Design of Detection Engine for Wormhole Attack in Adhoc Network Environment

*Husain Shahnawaz[1, 2], Joshi R.C[3,4], Gupta S.C.[4]
[1] (Research Scholar) Graphic Era University, Dehradun, (India)
[2](Lecturer) Deptt. of Electrical Engineering, King Khalid University, ABHA, (KSA)
[3] (Chancellor) Graphic Era University, Dehradun, (India)
[4] (Ex Prof. & Head) Deptt. ECE, IIT Roorkee (India)
shahnawaz.husain}@ieee.org, hotmail.com, shseen@kku.edu.sa, sureshprem1938@gmail.com

Abstract -- Adhoc network is a collection of nodes that are capable to form dynamically a temporary network without the support of any centralized fixed infrastructure. There is no central controller to determine the reliable & secure communication paths in Mobile Adhoc network. Each node in the Adhoc network has to rely on each other in order to forward packets, thus highly cooperative nodes are required to ensure that the initiated data transmission process does not fail. In a mobile Adhoc network (MANET) where security is a crucial issue and they are forced to rely on the neighbour node, trust plays an important role that could improve the number of successful data transmission. Larger the number of trusted nodes, higher successful data communication process rates could be expected. In this paper, a model is proposed for Intrusion Detection System and then Worm-Hole attack is assumed in the network, statistics are collected to design intrusion detection engine for MANET Intrusion Detection System (IDS). Important features extraction and rule inductions are applied to classify the data set. Training of data set and on the basis of confidence value generated in training is used for testing of data set and investigated the accuracy of detection engine by using support vector machine. In this paper True Positive generated by the detection engine is very high and this is a novel and statistics based approach in the area of Mobile Adhoc Intrusion detection system. Though this research is carried out for Adhoc network environment but this is also applicable to Wireless Sensor network

Keywords: Worm Hole Attack, Denial of Service Attack, Detection Engine, Intrusion Detection System, Friend Features, Trust establishment, Mobile Adhoc Network, Security in Adhoc Network, Wireless Sensor Network.

I. INTRODUCTION

Security is the critical issue in the communication system, there are three broad areas for security is identified, Intrusion prevention system, Intrusion detection system and Network forensics. These three areas are complement to each other. If a system is equipped with these areas then we can say that system is fully secure. Intrusion prevention system deals with the security mechanism (X.800). In which algorithms and devices are incorporated to provide the security. If cryptographic information is shared by the malicious user then Intrusion detection system analyzes the behaviour of the node to detect whether a node is trusted or malicious. And third area which is emerging field in security is network forensics, which is based on the concept to backtrack and identify the physical location of the intruder to punish them. If you identify the intruders attack but unable to track their location then they will attack again by changing their identity. In this research we are focused only on Intrusion detection system for the mobile Adhoc environment.

Intrusion detection is a security technology that attempts to identify individuals who are trying to break into and misuse a system without authorization and those who have legitimate access to the system but are abusing their privileges [1]. An intrusion detection system (IDS) dynamically monitors the system and user actions in the network in order to detect intruders. An information system can pursue from various kinds of security vulnerabilities, it is both technically difficult and economically costly to build and maintain a system which is not susceptible to attack. Experience has taught us never to rely on a single defensive line or technique. IDSs, by analyzing the system and user operations in search of activity undesirable and suspicious, can effectively monitor and protect against threats.

Research on IDSs began with a report by Anderson [2] followed by Denning's Seminal paper [3], which lays the foundation for most of the current intrusion detection prototypes. Since, many research efforts have been devoted to the wired intrusion detection systems. Numerous detection techniques and architecture for host machines and wired networks have been proposed. A good taxonomy of wired IDSs is presented in [4]. With the rapid proliferation of wireless networks and mobile computing applications, new vulnerabilities that do not exist in wired networks have appeared. Security poses a serious challenge in deploying wireless networks in reality. However, the vast difference between wired and wireless networks make traditional intrusion detection

techniques inapplicable. Wireless IDSs, emerging as a new research topic, aim at developing new architecture and mechanisms to protect the wireless networks.

In MANETs, intrusion prevention and intrusion detection techniques need to complement each other to guarantee a highly secure environment. They play different roles in different states of the network. Intrusion prevention measures, such as encryption and authentication, are more useful in preventing outside attacks. Once the node is compromised, intrusion prevention system will have a very little effect in protecting the network, in this situation, the role of intrusion detection is more important. When a node is compromised, the attacker owns all its cryptographic key information. Therefore, encryption and authentication cannot defend against a trusted but malicious node. Type of attacks possible in the mobile Adhoc network is given in Table 1. These attacks are limited only for MAC layer and network layer but attacks for rest layers are also possible and needs to classify.

II. RELATED WORK

Reputation based schemes detect the malicious node and notify other nodes about the misbehaving node. This scheme is based on the fundamental of punishing the nodes by blocking malicious node forever from the network. Incentive based approaches aim to promote positive behavior instead of reporting and punishing misbehaving nodes. This scheme is based on the fundamental to identify the trust level of node and promotes the node which is more trusted.

[5], [6], and [7] have developed a distributed and cooperative intrusion detection system (IDS) where individual IDS agents are placed on each and every node. Each IDS agent runs independently, detects intrusion from local traces and initiates response.

Bhargava and Agrawal [9] have extended the IDS model described in [10] to enhance the security in Adhoc on Demand Distance Vector (AODV) routing protocol. Watchdog [11], proposes to monitor packet forwarding, and has the limitation to rely on overhearing of packet transmissions for neighbouring nodes for detection of anomalies in packet forwarding. Kong J. [8], follows the concept of watchdog but works with ADOV. It adds a next hop field in AODV packets so that a node can be aware of the correct next hop of its neighbours and considered more types of attacks, such as packet modification, packet duplication, and packet jamming, DoS attacks. Bal Krishnan [12] has proposed a way to detect packet dropping in Adhoc networks. There are various research is carried out in the direction in which researcher used the trust features in existing trust based routing schemes for Adhoc network. [13], [14], [15], [7], [16] & [17] are based upon the trust based detection schemes for MANET.

Razak et Al. [13], discussed the issues regarding the intruder and security of Adhoc network, along with the discussion of the existing research works they proposed a model to secure MANET. After considering these issues, a novel but the conceptual IDS framework (a two tier IDS for MANET), is proposed to improve the performance of existing IDS in MANET environment. They proposed the model for anomaly detection and misuse detection on the basis of signature based and friendship based detection mechanism.

Abusalah et Al. [14], proposed a Trust Aware Routing Protocol (TARP) for secure trusted Adhoc routing. In TARP, security is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes. TARP, is not an intrusion detection system.

Pirzada et Al. [15], describes that dependence on a central trust authority is an impractical requirement of Adhoc network. They presented a model for trust based communication in Adhoc networks. The model introduced the notion of belief and provides a dynamic measure of reliability and trustworthiness based on direct trust mechanism in an Adhoc network. They quantized the trust for different trust groups and finally compute the trust to differentiate between malicious and trusted node.

Yan et Al. [7], used the trust evaluation based security solution for mobile Adhoc network but it is best suited for reputation based schemes.

Eschenauer et Al. [16], presented a framework for trust establishment that supports the requirements for MANETs and relies on peer to peer file sharing for evidence distribution through the network. They describe that problem of evidence distribution for trust establishment is somewhat different than the usual file sharing problem in peer to peer networks. For this reason, they proposed to use a swarm intelligence approach for the design of trust evidence distribution instead of simply relying on an ordinary peer to peer file sharing system. They also argued that the design of metrics for the evaluation of trust evidence is a crucial aspect of trust establishment in MANETs.

Though Reputation based schemes are very good in case of wired network or where there is concept of central authority or some monitoring points, but these algorithms / models are failing when we applied them to the mobile Adhoc environment. Due to issues like no central authority and self configurable network and highly dynamic topology with a high degree of mobility makes very difficult to design a perfect intrusion detection system for mobile Adhoc network. One of the main issues in MANET IDS is on the number of false alarms raised on the network as a result of false claims / reports made by individual nodes. This anonymity problem is a

big challenge in Adhoc network because it is difficult for nodes to distinguish between trusted and malicious nodes in such autonomous networks.

A Identified Rules of Thumb, to design the IDS for Adhoc Environment

The limitations of previous research are given in Table 2 on the basis of discussion on a literature review of intrusion detection system for the Adhoc environment. Now we have to discuss about the identified Rules of Thumb which will be required in preceding this research and also these rules are helpful for designing of any kind of intrusion detection system and designing the security related algorithms in the mobile Adhoc environment.

i. It should be Platform Independent & Geographical independent.
ii. No Restriction over mobility while designing and during deployment of IDS.
iii. IDS for MANET should not be routing protocol dependent.
iv. It should be Light Weighted and Fast Responsive.
v. Reduced False Alarm and high number of True Positive.
vi. No overhead while number of nodes increases (It should be easy to adapt scalability).
vii. Not only to prevent the specific kind of attacks and allows the attack which are not defined in definitions of attacks.
viii. Suitable deployment of IDS in layered Architecture.
ix. A node should not be declared permanently as an Intruder.

B Decision to Select Approach

On the basis of literature review and discussion for incentive based intrusion detection system and reputation based intrusion detection system for mobile Adhoc network. Now, we will investigate that which approach is suitable for this research and why?

a. Reputation Based Scheme

i. If false Alarms are high then network itself will be disrupted because it will punish the nodes and normal nodes which are identified wrongly as intruder will be blocked by the network.
ii. No doubt this scheme is very good for the wired IDS system but it is not suitable for mobile Adhoc network where there is no central authority to establish the network and high degree of probability to generate false alarms.
iii. Reputation based schemes blocked the node permanently if once it is declared as intrusive, and there is no next chance to confess.
iv. Most of the Reputation based schemes are reactive, means they are active only when a route request in progress or data transfer is there and it looks like a greedy approach and it is not necessary that greedy approach will provide the optimum solution. And one reason is that if node wants to send the data or establishing the route then this is not the correct time to run the detection algorithms because it will increase the overhead over the network at the crucial time.
v. Most of the Reputation based schemes are directly or indirectly using Watchdog techniques, and Watchdog is suitable where only one or two intruders are present in the network but if multiple intruders are there then this scheme has no impact on system performance.

b. Incentive Based Scheme

For the Incentive Based approaches there are a number of good reasons to adopt the scheme, few of them can be described as:

i. Incentive based schemes are best suited to Adhoc environment, where there is no central authority.
ii. They are proactive in nature, they never punish the nodes, and voting result is shared among all the nodes. It is an individual decision of nodes to involve that node whose Trust level is less, in the communication or not.
iii. If the intruder is a result of False Positive then there is a next chance for confession and to improve the Trust level.
iv. This kind of IDS schemes we can run on monitoring nodes or we can deploy them on a standalone basis, whatever requirement of the network.

The Decision to further precede the Research work is Incentive Based Approach to design the Intrusion Detection System for Mobile Adhoc Network.

The model is derived from previous research based on the incentive based approach means instead of punishing the nodes we foster the positive behavior nodes in the network. [19], [21], & [26] provided the evidences on how a friendship mechanism could be used to improve the accuracy of IDS in MANET.

III. PROPOSED MODEL

A. *Assumptions and Prerequisite*

a. Direct Friend Mechanism

Initially some assumptions are made that each node has a list of initial trust shown in the Table 3 but it is not recommended we can start an IDS system in the network from the zero knowledge about the friends, and that list is shared with other nodes present in the network. This initial trust list maintained on the basis of the profile database shown in Figure 1 and discussed in the next section. These initial lists are known as a Direct Friend Mechanism (DFM) and given in Table 3.

b. IDS Alarm Analysis

Before continuing discussion it is mandatory to discuss about the outcomes of the IDS alarm analysis. The IDS alarm analysis provides four possible results for each traffic trace analyzed by the IDS.

True Positive (TP) when the attack succeeded and the IDS was able to detect it.

$$(Success \wedge Detection)$$

True Negative (TN) when the attack failed and the IDS did not report it.

$$(\neg Success \wedge \neg Detection)$$

False Positive (FP) when the attack failed and the IDS reported on it.

$$(\neg Success \wedge Detection)$$

False Negative (FN) when the attack succeeded and the IDS was not able to detect it.

$$(Success \wedge \neg Detection)$$

True Positive and True Negative is the correct classification.

c. Accuracy of the System

Recall: The percentage of the total relevant documents in a database retrieved by search [45]. If the user knew that there were 1000 relevant documents in a database and his search retrieved 100 of these relevant documents, his recall would be 10%.

$$Recall = TP/(TP+FN); (I)$$

Precision: The percentage of relevant documents in relation to the number of documents retrieved [45]. If the search retrieves 100 documents and 20 of these are relevant, then precision is 20%.

$$Precision = TP/(TP+FP); (II)$$

And the accuracy of the IDS system is based on above mentioned parameters.

$$Accuracy\ of\ the\ System = TP+TN / TP+TN+FP+FN; (III)$$

B. *A Proposed Two Tier Architecture for IDS*

A two tier novel Architecture for IDS in MANET is proposed to improve the efficiency of existing MANET IDS architectures, model is derived from [27], [28], [29], and [51]. The main idea of the system is to provide reliable IDS that can detect any kind of intrusion attempts and at the same time can reduce the number of false alarms raised by the system. With the focus to improve the detection strategies, only a simple response mechanism is deployed in the system as a complement to the detection mechanisms. The conceptual framework of the proposed IDS architecture is as illustrated in Figure 1 and Figure 2.

Two main modules of IDS are Local IDS and Global IDS. Each module has several components and discussed in further sections. At this IDS, 20:80 rule is followed for detection (It is not compulsory to set this limitation but to increase the response rate quicker and faster from Local IDS). In this ratio rule, for Local IDS we set 20% of induction rules with high detection threshold value so that it will easily detect the highly misbehaving activity and it will generate the friend list very fast. Generated friend list is used in the Global IDS, and for Global IDS rules are applied to normal intruder detection threshold value for rigorous checking before declaring a node as the trusted node.

C. *Local IDS*

The Local IDS module is shown in Figure 1 has five major components and each component has its specific functionality to perform.

a. Data Collection Module

As in a wired network, data in MANET can be gathered from two sources: host-based and network based audit data sources. Since host based audit data source is not dependent on any network architecture, similar data collection techniques as applied in wired networks can be used in MANET. For instance, we can use a Simple Network Monitoring Protocol (SNMP) to log user activities or by using agent technology to collect available audit data. However, this does not apply to the network-based audit data source. No such concentration point or

dedicated node exists in the MANET that can be used to collect the whole network information like in the wired network. However, this does not mean that the network information cannot be collected in MANET environment. One of the most common assumptions made by researchers is that, each node in MANET is capable of hearing the transmission in and out from other nodes in the networks as long as they are within each other's radio range. Researchers claimed that by using this assumption, partial or localized network activities can be collected by each node, which later can be shared among them as a virtual network based audit data source Sergio et Al. [30].

Raw data should be processed before further processing; Data auditing included noise reduction, identifying the important features, secondary features and useless features [40]. And then data set is converted into a common format and which is depend upon the algorithm used for prediction, like neural network based algorithms, fuzzy based algorithms or data mining based algorithms.

b. Detection Engine

After finishing the first module, we applied the detection engine module on the audited data for further processing. A model of the detection engine for current research is based on the attacks applied to MAC and network layer. These two layers are the soft target for attacks in Adhoc environment. Most of the attacks identified are used to disrupt the services of these layers but we can extend the detection engine for the rest of the layer.

In this model detection engine has two main components and we will discuss them one by one.

Unfair Use of Transmission channel based detection Engine (UDE)

Unfair use of transmission channel based detection techniques operate based on the known attack scenarios and system vulnerabilities shown in Table 1. Their main disadvantage is that they are only effective in detecting known attacks.

Anomaly Based Detection Engine (ADE)

Anomaly based detection techniques are based on anomalies in packet forwarding (APF), and they play an important role in the Adhoc environment.

c. Feed-Back Table

Feedback table shows that whether a node is intruder or trusted by the detection engine. Its value is considered from both the detection engine. If value is 0 then it is a friend and if it is 1 then it is an intruder as given in Table 4.

d. Profile Data Base

Profile database will maintain the list of trusted neighbours on the basis of Feedback Table. And friend list generated by the Local IDS will send to Global IDS module for rigorous checking before declaring a node as a trusted node by the IDS.

D. Global IDS

a. Global Data Collection Module

Audited data in Local IDS are used in global data collection module, no need to recollect the data and audit it. Friend list generated by the Local IDS, audited data from Local IDS and indirect profile list of the neighbours are raw inputs in the global detection module.

b. Detection Engine

Unfair Use of Transmission channel based detection Engine (UDE)

Same as discussed in section 3.3.2, only difference is that in association rules, we set here detection threshold for intruders at normal level.

Anomaly Based Detection Engine (ADE)

Same as discussed in section 3.3.2 but the only difference is that association rules, we set here detection threshold for intruders at normal level.

c. Feed Back Table

Feedback table generated here is more precise and accurate and known as a direct friend mechanism.

d. Global Detection Engine (Voting)

The final list generated by the global detection engine module on the basis of the friend list provided by the local detection engine module is known as direct friend list. And this list will become the indirect profile to its neighbours.

Global detection engine will generate a global friend list of trusted nodes and known as indirect friend list for its neighbours. This list is purely based on the voting mechanism and result of direct friend list and indirect profile provided by neighbours.

e. Global Profile

Trusted node list which the IDS evaluated on the basis of voting mechanism based on Direct Friend lists and the Indirect Friend list is given in Table 5. This profile is used to decide the routing path and can be used for any other purpose which is confidential and needs reliability.

Designing of full fledged intrusion detection engine for Adhoc network for anomaly and misuse based detection is very difficult. But incremental approach can be used. In this research only anomaly detection is evaluated for wormhole attack. But work can be extended for known attacks using TCP segment, denial of service attack, blackhole attack and wormhole attack. Most of the definitions of attacks for Adhoc network are included in these three kinds of attacks like packet dropping, cache poisoning, selfishness, routing loop, false source route and delay in packet transmission,.

In this model friends will be reported very fast in Local IDS module and friend list generated by the Local IDS module sent to the Global IDS module for further investigation. The global detection engine will generate the friend list according to trust level, higher the trust level of the node may be used for other processes like routing, and deciding the cluster head for scalable Adhoc networks.

Though this model is based on previously discussed models but this is light weighted and fast responsive, models [17], [31] and [32] are using trust management, signature management and intrusion detection engine definition in their models.

IV. PROBLEM DEFINITION FOR WORM HOLE ATTACK IN MOBILE ADHOC NETWORK

A Wormhole attack is composed of two attackers and a Wormhole tunnel. To establish a Wormhole attack, attackers create a direct link, referred to as a Wormhole tunnel, between them [33], and [34]. The wormhole tunnel can be established by means of a wired link, a high quality wireless out of band links, or a logical link via packet encapsulation. After building a wormhole tunnel, one attacker receives and copies packets from its neighbours and forwarded them to the other colluding attacker through the wormhole tunnel this node is known as a source of the tunnel. The latter node receives these tunnelled packets and replays them into the network in its vicinity. This receiver node is known as sink of the tunnel. In a wormhole attack using a wired link or a high quality wireless out of band link, attackers are directly linked to each other, so they can communicate swiftly. However, they need special hardware to support such communication. On the other hand, a wormhole using packet encapsulation is relatively much slower. But it can be launched easily since it does not need any special hardware or special routing protocols. [31], [33], [34], [35], [36], and [37] given a mechanism to defend against the wormhole attack but most of them are analytical and theoretical based approaches, none of them are based on the statistical based approach.

A. Simulation Environment

Opnet Modeler is used for simulation; and simulation area is 1000*1000 meter we are considering this area because most of the researchers are using this and it will be easy to compare results. There are 21 MANET workstations; with random mobility of (0-20) m/s, following a random way point trajectory during simulation. This trajectory is predefined in Opnet for mobile nodes. All nodes are AODV enabled, sending the route request for destination node and in this simulation mobile node 20 is the destination node. Figure 4 shows the environment of simulation. In this scenario mobile node 6 is a source of the wormhole tunnel and mobile node 12 used as wormhole sink. To apply wormhole attack, AODV parameters for normal and malicious nodes are given in Table 6 and MANET Traffic[#] generated parameters for normal and malicious nodes are given in Table 7. Wireless attribute to create the tunnel between source and sink, parameters are given in Table 8.

Initially simulation is carried out without malicious node. Then after two malicious nodes, node 6 and node 12 created a wormhole tunnel by increasing their transmission range. Node 12 is far away from the network or may be part of another network. The performance of the system is compared with and without wormhole attack.

B. Results Comparison With & Without Wormhole Attack

From Figure 5 it is clear that wormhole source is not actively participating in the routing process but actively receiving the routing information shown in Figure 6. Figure 7 shows that no reply received by the wormhole source node from destination. It means, the values generated in Figure 5 are suspicious. Data traffic sent from the network in Figure 8 and data traffic sent by the wormhole source is near about the same. But that node was not participated in routing then how it can send data in the network. Figure 9, shows that maximum control packet received by the wormhole source is dropped.

Wormhole attack is very difficult to identify because due to wormhole sink there is no effect on the performance of the network. The objective of this research is to design the detection engine for Wormhole attack and not concentrating on performance degradation due to Wormhole attack.

C. Feature Extraction

Following features can be extracted on the basis of simulation carried out in section 4.1. For training and classification SVM^{LIGHT} [38] is used for prediction for test data set and checking the accuracy of the system. Support Vector Machine (SVM) is a supervised learning algorithm and best among the tools available [40], [46], [47], [48], [49], and [50]. SVM is used for solving a variety of learning, classification and prediction problems. SVMs are learning machine systems that use a hypothetically a space of linear functions, training is given to the training data set with a learning algorithm for optimization based theory. Feature extraction rules can be obtained from [39], [40], and [41].

The simulation carried out in section 4.1 and visualized forms are given in Figure 5 to Figure 9. Statistics generated during simulation are used to extract the useful features for identifying the wormhole attack.

i. *Ratio of Routing Traffic Received (RRTR) = (Total Routing Traffic Received by the malicious node / Total Routing Traffic Sent by complete N/W) * 100;*
ii. *Ratio of Routing Traffic Sent (RRTS) = (Routing Traffic sent by Malicious Node / Routing Traffic Received by Malicious Node) *100;*
iii. *Route Request Ratio (RRReq) = (Route Request generated by malicious node/ Route Request generated by Total Network) *100;*
iv. *MANET Traffic Ratio (MTR) = (Malicious Node MANET Traffic Sent Ratio / Malicious node MANET Traffic Received Ratio) *100;*
i. *Ratio of Packet Drop (PDR) = (Packet Drop by Malicious Node / Total Packet Drop in N/W) *100;*

D. Rule Set

After extensive simulation following rule sets are induced to Wormhole attack

If (((RRTR > 50% ^ RRTS < 10% ^ RRReq < 5%) ^ MTR > 50%) PDR >25%)

Then

{Not A Friend};

*The dictionary of the above rule set may be changed according to the need of network; threshold value may be changed according to experience and other requirement of the network.

E. Training

Raw data set generated by the simulation in section 4.2 is processed for noise reduction, and conversion of data in proper format. This processed data are again classified according to the rule sets given in section 4.4 using SVM^{LIGHT} which used the binary classification. (+1) is used for a friend and (-1) is used for malicious node. For identified features size of the training data set and kernel function applied are given in Table 9.

F. Testing

When training is completed a model file is generated for each function for different C and γ parameters. This model file is confidence value of the system and model file is used for testing the test data set to check the accuracy of the system. Test data set given in Table 10 and shows the accuracy of the model file for giving tests data set. Maximum accuracy generated for radial function in C and γ parameters subsequently 2.0, and 1.0. The model file generated for these values has the highest accuracy and this model file will be used to deploy in the intrusion detection system as a detection engine. This detection engine is based on wormhole attack only, but incremental approach can be used to deploy the detection engine for all known attacks. This approach is a novel approach in the field of detection system which is based on statistical analysis.

V. RESULTS AND VALIDATION FOR WORMHOLE ATTACK

For Wormhole attack accuracy of the system is given in Table 10. Achieved accuracy is observed more than 99% in case of radial function. Performance comparison of the proposed framework is given with other conventional models available in Table 11. The performance of the proposed detection engine is increased in comparison with the conventional models.

VI. CONCLUSION

In this Paper, a model for intrusion detection system for the mobile Adhoc network is proposed which is light weight and fast responsive in comparison to other models in Adhoc environment. Though it is very difficult to design a detection system in one shot but in this approach incremental based technique is used. Wormhole attack is applied in the Adhoc network using reactive routing protocol AODV. Evidences are collected, Features are extracted and Rule sets are generated to detect the intruder. SVM^{LIGHT} is used to train the train data set and then test data set are used to check the accuracy of system, in this we used Linear, Radial and Sigmoid function to train and generate the model file to test the data set and identifying the accuracy of the system, the higher accuracy shows the lowest false positive. When accuracy is best in the functions for different cost and gamma parameters that model file will be considered as a detection engine for IDS. Accuracy of the

system for Wormhole attack is very good in comparison with conventional models. And the performance of the system is satisfactory for Adhoc environment.

Though this research is only limited to Wormhole attack but extendable for all known attacks like Blackhole attack, Denial of Service attack. And all known attacks for Adhoc environment discussed in Table 1 are included with these three kinds of attack. Proposed model and mechanism to design detection system can be used with little modification in the sensor network environment.

REFERENCES

[1] Y. Zhang and W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (ACM MobiCom’00), Boston, MA, pp. 275-283, Aug. 2000. ISBN: 1-58113-197-6 doi: 10.1145/345910.345958
URL: http://portal.acm.org/citation.cfm?id=345958

[2] J. P. Anderson, “Computer Security Threat Monitoring and Surveillance,” Technical Report, James P. Anderson Co., Fort Washington, PA, April, 1980.
URL: http://csrc.nist.gov/publications/history/ande80.pdf

[3] 30 Denning, D.E.; , "An Intrusion-Detection Model," *Software Engineering, IEEE Transactions on* , vol.SE-13, no.2, pp. 222- 232, Feb. 1987, doi:10.1109/TSE.1987.232894URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1702202&isnumber=35884

[4] 24 H. Debar, M. Dacier, and A.Wespi, “A Revised Taxonomy for Intrusion Detection Systems,” Annales of Telecommunications, vol. 55, pp. 361-378, 01July,2000 Springer Paris ISSN- 0003-4347. doi: 10.1007/BF02994844
URL: http://www.springerlink.com/content/4xq65ng0l0801626/

[5] Otrok, H.; Debbabi, M.; Assi, C.; Bhattacharya, P.; , "A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks," Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference, pp.86, 22-29 June 2007, doi:10.1109/ICDCSW.2007.91
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4279094&isnumber=4278984

[6] Davis, J.; Hill, E.; Spradley, L.; Wright, M.; Scherer, W.; Zhang, Y.; , "Network security monitoring - intrusion detection," Systems and Information Engineering Design Symposium, 2003 IEEE , vol., no., pp. 241- 246, 24-25 April,2003,doi:10.1109/SIEDS.2003.158030URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1242425&isnumber=27841

[7] Yan, Z., Zhang, P. and Virtanen, T. "Trust Evaluation Based Security Solution in Ad Hoc Networks". In Proceedings of the 7th Nordic Workshop on Secure IT Systems, NordSec 2003, Gjovik, Norway, pp. 1-14.
URL: http://www.citmo.net/library/Trust_Evaluation_Based_Security_Solution_in_Ad_Hoc_Networks.pdf

[8] Jiejun Kong; Petros, Z.; Haiyun Luo; Songwu Lu; Lixia Zhang; , "Providing robust and ubiquitous security support for mobile ad-hoc networks," Network Protocols, 2001. Ninth International Conference on, vol., no., pp.251-260, 14 Nov. 2001, doi: 10.1109/ICNP.2001.992905
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=992905&isnumber=21404

[9] Bhargava, S.; Agrawal, D.P. , "Security enhancements in AODV protocol for wireless ad hoc networks ," Vehicular Technology Conference, 2001. VTC 2001 Fall. IEEE VTS 54th, vol.4, no., pp.2143-2147 vol.4, 2001, doi: 10.1109/VTC.2001.957123URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=957123&isnumber=20686

[10] Yongguang Zhang and Wenke Lee. 2000. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking (*MobiCom '00). ACM, New York, NY, USA, 275-283. DOI=10.1145/345910.345958.
URL: http://doi.acm.org/10.1145/345910.345958

[11] Chengqi Song, Qian Zang,”Suppressing selfish behavior in Adhoc networks with one more hop” 5th International ICST Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, 2008, ISBN:978-963-9799-26-4 , published in Lecture Notes in Mobile Networks and Applications , Computer Science, vol - 14 Issue- 2, 01 April, 2009, Springer Netherlands, pp. 178-187, doi: 10.1007/s11036-008-0145-2
URL: http://dx.doi.org/10.1007/s11036-008-0145-2

[12] Balakrishnan, K.; Jing Deng; Varshney, V.K.; , "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE , vol.4, no., pp. 2137- 2142 Vol. 4, 13-17 March, 2005, doi: 10.1109/WCNC.2005.1424848
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1424848&isnumber=30731

[13] Razak, S.A., Furnell, S., Clarke, N. Brooke, P. Mehrotra, Sharad. Zeng, Daniel, Chen, Hsinchun. Thuraisingham, Bhavani. “A Two-Tier Intrusion Detection System for Mobile Ad Hoc Networks--A Friend Approach”, Lecture Notes In Computer Science, volume 3975, pp. 590-595, 2006, Springer Berlin / Heidelberg .doi: 10.1007/11760146_62
URL: http://dx.doi.org/10.1007/11760146_62

[14] Abusalah, L.; Khokhar, A.; Guizani, M.; , "NIS01-4: Trust Aware Routing in Mobile Ad Hoc Networks," Global Telecommunications Conference, 2006. GLOBECOM '06. IEEE, vol., no., pp.1-5, Nov. 27 Dec.1, 2006, doi:10.1109/GLOCOM.2006.264;
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4150894&isnumber=4150630

[15] Pirzada, A. A and McDonald, C. “Establishing Trust in Pure Ad-Hoc Networks”. In Proceedings of the 27th Australasian Computer Science Conference (ACSC’04), Dunedin, New Zealand, vol 26, pp. 47-54, 2004.
URL: http://portal.acm.org/citation.cfm?id=979929

[16] Eschenauer, L. “On Trust Establishment in Mobile Ad-Hoc Networks,” Master’s Thesis, Department of Electrical and Computer Engineering, University of Maryland, 2002.
URL: http://drum.lib.umd.edu/bitstream/1903/6336/1/MS_2002-10.pdf

[17] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, Roshan K. Thomas, E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks, Ad Hoc Networks, Volume 7, Issue 6, August 2009, Pages 1156-1168, ISSN 1570-8705, 10.1016/j.Adhoc.2008.10.003.
URL: http://www.sciencedirect.com/science/article/pii/S1570870508001431

[18] Yi-an Huang and Wenke Lee. 2003. A cooperative intrusion detection system for ad hoc networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks* (SASN '03). ACM, New York, NY, USA, 135-147. DOI=10.1145/986858.986877
URL: http://doi.acm.org/10.1145/986858.986877

[19] Madhavi, S.; , "An Intrusion Detection System in Mobile Adhoc Networks," *International Conference on Information Security and Assurance, 2008. ISA 2008.*, vol., no., pp.7-14, 24-26 April 2008, doi: 10.1109/ISA.2008.80
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4511525&isnumber=4511515

[20] Mahmoud, M.M.E.A.; Xuemin Shen; , "FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multihop Cellular Networks," *Mobile Computing, IEEE Transactions on* , vol.11, no.5, pp.753-766, May 2012, doi: 10.1109/TMC.2011.92
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5765975&isnumber=6172599

[21] Razak, S.A.; Samian, N.; Maarof, M.A.; , "A Friend Mechanism for Mobile Ad Hoc Networks," *Fourth International Conference on Information Assurance and Security, 2008. ISIAS '08*, pp.243-248, 8-10 Sept. 2008, doi: 10.1109/IAS.2008.27
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4627093&isnumber=4627043

[22] Yi Ping, Zou Futai, Jiang Xinghao, Li Jianhua, Multi-agent cooperative intrusion response in mobile Adhoc networks, Journal of Systems Engineering and Electronics, Volume 18, Issue 4, December 2007, Pages 785-794, ISSN 1004-4132, 10.1016/S1004-4132(08)60021-3.
URL: http://www.sciencedirect.com/science/article/pii/S1004413208600213

[23] Nikos Komninos, Dimitris Vergados, Christos Douligeris, Detecting unauthorized and compromised nodes in mobile ad hoc networks, Ad Hoc Networks, Volume 5, Issue 3, April 2007, Pages 289-298, ISSN 1570-8705, 10.1016/j.Adhoc.2005.11.005.
URL: http://www.sciencedirect.com/science/article/pii/S1570870505001113

[24] Chandrasekar Ramachandran, Sudip Misra, Mohammad S. Obaidat, FORK: A novel two-pronged strategy for an agent-based intrusion detection scheme in ad-hoc networks, Computer Communications, Volume 31, Issue 16, 25 October 2008, Pages 3855-3869, ISSN 0140-3664, 10.1016/j.comcom.2008.04.012.
URL: http://www.sciencedirect.com/science/article/pii/S0140366408002314

[25] Jochen Mundinger, Jean-Yves Le Boudec, Analysis of a reputation system for Mobile Ad-Hoc Networks with liars, Performance Evaluation, Volume 65, Issues 3-4, March 2008, Pages 212-226, ISSN 0166-5316, 10.1016/j.peva.2007.05.004.
URL: http://www.sciencedirect.com/science/article/pii/S016653160700048X

[26] S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke, Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks, Ad Hoc Networks, Volume 6, Issue 7, September 2008, Pages 1151-1167, ISSN 1570-8705, 10.1016/j.Adhoc.2007.11.004.
URL: http://www.sciencedirect.com/science/article/pii/S1570870507001618

[27] Shahnawaz, Husain; Gupta, S. C.; Mukesh, Chand; , "Denial of Service attack in AODV & friend features extraction to design detection engine for intrusion detection system in Mobile Adhoc Network," *Computer and Communication Technology (ICCCT), 2011 2nd International Conference on* , vol., no., pp.292-297, 15-17 Sept. 2011, doi: 10.1109/ICCCT.2011.6075162
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6075162&isnumber=6075092

[28] Husain Shahnawaz, Gupta S.C., "Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network", Published in International Journal of Computer Science & Information Technology, ISSN 0975-9646, Vol (2) Issue 4, 2011, pp 1569-1573
URL:http://www.ijcsit.com/docs/Volume%202/vol2issue4/ijcsit2011020440.pdf

[29] Husain, S.; Gupta, S.C.; Chand, M.; Mandoria, H.L.; , "A proposed model for Intrusion Detection System for mobile Adhoc network," *Computer and Communication Technology (ICCCT), 2010 International Conference on* , vol., no., pp. 99-102, 17-19 Sept. 2010, doi: 10.1109/ICCCT.2010.5640420
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5640420&isnumber=5640373

[30] Sergio M., T. J. Giuli, Kevin L., and Mary B. (2000) *Mitigating routing misbehaviour in mobile ad hoc networks*, Sixth annual international conference on Mobile computing and networking, pp255-265.
URL: http://www.hpl.hp.com/personal/Mary_Baker/publications/mitigating.pdf

[31] Sanjay Madria, Jian Yin, SeRWA: A secure routing protocol against Wormhole attacks in sensor networks, Ad Hoc Networks, Volume 7, Issue 6, August 2009, Pages 1051-1063, ISSN 1570-8705, 10.1016/j.Adhoc.2008.09.005.
URL: http://www.sciencedirect.com/science/article/pii/S1570870508001297

[32] S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke, Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks, Ad Hoc Networks, Volume 6, Issue 7, September 2008, Pages 1151-1167, ISSN 1570-8705, 10.1016/j.Adhoc.2007.11.004.
URL: http://www.sciencedirect.com/science/article/pii/S1570870507001618

[33] Lijun Qian, Ning Song, Xiangfang Li, Detection of Wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach, Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 308-330, ISSN 1084-8045, 10.1016/j.jnca.2005.07.003.
URL: http://www.sciencedirect.com/science/article/pii/S1084804505000342

[34] Issa Khalil, Saurabh Bagchi, Ness B. Shroff, MobiWorp: Mitigation of the Wormhole attack in mobile multihop wireless networks, Ad Hoc Networks, Volume 6, Issue 3, May 2008, Pages 344-362, ISSN 1570-8705, 10.1016/j.Adhoc.2007.02.001.
URL: http://www.sciencedirect.com/science/article/pii/S1570870507000194

[35] Lijun Qian, Ning Song, Xiangfang Li, Detection of Wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach, Journal of Network and Computer Applications, Volume 30, Issue 1, January 2007, Pages 308-330, ISSN 1084-8045, 10.1016/j.jnca.2005.07.003. URL: http://www.sciencedirect.com/science/article/pii/S1084804505000342

[36] Ming-Yang Su, WARP: A Wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks, Computers & Security, Volume 29, Issue 2, March 2010, Pages 208-224, ISSN 0167-4048, 10.1016/j.cose.2009.09.005.
URL: http://www.sciencedirect.com/science/article/pii/S0167404809001072

[37] Radu Stoleru, Haijie Wu, Harsha Chenji, Secure neighbor discovery and Wormhole localization in mobile ad hoc networks, Ad Hoc Networks, Available online 28 March 2012, ISSN 1570-8705, 10.1016/j.Adhoc.2012.03.004.
URL: http://www.sciencedirect.com/science/article/pii/S1570870512000443

[38] Joachim's. Thorsten; "SVM LIGHT: Support Vector Machine", URL: http://svmlight.joachims.org/

[39] Hofmann, A.; Horeis, T.; Sick, B.;, "Feature selection for intrusion detection: an evolutionary wrapper approach," Neural Networks, 2004. Proceedings. 2004 IEEE International Joint Conference on, vol.2, no., pp. 1563 - 1568 vol.2, 25-29 July 2004, doi:

10.1109/IJCNN.2004.1380189
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1380189&isnumber=30097

[40] Andrew H. Sung, Srinivas Mukkamala, "Feature Selection for Intrusion Detection using Neural Networks and Support Vector Machines", Transport Research Record published by TRB Journal 2003,Issue number 1822, ISSN: 0361-1981, pp 33-39.
URL: http://dx.doi.org/10.3141/1822-05

[41] R. P. Lippmann and R. K. Cunningham. "Improving intrusion detection performance using keyword selection and neural networks: Computer Networks, The International Journal of Computer and Telecommunications Networking vol. 34, no. 4, pp. 597403, 2000. Elsevier North-Holland, Inc. New York, NY, USA, doi : 10.1016/S1389-1286(00)00140-7
URL: http://portal.acm.org/citation.cfm?id=361122

[42] Zhibin Zhao; Bo Wei; Xiaomei Dong; Lan Yao; Fuxiang Gao; , "Detecting Wormhole Attacks in Wireless Sensor Networks with Statistical Analysis," Information Engineering (ICIE), 2010 WASE International Conference on , vol.1, no., pp.251-254, 14-15 Aug. 2010, doi: 10.1109/ICIE.2010.66
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber=5571080andisnumber=5570817

[43] Nait-Abdesselam, F.; , "Detecting and avoiding Wormhole attacks in wireless ad hoc networks," Communications Magazine, IEEE , vol.46, no.4, pp.127-133, April 2008, doi: 10.1109/MCOM.2008.4481351
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber=4481351andisnumber=4481327

[44] Hon Sun Chiu; King-Shan Lui; , "DelPHI: Wormhole detection mechanism for ad hoc wireless networks," Wireless Pervasive Computing, 2006 1st International Symposium on , vol., no., pp. 6 pp., 16-18 Jan. 2006, doi: 10.1109/ISWPC.2006.1613586
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber=1613586andisnumber=33870

[45] Vapnik, V.N., "*The Nature of Statistical Learning Theory*", 1st ed., Springer-Verlag, New York, 1995, series: Information Science and Statistics, ISBN: 978-0-387-98780-4.

[46] Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, Intrusion detection using an ensemble of intelligent paradigms, Journal of Network and Computer Applications, Volume 28, Issue 2, April 2005, Pages 167-182, ISSN 1084-8045, 10.1016/j.jnca.2004.01.003.
URL:http://www.sciencedirect.com/science/article/pii/S1084804504000049

[47] L.V. Ganyun, Cheng Haozhong, Zhai Haibao, Dong Lixin, Fault diagnosis of power transformer based on multi-layer SVM classifier, Electric Power Systems Research, Volume 74, Issue 1, April 2005, Pages 1-7, ISSN 0378-7796, 10.1016/j.epsr.2004.07.008.
URL: http://www.sciencedirect.com/science/article/pii/S0378779604001944

[48] Emre Çomak, Ahmet Arslan, İbrahim Türkoğlu, A decision support system based on support vector machines for diagnosis of the heart valve diseases, Computers in Biology and Medicine, Volume 37, Issue 1, January 2007, Pages 21-27, ISSN 0010-4825, 10.1016/j.compbiomed.2005.11.002.
URL: http://www.sciencedirect.com/science/article/pii/S0010482505001484

[49] Shang-Ming Zhou; Gan, J.Q.; , "Constructing L2-SVM-Based Fuzzy Classifiers in High-Dimensional Space With Automatic Model Selection and Fuzzy Rule Ranking," *Fuzzy Systems, IEEE Transactions on* , vol.15, no.3, pp.398-409, June 2007, doi: 10.1109/TFUZZ.2006.882464
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber=4231867andisnumber=4231848

[50] Jung-Hsien Chiang; Pei-Yi Hao; , "Support vector learning mechanism for fuzzy rule-based modeling: a new approach," *Fuzzy Systems, IEEE Transactions on* , vol.12, no.1, pp. 1- 12, Feb. 2004, doi: 10.1109/TFUZZ.2003.817839
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=andarnumber=1266382andisnumber=28327

[51] Husain S.; Gupta, S.C.; , "Black Hole Attack in AODV & Friend Features Extraction to Design Detection Engine for Intrusion Detection System in Mobile Adhoc Network**",** published in Journal of Engineering Science and Technology (JESTEC) Vol 7 issue 5, October 2012; ISSN : 1823-4690, pp 591-601.
URL: http://jestec.taylors.edu.my/V7Issue5.htm

TABLE I

List of UTC & APF

1. Unfair use of the transmission channel (UTC)(Applied on the MAC Layer)	2. Anomalies in Packet Forwarding (APF) (Applied on the Network Layer)
• Ignoring the MAC protocol • Jamming the transmission channel with garbage • Ignoring the bandwidth reservation scheme • Malicious flooding • Network Partition • Sleep Derivation	• Drop packets • Blackhole Attack • Gray hole Attack • Delay packet transmissions • Wormhole Attack • Packet dropping • Routing Loop • Denial of Service (DoS) • Fabricated route messages • False Source Route • Cache Poisonings • Selfishness • Spoofing

TABLE II

Breif discription about the work done by previous researchers and limitations of their work

S.No.	Author	Model/Algorithm Based on	Limitation of Algorithms/Models
1.	Zhang et al. [1]	Incentive Based	Limited only for Misuse Detection
2.	Huang et. Al [18]	Incentive Based	Rules are very brief only Packet Drop is consider
3.	Bhargava and Agrawal [9]	Incentive Based	Generalized and Protocol Dependent
4.	Balkrishnan [12]	Incentive Based	Protocol Dependent
5.	Razak et Al.[13]	Incentive Based	Conceptual Model, no statistics
6.	Abusalah et. Al [14]	Incentive Based	Not IDS only Reliable Routing
7.	Pirzada et. Al [15]	Incentive Based	Protocol dependent
8.	Eschenauer et. Al [16]	Incentive Based	Conceptual Frame work without statistics
9.	Razak et. Al [21]	Incentive Based	Validating previous model and Friendship based approach
10.	Mahmoud et. Al [20]	Incentive Based	Multihop cellular system based model not tested for Adhoc environment
11.	Razak et. Al [26]	Incentive Based	Tested previous model only for blackmail attacks
12.	Ping Y. et. Al [22]	Incentive Based	Geographical and Architecture dependent
13.	Komninos N. [23]	Incentive Based	Concept of Key Management but no Intrusion Prevention Mechanism is described
14.	Ramachandran, C. et Al. [24]	Incentive Based	Auction to monitoring node, it means Architecture dependent, no auction controlling mechanism if intruder Participate in the auctions and if it win the auction
15.	Song et. Al [11]	Reputation Based	Encrypted Packet Transfer
16.	Yan et. Al [7]	Reputation Based	Routing Protocol dependent
17.	Mundinger J. et. Al [25]	Reputation Based	Analytical approach not sufficient to describe all attacks
18.	Haiyun Luo et Al. [8]	Reputation Based	Based on Central Authority
19.	Madhavi et. Al [19]	Reputation Based	Based on Central Authority
20.	H. Otrok et Al. [5]	Reputation Based	Increases the detection rate but limitation is central authority.

TABLE III

Node's initial trust (DFM)

Node ID	Initial Trust
A	B & C
B	C,D,E
C	A,D,B
D	C,B
E	A,C

TABLE IV

Feedback table (FBT)

UDE	**ADE**	**UDE ^ ADE**
0	0	0
0	1	1
1	0	1
1	1	1

TABLE V

Trust level generated by global detection engine

Node Id	Trust Level
A	2/5
B	3/5
C	4/5
D	2/5
E	1/5

TABLE VI

AODV parameters for malicious and normal node

Parameters	**Value (Normal Node)**	**Value Malicious Node)**
Route Discovery Parameters	Default	Custom Level
Route Request Retries	5	100
Route Request Rate Limit (Packets/Sec)	10	1000
Gratuitous Route Reply Flag	Enabled	Enabled
Destination only Flag	Enabled	Enabled
Acknowledgement Required	Enabled	Enabled
Active Route Timeout	3	3
Hello Interval	Uniform (1,1.1)	Uniform (1,1.1)
Net Diameter	35	**1**
Timeout Buffer	2	2
TTL	Default	Default
Packet Queue Size (packets)	Infinity	Infinity

TABLE VII

MANET traffic generation parameters

Parameters	**Value (Normal Node)**	**Value (Malicious Node) Wormhole Source**
Start Time	10	10
Packet Inter Arrival Time	Exponential(1)	Exponential(1)
Packet Size	Exponential(1024) bits	Exponential(1024) bits
Destination IP Address	Mobile Node 20 (192.168.3.20)	Mobile Node 12 (192.168.3.12)

TABLE VIII

Wireless attribute

Parameters	Normal Node	Malicious Node
Transmit Power	0.005	0.100
Packet Reception-Power Thresh hold	-95	-95

TABLE IX

Training data set

Input Features	Train Data Set	Function	Parameters (C,γ)	CPU Run Time (in Sec)	Mis-Classified	Support Vector
5	3590	Linear	DEFAULT	0.54	44	347
5	3590	Linear	0.5,0.5	6.51	42	274
5	3590	Linear	1.0,0.5	22.36	42	274
5	3590	Linear	1.0,1.0	10.69	42	274
5	3590	Linear	2.0,1.0	12.52	42	274
5	3590	Radial	DEFAULT	4.15	10	1479
5	3590	Radial	0.5,0.5	2.45	13	1001
5	3590	Radial	1.0,0.5	2.73	10	953
5	3590	Radial	1.0,1.0	4.55	9	1392
5	3590	Radial	2.0,1.0	4.65	6	1379
5	3590	Sigmoid	DEFAULT	1.22	937	1874
5	3590	Sigmoid	0.5,0.5	1.19	937	1874
5	3590	Sigmoid	1.0,0.5	1.14	937	1874
5	3590	Sigmoid	1.0,1.0	1.20	937	1874
5	3590	Sigmoid	2.0,1.0	1.23	937	1874

TABLE X
Test data set

Input Features	Test Data Set	Function	Correct	Incorrect	Accuracy	Precision/Recall
5	1344	Linear	1329	15	98.88%	97.69%/98.45%
5	1344	Linear	1331	13	99.03%	98.19%/98.45%
5	1344	Linear	1331	13	99.03%	98.19%/98.45%
5	1344	Linear	1331	13	99.03%	98.19%/98.45%
5	1344	Linear	1331	13	99.03%	98.19%/98.45%
5	1344	Radial	1341	3	99.78%	99.74%/99.48%
5	1344	Radial	1340	4	99.70%	99.48%/99.48%
5	1344	Radial	1341	3	99.78%	99.74%/99.48%
5	1344	Radial	1342	2	99.85%	99.74%/99.74%
5	1344	Radial	1343	1	99.93%	100%/99.74%
5	1344	Sigmoid	958	386	71.28%	71.28%/88.26%
5	1344	Sigmoid	958	386	71.28%	71.28%/88.26%
5	1344	Sigmoid	958	386	71.28%	71.28%/88.26%
5	1344	Sigmoid	958	386	71.28%	71.28%/88.26%
5	1344	Sigmoid	958	386	71.28%	71.28%/88.26%

TABLE XI

Result comparison with previous models for worm-hole attack

S.No.	Model	Accuracy
1.	DelPHI (Hon Sun Chiu et. Al) [44]	89%
2.	Farid Naït-Abdesselam et.Al.[43]	92%
3.	Regular Distribution (Zhibin Zhao et. Al) [42]	94%
4.	Stochastic Distribution (Zhibin Zhao et. Al) [42]	84%
5.	***Proposed Model***	99.93%

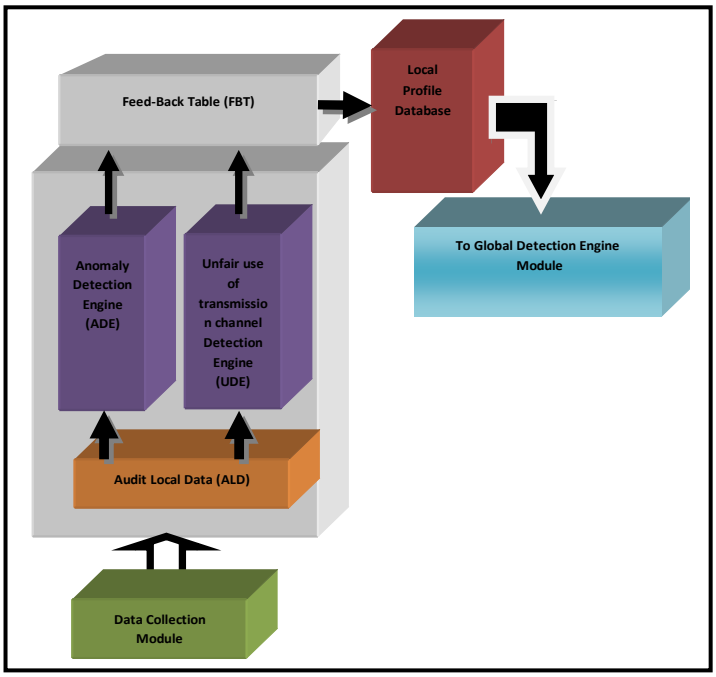

Figure 1: Local detection engine module [29]

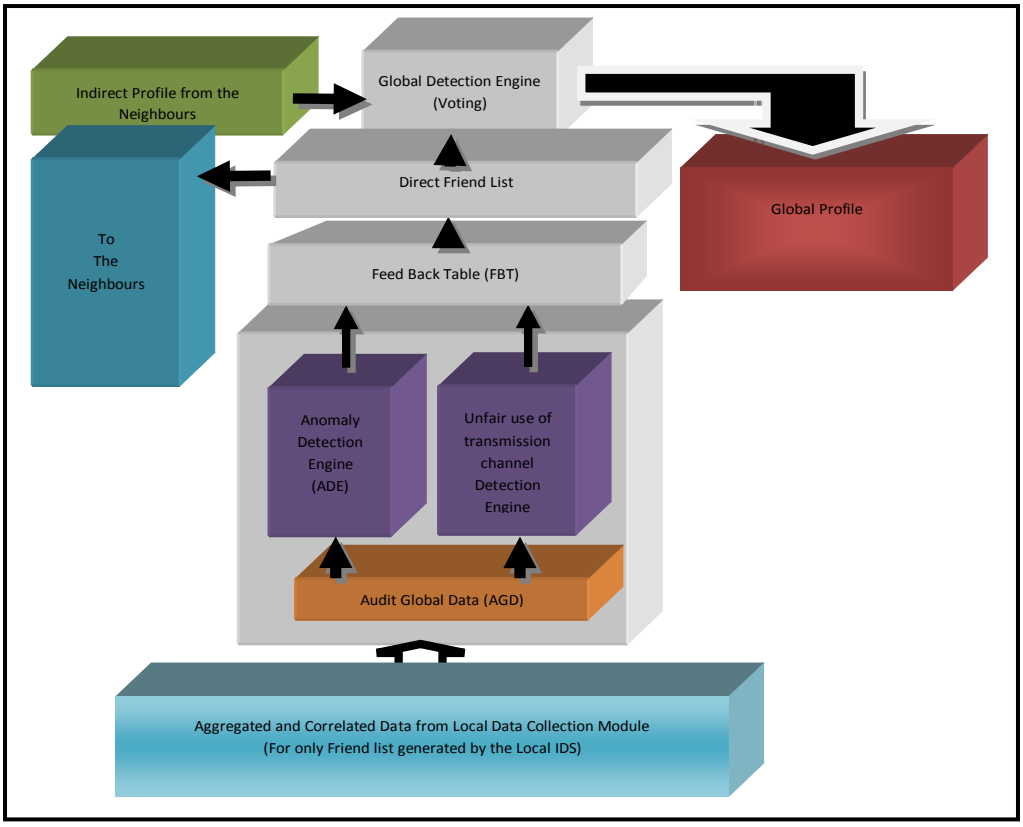

Figure 2: Global detection engine module

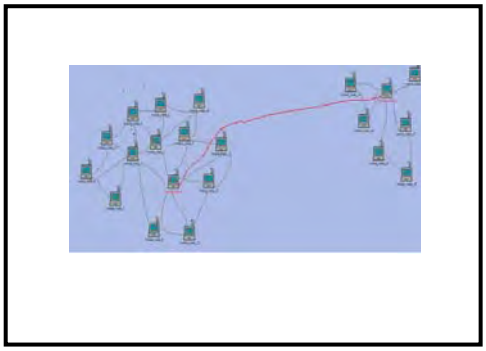

Figure 3: Wormhole attack

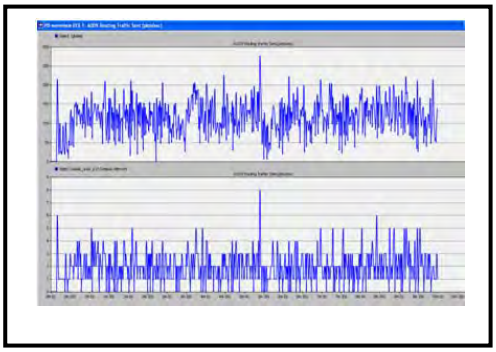

Figure 5: Routing traffic send (Global network vs. Malicious node (Source of wormhole tunnel))

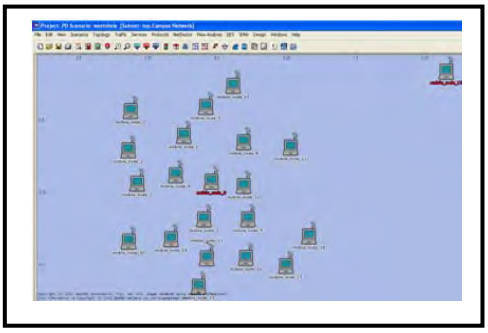

Figure 4: Simulation environment

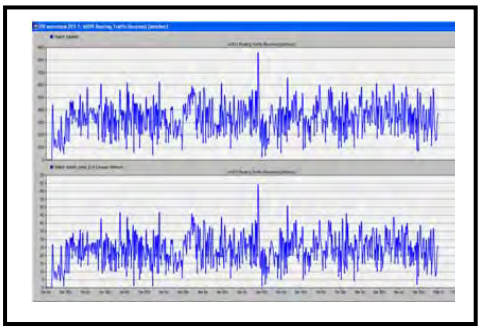

Figure 6: Routing Traffic Received (Global network vs. Malicious node)

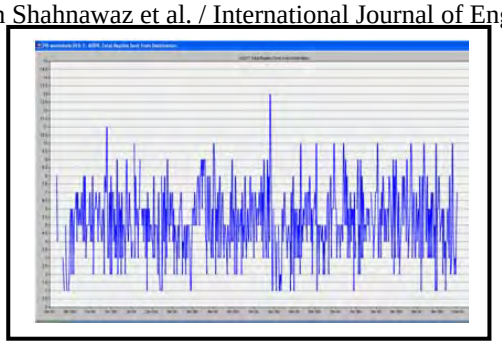

Figure 7: Total reply sent from destination but malicious node has no reply from destination
(Result not generated for source node)

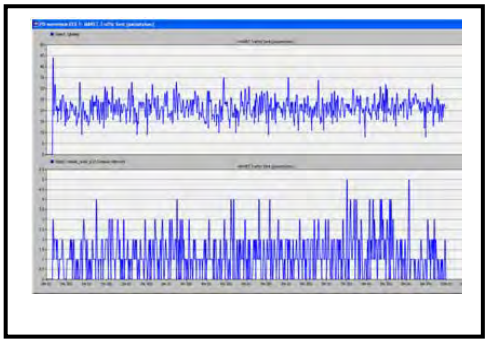

Figure 8: Total MANET traffic sent (Global network vs Malicious node (source of wormhole tunnel))

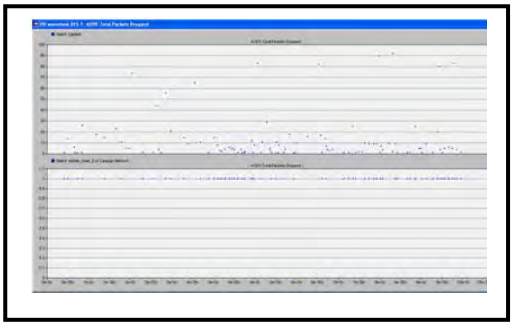

Figure 9: Packet drop Global network vs Malicious node (source of wormhole tunnel))