A Multiplayer Cooperative Game Approach For Detecting Misbehaving Nodes In Intrusion Detection System

Dr.R.Saminathan[1], Dr.P.Anbalagan[2], R.Suganya [3]
[1, 2, 3] Department of Computer Science and Engineering
[1, 2, 3] Annamalai University, Annamalai Nagar

Abstract- *A mobile ad hoc network (MANET) is a self-organized collection of mobile nodes which communicate with each other without the help of any fixed infrastructure or central coordinator. Intrusion Detection Systems (IDS) are used in MANETs to monitor activities so as to detect any intrusion in the attack vulnerable network. Usually, an IDS has to run all the time on every node to oversee the network behavior. A probabilistic model is proposed that makes use of cooperation between IDSs among neighborhood nodes to reduce their individual active time. Hence, proposed work reduces the duration of active time of the IDSs without compromising on their effectiveness. To validate proposed approach, the interactions between IDSs are modeled as a multi-player cooperative game in which the players have partially cooperative and partially conflicting goals. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighborhood at a desired security level so as to detect any anomalous behavior, whereas, the secondary goal of the IDSs is to conserve as much energy as possible. To achieve these goals, each of the nodes has to participate cooperatively in monitoring its neighbor nodes with a minimum probability.*

Keywords- Ad hoc networks, intrusion detection, energy efficiency.

I. INTRODUCTION

A wireless sensor network is a collection of nodes organized into a cooperative network. Each node consists of processing capability (one or more micro controllers, CPU or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transreceiver usually with a single omnidirectional antenna, have a power source, and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Wireless networking is the platform for working with the current technology widely used in several applications. MANET(Mobile Ad hoc Network) is a collection of wireless mobile node consists of both wireless transmitters and receivers which dynamically forming a temporary network and communication between transmitter and receiver by using bi-directional link. Either directly, if nodes in MANET are within communication range or indirectly means transmitter node rely on intermediate node, for forwarding data to destination node. Various features of MANET overcomes the problem in contemporary application of wireless network such as dynamic topology and decentralized network feature of MANET, means all the nodes are free to move randomly. The self-configuring ability of nodes in MANET, minimal configuration and quick development makes MANET ready to be used in emergency condition where an infrastructure is unavailable or difficult to install network in scenarios like natural disasters and military conflicts. Due to these various unique characteristics MANET is becoming popular among all other wireless application as well as widely implemented in industry. Network security has vital importance in every wireless network technology. But open medium and remote distribution of nodes make MANET vulnerable to various types of attacks. So it is necessary to develop an efficient secure Intrusion Detection System (IDS) to protect MANET from various attacks. IDS is one of the Research field in MANET. Mostly researchers are focusing on developing a new detection, prevention and response mechanisms for MANET.

- To optimize the active time duration of IDSs in a MANET.
- To reduce the IDS active time as much as possible without compromising on its effectiveness.
- To reduce the computational cost and to save energy.

Intrusion is any set of actions that attempt to comprise the integrity, confidentiality or availability and an IDS is a device or software application that monitors network traffic and if any suspicious activity found then it alerts the system or network administrator. There are three main modules of IDS such as Monitoring, Analyses and Response. The Monitoring Module is responsible for controlling the collection of data. Analyses Module is responsible for deciding whether the collected data indicated as an intrusion or not. Response Module is responsible for managing and using the response actions to the intrusion. Due to the limitations of most MANET routing protocols, nodes in MANETs assume that other nodes always cooperate with each other to relay data. This assumption leaves the attackers with the opportunities to achieve significant impact on the network with just one or two compromised nodes. To overcome this problem, IDS should be added to enhance the security level of MANETs. If MANET knows how to the detect the attackers as soon as they enters in the network, it will able to completely remove the potential damages caused by compromised nodes at the first time. IDS usually acts as the second layer in MANETs. It is a great complement to exiting proactive approaches. So intrusion detection system is a very important aspect of defending the cyber infrastructure from attackers.

Hence, the main contribution of this article is detecting misbehaving nodes in intrusion detection system. The rest of the paper organized as follows. Section II gives an overview of related works. Section III describes the System overview. Section IV describes the modules of my paper. Section V discusses about Results and discussion**.**

II. RELATED WORKS

In this section the paper are related to MANET. We discuss the aspects related to detecting misbehaving nodes in intrusion detection system

N. Marchang, et al..,[1], have described about the Light-Weight Trust-based Routing Protocol for Mobile Ad Hoc Networks. MANETs were originally designed for a cooperative environment. Most of the MANETs secure routing protocols. To use them in hostile environments, trust-based routing can be used, where instead of establishing the shortest routes as done in traditional routing protocols, most trusted routes are established. In the proposed system is a light-weight trust-based routing protocol [3]. The proposed trust estimation technique, which is executed by every node in the network independently uses only local information thereby making it scalable. Every node in the network independently executes a trust model to estimate the trust it has on other nodes in network. This estimated trust value is used during routing decisions. Trust-based routing protocols attempt to establish most trusted routes rather than shortest routes as is done in traditional routing protocols. The light-weight IDS takes care of two kinds of attacks, namely, the blackhole attack and the grey hole attack. Whereas proposed approach can be incorporated in any routing protocol, used AODV as the base routing protocol to evaluate proposed approach and give a performance analysis. Most of the Mobile ad hoc networks (MANETs) secure routing protocols in the literature use cryptographic techniques to secure the routing protocol. However, the downside of using cryptographic tools is that they are known to be computationally very expensive, which does not lend well to incorporating them in resource-constrained mobile devices. Hence, in the attempt to prevent some attacks, these protocols create new avenues for Dos (Denial of Service) attacks. Besides, several such secure routing protocols presume the existence of a centralized or distributed trusted third party in the network.

Seyhun Mehmet Futaci, et al.., describe about On Modeling Energy-Security Trade-Offs for Distributed Monitoring in Wireless Ad hoc Networks [2] The proposed system is a distributed solution based on a game theoretic decides to monitor or not independently, aiming to maximize a utility function which represents a balance between the gains obtained by monitoring and the energy costs involved.Since the results of the monitoring are shared with the entire neighborhood, an important issue of selfishness arises, yielding a problem similar with the classic tragedy of the commons scenario. It is energy efficient distributed monitoring protocol based on a non-cooperative game framework.It achieves the security level.It improves the network lifetime.

Y. Liu,et al.., have described about the Modeling Misbehavior in Ad hoc Networks: A Game Theoretic Approach for Intrusion Detection In wireless ad hoc networks, although defense strategies such as IDSs can be deployed at individual nodes, significant constraints are imposed in terms of the energy expenditure of such systems[10]. The proposed system is a game theoretic framework to analyze the interactions between pairs of attacking/defending nodes, in both static and dynamic contexts, and considering both complete and incomplete information regarding the maliciousness of neighboring nodes. The static case analysis provides the defender with an overview of the security situation in terms of risk and monitoring cost. A dynamic Bayesian game formulation allows the defender to adjust his belief about his opponent based on his observations and the game history, and consequently to influence the achievable Nash equilibrium for new stage game. A new Bayesian hybrid detection system is proposed for the defender, which balances energy costs and monitoring gains. Wireless ad hoc networks bring a new perspective to wireless communications, but also raise important concerns in the context of network security. Ad hoc network misbehavior may be inflicted by malicious nodes, each of which intentionally aims at harming the network operation. To improve monitoring efficiency, we seek monitoring strategies that maximize the utility of a defending node, which is comprised of both security values and energy resources. To determine efficient monitoring strategies for a defending node, we model attacker/defender system as a game.

Sergio Marti, et al.., have described about the Mitigating Routing Misbehavior in Mobile Ad hoc Networks. The analyzing the two possible extensions of DSR routing protocol to mitigate the effects of routing misbehavior in ad hoc networks the watchdog and the path rater. It describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, propose categorizing nodes based upon their dynamically measured behavior[16]. A watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes. Through simulation evaluate watchdog and path rater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput in the presence of misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocols. Watchdog detects misbehavior at the forwarding level. It increases the throughput. There is still a drawback, it is impracticable to approve and confirm the number of packets with the destination node if the actual misbehaving node exists in all active paths from source to destination. Watchdog is might not detect a misbehaving node in the presence of receiver collision, ambiguous collision, false misbehavior reporting, limited transmission power, partial dropping and collusion.

III. SYSTEM OVERVIEW

In this section discuss about the probabilistic model which make use of cooperation between IDS among neighbourhood nodes to reduce their individual active time.

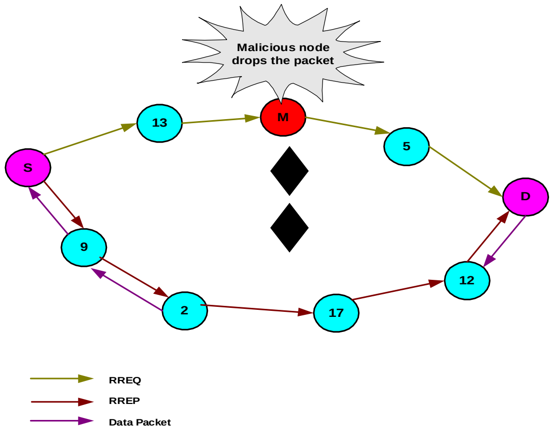


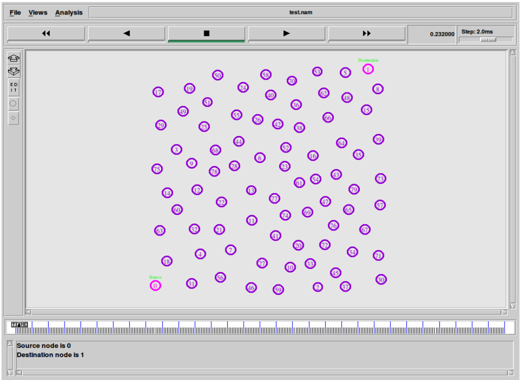
Figure 1. GreyHole Attack Model Creation

The route discovery process between source (S) and destination (D) under the gray hole attack model creation is illustrated in Fig.1. The source broadcasts a RREQ(Route Request) message with unique identifier to all its one hop neighbors. Each receiver rebroadcasts this message to its one hop neighbors until reaches the destination. The destination on receiving the message,updates the sequence number of the source and sends a RREP(Route Reply) message back to its neighbor which relayed the RREQ.

IV. MODULES

1. Packet Dropping Attack

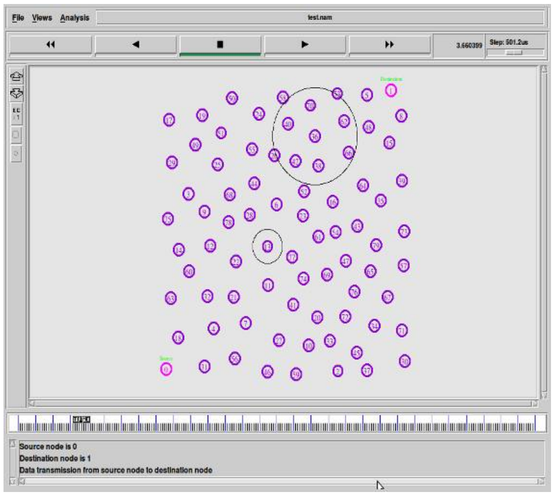
In GreyHole attack, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network [14]. It then selectively discards/forwards the data packets when packets go through it. Fig.4.2 shows the packet dropping attack. Data Dropping is a type of attack in which node does not forward the information it is supposed to forward.



Source node is 0
Destination node is 1

Figure 2. Network Environment

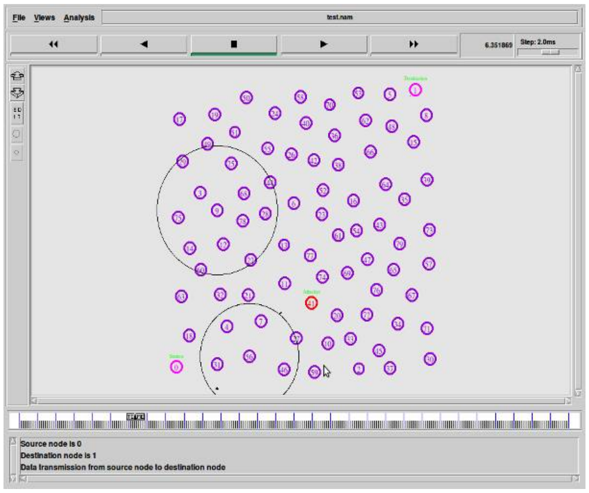
Fig.2 shows the architecture of network with random number of mobile nodes which are blue in color. The node 0 which is rose in color represents the source node from where the packets are transmitted to the destination node 1 through the intermediate nodes.



Source node is 0
Destination node is 1
Data transmission from source node to destination node

Figure 3. Data Transmission

Fig.3 shows the data transferred from source node 0 to destination node 1 through the intermediate nodes. 0 - 31 - 7 - 41 - 69 - 61 - 64 - 48 -1



Source node is 0
Destination node is 1
Data transmission from source node to destination node

Figure 4. Grey Hole Attack Creation

Fig.5 shows GreyHole attack, where the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it.

2. Probability Calculation Using LDK Algorithm

Every node employs this scheme to determine the ideal probability with which its IDS has to remain active so that all nodes in the network are monitored with the desired security level[15]. Let pi min be the optimal (minimum) probability with which node i has to monitor so that its neighbors are monitored with the desired security level. LDK refer to pi min as the minimum monitoring probability of node i. LDK define the degree of a node to be the number of its neighbors at any instant of time. Let mi denote the minimum degree of the neighbors of node i. Assign mi to k neighbors in the optimization problem of equation two to obtain the following optimization problem whose solution is pimin.To define an optimization problem as follows

Minimize p

$$\text{Subject to} \sum_{j=1}^{m_i} \binom{m_i}{j} p^j (1-p)^{m}_{i-j} \geq T$$

where, T + ∊ = 1 and ∊ is a very small positive number. The term T denotes a threshold value, which is the minimum probability with which the desired security level (l) is maintained, albeit for the whole network. The mechanism employed by each node in the network to determine the minimum monitoring probability is best presented by the simple algorithm, called LDK, which stands for Least Degree for k. Each node (say M) initiates this algorithm to determine the probability with which it has to monitor its neighbourhood.

In step 1, M broadcasts the message Send-Degree. This message is limited to only one hop.

In step 2, the neighbors of M reply back with their respective degrees.

In step 3, the least of these degrees is assigned to k in the formula, and the minimum monitoring probability of M (pm min) is calculated.

In step 2 of LDK, a malicious neighbor may send a false degree information to M and try to disrupt the algorithm. However, LDK is resilient to such an attack under the following assumption. Assume that a malicious neighbor of M would like pm min to be as less as possible so that the chance of M being detected is reduced. It cannot change its security level and thus to be monitored with a low monitoring probability. It can only send a high degree to M in step 2. Since the minimum degree of the neighbors is chosen by M in step 3 to determine the value of pm min , the high degree sent by M the (malicious neighbor) will not most likely be chosen. Even if several malicious neighbors collude and report an inflated high degree, if there is at least one honest neighbor which reports correctly, the honest neighbor's degree will be chosen as the minimum degree and pm min will be correctly calculated. In this context it is safe enough to assume that at least one neighbor is honest.

Probability Calculation using LDK Algorithm

Probability = 1 / neighbor count

```
Probability of Node 72 =0.066667
Probability of Node 45 =0.090909
Probability of Node 33 =0.076923
Probability of Node 41 =0.071429
Probability of Node 47=0.058824
Probability of Node 74 =0.066667
Probability of Node 69 =0.066667
Probability of Node 34=0.076923
```

For node 34:

From all one hop neighbors of node 34, node 41 has less number of neighbors and its corresponding probability is chosen for the decision making process of ON/OFF IDS.

```
Least neighbor count = 7
Node id = 41
Probability = 0.142857
Probability of Node 41 = 0.142857
P min [index] = 41
Least Degree Probability = 0.142857
Index = 0
Random Number =0.365890
If ( rand_number < Probability of Node 41 )
{
 Monitor the packet reception ratio of each neighbor node, so IDS is ON
} else {
Does not monitor the neighbor node, so IDS is OFF.
}
```

3. Malicious Node Detection Using IDS Algorithm

Each node monitors its neighbors for malicious activities, which here as dropping of data packets. A fixed-size interval, called IDS-interval is used by all nodes. Each node divides the simulation time into slots of IDS-interval (2sec in case) independently. There is no synchronization of the nodes. At the start of each interval, each node implements LDK algorithm and determines the probability with which it has to monitor. Depending on the probability thus obtained, it either monitors during that interval or does not do so. At the end of each interval, a node broadcasts a VOTE message that a neighbor is suspected to be malicious if it drops data packets beyond a predefined threshold. This threshold is configurable.
Since the transmission range of a node cannot be changed dynamically in ns2.A 1-hop broadcast is employed. Thus, votes about a node are aggregated at that node. A amper-resistant module which does the aggregation for the use of a broadcast authentication mechanism for broadcasting the votes. To aggregate the VOTE messages, the simulation time is also divided into slots of RA-interval (Result Aggregation interval) which is an integral multiple of IDS-interval. In the simulation, have taken RA-interval is similar to IDS-interval. If the number of VOTE messages about a node during an RA-interval reaches a predefined threshold, then the node is said to be detected as malicious during that RA-interval. Otherwise, it is not detected as malicious.

In design of the IDS, have used the security level (l) is used as the threshold value. Thus, the detection process of the IDS is strict in the sense that in the scenario when at least l nodes are monitoring, at least l votes are required to convict a malicious node as detected. One may choose a more lenient measure by choosing a value less than (l) for the threshold. False vote messages can be taken care of by increasing the security level and setting (increasing) the threshold so that even if some neighbors collude to send false VOTE messages about a node, it will not be detected as malicious.

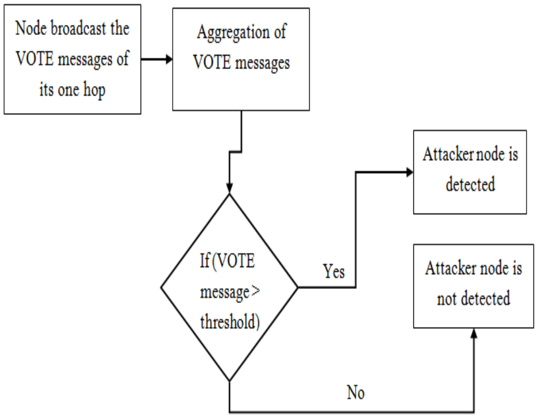

Node broadcast the VOTE messages of its one hop
Aggregation of VOTE messages
If(VOTE message > threshold)
Yes
No
Attacker node is detected
Attacker node is not detected

Figure 5. Malicious Node Detection Using IDS

4. Elimination of Malicious Node Using Trust Table

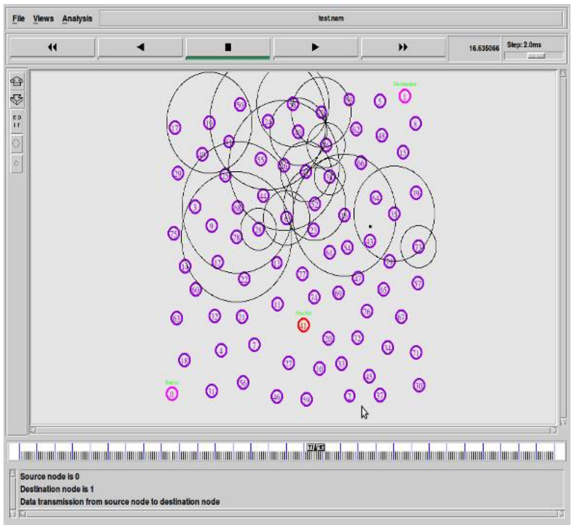
Initially, equal trust value is maintained for all the nodes in the network. Whenever a node is detected as the malicious node, its trust value is reduced and the source broadcast an “alert” message to all the nodes in the network. Every node in the system is given second chance to increase its trust level by properly participating in the routing process. Every other node updates its trust table. If the particular node repeats its misbehavior in the second chance, it is eliminated from the network. It means, no other nodes should communicate with the misbehaving nodes in the future.

Detection Process based on Trust Calculation

```
Node=0 Next hop=4 Received Count=5 Forwarded Count=4 PDR=0.800000 Neighbor Count=4 Probability=0.142857 Time=6.100000
```

```
IDS Information=1
Node=21 Next hop=13 Received Count=2 Forwarded Count=1
PDR=0.500000 Neighbor Count=12 Probability=0.125000
Time=6.120546
IDS Information=1
Node=13 Next hop=52 Received Count=2 Forwarded Count=1
PDR=0.500000 Neighbor Count=15 Probability=0.090909
Time=6.130519
IDS Information=1
Node=52 Next hop=66 Received Count=2 Forwarded Count=1
PDR=0.500000 Neighbor Count=17 Probability=0.076923
Time=6.140578
IDS Information=1
Node=66 Next hop=8 Received Count=2 Forwarded Count=1
PDR=0.500000 Neighbor Count=15 Probability=0.142857
Time=6.150625
IDS Information=1

Node=8 Next hop=1 Received Count=2 Forwarded Count=1
PDR=0.500000 Neighbor Count=7 Probability=0.166667
Time=6.160603
IDS Information=1
.......................................
After some time
Node=13 Next hop=52 Received Count=97 Forwarded
Count=42 PDR=0.432990 Neighbor Count=15
Probability=0.090909 Time=9.161425
IDS Information=1
.................
Node=13 Next hop=52 trust Value =0.432990 Time=9.161425
The Attacker node is detected. Node (13) is an Attacker
index=52 mark=0
```



```
Source node is 0
Destination node is 1
Data transmission from source node to destination node
```

Figure 6. Trust Based Intrusion Detection Scheme

Fig.6 shows the trust based IDS scheme after the attacker is detected. The alternative path is found between source and destination nodes. So source sends data to destination via alternative path.

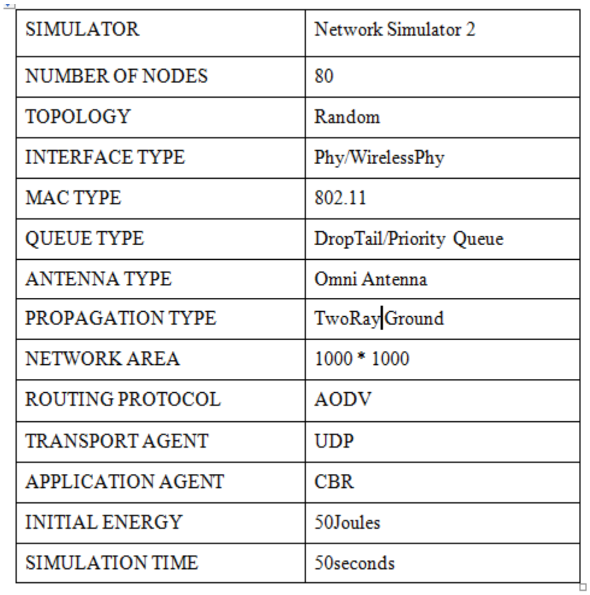
0 - 4 - 56 - 59 - 20 - 47 - 35 - 15 – 1

V. RESULTS AND DISCUSSION

The performance of IDS is analyzed using NS2.The experimental model is built with 80 nodes distributed randomly on square surface of 600 X 600 m2.A novel technique, based on a probabilistic model, to optimize the active time duration of IDSs in a MANET. The scheme reduces the IDSs' active time as much as possible without compromising on its effectiveness[1].To validate proposed approach, also present a multi-player cooperative game that analyzes the effects of individual intrusion detection systems with reduced activity on the network[7]. Through simulation, a considerable saving in energy and computational cost is achieved using proposed technique of optimizing the active time of the IDSs while maintaining the performance of the IDS [12].The proposed scheme uses local information, thus making it distributed and scalable. Moreover, it works on both static and mobile networks

VI. PERFORMANCES AND EVALUATION

A. Simulation Model



SIMULATOR	Network Simulator 2
NUMBER OF NODES	80
TOPOLOGY	Random
INTERFACE TYPE	Phy/WirelessPhy
MAC TYPE	802.11
QUEUE TYPE	DropTail/Priority Queue
ANTENNA TYPE	Omni Antenna
PROPAGATION TYPE	TwoRayGround
NETWORK AREA	1000 * 1000
ROUTING PROTOCOL	AODV
TRANSPORT AGENT	UDP
APPLICATION AGENT	CBR
INITIAL ENERGY	50Joules
SIMULATION TIME	50seconds

Figure 7.

a) Throughput

It is the amount of time taken by the packet to reach the destination.

Throughput (bits/s) = Total Data / Data Transmission duration

b) Energy Consumption

The energy consumption is proportional to the square of data transmission range. Energy consumption is defined as the sum of energy consumption of data transmissions and data requests.

c) Detection Rate

Detection rate (DR) is calculated as the ratio of the number of times malicious nodes are detected to the total number of times they should have been detected.

d) False Detection Rate

False detection rate (FDR) is calculated as the ratio of the number of times begins nodes are detected to the total number of times malicious nodes should have been detected.

Comparative Graph

Throughput

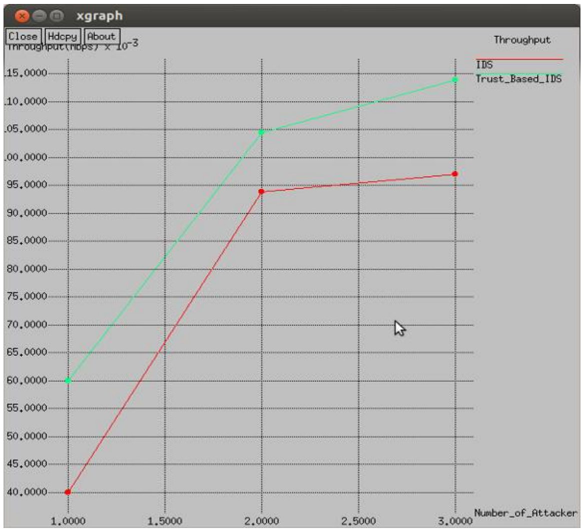


Figure 8. shows the number of data transmission flows increased while increasing the attackers. When the number of attackers is increased, the throughput value is increased. The trust based intrusion detection scheme produces increased throughput when compared to the existing intrusion based scheme due to the alternate path data transmission process.

Energy Consumption

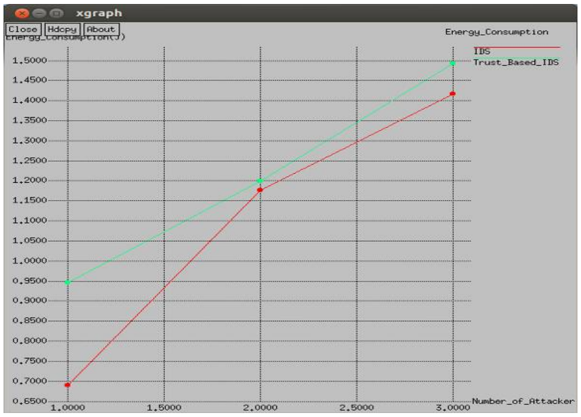


Figure 9. shows the number of attacker increased while the energy consumption is increased. The trust based intrusion detection scheme produces increased energy consumption when compared to the existing intrusion based scheme.

Detection Rate

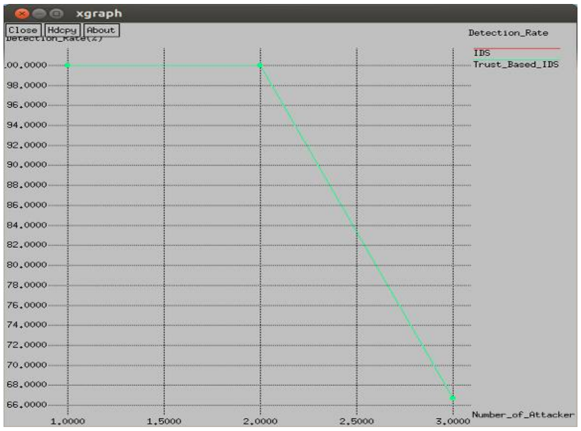


Figure 10. shows the number of attacker increased while the detection rate is decreased. The trust based intrusion detection scheme and intrusion based scheme both provides similar performance.

VII. CONCLUSION

The proposed method is an efficient way of using IDSs that sits on every node of MANET. The minimization of the active duration of the IDSs in the nodes of a MANET as an optimization problem. Then described a cooperative game model to represent the interactions between the IDSs in a neighbourhood of nodes. The game is defined in such a way that the primary goal of the IDSs is to monitor the nodes in its neighbourhood at a desired security level so as to detect any anamolous behavior, whereas, the secondary goal of the IDSs is to conserve as much energy as possible. To achieve these goals, each of the nodes has to participate cooperatively in monitoring its neighbor nodes with a minimum probability. A distributed scheme to determine the ideal probability with which each node has to remain active (or switched on) so that all the nodes of the network are monitored with a desired security level. The evaluation of the proposed scheme is done by comparing the performances of the IDSs under two scenarios: (a) keeping IDSs running throughout the simulation time and (b) using proposed scheme to reduce the IDS active time at each node in the network. The simulation results observe that the effectiveness of the IDSs in the network is not compromised while using the proposed scheme, rather, there is considerable reduction of energy consumption in each of the nodes that increases the network lifetime significantly. Homogeneous network is assumed in a way that all the nodes have the same capacities in terms of their computational and energy resources.

REFERENCES

[1] R. Muradore and D. Quaglia,"Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security," IEEE Transactions on Industrial Informatics, Vol. 11, no. 3, pp. 830-840, 2015.

[2] N. Tsikoudis, A. Papadogiannakis and E. P. Markatos, "LEoNIDS: a Low-latency and Energy-efficient Network-level Intrusion Detection System," IEEE Transactions on Emerging Topics in Computing, Vol. PP, no. 99, 2014.

[3] N. Marchang and R. Datta, "Light-Weight Trust-based Routing Protocol for Mobile Ad Hoc Networks," The Institution of Engineering and Technology (IET) Information Security, Vol. 6, No. 4, pp. 77 - 83, 2012.

[4] F. Li, Y. Yang and J. Wu, "Attack and Flee: Game-Theoretic-Based Analysis on Interactions Among Nodes in MANETs," IEEE Transactionson Systems, Man, and Cybernetics-Part B:Cybernetics, vol 40, no. 3, June 2010.

[5] N. Zhang, W. Yu, X. Fu and S. K. Das, "Maintaining Defender's Reputation in Anomaly Detection Against Insider Attacks," IEEE Transactions on Systems, Man, and Cybernetics-Part B:Cybernetics, vol 40, no. 3, June 2010.

[6] TeerawatIssariyakul,EkramHossin,"Introduction to network Simulator NS2",Springer,2009.

[7] L. Chen and Jean Leneutre, "A Game Theoretical Framework on Intrusion Detection in Heterogeneous Networks," IEEE Transactions of Information Forensics and Security, vol. 4, no. 2, June 2009.

[8] Seyhun Mehmet Futaci, Katia Jaffrès-Runser and Cristina Comaniciu, "On Modeling Energy Security Trade-offs for Distributed Monitoring in Wireless Ad Hoc Networks" In Proceeding of Military Communications Conference (MILCOM), IEEE, Vol. 16, No. 19, pp.1-7, 2008.

[9] Issa Khalil, Saurabh Bagchi and Ness B. Shroff, "SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks" In Proceeding of 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, pp. 565-574, 2007.

[10] Y. Liu, C. Comaniciu and H. Man, "Modeling Misbehavior in Ad Hoc Networks: A Game Theoretic Approach for Intrusion Detection" International Journal of Security and Networks, Vol. 1, No. 3-4, 2006.

[11] Mark Felegyhazi, Jean-Pierre Hubaux and Levente Buttyan, "Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks" IEEE Transactions on Mobile Computing, Vol 5, No. 5, pp. 463-476, 2006.

[12] Patcha and J. Park, "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks," International Journal of Network Security, vol. 2, no. 2, pp. 146-152, March 2006.

[13] Anand Patwardhan, Jim Parker, Tom Karygiannis, Michaela Iorga and Anupam Joshi, "Secure Routing and Intrusion Detection in Ad Hoc Networks" In Proceeding of 3rd IEEE International Conference on Pervasive Computing and Communications, pp.8-12, 2005.

[14] Khalil, S. Bagchi and N. B. Shroff, "LiteWorp: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks," Proc. IEEE International Conference on Dependable Systems and Networks (DSN'05), pp. 612-621, 2005.

[15] P. Michiardi and R. Molva, "A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks," Proc. WiOpt 2003: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, March 2003.

[16] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" In Proceeding of 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, 2000.