Comprehensive Survey on Game Theory based Intrusion Detection System for Mobile Adhoc Networks

Dr B. Paramasivan[1] and K. Mohaideen Pitchai[2]
[1]Professor & Head, [2]Asst. Professor (SG)
National Engg.College
Tamilnadu, India

ABSTRACT
Mobile Adhoc Networks (MANET's) are autonomous distributed systems that comprise a number of mobile nodes connected by wireless links, forming arbitrary time varying wireless network topologies. Security in mobile ad-hoc networks are particularly difficult to achieve, notably because of the limited physical protection to each of the nodes, the sporadic nature of connectivity, the absence of a certification authority, and the lack of a centralized monitoring or management unit, so it is not practically possible to prevent the network all the time. But Intrusion Detection System (IDS) can act as a frontier security area in relation to mobile ad hoc networks. In this paper the existing intrusion detection methods in mobile ad hoc network that uses game theory concepts are critically analyzed and their advantages, limitations over the other models are also explained. This paper can give a very good exposure to researchers who are willing to develop new algorithms for mobile adhoc network security.

General Terms
Game Theory, Intrusion Detection System, Mobile Adhoc Network.

Keywords
Bayesian Game, Cooperative Game, Signaling Game, Shapley Value, Nash Equilibrium.

1. INTRODUCTION
A Mobile Adhoc Network (MANET) is a collection of mobile hosts that can communicate with each other without any pre established infrastructure. Each node in the MANET [9] [12] can act as router as well as host. In order to maintain connectivity in a mobile ad hoc network all participating nodes have to perform routing of network traffic. The success of communication highly depends on other nodes cooperation. Therefore, MANET has the property of rapid infrastructure-less deployment and no centralized controller which makes it convenient to many environments, such as soldiers relaying information for situational awareness on the battlefield, business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference; and emergency disaster relief personnel coordinating efforts after a fire, hurricane, or earthquake. The other possible applications include personal area and home networking, location based services, and sensor networks. Due to the inherent characteristics of a MANET, such as mobility, wireless communication and lack of any centralized authority, providing security in a MANET is a challenging task to say the least, also intrusion Prevention is not guaranteed to work all the time, therefore the intrusion detection act as a frontline security research area of ad hoc network security. Intrusion Detection System (IDS) [6] are important tools to detect malicious node behavior. In ad hoc networks, most IDS are proposed to individual nodes due to the lack of centralized management. In this paper, the main focus is on using game theory for intrusion detection [2] in mobile ad hoc networks [1].

Game theory [4] is a branch of applied mathematics that uses models to study interactions with formalized incentive structures "games." Game theory provides us with tools to study situations of conflict and cooperation. Game theory is concerned with finding the best actions for individual decision makers in such situations and recognizing stable outcomes. It has been traditionally divided into cooperative and non-cooperative. These two branches of game theory differ in how they formalize interdependence among the players. Non-cooperative games can be classified as static or dynamic based on whether the moves made by the players are simultaneous or not. Non-Cooperative games can also be classified as games of complete information incomplete information, based on whether the players have complete or incomplete information about their adversaries in the game. In contrast, cooperative game theory abstracts away from this level of detail and describes only the outcomes that result when the players come together in different combinations.

Game theory [3] has been extensively used in the field of managerial economics, policy making etc. In recent years, we have seen researchers using game theory in the area of computer networks. It is a powerful tool in that it can be used to model any system which exhibits the characteristics of a game. We have used game theory to model the interactions between an intrusion detection system and an attacker in a MANET. Each regular node is equipped with IDS in order to monitor the activities of an attacker.

2. LITERATURE SURVEY
IDS in MANET's are a great challenge for civilian and military applications. Game theory is an applied mathematics, which has vast applications in a variety of applications. Currently researchers are working to apply the various game theoretical models like strategic form games, repeated and markov games, bayesian games, coalitional games for developing energy efficient IDS mechanisms. Some of the works are briefly described as follows.

H.Otrok et al [5] designed the cooperative intrusion detection technique in MANET using cooperative game theory concept (shapely value). They devised a flexible scheme using security

classes with the IDS being able to operate in different modes at each security class. This helped on decreasing the number of false positives. Also it classifies the intrusion into one of our predefined security classes with its associated intrusion response. The paper specifically took into consideration cache poisoning and malicious flooding intrusions. Finally, Shapley value was used to formally express the contribution of each node in detecting an intrusion in MANET's

A.Patcha and J.Park [7] designed the host based IDS using multi-stage dynamic non-cooperative game with incomplete information (basic signaling game). The objective of this paper is to detect the malicious message from some attack node with the intension of attacking the target node. The model is theoretically consistent as long as the beliefs are consistent with the information obtained and the actions are optimal given the beliefs.

H.Otrok et al [10] designed the leader-IDS using cooperative game [11] theoretic model for increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. They proposed a unified framework that is able to prolong the lifetime of IDS in a cluster by balancing the resource consumptions among all the nodes. Additionally, a zero-sum non cooperative game was given to help the leader-IDS maximize the probability of detection. This game was played between the leader IDS and intruder with incomplete information about the intruder's identity. The solution of the game advised the leader-IDS to their optimal sampling strategy.

A. Panaousis and C.Politis [13] used the non cooperative game theory to model [14] the interaction between a legitimate node (equipped with IDS) and a coalition of malicious nodes to detect the network intrusion. The work of the paper starts by finding the defending and attacking probability distributions, of any MANET and malicious coalition that maximize the utility of the players at the Nash Equilibrium (NE) it is also shown that at the NE point, the MANET and the malicious coalition have to equally distribute their defending and attacking probabilities correspondingly.

Feng Li et al [15] modeled a Bayesian game between the IDS and the attacker and obtained the optimum strategy profile for both the players. The regular node forms belief, chooses the probability to cooperate with its opponent based on its belief, and follows a rational decision rule to report. The malicious node keeps evaluating the risk of being caught and exploits its flee strategy to avoid punishment. The Perfect Bayesian Equilibrium (PBE) is analyzed in this game and emphasizes the advantages that malicious nodes would gain from the flee strategy.

3. IDS USING GAME THEORETIC APPROACH

3.1 Cooperative IDS using shapley value approach:

H.Otrok et al [5] designed the cooperative intrusion detection technique in MANET using cooperative game theory concept (shapely value) for reducing the number of false positives generated in an IDS. Main contribution of the paper is to increase the efficiency of intrusion detection system, in MANET, by decreasing the false-positives. Cooperative game theory (Shapley value) is used to analyze the contribution of each node in detecting an intrusion. An intruder that compromises a mobile node can destroy the communication by broadcasting false routing information, providing incorrect link state information, and overflowing other nodes with unnecessary routing traffic.

A cooperative intrusion detection system is needed to detect intrusions and consequently generate an appropriate response. Detecting an unusual activity will be done through monitoring the network. False-alarms are considered as one of the main problems that IDS is facing, significantly making it less trustworthy. The IDS will generate false-alarms or false positives when it considers normal data or traffic as intrusions. Moreover, the reputation of the nodes in the aggregate function is also considered. The reputation of a node reflects its behavior when detecting an intrusion. Then, they introduce a set of security classes depending on the value of the function. The security classes help on reducing false positives by choosing a security class according to the severity of the intrusion. According to the selected class an appropriate response is taken. Shapley value helps in analyzing the contribution of each mobile node on each security class in order to decrease the false positives.

The paper describes the model as a cooperative distributed intrusion detection system, in which every node in the network participates in detecting and responding to intrusions. Furthermore, every mobile node runs IDS locally to perform local data collection and anomaly detection also only two common intrusions: Cache poisoning and malicious flooding is considered. In the former, an adversary can compromise the information in the routing table through modifying its content, deleting information from it, or by injecting fake information [8]. Malicious flooding is to flood the whole network or some victim nodes with large amount of data or control packets. This leads to DoS via consuming the victim's resources (e.g. battery). Here, cooperation between mobile nodes is needed to detect the intrusion with low false positives.

Consider the model of a network in which sets of cache poisoning and malicious flooding are defined as follows: C = {0, 1} and M = {0, 1}. Each node is able to detect both intrusions. A one-to-one mapping O from the set of nodes N to C ×M, is defined as O: $N \rightarrow C \times M$, where $O(N_i) = (c_i, m_i)$ means node Ni has detected cache poisoning (malicious flooding) attack, if $c_i(m_i)$ is equal to one and has not detected otherwise. These sets will be used later on to indicate whether a node has sensed an intrusion or not. Here the MANET is modeled as an undirected graph G = (N,E), where $N = \{N_1,....,N_l\}$ is the set of mobile nodes.

A coalition is introduced where x being the members of the coalition in the set of N mobile nodes are defined in such a way that each node reports at least one type of intrusion. Now an aggregate function over the coalition is used to assign the intrusion to its equivalent security class which is achieved by proposing a function f, that represents both attacks (malicious flooding and cache poisoning) and mapping the severity of an intrusion to its corresponding security class.

$$F(N_i) = c_i \frac{NFP(N_i)}{NR\_ack(N_i)} + m_i \frac{NRP(N_i)}{ENRP(N_i)}$$

- NFP (N_i) is the number of packets forwarded by node N_i.
- NR_ack (N_i) is the number of received acknowledgments by node N_i.
- NRP (N_i) is the number of received packets by node N_i.
- ENRP (N_i) is the expected number of received packets by node N_i.

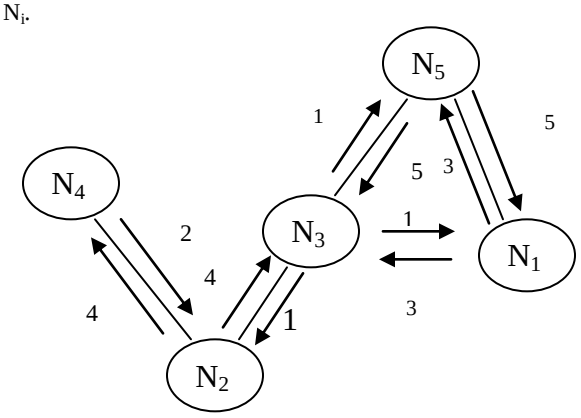

Fig 1 : Example of MANET

If the node does not receive any acknowledgments for the packets it sent, it would assume that the packets did not reach their destinations and therefore NR_ack will be less than NFP. This means that there is a problem in the routing protocol that could be due to a cache poisoning attack. Higher the loss rate is, higher is the probability of the cache poisoning. For example, if NFP(N_1) is equal to 20 and NR_ack(N_1) is equal to 5 then the ratio is 4 while in normal cases the ratio must be equal to 1 also if NRP(N_1) is equal to 40 and ENRP_ack(N_1) is equal to 10 then the ratio is equal to 4 while in normal cases the ratio must be equal to 1. This indicates the possibility of malicious flooding attack. The paper proposed the concept of security classes, CL = $\{cl_1, \ldots, cl_k\}$. These security classes represent the severity in attacks. Also a set of k-1 thresholds is used to tune the security classes in order to have trustworthy IDS, where T = $\{t_1, \ldots, t_{k-1}\}$. Now the aggregate F( ), is calculated by a node that suspects an intrusion and has asked other nodes to sense it, also the contribution of a node in a coalition is found by considering all the different permutations for the nodes, in the coalition. Now the shapley value of the node N_i in the coalition is the average of this value over all possible coalitions

Consider five mobile nodes communicating with Each other in MANET as shown in Figure 1. One of the mobile nodes received abnormal number of route-requests from other nodes asking for routing information. The node that received such requests has to check whether this amount is due to loosing many links in the network, many nodes are no more participating, or due to malicious flooding. So, the node has to cooperate with its neighbor nodes to decide if it is under attack or not. Consider that there are four security classes CL = $\{cl_1, cl_2, cl_3, cl_4\}$. The threshold set T = {2, 4, 6}, the security classes CL are classified as : $cl_1 < 2$, $2 \leq cl_2 < 4$, $4 \leq cl_3 < 6$, $cl_4 \geq 6$, the reputation of nodes $r_1 = 0.5$, $r_2 = 0.8$, $r_3 = 0.2$, $r_4 = 0.5$, $r_5 = 0.6$, and f(1) = 3, f(2) = 4, f(3) = 1, f(4) = 2, Now the participation of each node in detecting the intrusion is as follows: N_1: 19.2, N_2: 40.96, N_3: 2.56, N_4: 12.8, N_5: 38.4 also the contribution of each node on each security class is found. If the contribution of a node with other nodes in coalition changes the security class to a higher value then it means the risk behind the detected intrusion is high and an immediate cooperative or local response is needed.

However the limitations in this scheme are, no response action was proposed for any type of intrusion detected and formation of coalitions and intrusion detection is time consuming, since it has to be computed over the permutations of all possible coalitions.

3.2 Host based IDS using basic signaling game:

A. Patcha and J. Park [7] designed a host based IDS using dynamic non-cooperative game with incomplete information. They model the interactions between the nodes of an ad-hoc network as a basic signaling game which falls under the gambit of multi-stage dynamic non-cooperative game with incomplete information. They believe that intrusion detection in MANET's can be modeled as a basic signaling game for a number of reasons. First, in a MANET environment, it is very hard to detect a friend from a foe in the absence of security mechanisms like PKI, digital certificates, etc. Therefore the type of a particular node is not easily verifiable by other nodes in the system. Secondly, in most intrusion detection systems, both for wired and wireless networks, the IDS respond to the intrusion after the intrusion has occurred. Therefore they believe that modeling intrusion detection in a game theoretic framework based on dynamic non-cooperative games is the right direction to take.

The intrusion detection game is played between an attacker and IDS. The objective of the attacker is to send a malicious message from some attack node, with the intension of attacking the target node. The intrusion is deemed successful when the malicious message reaches the target machine without being detected by the host IDS. They assume that an intrusion is detected and the intruding node is blocked when a message sent by a probable intruder is intercepted and the host IDS can say with certainty that the message is malicious in nature. In their model, the cost associated with an undetected intrusion to be much more severe than the cost associated with false alarms.

In their proposed signaling game model, a node is the sender and a host based IDS is the receiver to which the message is directed. The sender node is assumed to be one of the 2 type's regular node or malicious node/attacker. The strategy of the IDS is to pick the optimal strategy out of its available set, in response to a message from the sending node. The choice of strategy is based on the receiver's prior beliefs, such that it is able to maximize the effective payoff by minimizing the cost due to false alarms and missed attacks.

The representation of the attacker-IDS game model is shown in Figure 2. Let s be the probability with which the malicious node exhibits malicious behavior and 1-s is the probability with which the node exhibits normal behavior. The particular choice that the malicious node makes is his "message" and let t be the probability with which IDS detects this message and 1-t is the probability with which it misses. The IDS has a gain of γ_{defend} on a successful detection, losses γ_{miss} for a missed detection and has a cost of γ_{falarm} for generating a false alarm. The attacker gains $\delta_{Intrude}$ on a successful intrusion and a losses δ_{Caught} on an unsuccessful intrusion where as the attacker has a zero cost value for a false alarm. The Nash Equilibrium for both players is found at which the players obtains an optimized payoff.

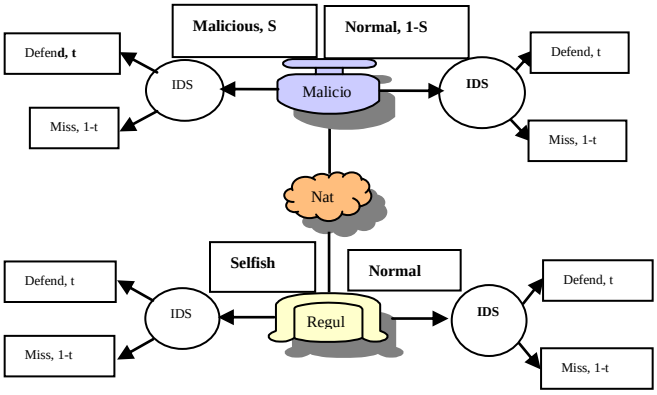

Fig 2 : An Attacker IDS Basic Signaling Game.

The game theoretic investigation presented in this paper gives us valuable insight into the behavior of the attacker and the IDS. However the proposed game model does not consider selfish node activity also the scenario of multiple malicious nodes forming a coalition to intrude the network.

3.3 Leader IDS using cooperative game approach:

H.Otrok et al [10] designed the leader-IDS for increasing the effectiveness of IDS for a cluster of nodes in ad hoc networks. To reduce the performance overhead of the IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster. However, most current solutions elect a leader randomly without considering the resource level of nodes. Such a solution will cause nodes with less remaining resources to die faster, reducing the overall lifetime of the cluster. It is also vulnerable to selfish nodes that do not provide services to others while at the same time benefiting from such services. To increase the effectiveness of IDS in MANET, a unified framework is proposed that is able to (i) Balance the resource consumption among all the nodes and thus increase the overall lifetime of a cluster by electing truthfully and efficiently the most cost-efficient node known as leader-IDS. (ii) Catch and punish a misbehaving leader through checkers that monitor the behavior of the leader.

A cooperative game-theoretic model is proposed to analyze the interaction among checkers to reduce the false-positive rate. A multi-stage catch mechanism is also introduced to reduce the performance overhead of checkers. (iii) Maximize the probability of detection for an elected leader to effectively execute the detection service. This is achieved by formulating a zero-sum non-cooperative game between the leader and intruder.

Here the MANET is modeled as an undirected set of mobile nodes and the set of bidirectional links. The network is divided into different clusters where every cluster has a set of nodes and a set of links. One-hop neighbor nodes form a cluster and nodes might belong to more than one cluster. It is assumed that each node has an IDS and a unique identity. Moreover, the neighbor nodes can always overhear each other using an omni directional antenna. Also it is assumed that every node will increase the reputation rate of a cooperative node since reputation is used to track whom to trust. A selfish node is defined as an economically rational node whose objective is to maximize its benefits (payoffs). Therefore, incentives must be given to nodes to motivate them in cooperating. Incentives are modeled in terms of the reputation of node. Reputation is used to decide whom to trust and motivate nodes to reveal truthfully their private information about their cost of analysis (C).

The objective of the proposed model is to find the most cost-efficient node that handles the detection process. Without loss of generality, assume that the leader node is at cluster (A) where nodes are asked to reveal truthfully their cost of analysis by motivating them through incentives. Incentives are given in the form of reputations and computed based on VCG (Vickrey, Clarke and Groves) mechanism [17], where truth telling is the dominant strategy. Reputations are needed to decide whom to trust among the nodes in a cluster. In the proposed model, nodes are asked to directly reveal their utility function to compute the Social Choice Function (SCF), which is the least cost of analysis value. Payments are computed using VCG. The SCF is computed in a distributed manner where all the nodes decide about the leader node. This guarantees that the same leader is elected by all.

To form the MANET into clusters, the cluster formation algorithm is used. Every node is aware of its neighbor nodes. Here the distributed election protocol is described where every node executes the following steps.

(1) $n_i \rightarrow Cluster^{A}_{-ni}$: Begin-Election (IDn_i, $H(IDn_i, C_i, TS_i), T_1$)
(2) $n_i \rightarrow Cluster^{A}_{-ni}$: Election ($IDn_i$, C_i,TS_i)
(3) If Leader IDS = n_i;
$n_i \rightarrow$ Leader IDS: Done-Election.
LeaderIDS $\rightarrow$ n_i: Confirm Leadership.
$n_i \rightarrow$ LeaderIDS: Deliver payment = $R^{t}_{ni}(n_j)$
(4) Else after T_2;
$n_i \rightarrow Cluster^{A}_{-ni}$: Confirm Leadership.
$Cluster^{A}_{-ni} \rightarrow n_i$: Deliver payment = $R^{t}_{nj}(n_i)$.

In the first step, node sends a Begin-Election message to all nodes in cluster A. The hash function is used to avoid nodes from cheating and delivering a fake C_i. The time T1 is used to identify the election start time, After all the nodes exchange the Begin-Election message within time T.

In the second step, node sends the Election message which includes its identity, the cost of analyzing the traffic and the time stamp. Nodes that did not contribute in sending the Begin-Election message will be excluded from cluster's services. On receiving the Election messages, node verifies each received message with its corresponding hash value that has been sent in Begin-Election message. After the verification is accomplished, each node computes the SCF, which is the minimum valuation of cost of analysis.

In the third step, if the leader is different from node then it sends a Done-Election message to inform the leader that he has been elected. In this case, elected leader forward a confirm leadership message that indicates its acceptance of leadership. Then, node calculates the payment using the VCG mechanism and sends a copy of the payment back, node increases its reputation table. Note that a node needs the copy of payment to calculate its reputation and compare it to the threshold TH to avoid punishment.

In the fourth step, if the leader is ni, it sets a timer T2 then starts verifying the origin of all the Done-Election messages. If T2

expires without receiving all the Done-Election messages, then nodes who did not participate are excluded from the cluster's services. Last but not least, once the leader has been chosen by all the nodes, all contributing nodes will be added to the protected list.

If the cluster did not change after TELECT expires, formation step and start leader election are omitted. Moreover, the reelection procedure is enforced either when the leader-IDS misbehave or quit from the cluster before TELECT expires. Finally, selfish nodes might misbehave after election, which motivates us to select random checkers to ensure a catch-and-punish scheme in order to motivate an elected node to be faithful during the detection process. Note that a random election ensures fairness. In the proposed model, the selected checker is assumed to be cooperative since the benefit of the intrusion detection service dominates resources consumption. This is because that the elected checkers mirror a portion of the computation done at the elected nodes which have a marginal effect on resource consumption.

The major advantages of leader-IDS mechanisms are to (i) increase the overall lifetime of IDS in MANET by truthfully electing the most cost-efficient node to handle the detection process on behalf of the whole cluster. This is achieved by balancing the resource consumption for the detection service among all the nodes in a cluster. (ii) Encourage selfish nodes are truthfully reveal their cost of analysis during a leader election. This is achieved by a reputation system based on the truth-telling mechanism and by binding the reputation of a node to the amount of services the node is entitled to. (iii) Encourage an elected leader to carry out its responsibility of intrusion detection. This is achieved with a decentralized catch-and-punish mechanism using random checker nodes. (iv) Reduce the false-positive rate of checkers in catching the misbehaving leader. This is achieved by formulating a cooperative decision game among the checkers and by a multi-stage catch mechanism. (iv) Maximize the probability of detection by optimally distributing the node's sampling budget among all its incoming-links. This is achieved by modeling a zero sum non-cooperative game between the leader and intruder with incomplete information about the intruder.

3.4 IDS using non cooperative game model:

A. Panaousis and C. Politis [13] used the non cooperative game theory to model the interaction between a legitimate node equipped with IDS and a coalition of malicious nodes to detect the network intrusion. The game is modeled as an interaction between an IDS and a malicious coalition, considering all IDS as one player and all attackers (malicious coalition) as one player. Hence the game is characterized as non- cooperative game. When an attack is indeed in progress one of the following cases may occur: (i) the MANET have not detected the attack due to IDS limitations. This might happen for instance in cases where the IDS software has not been updated with a known or a new attack or the IDS capabilities are limited, (ii) the MANET has not recognized the attack due to malfunction, (iii) the MANET has recognized the attack and triggers an alarm.

The strategies for the 2 players are considered as {Defending, Non Defending} for the IDS and {Attacking, Non Attacking} for the malicious coalition. The utility function for both players are calculated based on their choice of strategy and tabulated. The IDS and the Attacker (malicious coalition) has a zero cost value when no attacks take place, also the attacker has a zero cost value when the attacker does not attack. Also the respective payoffs for each strategy chosen by the attacker and the IDS are tabulated as shown in Table 1. Let rd be the attack detection rate and 1-rd be the misdetection rate, Vni represents the security value of the node n_i and $cost_a$, $cost_d$, $cost_f$ represents the attacking cost, intrusion detection cost, cost due to false alarm respectively. Using the table the utility function for both the players is found.

The utility of the MANET is defined as a function of: (i) The attack detection rate, (ii) The security loss due to a successful attack, (iii) The cost for a false alarm, (iv) The rate of a false alarm and (v) The cost of defending a MANET node. On the other hand, the utility of the malicious coalition is defined as a function of: (i) The attack detection rate, (ii) The security loss for a legitimate MANET node when the attacker succeeds to harm a node and (iii) The cost of attacking a MANET node.

Nash equilibrium is derived for the game and its validity is proved, also it is found that malicious coalition does not have any profit at Nash Equilibrium(NE) even if it decreases its attack cost, this happens because in this case the MANET will increase its monitoring probability reducing the utility of the malicious coalition to zero. In this game model the defending and attack probability distributions of any MANET and malicious coalition that maximizes the utility of the players at the NE is found. The main advantage of this model is that the author has figured the attack as a malicious coalition since a network might face this scenario most of the time. However this type of IDS detection technique will not be energy efficient in a larger network since the IDS will use all the residual energy of a node to detect the intrusions

Table 1. Payoff matrix of the game

Strategy	**Attacking**	**Non Attacking**
Defending	$-(1-r_d)V_{ni}-r_f cost_f V_{ni}-cost_d V_{ni}$, $(1-r_d)V_{ni} - cost_a V_{ni}$	$-r_f cost_f V_{ni}-cost_d V_{ni}$, 0
Non Defending	$-V_{ni}$, $V_{ni}-cost_a V_{ni}$	0, 0

3.5 IDS employing Bayesian game approach:

Feng Li et al [15] modeled the wrestling between the regular and the malicious node as a dynamic Bayesian game between the regular and malicious node. Each Node's type (regular or malicious) is its own private information. Its neighbor's actual type is the incomplete information in the game. Each node forms beliefs toward neighbors and updates the beliefs according to the neighbors' actions as the game proceeds. The regular node sets a reputation threshold and judges other nodes' types based on the evaluated belief and this threshold. The malicious node continuously evaluates the risk, which is decided by the possibility that a regular node would choose to report under current conditions. On the basis of the risk and expected fleeing cost, the malicious node makes a decision on fleeing. A

monitoring and reputation system [16] is used as a basic setting for regular nodes.

Node i can be one of the 2 types regular or malicious, node j is considered as a regular node. A regular node has 3 actions to choose from his available strategies {cooperate, decline, report} and there are 3 choices for a malicious node {cooperate, attack, flee}. In this game model nodes keep track of the outgoing packets of their one-hop neighbors through passive observation. Based on these observation two discrete variables are incremented if there is either a detected C or detected A/D where C is a cooperation and A/D are defined as Attack or Decline in one round of communication. Also when a regular node decides to report (R) one of its neighbors as a malicious node, it broadcasts the report in its current cluster. If the report is considered to be true, the malicious node being reported will be punished. Otherwise, the reporting node's accountability will be affected for the false alarm also the malicious node calculates the risk of being caught and makes a decision to flee fearing for the punishment. Node j (regular node) keeps updating its belief about its neighbor in each stage game. The expected payoffs for both the players are calculated and the Bayesian Nash equilibrium is found. The stage game is analyzed without considering the strategies Report and Flee. The strategic representation of the game is shown in figure 3.

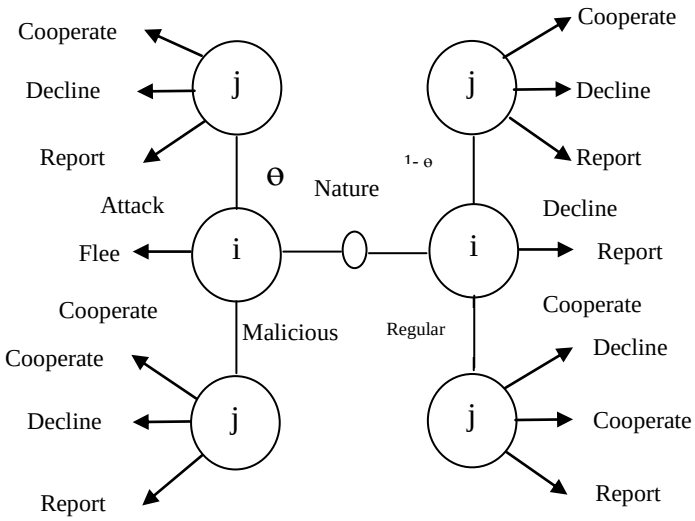

Fig 3: Single Stage of the game

A regular node j decides to report in a stage, in two possible cases: 1) i is malicious, and the report is correct, and 2) i is regular, and the report is a false alarm. The regular node j's decision depends on the comparison between the expected correct report gain and the expected false alarm cost. j also needs to evaluate the sufficiency of the evidence before making a decision to report. On the other hand malicious node decides to flee based on node j's current belief on node i. An equilibrium for both the players are found and it is shown that the proposed equilibrium strategy profile outperforms other pure or mixed strategies However the game model does not consider the scenario of a multiple attacker coming together in a group/combination.

4. COMPARATIVE ANALYSIS

The IDS mechanisms based on various game theoretical models has been explained in section 3. These mechanisms are not reached the expected level of user satisfaction. Also these mechanisms have some major limitation as well as some merits. The table 2 describes some of the limitations and merits of each IDS models.

Table 2 Limitations of the Existing IDS Model

Types of IDS	Game Type	Merits	Limitations
Cooperative IDS	Cooperative Game (Shapley value Approach)	Decreasing the generation of false-positives and false alarm rates	No IDS response action Time consuming
Host Based IDS	Dynamic Non Cooperative Game (Basic Signaling game)	Maximize the effective payoff by minimizing the cost due to false alarms and missed attacks.	No consideration about selfish node activity. No consideration about malicious node coalitions.
Leader IDS (Leader Election Alg.)	Cooperative Game Approach	Catch and punish a misbehaving leader through checkers that monitor the behavior of the leader.	Time consuming Leader IDS election algorithm
Host Based IDS	Bayesian Game	To detect the intrusion based on the belief updated by the regular node about its neighbor	Does not consider the scenario when attackers come in a group / combination
Host Based IDS	Non Cooperative game	Increase its monitoring probability by reducing the utility of the malicious coalition.	Not energy efficient in a larger network.

5. CONCLUSION

Ad hoc network security has come into the lime light of network security research over the past couple of years. However, little has been done in terms of defining the security requirements specific to MANET's. Such security requirements must include countermeasures against node misbehavior and denial of service attacks. In this paper we did a brief survey about intrusion detection techniques in MANET using different game theoretic methods and analyzed the advantages and disadvantages of each methodology. Our plans for future work will be to identify an appropriate game theoretic method, formulate a game model between the attacker and the host/administrator and use it in developing an Intrusion Detection system that detects the intrusions in network layer, also ensure that it defends against all types of attacks including Selfish nodes and colluding attackers. Our foremost idea is to implement the developed IDS model in a MANET or a real time environment and study the behavior of the network when subjected to different kinds of attacks and to make sure that running such IDS in a MANET will be energy and cost efficient.

6. REFERENCES

[1] Sunita Sahu & Shishir K. Shandilya "A Comprehensive Survey on Intrusion Detection in MANET" International Journal of Information Technology and Knowledge Management, July-December 2010, Volume 2, No. 2, pp. 305-31

[2] Prof.A.K.Gulve, D.G.Vyawahar "Survey On Intrusion Detection System" International Journal of Computer Science and Applications Vol. 4, No. 1, April / May 2011.

[3] Roy. S, Ellis. C, Shiva. S, Dasgupta. D, Shandilya. V, Qishi Wu "A Survey of Game Theory as Applied to Network Security" System Sciences (HICSS), 2010 43rd Hawaii International Conference 11 March 2010.

[4] D. Fudenberg and J. Tirole, Game Theory. Cambridge, MA: MIT Press, 1991

[5] Hadi Otrok, Mourad Debbabi, Chadi Assi and Prabir Bhattacharya "A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks" 27th International IEEE Conference on Distributed Computing Systems Workshop (ICDCSW'07) 2007.

[6] A. Agah, S. Das, and K. Basu, "Intrusion Detection in Sensor Networks: A Non-cooperative Game Approach", Proc. 3rd IEEE International Symposium on Network Computing and Applications, IEEE press, 2004.

[7] Animesh Patcha and Jung-Min Park (Corresponding author: Animesh Patcha) "A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks" International Journal of Network Security, Vol.2, No.2, PP.131–137, Mar. 2006

[8] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile Ad hoc networks," in Proceedings of the 6th annual international conference on Mobile computing and networking (ACM MobiCom 2000:), pp. 255–265, New York, NY, USA, 2000.

[9] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proc. MOBICOM 2000, Boston, ACM press, pp: 275-283, 2000.

[10] Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbabi, Prabir Bhattacharya. "A game theoretic intrusion detection model for mobile ad hoc networks" 2007 Elsevier B.V

[11] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, R.R. Rao, Cooperation in wireless ad hoc networks, in: Proceedings of the INFOCOM03, IEEE, 2003, pp. 808–817

[12] H. Yang, X. Meng, S. Lu, Self-organized network-layer security in mobile ad hoc networks, in: Proceedings of the ACM Workshop on Wireless Security, ACM, 2002, pp. 11–20

[13] Emmanouil A. PANAOUSIS and Christos POLITIS "Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANET's" proceedings of the future network and mobile summit 2011 conference

[14] Y. Liu, C. Comaniciu, and H. Man, "A bayesian game approach for intrusion detection in wireless ad hoc networks," in Proc. GAMENETS,(NY, USA), p. 4, 2006

[15] Feng Li, Member, IEEE, Yinying Yang, Student Member, IEEE, and Jie Wu, Fellow, IEEE "Attack and Flee: Game-Theory-Based Analysis on Interactions among Nodes in MANET's" IEEE Transactions on Systems, Man and Cybernetics, Part B 2010, pp.612-622.

[16] A. Josang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision" Decis. Support Syst., vol. 43, no. 2, pp. 618–644, Mar. 2007.

[17] J. Feigenbaum, C. Papadimitriou, R. Sami, S. Shenker, A BGP based mechanism for lowest-cost routing, in: Proceedings of the 21st annual symposium on Principles of distributed computing, ACM, 2002, pp. 173–182.