Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

A hybrid intrusion detection by game theory approaches in MANET

Marjan Kuchaki Rafsanjani[1*], laya Aliahmadipour[1] and Mohammad Masoud Javidi[1]
[1]*Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran.*
kuchaki@mail.uk.ac.ir*

Abstract

In general, mobile ad hoc networks (MANET) are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using an existing network infrastructure or centralized administration. The hosts establish infrastructure and cooperate to forward data in a multi-hop fashion. Due to their communication type and resources constraint, MANETs are vulnerable to diverse types of attacks and intrusions. In this paper, we proposed a method for prevention internal intruder and detection external intruder by using game theory in mobile ad hoc network. One optimal solution for reducing the resource consumption of detection external intruder is to elect a cluster head for each cluster to provide intrusion service to other nodes in the its cluster, we call this mode, normal mode. Normal mode is only suitable when the probability of attack is low. Once the probability of attack is high, victim nodes should launch their own IDS to detect and thwart intrusions and we call perfect mode. In this paper cluster head should not be malicious or selfish node and must detect external intrusion in its cluster with enough resource and honest behavior. Our hybrid method has three phases: the first phase building trust relationship between nodes and estimation trust value for each node to prevent internal intrusion. In the second phase we propose an optimal method for cluster head election by using trust value; and in the third phase, finding the threshold value for notifying the victim node to launch its IDS once the probability of attack exceeds that value. In first and third phase we apply Bayesian game. Our hybrid method due to using game theory, trust value and honest cluster head election algorithm can effectively improve the network security, performance and reduce resource consumption.

Keywords: Mobile Ad hoc Network (MANET), Intrusion detection system (IDS), Cluster head, Trust value, Game theory.

Introduction

Mobile ad hoc networks (MANET), also called spontaneous networks, are comprised of a collection of dynamic cooperating peers and consist one of the most promising wireless technologies. The peer nodes in a MANET may show a short duration in their membership with many joins and leaves from the network. They may also employ a multi-hop information transfer without relying on an infrastructure. The mobile devices in a MANET create a wireless communication channel whereas; each of them contributes in the routing decisions of the network since there are no central stations. Mobile nodes communicate directly with nodes in their vicinity and they relay messages on behalf of others to enable communication with devices not in direct radio-range of each other (Mitrokotsa *et al*., 2007). Each node operates in distributed peer-to-peer mode, acts as an independent router, and generates independent data. No dedicated routers are necessary; every node acts as a router and forwards each others' packets to enable information sharing between mobile hosts. Each node is free to move about while communicating with other nodes (Lima *et al.*, 2009). The main advantages that MANET has presented are flexibility, adaptability, easy collaboration and efficient communication in infrastructure-less environments. Because of the special advantages that wireless ad hoc networks present, their applications vary from battlefield scenarios to recovery operations in case of disasters, such as in hurricanes, floods and terrorist acts. Although MANET presents many advantages, they also present a number of inherent vulnerabilities that increase their security risks. MANETs are often subject to types of attacks and intrusions. Due to the open medium, the dynamically changing topology, the lack of a centralized monitoring and management point, the limited resources and the lack of physical security of the member nodes (Mitrokotsa *et al*., 2007).

Intrusion detection can be defined as a process of monitoring activities in a system which can be a computer or a network. The mechanism that performs this task is called an intrusion detection system (IDS). Studies show that intrusion detection techniques just like encryption and authentication system which are the first line defence, are not enough; as the system grows in complexity their weaknesses grow causing the network security problems. Intrusion detection can be considered as a second line of defence for network security. So, IDS should analyze system activities and ensure whether or not an intrusion has occurred (Kuchaki Rafsanjan, 2009).

Intrusion Detection Systems (IDS) are security tools that, like other measures such as antivirus software, firewalls and access control schemes, are intended to strengthen the security of information and communication systems (Garcı´a-Teodoroa, 2009). The cooperation among nodes is a crucial requirement for intrusion detection in Mobile Ad hoc Networks (MANETs), due to their autonomous nature (Hu & Perrig, 2004). The cooperation usually requires all the nodes to launch their own IDSs to increase the detection capability and resource consumption. But nodes in MANET have only limited resources. A common approach for reducing the overall resource consumption of intrusion detection is for

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

nodes to acquiesce in electing a cluster head to serve as the intrusion detection system (IDS) for a cluster of one-hop nodes (Otrok *et al*., 2008).

Game theory (Morris, 1994) has been successfully applied to many disciplines including economics, political science, and computer science. Game theory usually considers a multi-player decision problem where multiple players with different objectives can compete and interact with each other. Game theory classifies games into two categories: Non-cooperative and cooperative. Non-cooperative games are games with two or more players that are competing with each other. On the other hand, cooperative games are multi-players cooperating with each other in order to achieve the greatest possible total benefits. A game consists of a set of players a set of moves (or strategy) available to those players, and a specification of payoffs for each combination of strategies. A player's strategy is a plan for actions in each possible situation in the game. A player's payoff is the amount that the player wins or loses in a particular situation in a game. A player has a dominant strategy if that player's best strategy does not depend on what other players do (Ganchev *et al*., 2008).

To predict the optimal strategy used by intruders to attack a network, the authors of (Liu & Zang, 2005) model a non-cooperative game-theoretic model to analyze the interaction between intruders and the IDS in a MANET. They solve the problem using a basic signaling game which falls under the gambit of multi-stage dynamic non-cooperative game with incomplete information. Jiang *et al.* (2009) proposed Bayesian game between neighboring node for estimating trust value for each other. Otrok *et al.* (2008) solve trade off security and resource consumption by a nonzero-sum non-cooperative game based on Bayesian Nash equilibrium is used to model the interaction between the cluster head and external intruder, in this game intruder has complete information about cluster head, but cluster head doesn't have complete information about intruder. The solution of such a game guides the IDS to inform the victims to launch their IDS according to the game derived threshold. For preventing of internal intrusion due to selfish or malicious nodes, first we must build trust relationship between each node. Trust is defined as "a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities". According to (Capra, 2004), Trust has also been defined as the degree of belief about the behavior of other entities or agents (Seshadri-Ramana *et al*., 2010). Therefore, building trust relationship between nodes in MANET plays a significant role in improving the network security, performance and quality of service.

We will introduce methods of calculating trust value and explain Bayesian game theory between neighboring nodes based on (Jiang *et al*., 2009). This method is used because it converges quickly since trust relationships are only established among neighbor nodes. After this phase, we should elect a trustee cluster head with the enough energy for each cluster of one-hop nodes. In the third phase we have a Bayesian game for detection external intruder based on (Otrok *et al*., 2008). Between cluster head and external intruder to find the threshold value for notifying the victim node to launch its IDS once the probability of attack exceeds that value. In this paper due to use combination of Game Theory in various positions will lead to discussion types of intrusion. So increase network security and network life time.

In this paper, we propose a hybrid intrusion detection method for MANETs.

Related works

There are many researches that are applying game theory in intrusion detection systems. A game theoretic platform is suitable for modeling security issues such as intrusion prevention and intrusion detection. An example of an intrusion prevention game model is presented in (Liu & Zang, 2005), where the authors propose a game theoretic approach to infer attacker intent, objectives, and strategies (AIOS). In the context of intrusion detection, several game-theatrical approaches have been proposed to wired networks, WLANs, sensor networks, ad hoc networks and mobile ad hoc network.

Kodialam & Lakshman (2003) have proposed a game theoretic framework to model the intrusion detection game between two players: the service provider and the intruder. A successful intrusion is when a malicious packet reaches the desired target. In the game, the objective of intruder is to choose a particular path between the source node and the target node, and the objective of the service provider is to determine a set of links on which sampling has to be done in order to detect the intrusion. Essentially, the game is formulated as a two-person zero-sum game, in which the service provider tries to maximize his payoff, which is defined by the probability of detection, and on the other hand, the intrude tries to minimize the probability of being detected.

Patcha & Park (2006) used the concept of multi-stage dynamic non-cooperative game with incomplete information to model intrusion detection in a network that uses a host based IDS. As long as the beliefs are consistent with the information obtained and the actions are optimal given the beliefs, the model is theoretically consistent. They believe that this game-theoretic modeling technique models intrusion detection in a more realistic way compared to previous approaches. Otrok *et al*. (2008) 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. This was achieved by truthfully electing the most cost-efficient node (IDS) that handles the detection process. Incentives were given in the form of reputations to motivate nodes in revealing truthfully their costs of analysis. Reputations are

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

computed using the well known VCG mechanism where truth-telling is the dominant strategy. They proposed a cooperative decision game theoretical model to efficiently catch the misbehaving leader-IDS with less false-positive rate. Additionally, a zero-sum non-cooperative game was given to help the leader-IDS to maximize the probability of detection. This game was played between the leader-IDS and intruder with incomplete information about the intruder's identity. Marchang *et al.* (2007) presented a game-theoretic model of intrusion detection systems (IDSs) for MANET. They believe that in most of the existing intrusion detection systems for MANETs, a detection system sits on every node, which runs all the time, which is a costly overhead for a battery-powered mobile device but they have used game theory to model the interactions between the intrusion detection system and the attacker to determine whether it is essential to always keep the IDS running without compromising on its effectiveness. Poongothai *et al.* (2008) presented a model for analyzing misbehaviors using game theory their model focuses on interaction between pair of attacking/regular nodes as a two player non-cooperative non-zero sum game. Agah & Das (2007) formulated the prevention of passive denial of service (DoS) attacks in wireless sensor networks as a repeated game between an intrusion detector and nodes of a sensor network, where some of these nodes act maliciously.

Our proposed method

Our hybrid method has three phase that is organized as follows: first we establish trust relationship between neighboring nodes to prevent internal intruder based on scheme that proposed by Jiang *et al*. (2009); then we proposed our cluster head election scheme and in the last phase we present method for detecting external intruder based on game that proposed by Otrok *et al*. (2008).

Trust establishment relationship phase

Mobile ad hoc network due to lack of routing infrastructure, they have to cooperate to communicate. Nodes are rational; their actions are strictly determined by self interest. Therefore, misbehavior exists. Malicious nodes join the network with the intent of harming it by causing network partitions, denial of service, etc. While selfish nodes are the nodes that utilize services provided by others but do not reciprocate to preserve resources. To save battery and bandwidth, nodes should not forward packets for others. If this dominant strategy is adopted, however, all nodes are worse off. Therefore, an ideal scheme is needed to give nodes an incentive to cooperate.

In most existing research that works on the trust establishment in MANET, trustor ranks the trust level of trustee using evaluation model based on the direct and indirect evidences collected respectively (Eschenauer *et al*., 2002; Ren *et al*., 2004) The advantage of this approach is that the trust value about trustee is computed based on comprehensive investigation in the whole network. Therefore, the trust value is more accurate and objective. On the other hand, in order to boot the process of trust establishment, existing approaches designate a default trust value to all trustees subjectively, such as 0.5, in the bootstrapping phase. That is, from the new node's point of view, all other nodes have the same trust level. This may result in hidden danger for not distinguishing between favorable nodes and malicious ones. Ren & Boukerche (2008)] proposed the novel trust system, which they refer to as the trust computation and management system (TOMS). TOMS not only includes a unique trust computation model that computes the trust effectively for each node, but also establishes the trust management mechanism that is responsible for every aspect of the trust system. The trust model is distributed to each node in the network and all nodes update their own assessments concerning other node accordingly.

Jiang *et al*. (2009) propose a trust establishment scheme for MANET based on game theory. In their scheme, trust is regarded as a node's private estimation about other nodes. Without using the indirect evidences which are often adopted in traditional approaches, their trust evaluation model is based on the game results and history interaction information. This method is used because it converges quickly since trust relationships are only established among neighbor nodes. At first we present game for estimating trust value.

Network model and computation trust value

We use a undirected graph $G =< V , E >$ to model a mobile ad hoc network, where V is the set of nodes, and E is the set of edges, in other words, the pair of nodes with a common edge are the neighbors of each other. We denote N_i as the set of all neighbors of node i and $\|N_i|$ represents the number of nodes in N_i , i.e., the degree of node i in the graph G In (Jing *et al*.,2009) they assume that each node has a property set $\Theta = \langle \theta_i(t), H_i(t), |N_i|(t) \rangle$ at time t.

Where $\theta_i(t)$ is the energy utilization rate of V_i at time t . $H_i(t) = \{h_i^j(t) | j = 1....|N_i|\}$ is the interaction history records such as packet forwarding behavior about all nodes in. N_i is the number of *i's* neighbors. $h_i^j(t) = \langle f_i^j, R_j^i \rangle$ is the interaction history record of node *i* on node *j*. f_i^j is the number of packets forwarded actually by V_j on behalf of V_i and R_j^i is the number of all packets that V_i ask V_j to forward at time *t*. $\Theta_i(t)$ is the private information for V_i about which other nodes do not know. The information about nodes' properties and history interaction records are indispensable for trust evaluation. Therefore, each node must have some

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

storage space called as information base. Each entry of information base records one of all neighbor node's information: node's properties, value of trust, and interaction records; Jing *et al*.(2009) propose trust value of node *i* on node *j*; that is T_j^i .

$$T_j^i = (1-\alpha)T_i^{j.g} + \alpha T_i^{j,o} \quad (1)$$

In equation (1) $T_i^{j,g}$ is predicted value of node *i* on node *j* by game analyzing based on the node's properties. To obtain this value, node *i* must play games with its neighbor and estimate the optimal expected utility U_i^j brought to it by the neighbor node *j* and then we can compute:

$$T_i^{j,g} = U_i^j \Big/ \sum U_i^j \qquad j \in N_i \quad (2)$$

For the detail analysis, refer to Jing *et al*., 2009.

$$T_i^{j,o} = F_j^i \Big/ R_j^i \quad (3)$$

$T_i^{j,o}$ is observed value obtained by direct interaction history. α is the weight factor reflecting the preferences. If there is not history, α =0, along with gathering of the interaction record, α increases gradually. The game is played between node *i* and node *i*'s neighbor. For estimation trust value node *j* by node *i,* according to equation (1) due to players don't have complete information about each other, Bayesian game is used. Assume a two-player Bayesian game is:

$$\Gamma = \langle N;\theta_i;A_i;U_i;P,_i\, i \in N_i;\rangle \quad (4)$$

$N = \{a,b\}$is the set of players. The θ set of player's types. A_i is the action set of player *i*. U_i is the utility function set of player *i*. Each player chooses the action based on its own type. In this step we need utility is the function of strategy and type, computation of $T_i^{j,g}$ and $T_i^{j,o}$.

Calculation of $T_i^{j,g}$: In MANET, energy E_i of each node *i* is limited. Besides, allocating some energy to forward packet for others is called forward energy, a node must reserve some energy to handle its own business is called self-energy, such as numerical computation, data generation, etc. they assume that node *i* has the action space $\langle a_{i1}, a_{i2}\rangle$ in the energy distribution game, where a_{i1} is the amount of self-energy and a_{i2} is the amount of forward-energy. Obviously, a_{i1} and a_{i2} satisfy the condition $a_{i1} + a_{i2} \le E_i$ so that E_i is dynamic changing with the passing of time and the increasing of interaction numbers.

The utility function of node *i* is U_i*:*

$$U_i = u_i[(a_{01}, a_{02}),(a_{11}, a_{12}),\theta] \quad (5)$$

Suppose the function of u_i is:

$$u_i = \left((x_i + \frac{a_{i1}}{1+a_{j1}})^{\beta} (y_i + \frac{\theta_i a_{i2}}{1+\theta_j a_{j2}})^{\gamma} \right) \quad (6)$$

Where $j = 1-i$, $\beta + \gamma = 1$, x_i and y_j are constants, which mean the existing previous profits foundations at the areas of self-energy and forward-energy. The constraint condition is $a_{i1} + a_{i2} \le E_i$ So we let

$$T_i^{j,g} = U_i^j \Big/ \sum_{j \in N_i} U_i^j \quad (7)$$

Another method is to integrate more numbers of interaction records:

$$T_i^{j,o} = \frac{\sum_{s=k-c+1}^{k-1} F_j^i(s)}{\sum_{s=k-c+1}^{k-1} R_i^j(s)} \quad (8)$$

In equation (8) *c* is the interactive numbers in history. Clearly, $c = k-1$ means to integrate all the history records into the estimation of $T_i^{j,o}$ *(k)*. In the realistic environment, recording all history information is impossible for a node. Therefore, the value of *c* should be determined in accordance with the actual situation. Calculation of weight factor*:* The weight factor α is important for the weighted average value of $T_i^{j,o}$. Assume the number of interactions between node *i* and node *j* is $\alpha(i, j)$ **.** Then we can calculate weight factor as:

$$\alpha = \frac{\delta(i,j)}{\sum_{j \in N_i} \delta(i,j)} \quad (9)$$

Where $(\sum \delta(i,j) \neq 0)$ if it is equal to 0, it means that there is no interaction between nodes). Obviously, the more $\delta(i, j)$ is, the larger α is. It shows that node *i* and node *j* have close relations, so the calculation of trust value should prefer relying on the direct observation.

Therefore nodes find out behavior of their neighbors after estimating trust value about them. We define the threshold of trust value T_0 it depends on network application; if network application is confidential then we let $(T_0 \rangle\rangle 0.5)$ otherwise $(T_0 = 0.5)$. When node *i* want to forward packets via its neighbor, at first look at T_j^i .in its information memory base and choose node *j* that has the most trust value. So selfish or malicious node be denied of network services. Described trust evaluation process is

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

classified into three phases: initial phase, update phase and reestablish phase (Wang *et al*., 2008). In this paper introduce initialization phase: when node *i* enter MANET for the first time, it should evaluate the trust value of all neighbors. This process is called trust relationship initialization. Before initialization, the information base of node *i* is empty. First, node *i* discovers all neighbors by broadcasting *hello* request within one-hop range. After that, node *i* evaluates the trust value of the neighbors using the equation (1) described in previous sections. So that, at this time in the first of initialization phase, node *i* has not any history information about its neighbors.

Initialization of Trust Relationship Algorithm

Step 1: Update the neighbor set *Ni*;

1.1 Node *i* send *hello (i)* massage to the all nodes within its radio rang.

1.2 Node *j* which received the *hello(i),* sends the *reply(j)* to node *i* and add node *i* to its own neighbor set.

1.3 After a time delay node *i* according to received *reply(j)s* message makes N_i set.

Step 2: Update the trust value T_i^j.

2.1 Node *i* plays game with neighbor node *j* and calculates $T_i^{j,g}$ and U_i^j.

2.2 Read the history records about node *j* and calculates $T_i^{j,o}$

2.3 Integrate the trust values T_i^j.

Step 3: Update the information base.

In this section we apply trust establishment relationship phase, therefore nodes can have an estimate of their neighbors' behavior. So if node be malicious or selfish then its neighbors estimate low trust value about it and it is denied of network services or is removed. But if malicious or selfish node has important role in network, for example bridge or gateway, we couldn't remove it, since losing it will cause a partition in the network and nodes will not be able to communicate between the clusters. Therefore in the next section, we proposed cluster head-IDS election scheme to always examine behavior of malicious or selfish node.

Our cluster head election phase

Related work: In the most of existing researches work on the election cluster head in MANET, the election process can be based on one of the following models: Random (Huang & Lee, 2003), in this model each node is equally likely to be elected regardless of its remaining resources and node's type. Connectivity index (Kachirski & Guha, 2003), in this approach elects a node with high degree of connectivity even though the node with both election schemes, some nodes will die faster than others, leading to a loss in connectivity and potentially the partition of network. Weight-based model (Mohammed *et al*., 2008), in this model elects a node with the most remaining resources without consider the type of node (selfish or malicious). Dagadeviren & Erciyes (2008) proposed a cluster based protocol to elect a cluster head in mobile ad hoc network. Mohammed *et al.* (2008) proposed design-based multi-cluster head election scheme. We investigated the advantages and disadvantages of last method and then improved the method proposed by Mohammed *et al*.(2008). In this approach authors consider appropriate criteria for electing the cluster head as most cost efficient and normal type and punish malicious node. To motivate nodes in behaving normally in every election round, they relate the detection service to nodes' reputation value.

The design of incentives is based on a classical mechanism design model, namely, Vickrey, Clarke, and Groves (VCG) (Otrok *et al.,* 2008). The model guarantees that truth-telling is always the dominant strategy for every node during each election. Authors justify the correctness of proposed method through analysis and simulation. Empirical results indicate that their mechanism can effectively improve the overall lifetime and effectiveness of IDSs in a MANET. Therefore, nodes behave normally during the cluster heads election mechanism. However, a malicious node can disrupt their election algorithm by claiming a fake low cost just to be elected as a cluster head. Once elected, the node does not provide IDS services, which eases the job of intruders. To catch and punish a misbehaving cluster head who does not serve others after being elected, authors have proposed a decentralized catch-and-punish mechanism using random checker nodes to monitor the behavior of the cluster head. To improve the performance and reduce the false positive rate of checkers in catching the misbehaving cluster head, they have also formulated a cooperative game-theoretical model to efficiently catch and punish misbehaving cluster heads with less false positive rates. This scheme can certainly be applied to thwart malicious nodes by catching and excluding them from the network. However, this method considers appropriate criteria for electing the cluster head but increases overhead on the network. In this paper we use trust value of each node for estimating node's behavior in cluster head election process. We improve the scheme that proposed by Mohammed *et al.* (2008) with establishment trust relationship between neighboring nodes instead of using VCG and checkers node in cluster head electing. We assume that every node knows its neighbors, and their trust value. Which is reasonable since nodes usually have information based storage about their neighbors for routing purposes.

Our proposed election algorithm two features intended for cluster head: First, cluster head should has maximum energy because it must serve to its cluster members and if it hasn't maximum energy, the election process at small intervals is repeated, this lead to each node consumes amount of its energy to participate in election process and consequently reduce the network life time. Second cluster head should be honest node with normal behavior we consider this feature in prior phase

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

through perform Bayesian game between neighboring nodes and cluster head should has high trust value view of its cluster members.

In this algorithm we consider tradeoff between security and network life time, that means in election process it may occurs that one node has maximum energy but it hasn't high trust value or vice versa. In this situation, each node uncertain to vote for a node with maximum energy or the node that has high trust value. To solve this problem we introduce a select function denoted by $F_{select}(i)$, node *i* in election algorithm vote to node *j* if node *j* maximize. $F_{select}(i)$,and defined it as follows:

$$F_{select}(i) = MT_i^j + N\lambda_j \qquad j \in N_i \qquad (10)$$

M is security factor on [0, 1] reflects the priorities of security and importance of being an honest cluster head in the network. In the normal networks with normal security $M = 0.5$ and whatever the network services is crucial thus we increase M.

T_i^j denotes the trust value of node *i* on node *j.*

N is life time factor on [0, 1] reflects *the priorities of* network life time. Normally $N = 0.5$. Therefore it can be adjusted to suit and more within the network is deployed.

λ_j is useful energy that initially node *j* at election algorithm announce it to its neighbors and computed as follows:

$$\lambda_j = \frac{E_j}{nt_j} \qquad (11)$$

Where E_j is remaining energy node *j* also we consider E_{IDS} is used to express the energy needed to run the IDS for one time slot. And must $E_j > E_{IDS}$ then node *j* computes λ_j Each node *j* a number of expected alive slots, denoted by nt_j.

N_i is the set of all neighbors of node *i.*

In this algorithm we assume that the cost of analyze for each node *i* is fixed and equal to one. Thus node *i* vote node *j* if maximize $F_{select}(i)$**.** *The elected cluster head* samples the incoming packets for a target node based on a sampling budget determined through that target node's reputation for intrusion detection*.*

We recall that, before propose cluster head election algorithm in MANET must establish trust relationship between nodes in order that reconnoiter selfish or malicious node. After a period of a lifetime network we can apply Trust establishment relationship and cluster head election mechanism at the same time.

To start a new election, the protocol uses four types of messages. Begin-Election, used by every node to initiate the election process; *Hello*, used to announce the cost of a node; *Vote*, sent by every node to elect a cluster head; *Acknowledge*, sent by the cluster head to broadcast its payment, and also as a confirmation of its cluster headship. For describing the protocol, we need the following notations:

Service-table (k): The list of all ordinary nodes, those voted for the cluster head node *k*. *reputation-table (k)*: The reputation table of node *k*. Each node keeps the record of reputation of all other nodes. *Neighbors (k)*: The set of node *k*'s neighbors. *Cluster head node (k)*: The ID of node *k*'s cluster head. If node *k* is running its own IDS then the variable contains *k*. *Cluster head (k)*: a boolean variable and set to TRUE if node *k* is a cluster head. Otherwise it is FALSE. Each node has information base memory to save its properties and neighbor trust value.

Cluster head election algorithm

Initially, all nodes start the election procedure by sending Begin−Election $(H(k,\lambda_k))$ messages. This message contains the hash value of its unique identifier (*ID*) and useful energy. This message is circulated among two hops of every node. On receiving the Begin−Election from all neighbors, each node sends its respective useful energy. Each node *k* checks whether it has received all the hash values from its neighbors. Then it sends Hello (ID_k, λ_k).

Step 0: For all nodes participate in cluster head election*.* If the number of nodes in *MANET is M*

For (k=1 to k=m)

{

If ($E_k > E_{IDS}$)

{

$$\lambda_k = \frac{E_k}{nt_k}$$

Else

$\lambda_{k=0}$

}

}.

Step 1: For all nodes participate in cluster head election when receive '*Begin Election'.*

1.1 If (received '*Begin-Election*' from all neighbors)

{

Send *Hello* (ID_k, λ_k)

}.

Upon receiving the *Hello* from a neighbor node *n*, first node *k* finds out $T_k^j > T_0$ if this condition is true then node *k* calculates the maximum value of $F_{select}()$ among its neighbors. T_0 is threshold of node's trust value in the network and depends on network application.

Step2: executed by every node

For ($i = 1$ to $i \le |N_k|$ && $n_i \in N_k$)

{

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

If ($T_k^i > T_0$)

{

$F_{select}(k) = MT_k^i + N\lambda_i$

If (node *i* has maximum value for $F_{select}(k)$ && unmark (node *i*)

{

Send *Vote (k, i)*;

Cluster head node (k) =i;

}

Else

Mark (node *i*)

}

}.

The elected node *i* sends an *Acknowledge* message to all the serving nodes. The *Acknowledge* message contains all the votes the cluster head received. The cluster head then launches its IDS.

Step 3 : executed by elected cluster head node

For ($i = 1$ to $i \le |N_k|$ && $n_i \in N_k$)

{

Send *Acknowledge (k)*

Cluster head (k):= TRUE;

Update *service−table* (*k*);

}

By this election algorithm we are sure cluster head be trustee and has enough remaining resource without we use VCG mechanism for incentive nodes to participate in election process and checkers node to punish malicious node.

Detection external intruder by cluster head phase

In this phase of our method, for detecting external intruder by cluster head, we use the method that proposed by Otrok *et al*. (2008), because they formalize the tradeoff between security and IDS resource consumption as nonzero-sum, non cooperative game between cluster head and intruder with complete information about cluster head. As a result of game, cluster head IDS find out the threshold that if probability of attack exceed threshold then notify to victim node to launch its own IDS. Game guides intruder to attack once the probability of stepping into the perfect mode is low. The game will be repeated such that in every election round the cluster head-IDS will be monitoring via sampling the protected node's incoming traffic and deciding according to the game solution whether to inform the victim node to launch its IDS or not.

In previous sections we discuss about trust establishment relationship in MANET and then proposed our cluster head election scheme. Now, we consider a MANET that nodes cooperate with each other without threat of internal intruder and they elect a low cost trustee cluster head in the their cluster to detect external intruders. In order to detect an intrusion, the cluster head-IDS samples the incoming packets for a target node based on a sampling budget determined through that target node's reputation. Once the probability of attack goes beyond a threshold, the cluster head-IDS will notify the victim node to launch its own IDS.

First we introduce details of game then propose solution of game based on (Otrok *et al*., 2008). Each player has private information about his/her preferences. In our case, the cluster head-IDS type is known to all the players while the external node type is selected from the type set: $\theta = \{Malicious(M), Normal(N)\}$. And we have the intruder's pure strategy as $A_{\text{int ruder}} = \{Attack, Not - Attack\}$. On the other hand, cluster head-IDS strategy is selected from the strategy space $A_{IDS} = \{Perfect, Normal\}$. Knowing that the external node type is a private information.

Bayesian Equilibrium dictates that sender's action depends on his/her type θ. By observing the behavior of the sender at time t_k , the cluster head-IDS can calculate the posterior belief evaluation function

$$\mu_{t_{k+1}}(\theta_i|a_i) . = \frac{\mu_{t_k}(\theta_i)P_{t_k}(a_i|\theta_i)}{\sum_{\theta_i \in \theta} \mu_{t_k}(\theta_i)P_{t_k}(a_i|\theta_i)} \qquad (12)$$

where $\mu_{t_k}(\theta_i) > 0$ and $P_{t_k}(a_i|\theta_i)$ is the probability that strategy a_i is observed at this phase of the game given the type θ of the node *i.* It is computed as follows:

$$P_{t_k}(Attack|\theta_i = M) = E_m O + F_m(1-O) \qquad (13)$$

$$P_{t_k}(Attack|\theta_i = N = F_m) \qquad (14)$$

where O is the probability of attack determined by the IDS. F_m is the false rate generated by the cluster head-IDS due to sampling and E_m is the expected detection rate via sampling in normal mode. We can show Competition between the cluster head-IDS and external intruder in this game as Table 1.

Table 1. Normal to perfect game

Strategy	*Normal*	*Perfect*
Attack	$\overline{E_m}V - C_a$; $E_mV - C_m$	$\overline{E_r}V - C_a$; $E_rV - C_r$
Not -Attack	*0 ;-C_m*	*0 ; -C_r*

By solving this game using pure strategy, there is no Nash equilibrium. Thus, mixed strategy is used to solve the game where *q* is the probability to run in perfect mode and *p* is the probability to attack by the attacker. In Table 1, the game is defined where the utility function of the IDS by playing the *Perfect* strategy while the attacker plays the *Attack* strategy is defined as $E_rV - C_r$ It represents the payoff of protecting the monitored node, which values V , from being compromised by the attacker, where

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

$E_r V >> C_r$. On the other hand, the payoff of the attacker if the intrusion is not detected is defined as $\overline{E_r} V - C_a$. It is considered as the gain of the attacker for compromising the victim node. Additionally, they define $E_m V - C_m$ as the payoff of IDS, if strategy *Normal* is played while the attacker strategy remains unchanged. Conversely, the payoff of the attacker if the intrusion is not detected is defined as $\overline{E_m} V - C_a$. Now, if the attacker plays *Not-Attack* strategy and the IDS strategy is *Perfect* then the losses of the IDS is C_r while the attacker gains/losses nothing. Moreover, the payoff of the attacker with the same strategy and IDS strategy is *Normal* is 0 while the losses of the IDS is defined as C_m which is the cost of running the IDS in normal mode. Where, $\overline{E_r} = 1 - E_r$, and E_r is the expected detection of an intrusion in the perfect mode. $E_r = E_{clusterhead} + E_{victim}$, where $E_{clusterhead}$ and E_{victim} are the expected detection by cluster head-IDS and monitored node (victim) respectively. $E_m = E_{clusterhesd}$ is the expected detection in the normal mode; so that only the cluster head-*IDS* is running the IDS to detect intrusions. On the other hand, $\overline{E_m}$ $\overline{Em}$ is equal to $1 - E_m$. C_r is the cost of running the IDS in perfect mode. We define the cost as the aggregation of the cost of monitoring by the cluster head $C_{ckusterhead}$ and cost of monitoring by the victim C_{victim}. C_m is the cost of running the IDS in normal mode which is equal to *Ccluster head*. C_a is the cost of attack by the intruder. V is the value of the protected victim node (asset). The value of V could vary from one node to another according to its role in the cluster. For example, gateway nodes are valued more than regular nodes.

To solve the game and find the optimal values of p and q, the IDS and attacker compute their corresponding utility functions followed by the first derivative of the functions. From Table 1 the IDS utility function U_{IDS} is defined as follows:

$$U_{IDS} = [qp(E_r - C_r) + p(1-q)(E_m V - C_m) - q(1-p)C_r - (1-q)(1-p)C_m]\mu(\theta = M) - [qC_r + (1-q)C_m](1 - \mu(\theta = M)) \quad (15)$$

The main objective of the IDS is to maximize this utility function by choosing for a fixed p^*, a q^* strategy that maximizes the probability of protecting the victim node and leads to equilibrium where the following holds:

$$U_{IDS}(p^*, q^*) \geq U_{IDS}(p^*, q) \quad (16)$$

To attain this aim, the IDS will calculate the optimal value of p^* by finding the first derivative with respect to q^* and setting it to zero. This will result to the following:

$$p^* = \frac{C_{victim}}{\mu v E_{victim}} \quad (17)$$

The value of p^* is used by the cluster head-IDS to decide whether to inform the victim node to launch its own IDS or not. Knowing that the cluster head-*IDS* is monitoring and analyzing traffic via sampling to detect an intrusion launched by an external attacker *i*. The IDS is computing the belief μ, as in Equation (8); each node to check whether it is behaving maliciously or normally. If the sender type is *malicious* and decided to attack by launching an intrusion the expected probability to be detected by cluster head-*IDS* is $E_{clusterhead}$. Since the intrusion could be launched iteratively and could be missed in the coming iterations, the IDS will decide to inform the victim node to launch its own IDS if the probability of attack is greater than p^*. On the other hand, the utility function U_a of the attacker is defined as follows:

$$U_a = qp(\overline{E_r} V - C_a) + p(1-q)(\overline{E_m} V - C_a) \quad (18)$$

The main objective of the attacker is to maximize this utility function by choosing for a fixed q^*, a p^* that maximizes the probability of compromising the victim node .To maximize the utility function, it is sufficient to set the first derivative with respect to p^* to zero which will be equal to:

$$q^* = \frac{\overline{E_{clusterhead}} V - C_a}{V E_{victim}} \quad (19)$$

From the solution of the game, the attacker best strategy is to attack once the probability of running the IDS by the victim node (perfect mode) is less than q^*. To achieve this, the attacker will observe the behavior of the IDS at time t_k to determine whether to attack or not at time t_{k+1} by comparing its estimated observation with the derived threshold. In this paper, three phases order to be implemented namely trust establishment relationship between neighboring node, election cluster head and detection external intruder, increase security, performance and reduce resource consumption for intrusion detection.

Summary and conclusions

In this paper, we proposed hybrid internal and external intrusion detection by using game theory approaches. Our hybrid method has three phases. In the first phase, neighboring nodes participate in the game and each node observes treat neighbors then estimates a trust value for them. If the estimated trust value of a node be less than a threshold, then it is detected as a misbehaving node, this way we prevent internal intrusion. In the second

Indian Journal of Science and Technology Vol. 5 No. 2 (Feb 2012) ISSN: 0974- 6846

phase, we hold cluster head election, this elected cluster head is ideal because it isn't misbehaving node and it has enough energy resource for intrusions detection in its cluster and lead to increase the network life time; and also has the lowest cost for packet analyzing. Due to being mobile nodes after passing a time period from the beginning of the network function, can run both Trust Establishment Relationship algorithm and Cluster head Election algorithm synchronously. In the last phase for detecting external intrusion with minimum cost we introduced a game between cluster head and external intruder based (Otrok *et al*., 2008). It is clear, in the first phase if misbehaving node, that has low trust value (selfish or malicious) is a connecting bridge between different parts of the network, we cannot remove it, but this node should be always monitored by cluster head in order to intrusion detection. All of all this method increase performance and security in mobile ad hoc network.

Time-frequency analysis based on a selected deconvolution technique was applied to biomedical signals for normal and abnormal subjects. The results obtained using this procedure provided a high resolution in time as well as in frequency. The disadvantage of the iterative deconvolution method is the time required to calculate the desired time frequency representation particularly with long duration test signals. The main advantage of this method is the ability to reveal the non-stationary behavior of this type of waves and detect any transits especially in the case of abnormal subjects, due to the two dimensional representation. Consequently, this method can be helpful in this particular field such as diagnosis of possible heart problems or in sleep scoring used to detect brain abnormalities.

References

1. Agah A and Das K (2007) Preventing DoS attacks in wireless sensornetworks: a repeated game theory approach. *Intl. J. Network Security.* 5, 145-153.
2. Capra L (2004) Toward a human trust model for mobile ad-hoc networks. *Proce. 2nd UK-UbiNet Workshop*. *Cambridge Univ.*
3. Dagadeviren O and Erciyes K (2008) A Hierarchical cluster head election protocol for mobile ad hoc network**.** *Lect. Notes in Comput. Sci.* pp: 509-518.
4. Eschenauer L, Gligor V and Baras J (2002) Trust establishment in mobile ad-hoc networks. MS. *Thesis.* University of Maryland Cambridge.
5. Ganchev A, Narayanan L and Shende S (2008) Games to induce specified equilibria. *Elsevier Theoretical Comput. Sci*. 409, 341-350.
6. Garcı´a-Teodoroa p, Dı´az-Verdejoa J, Macia´-Ferna´ndeza G and Va´zquezb E (2009) Anomaly-based network intrusion detection: *Techniques, Sys. & Challenges*. Elsevier. 28,18-28.
7. Hu Y and Perrig A (2004) A survey of secure wireless ad hoc routing. *IEEE Security &d Privacy*. 2, 28-39.
8. Huang Y and Lee W (2003) A cooperative intrusion detection system for ad hoc networks. *ACM Workshop Security of ad hoc & Sensor Network.*
9. Jiang X, Lin C, Yin H, Chen Z and Su L (2009) Game-based trust establishment for mobile ad hoc networks. *IEEE Intl. Conf. Commun. & Mobile Comput.,* CMC. pp: 475-479.
10. Kachirski O and Guha R (2003) Effective intrusion detection using multi sensors in wireless ad hoc networks. *Intl. Conf. Sys. Sci.* 8**.**
11. Kodialam M and LakshmanT (2003) detecting network intrusions via sampling:agame theoretic approach*. IEEE Comput. & Commun.* INFOCOM. pp: 1880-1889.
12. Kuchaki Rafsanjani M (2009) Evaluating intrusion detection system and comparison of intrusion detection and detecting misbehaving nodes for MANET. *Advanced Technologies*. Ch.6. Kankesu Jayanthakumaran (Ed.). In-Teh. Croatia. 91-104.
13. Lima M, Santos A and Pujolle G (2009) A survey of survivability in mobile ad hoc networks. IEEE *Commun. Sur. & Tutorials.* 11, 66-77.
14. Liu P and zang W (2005) Incentive based modeling and inference of attacker intent, objectives, and strategies*. J. ACM Trans. Info. & Sys. Security (TISSEC)*. 8,1-41.
15. Marchang N and Tripathi R (2007) A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks. *Intl. Conf. Advanced Comput. & Commun.* pp: 460-464.
16. Mitrokotsa A, Komninos N and Douligeris C (2007) Intrusion detection with neural network and watermarking Techniques for MANET. *IEEE Conf. Turkey*. pp: 118-127.
17. Mohammed N, Otrok H, Wang L, Debbabi M and Bhattacharya P (2008) A mechanism design-based multi-cluster head election scheme for Intrusion detection in manet. *IEEE Trans. Dependable & Secure Comput.* pp: 89-103.
18. Morris P (1994) introduction to game theory. Springer. 1*st* edition.
19. Otrok H, Mohammed N, Wang L, Debbabi M and Bhattacharya P (2008) A moderate to robust game theoretical model for intrusion detection in manets. *IEEE Intl. Conf. Wireless & Mobile Comput. Networking & Commun.* WIMOB. pp: 608-612.
20. Otrok H, Mohammed N, Wang L, Debbabi M and Bhattacharya P (2008) A game-theoretic intrusion detection model for mobile ad hoc networks. Elsevier. *Algorithmic & Theoretical Aspects of Wireless ad hoc & Sensor Networks.* 31, 708-721.
21. Patcha A and Park J (2006) A game theoretic formulation for intrusion detection in mobile ad hoc networks*. Intl. J. Network Security.* 2,131-137.
22. Poongothai T and Jayarajan K (2008) A noncooperative game approach for intrusion detection in mobile ad hoc networks. *IEEE Comput. Commun. & Networking*. pp:1-4.
23. Ren K, Li T, Wan Z, Bao FR, Deng R and Kim K (2004) Highly reliable trust establishment scheme in ad hoc networks. Elsevier. *Comput. Networks*. 45, 687-699.
24. Seshadri K, Ramana A andKasiviswanth N (2010) A survey on trust management for mobile ad hoc networks. *Intl. J. Network Security & Its Appl.*(IJNSA). 2, 75-85.
25. Wang K, Wu M and Shen S (2008) A trust evaluation method for node cooperation in mobile ad hoc networks. *IEEE Conf. Information Technol.* pp: 1000-1005.