GAME THEORETIC AND INTRUSION DETECTION SYSTEM IN HETEROGENEOUS NETWORK

T.Ajith kumar[1], T.Dhivakaran[2], R.Ishwarya[3], Dr.R.Gopinath[4]
[1,2,3,4]Dept. of Computer Science and, Engineering, K.S.Rangasamy College of Technology
Tiruchengode, India
[1]tmajithkumar1997@gmail.com, [2]dhivajith35@gmail.com, [3]ishwaryabalaji4@gmail.com,
[4]gopinath@ksrct.ac.in

ABSTRACT

Mobile Ad Hoc Networks (MANET) are infrastructure-less wireless network containing self-configuring mobile nodes that forms a dynamic network topology. Due to dynamic network topology, Intrusion Detection Systems (IDS) are implemented in MANET to detect the malicious activity of mobile nodes. This in turn makes the IDS to remain active all the time that increases costly overhead for battery powered and energy consumption of nodes in the network. Thus a probabilistic model is proposed which makes use of cooperation between IDS among neighborhood nodes to reduce their individual active time. The existing scheme is used in Homogeneous network for simulation which consists of same capacity nodes that have effective energy consumption. The proposed approach is used to implement the game theory used to avoid the hacker's node and by extracting the nodes we find the inactive nodes also. Hence, by using the approach of game theory in heterogeneous network to reduce transmit power and flexible deployment of nodes in dense areas.

1 INTRODUCTION

1.1 MOBILE AD HOC NETWORK (MANET)

Mobile Ad Hoc Network (MANET) is a wireless ad hoc network which can change location and configure itself automatically. The vehicle data is measured including the traffic conditions and kept track of trucking fleets. The MANETs are not more secure due to their dynamic nature so it is very important to be alert what data is sent over a MANET.

The MANET is an independent system so the mobile hosts are connected to wireless links and can move randomly.

1.1.1 Types of MANET

The MANET has several types which includes,

1. Intelligent Vehicular ad hoc networks (INVANETs) which are used in artificial intelligence to handle unexpected situation such as vehicle collision and accidents.
2. VANET enables effective communication with another vehicle or help the vehicle to communicate with roadside equipment's.
3. Internet Based Mobile Ad hoc Networks (iMANET) are used to fix link between mobile nodes.

1.1.2 Characteristics of MANET

The MANET has several characteristics which include,

1. The each node in the MANET, acts as both host and router so that it is autonomous in behaviour.
2. Multi hop radio relying is used when a source node and destination node is out of the radio range. MANETs have the ability of multi hop routing. MANET has no Centralized firewalls for security, which makes routing and host configuration as distributed in nature.

1.1.3 Features of MANET

In MANET each terminal is an autonomous node which may act as both Host and a router. On the other hand the basic processing ability is a host and each node performs switching function as a router. So generally the end points and switches are different in MANET.

1. Distributed operation

Since the MANET has no backbone network to control the entire network, which is distributed among the terminals. Each node in MANET should perform together amongst themselves and each node acts as a relay as wanted, to enforce features e.g. security and routing.

2. Multihop routing

The standard ad hoc routing algorithms are single hop but multihop is based on different link layer entities and routing protocols. The single hop MANET is simpler than multihop via structure and implementation with less cost and features. When delivering the data packets from source to destination through the direct wireless transmission range, the packets should be transmitted through one or more intermediate nodes.

3. Dynamic network topology

Since the nodes are mobile, the network topology may vary rapidly and unpredictably and the connectivity within the terminals changes with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. Each mobile node in the network dynamically creates the routing amongst themselves as they move about, forming their own network. Furthermore each user in MANET may not cooperate within the network but may need access to a public standard networks like internet.

1.1.4 MANET Challenges

The MANET environment is required to solve certain issues of limitation and inefficiency which includes,

1. The characteristics of wireless links are time varied in nature

There is transmission obstacle such as fading, path loss, blockage and interference that includes the susceptible nature of wireless channels. The reliability of wireless transmission is restricted by several factors.

2. Limited range of wireless transmission

The radio bond has minimum data rates compared to the wireless networks. Since the optimal usage of bandwidth is to be maintained with low overhead as possible.

3. Packet losses are occurs if transmission contain errors

MANETs faces high packet loss because of the errors in transmission such as hidden terminals that outcome in collisions, wireless channel issues such as high Bit Error Rate (BER), inference, frequent breakage in paths origin by mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links.

1.2 Routing Protocols in MANET

Several protocols are used in MANET. Routing protocols can be classified into three types such as Proactive, Reactive routing protocol and hybrid protocols. The routing protocol in MANET efficiently handles more number of nodes with restricted resources. The major problem in routing protocol is disappearing or appearing of the nodes in several places. It is mainly reduces the routing message overhead despite of the growing number mobile nodes. Another major problem is maintaining the size of routing table small and if the size of the routing protocol is large, then it can affect the control packet transferred in the network.

The routing protocol is classified on the basis of how and what time the routes are discovered, since both pick the shortest path to the destination.

1. Proactive Routing Protocols

Proactive routing protocols are used in link state Routing algorithms, which flood link data about the neighbors frequently. Proactive routing protocol stores the routing data and manages the information up to date by exchanging the control packet from their neighbors. Examples of proactive routing protocols are Destination-Sequenced Distance Vectoring (DSDV), Optimized Link State Routing (OLSR) and Wireless Routing Protocol (WRP) etc.

2. Reactive Routing Protocols

Reactive routing protocol reduces the overheads that are present in proactive protocols. It uses distance vector routing algorithm and enhances the route to given destination, only when a node request it by initiating the route discovery process. More number of reactive protocols are available in MANET such as Demand Signal Repository (DSR), Ad Hoc On-Demand Vector (AODV), Temporally Ordered Routing Algorithm (TORA) and Lan Modem Riser (LMR) etc.

3. Hybrid Routing Protocols

The combinations of reactive and proactive routing protocols are called as hybrid

routing protocols. Some of the hybrid routing protocols are Zone Routing Protocol (ZRP), Border Gateway Protocol (BGP) and Enhanced Interior Gateway Protocol (EIGRP).

1.3 Security in MANET

The MANET has very less physical security. Attacks are of two types, active attacks and passive attacks. The common type of attack is passive attack, which include eavesdropping and information disclosure. The active attacks contain Denial of service, Data modification by viruses like Trojans and worms. The more specific problems in MANET are vulnerability of channels and nodes, Byzantine black hole and Byzantine wormhole attack. The security issues may inject erroneous routing data and diverting network traffic thus making routing inefficient. There are many methods to minimize the effect of these attacks which include secure routing using public and private key to get a certified authority and use of digital signatures and prior trust relationships. The limitation of the system is that the prior trust require to be placed before the network is constructed, which is not possible in disaster affected areas.

Similar to other wireless networks, ad hoc network attacks are categorized into routing, multipart and performance. The routing attacks include Wormhole attack, Black hole attack, Byzantine attack, Resource consumption attack, IP Spoofing attack, State Pollution attack and Sybil attack etc.

1.4 Intrusion Detection System

Many historical events have shown that intrusion prevention techniques like encryption and authentication, which are usually the first line of defense, are not sufficient in protecting the network. As the system become more complex as well as there is more weakness, which leads to more security issues. The intrusion detection can be used as second wall of defense to protect the network from such problems. If the intrusion is detected, a response time can be initiated to restrict or reduce damage to the system. The intrusion detection system can be categorized based on audit data which is either host based or network based. A network based IDS captures and analyses the packets from network traffic while a host based IDS uses operating system or application logs in its analysis.

Depends on the detection technique, the IDS is categorized into three categories as follows,

1. Anomaly detection systems

The normal profiles or normal behaviours of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response.

2. Misuse detection systems

The system keeps patterns or signatures of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion. Like a virus detection system, it cannot detect new kinds of attacks.

3. Specification-based detection

The system defines a set of constraints that describe the correct operation of a program or protocol. Then it monitors the execution of the program with respect to the defined constraints.

1.4.1 Architecture for Intrusion Detection in MANETs

Intrusion detection and response systems are distributed and cooperative to suit the needs of mobile ad-hoc networks. In the IDS architecture every node in the mobile ad-hoc network participates in intrusion detection and response.

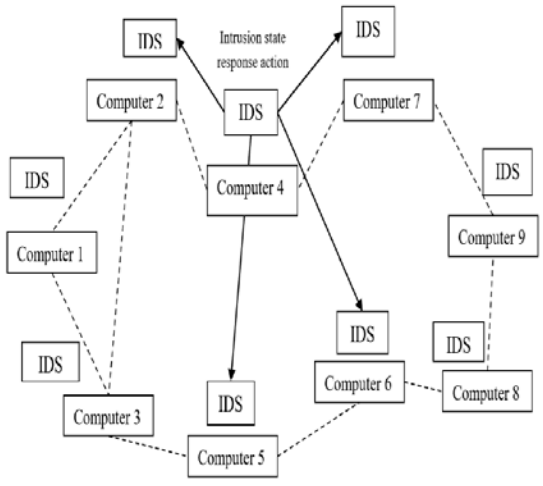

Figure 1.1 Architecture of IDS in MANET

Each node is managed the detecting signs of intrusion locally and independently, but neighboring nodes can collaboratively

investigate in a broader range as represent in Figure 1.1.

1.4.2 Intrusion Detection Techniques

An intrusion is a set of actions that compromises confidentiality, availability, and integrity of a system. Intrusion detection is a security technology that analysis to identify those who tried to break in and misuse a system without authorization and those who have legitimate access to the system but abuse their privileges. The system may be a host computer, network equipment, a firewall, a router, a corporate network, or any information system being monitored by an IDS.

An IDS dynamically monitors a system and user actions in the system to detect intrusions. Because an information system is suffered from several types of security vulnerabilities, it is both technically difficult and economically costly to construct and manage a system that is not susceptible to attacks. Experience teaches us never to rely on a single defensive technique. The IDS by analyzing the system and user operations, in search of undesirable and suspicious activities, may effectively monitor and protect threats.

1.5 Problem Statement

The problems considered for the research work are listed as follows,

1. Homogeneous network was difficult to remove from the products for reuse.
2. High transmit power.
3. Data speed was low.

1.6 Objectives

The objectives of the research work can be structured as follows,

1. To enhance the user data rate near the access point.
2. To improve the data speeds.
3. To achieve flexible deployment in dense area.
4. To decrease the transmit power.

2 PROPOSED SYSTEM

The minimization of the active duration of the IDS in the nodes of a MANET as an optimization problem is presented. After that, a cooperative game model is described to represent the interactions between the IDS in neighbor nodes. The game is defined to monitoring the neighbor nodes at a desired security level in order to detect any anomalous behavior and conserve as much energy as possible. Each of the nodes has to participate cooperatively in monitoring its neighbor nodes with a minimum probability. In addition, a distributed scheme is developed to determine the ideal probability with which each node has to remain active so that all the nodes of the network are monitored with a desired security level. The proposed approach, heterogeneous network is used to reduce transmit power and flexible deployment in dense areas.

2.1 Efficient Usage of IDSs as an Optimization Problem

The efficient usage of IDS can be solved in two phases: First, the problem from the point of view of a node being monitored by its one-hop neighbors. Optimization problems are presented for the same and analyzed using game theory. Second, The problem from the point of view of a node which monitors its neighbors. The solution used to the optimization problem to arrive an efficient distributed algorithm which every node in the network is employed. More importantly, the neighbors spend their valuable computational resources and energy while monitoring node all the time. It may not be required to keep the IDS running on each node all the time. The redundancy, thereby saving the afore-mentioned resources.

Further, there is no assumptions about the detection rate of the IDS. The detection rate and false detection rate of an IDS depends on factors such as the design of the IDS and how the afore-mentioned characteristics affect the effectiveness of the IDS. The work, do not focus on designing IDS but present a scheme for its efficient usage. The number of IDSs actively monitoring the neighborhood may depend upon the level of security which is needed in there. The security level is defined as follows: A security level of l means that a node is monitored by at least l of its neighbors at any instant of time. The security level also provides a trade-off between security and energy consumption. The higher the security level, the more is the number of neighbors that monitor a node at a time, which results in higher energy consumption.

Assume that a node a has k neighbors (IDSs) at a particular instant. Each neighbor is monitored independently with a probability of p. The probability that node a is monitored at security level l as follows in equation (1),

$$P(l/k) = \sum_{i=1}^{k} \binom{k}{i} p^i (1-p)^{k-i}$$

An optimization problem as follow,

$$Minimize\ p$$

$$\mathbf{TV} \leq \sum_{j=s}^{m} \binom{m}{j} p^i (1-p)^{m-j} \quad (1)$$

2.2 A Game Theoretic Analysis of IDSs Usage in a Network

The solution to the optimization problem must be profitable from the point of cooperating IDS. In other words, the energy saving achieved by the approach should be in equilibrium. A cooperative game model to represent the interactions between the neighbor nodes. Each player's (IDS's) objective is to monitor the nodes in its neighborhood at the desired security level in order to detect any malicious activity. Another objective is to conserve energy. Here, The first objective as the primary goal and the second one as the secondary goal. If the second objective is saving the battery power, then in the main objective each node would independently decide to sleep all the time resulting in totally inactive IDS. Since the nodes are independent, they have to cooperate to achieve the above goals. According to, cooperative game theory analyses in these situations the participants' objectives are partially cooperative and partially conflicting. Thus the scenario can be modelled as an n-player cooperative game.

A coalitional (cooperative) game with transferable utility (a TU game) is defined as a pair (N,v) where N is a set of players and v is a function that associates a real number $v(S)$ with each subset, $S\ of\ N$. $(\varphi) = 0$. If a coalition S forms, then it can divide its worth, (S) in any possible way among its members.

Now, to get a node monitored with the desired security level, each of its neighbors (IDSs) have to participate in monitoring the minimum probability solution of problem of (2). This can be modelled as an n-person cooperative TU game in the characteristic form denoted by $[N,]$, where $N = \{1, 2, 3, n\}$ is a set of players neighbors and v is a real-valued characteristic function on $2N$, the set of all subsets of N. Here v assigns a real value (S) to each subset, $S\ of\ N$, and $(\varphi) = 0$. Assuming that the energy consumption of the IDSs is linear,

$$v(S) = \begin{cases} s(1-p_s)E & if\ s \geq l \\ 0 & if\ s < l \end{cases} \quad (2)$$

In the equation, E = the energy consumed by an IDS if it monitors all the time, $s = |S|$,ps = the probability with which each player monitors solution of the optimization problem of equation 2 in a coalition consisting of s players, and l = security level. The utility of the game is the energy saved by a player. If $s \geq l$, the desired security level (l) can be achieved and thus the payoff $v(S) = s(1- ps)E$. Otherwise, the security level cannot be achieved and $v(S) = 0$. Note that the payoff of subset S depends on the cardinality $(|S|)$ of the subset and not on the identity of the players in the subset.

A solution to every cooperative game is given by the Shapley value of a player, i,

$$\varphi_i[v] = \sum_S \frac{(s-1)!(n-s)!}{n!}[v(S) - v(S-i)] \quad (3)$$

In the equation, n is the number of players, $s = |S|$ and the summation is taken over all subsets, $S\ of\ N$. In equation (3), since $[(S) - (S - i)] = 0$ if the player $i \notin S$, the summation is effectively taken over all subsets S of which player i is a member. The value of (S) depends on the cardinality $(s = |S|)$ of S. Therefore, the subsets depending on their cardinality and the summation is taken over these groups of subsets such that $s = 1$ to n. The number of subsets of size s of which player i is a member is given by $(n-1\ s-1)$. Thus, the Shapley value of player. It can be written as,

$$\varphi_i[v] = \sum_{s=1}^{n} \binom{n-1}{s-1} \frac{(s-1)!(n-s)!}{n!}[s(1-p_s) - (s-1)(1-p_s-1)]E$$

$$= \frac{E}{n}\sum_{s=1}^{n} 1 - sp_s + (s-1)p_{s-1}$$

$$= (1-p_n)E \quad (4)$$

In the equation (4), pn represents the probability with which each player monitors in the grand coalition consisting of all the n players.

2.2.1 THROUGHPUT

Throughput refers that the data transfer from one location to another in given amount of time. It is used to measure the energy consumption between the hacker nodes and inactive nodes as shown in the fig 2.2.1.

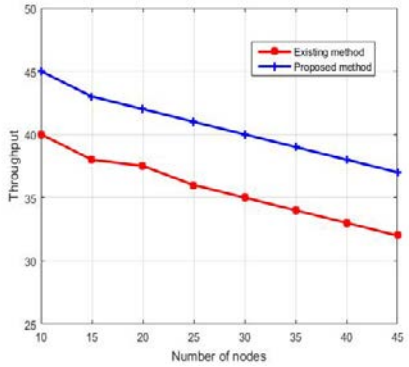

Fig 2.2.1 Throughput

2.2.2 PERFORMANCE EVALUATION

The connection established within its radio range will starts at the beginning of simulation and continues till the end without having any degradation has represented in Fig 2.2.2.

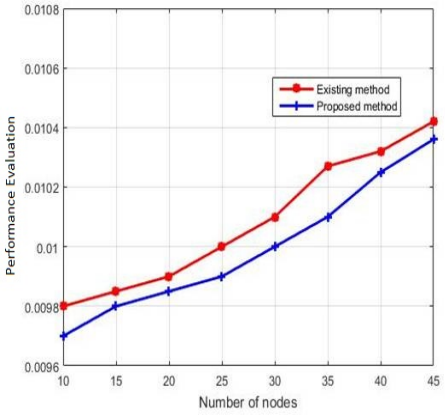

Fig 2.2.2 Graph of Performance Evaluation

2.3 The IDSs Usage Algorithm

The problem of efficient usage of IDS from the perspective of a node monitored by its neighbors. Next, the use of optimization problem as a building block and develop a distributed scheme for the IDSs. Every node employs this scheme to determine the ideal probability with which it's IDS has to remain active so that all nodes in the network are monitored with the desired security level. The mechanism employed by each node in the network to determine the minimum monitoring probability is represented by the simple algorithm, called Least Degree for K neighbor's algorithm (LDK), which stands for Least Degree for k. The LDK algorithm is illustrated pictorially. Each node (say M) initiates this algorithm to determine the probability with which it has to monitor its neighborhood. 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 is calculated. In addition, the message complexity of LDK algorithm and security level.

$$Minimize\ P$$

$$TV \leq \sum_{j=s}^{m} \binom{m}{j} p^{i}(1-p)^{m-j}$$

2.4 Advantages of Proposed System

1. Decrease the transmit power
2. Improve the user data rate near the access point
3. Faster data speeds

3 MODULE DESCRIPTION

3.1 GAME THEORY

Game theory is a branch of applied mathematics that uses models to study interactions with formalized incentive structures ("games"). It has applications in a variety of fields, including economics, international relations, evolutionary biology, political science, and military strategy. Game theory provides us with tools to study situations of/ conflict and cooperation. Such a situation exists when two or more decision makers who have different objectives act on the same system or share the same set of resources. Therefore, game theory is concerned with finding the best actions for individual decision makers in such situations and recognizing stable outcomes.

The total communication between each and every node and interaction of the heterogeneous network nodes has been

extracted and clearly represented by the figure 3.1

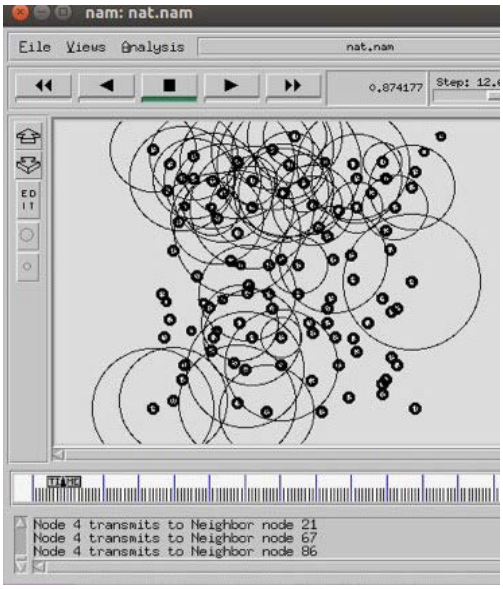

Fig 3.1 Communication between Nodes

3.2 INTRUSION DETECTION SYSTEM

The very nature of MANETs, dictates that any IDS designed for such a network has to be distributed in nature. Centralized solutions that have a single point of failure cannot be used. Assuming a host based IDS, An intrusion detection game played between a host and an intruder.

Game theoretic framework to analyses and model the response of an IDS. Examples of IDS response actions setting off an alarm, watching suspicious activity before setting off an alarm, and a total system reconfiguration.

The interaction between an attacker and a host based IDS as a two player signaling game which falls under the gambit of multi-stage dynamic no cooperative game with incomplete information.

In the intrusion detection game, the objective of the attacker to send a malicious message from attack node with 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. The 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 certainly that the message in nature.

3.3 MOBILE AD HOC NETWORK

A mobile ad hoc network is characterized by a distributed, dynamic, self-organizing architecture. Each nodes in the network is capable of independently adapting its operation based on the current environment according to predetermined algorithms and protocols. Analytical models to evaluate the performance of ad hoc networks have been scarce due to the distributed and dynamic nature of such networks. BGame theory offers a suite of tools that may be used effectively in modelling the interaction among independent nodes in an ad hoc network.

Mobile ad hoc network rely on the cooperation of participating nodes to route data between source and destination pairs that are outside each other's communication range. Because such data forwarding consumes valuable battery power, each node along the path has an inherent disincentive to cooperate. This tension between cooperation and cost invites a game-theoretic study, where each node must strategically decide the degree to which it must volunteer its resources for the common good of the network.

4 CONCLUSION

The minimization of the active duration of the IDSs in the nodes of a MANET is presented as an optimized problem. A cooperative game model is described to represent the interactions between the IDSs in the neighborhood nodes. The game is defined to monitor the nodes in its neighborhood at a desired security level in order to detect any anomalous behavior and conserve as much energy as possible. Each of the nodes has to participate cooperatively in monitoring its neighbor nodes with a minimum probability. Moreover, a distributed scheme is developed to determine the ideal probability with which each node has to remain active so that all the nodes of the network are monitored with a desired security level. Thus the heterogeneous network is used to reduce transmit power and enable flexible deployment in dense areas. The experimental results show that the proposed approach will provide better results in terms of optimized problem in MANET by using the IDSs and Game Theory

The future enhancement includes implementation of intrusion detection system that detects malicious nodes in ultra-dense heterogeneous network which has high data rate

that increases capacity and improves user experience.

"We acknowledge DST-File No.368. DST-Fist (SR/FIST/College-235/2014 dated 21-11-2014) for financial support and DBT-STAR-College-Scheme-ref.no: BT/HRD/11/09/2018 for providing infrastructure support."

REFERENCES

1. Alpcan T., Basar T.(2004),'A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection', IEEE Conference of Decision and Control, vol. 2, no. 6, pp. 2595-2600.
2. Andrea Lupia., Floriano De Rango,(2016), 'Trust Management using Probabilistic Energy-Aware Monitoring for Intrusion Detection in Mobile Ad_hoc Networks', in Proceeding of ACM/IEEE of Wireless Telecommunications Symposium, pp.1-6.
3. Asra Anjum T., Shaik Apsar Pasha R. (2015), 'A Brief View of Computer Network Topology for Data Communication and Networking' International Journal of Engineering Trends and Technology, vol. 22, no. 7, pp. 319-324.
4. Bouhaddi M., Radjef M.S., Adi K. (2014), 'An Efficient Intrusion Detection in Resource-Constrained Mobile Ad-Hoc Network', International Journal of Computer and Security, vol. 76, pp. 156-177.
5. R.G., Clayman S., Pavlou G., Mamatas L., Galis A. (2013),'On the Selection of Management/Monitoring Nodes in Highly Dynamic Networks', IEEE Transactions of Computers, vol. 62, no.6, pp. 1207-1220.
6. Gilles R.P., Owen G., van den Brink R.(1992),'Games with permission Structures: The conjunctive approach', International Journal of Game Theory, vol.20, no. 3, pp. 277-293.
7. Kiran Dhangar., Deepak Kulhare., Arif Khan. (2013), 'A Proposed Intrusion Detection System', International Journal of Computer Applications, vol. 65, no. 23, pp.46-50.
8. Krishnan D. (2015), 'A Distributed Self Adaptive Intrusion Detection System for Mobile Ad-hoc Networks using Tamper Evident Mobile Agents', International Journal of Procedia Computer Science, pp.1203-1208.
9. Li F., Yang Y., Wu J. (2010), 'Attack and Flee: Game-Theoretic-Based Analysis on Interactions Among Nodes in MANETs', IEEE Transactions Systems, vol. 40, no. 3, pp. 512-622.
10. Liu Y., Comaniciu C., Man H. (2006), 'Modelling Misbehaviour in Ad Hoc Networks: A Game Theoretic Approach for Intrusion Detection', International Journal of Security and Networks, vol. 1, no. 3, pp. 65 80.
11. Mohsin Ur Rahman Salfri. (2015), 'A Study of Mobile Ad-Hoc Networks - Issues and Challenges', in Proceeding of ACM/IEEE Explore, vol. 6, no. 7, pp. 93-96.
12. Partwardan A., Parker J., Joshi A., Iorga M., Karygiannis T. (2005), 'Secure Routing and Intrusion Detection in Ad Hoc Networks', IEEE explore of Pervasive Computing and Communications, pp. 1-9.
13. Patcha A., Park J. (2006), 'A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks', International Journal of Network Security, vol. 2, no. 2, pp. 131-137.
14. See-Kee Ng. Winston Seah W.G.K. (2010), 'Game-Theoretic Approach for Improving Cooperation in Wireless Multihop Networks', IEEE Transaction Systems, Man and Cybernetics-Part B: Cybernetics, vol. 40, no. 3, pp. 559-574.
15. Subba B., Biswas S., Karmakar S. (2016), 'Intrusion Detection in Mobile Ad-hoc Networks: Bayesian Game Gormulation', International Journal of Engineering Science and Technology, vol. 19, no.2, pp. 782–799