command Language is somewhat difficult to understand and write. Secondly, sometimes using NS-2 is more complex and time-consuming than other simulators to model a desired job. Thirdly, NS-2 provides a poor graphical support, no Graphical User Interface (GUI) the users have to directly face to text commands of the electronic devices. Fourthly, due to the continuing changing the code base, the result may not be consistent, or contains bugs.

Parameter used in the Simulation

Parameter	Value
Simulation time	300
Number of nodes	46
Traffic model	CBR
Node Placement	Uniform
Performance parameter	Energy consumption, End to End delay
Routing protocol	AODV
No Coding	TCL
Node ID	1
Signal Strength	70%
Mobility	Clustering Head
Connection	

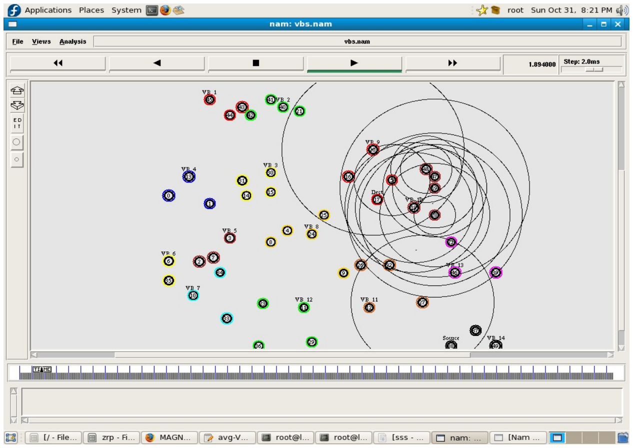
Table 5.1: Simulation Parameters



Red- Clustering; black- clustering ; black – No of Node; green- Energy, yellow- Intrusion node

Fig 5.1: Proposed Node

For the experimental results presented in this section, a network of sensors randomly distributed in a 1000m * 1000m field is considered. The number of sensors in the network, i.e. the network size, is kept at 100, 200, 300 and so on. Each sensor has an initial energy of 1.Joule and the base station is located at (250, 330). Each sensor generates packets of size 1000 bits. The energy model for the sensors is based on the first order radio model.



Red- Clustering; Blue – Neighbor node ; black – No of Node; Green- Energy

Fig 5.2:Fuzzy based Model

The manner in which tree leaders are selected in each level of the hierarchy is examined. Obviously an aggregation tree, for every round of data gathering is defined. For comparison, the MST tree to perform data gathering, with and without aggregation is implemented. In the case of no aggregation, sensors use the similar chain-based hierarchy to transmit their packets to the base station.

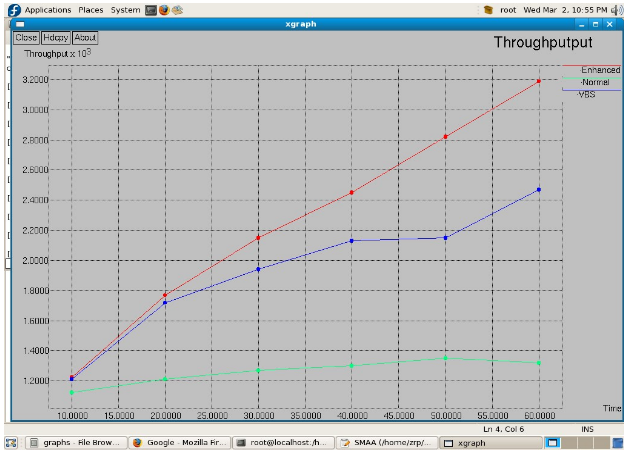


Fig 5.3: Throughput

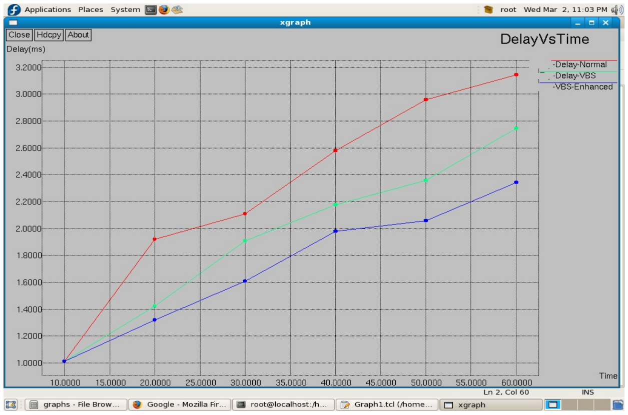


Fig 5.4 : Delay Vs Time

CONCLUSION

This research designed and developed the intrusion detection and response model for mobile ad hoc networks (IDRMAN). This model consists of the intrusion detection framework and the intrusion response framework. These two frameworks complement each other to make a complete intrusion detection based security model for MANETs. The functionality and effectiveness of this model was validated by applying this model for simulated Denial of Service attacks(DoS) in MANET.The detection framework of the IDRMAN uses CART based data mining methodology to identify the parameters that are significant for a particular attack. It then uses the six sigma methodology to set the thresholds for the significant parameters identified. The detection framework then quantifies an attack using a metric called Threat Index (TI) by applying fuzzy logic on the measured values of the significant parameters.The response framework of the IDRMAN is invoked when the detection framework identifies an attack. The response framework has an intruder identification component and an intrusion response component. The intruder identification component uses the significant parameters and their thresholds in a reputation management mechanism to identify the intruder and flag its status. The response action plan is then executed by the response framework based on the intruder status indicated by the reputation management mechanism.

FUTURE WORK:

- Focusing on DSDV and AODV as the routing protocol, and DoS attacks as the threat model, we have designed and developed IDRMAN model to the full. Further work can be performed to extend this model to other passive attacks like unauthorized access, probing, selfishness and non-repudiation attacks in mobile ad hoc networks and active routing attacks.

- Further research could also be devoted to apply the proposed model to secure the integrated wired and wireless networks like cellular networks/sensor networks.

REFERENCES:

[1] Y. Li and J. Wei., *“Guidelines on selecting intrusion detection methods in MANET*”, In Proceedings of the Information Systems Educators Conference, 2004.

[2] Bo Sun and Lawrence Osborne: *“Intrusion detection techniques in mobile ad hoc and wireless sensor network”.* In: IEEE Wireless Communications,1536-1284, 2007.

[3] R. Heady, G. Luger, A. Maccabe, and M. Servilla, *“The architecture of a network level intrusion detection system”* Technical National Conference on Emerging Trends and Applications in Computer report, Computer Science Department, University of New Mexico, August 1990.

[4] B. Shanmugam and N. B. Idris, *“Anomaly Intrusion Detection based on Fuzzy Logic and Data Mining”,* In Proceedings of the Postgraduate Annual Research Seminar, Malaysia 2006.

[5] M. Wahengbam and N. Marchang, *“Intrusion detection in manet using fuzzy logic”*, 3rd IEEE Science (NCETACS), ISBN: 978-1-4577-0749-0, pp. 189 – 192, Shillong, 30-31 March 2012.

[6] S. Sujatha, P. Vivekanandan, A. Kannan, *“Fuzzy logic controller based intrusion handling system for mobile ad hoc networks”,* Asian Journal of Information Technology, ISSN: 1682- 3915, pp.175-182, 2008.

[7] S. Ahmed & S.M. Nirkhi, *“A Fuzzy approach for forensic analysis of DDoS attack in manet”* International Conference on Computer Science and Information Technology, ISBN: 978-93-82208-70-9, Hyderabad, 10th March 2013.