# A Taxonomy of Game Theory Approaches for Intrusion Detection in MANETs

Mohammad Masoud Javidi, Marjan Kuchaki Rafsanjani, Laya Aliahmadipour

Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran
Javidi@uk.ac.ir, kuchaki@uk.ac.ir

**Abstract:** MANETs are self configuring networks that are formed by a set of wireless mobile nodes and have neither fixed network infrastructure nor administrative support. Since transmission range of wireless network interfaces is limited, forwarding hosts may be needed each node in a wireless ad hoc network functions as both a host and a router, and the control of the network is distributed among the nodes. Due to their communication type and resources constraint, MANETs are vulnerable to diverse types of attacks and intrusions. Because of these, security is a critical issue. Network security is usually provided in the three phases: intrusion prevention, intrusion detection and intrusion tolerance phase. However, the network security problem is far from completely solved. Researchers have been exploring the applicability of game theoretic approaches to address the network security issues. This paper surveys the existing game theoretic solutions which are designed to enhance network security in the intrusion detection phase.

[Mohammad Masoud Javidi, Marjan Kuchaki Rafsanjani, Laya Aliahmadipour. **A Taxonomy of Game Theory Approaches for Intrusion Detection in MANETs.** *Researcher* 2017;9(2):88-96]. ISSN 1553-9865 (print); ISSN 2163-8950 (online). http://www.sciencepub.net/researcher. 10. doi:10.7537/marsrsj090217.10.

**Keywords:** Mobile Ad hoc Network (MANET); Intrusion Detection System (IDS); Host based; Game theory.

## 1. Introduction

The Mobile Ad Hoc Network (MANET) is one of the wireless networks that have attracted most concentrations from many researchers In general, MANETs 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 (Kuchaki Rafsanjani et al, 2011). Nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other, this is known as multi-hop communication. 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 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 access 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 (Mitrokotsa et al, 2007). Also the MANET has the following typical features (Mishra and Nadkarni, 2003):

Unreliability of wireless links between nodes, Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.

Constantly changing topology, Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.

Lack of incorporation of security features in statically configured wireless routing protocol not meant for MANET environments. Because the topology of the networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Due to these features, MANETs are more susceptible to variety to the intrusions from the malicious behaviors than the traditional wired networks. Therefore, is needed to pay more attention to the security issues in the mobile ad hoc networks. Many solutions have been proposed for security

problems on ad hoc networks (Lima et al, 2009). In general, there are three defence lines to provide security, such as: prevention, detection and tolerance of intrusions mechanism and apply techniques to protect basic protocols and applications. Essentially, the solutions use specialized hardware, cryptographic primitives, and mechanisms for overhearing neighbor communication or protocols designed for path diversity. In recent years researchers proposed several methods to improve security in the three defence lines by applying various approaches such as: statically methods, neural networks, data mining, genetic algorithm, game theory and etc. In this paper we focus on intrusion detection mechanism and investigate proposed game theory approaches to enhance security and capability of intrusion detection mechanisms.

The remainder of the paper is structured as follows. Section 2 provides an overview of the security requirements specially intrusion detection. Section 3 briefly describes game theory. There are many methods about using game theory approaches in the field of intrusion detection. In section 4 is investigated some game theory approaches to improve performance of intrusion detection in MANET, and section 5 constitutes conclusions.

## 2. Intrusion Detection

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). Many experiences show that intrusion detection techniques just like encryption and authentication system which are the first line defence (intrusion prevention techniques), are not sufficient. As the system become complicated, their weaknesses grow causing the network security problems. Intrusion detection can be used as a second line of defense to secure the network from such problems. So, IDS should analyze system activities and ensure whether or not an intrusion has occurred (Kuchaki Rafsanjani, 2009) if the intrusion is detected, a response can be initiated to prevent or minimize damage to the system. Intrusion detection system can be classified based on various criteria such as: audit data, the detection methods and IDS architecture. Intrusion detection system based on audit data source categorized in host based and network based. A network-based IDS captures and analyzes packets from network traffic while a host-based IDS uses operating system or application logs in its analysis.

IDSs fall into two categories according to the detection methods they employ, misuse/ signature detection, anomaly detection and Specification detection. Misuse detection identifies intrusions by matching observed data with predefined descriptions of intrusive behavior. Therefore, well-known intrusions can be detected efficiently with a very low false alarm rate. However, intrusions are usually polymorph, and evolve continuously. Misuse detection will fail easily when facing unknown intrusions. While Anomaly detection is defined as the process of comparing definitions of activity that is considered normal against observed events in order to identify significant deviations. Moreover, an anomaly in a dataset is defined as an observation that appears to be inconsistent with the remainder of the dataset (Hodge and Justin, 2004). There are two types of anomaly detection (Chebrolu, 2005) The first is static anomaly detection, which assumes that the behavior of monitored targets never changes, such as system call sequences of an Apache service. The second type is dynamic anomaly detection. It extracts patterns from behavioral habits of end users, or usage history of networks/hosts. Sometimes these patterns are called profiles.

Clearly, anomaly detection has the capability of detecting new types of intrusions, and only requires normal data when building profiles. However, its major difficulty lies in discovering boundaries between normal and abnormal behavior, due to the deficiency of abnormal samples in the training phase. Another difficulty is to adapt to constantly changing normal behavior, especially for dynamic anomaly detection. Specification-based detection 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.

The third classification of IDS criteria is IDS architecture The MANET can be configured to either flat or hierarchical infrastructure. The optimal IDS architecture for the MANET depends on the network infrastructure itself. There are four main IDS architectures on the network (Anantvalee and Wu, 2007), as follows: 1) Standalone IDS, 2) Distributed and Collaborative IDS, 3) Hierarchical IDS, and 4) Mobile Agent for Intrusion Detection Systems.

*In the standalone architecture*, the IDS runs on each node to determine intrusions independently. There is no cooperation and no data exchanged among the IDSs on the network. This architecture is also more suitable for flat network infrastructure than for hierarchical network infrastructure.

*The distributed and collaborative architecture* has a rule that every node in the MANET must participate in intrusion detection and response by having an IDS agent running on them. The IDS agent is responsible for detecting and collecting local events and data to identify possible intrusions, as well as initiating a response independently.

*The hierarchical architecture* is an extended version of the distributed and collaborative IDS

architecture. This architecture proposes using multi-layered network infrastructures where the network is divided into clusters. The architecture has cluster heads, in some sense, act as control points which are similar to switches, routers, or gate ways in wired networks.

*The mobile agent* for IDS architecture uses mobile agents to perform specific task on a nodes behalf the owner of the agents. This architecture allows the distribution of the intrusion detection tasks. There are several advantages using mobile agents for intrusion detection (Mandala, 2007). The classification of the intrusion detection illustrate in figure 1.

**3. Game Theory**

Game theory is a discipline aiming to model situations in which decision makers have to make specific actions that have mutual possibly conflicting consequences. Game theory is concerned with finding the best actions for individual decision makers in such situations and recognizing stable outcomes. It has been used primarily in economics, in order to model competition between companies.

It is a powerful tool in that it can be used to model any system which exhibits the characteristics of a game In the recent years game theory has been extensively used in the most fields such as economic, computer, network communication, biology and, political science and etc. Also, we have seen researchers using game theory in the area of network security (Morris, 1994).

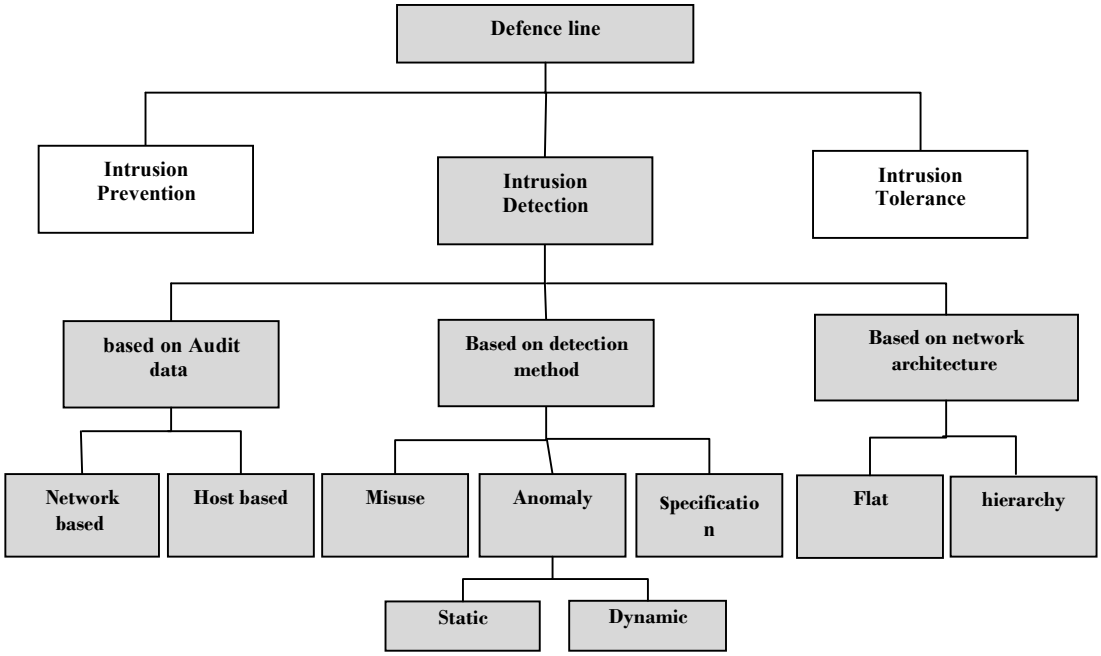


Figure 1. Classification of IDS

Game theory usually considers a multi-player decision problem where multiple players with different objectives can compete and interact with each other 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, 2008). 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 games with multi-players cooperating with each other in order to achieve the greatest possible total benefits. Also can 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 (Paramasivan, 2011).

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 (Kuchaki Rafsanjani, 2010). The equilibrium strategies are chosen by the players in order to maximize their individual payoffs. In game theory, the Nash equilibrium is a solution concept of a game involving two or more players, in which no player has anything to gain by changing only his own strategy unilaterally. If each player has chosen a strategy and no player can benefit by changing his strategy while the other players keep their unchanged, then the current set of strategy choices and the corresponding payoffs constitute a Nash equilibrium. Some games can be solved by iterated dominance, which systematically rules out strategy profiles. On the other hand, when a player makes a decision, he can use either a pure or a mixed strategy. If the actions of the player are deterministic, he is considered to use a pure strategy. If probability distributions are defined to describe the actions of the player, a mixed strategy is used (Charilas and Panagopoulos, 2010).

Ad hoc network can be model to a game. In a game, players are independent decision makers whose payoffs depend on other players 'actions. Also Nodes in an ad hoc network are characterized by the same feature. This similarity leads to a strong mapping between traditional game theory components and elements of an ad hoc network.

Benefits of applying game theory to ad hoc networks: Game theory offers certain benefits as a tool to analyze distributed algorithms and protocols for ad hoc networks. Thus here is introduced highlight three of these benefits:

- Analysis of distributed systems: Game theory allows us to investigate the existence, uniqueness and convergence to a steady state operating point when network nodes perform independent adaptations. Hence it serves as a strong tool for a rigorous analysis of distributed protocols.
- Cross layer optimization: Often in ad hoc networking games, node decisions at a particular layer are made with the objective of optimizing performance at some of the other layers. With an appropriate formulation of the action space, game theoretic analysis can provide insight into approaches for cross layer optimization.
- Design of incentive schemes: Mechanism design is an area of game theory that concerns itself with how to engineer incentive mechanisms that will lead independent, self-interested participants towards outcomes that are desirable from a system-wide point of view. This may prove especially helpful in the design of incentive schemes for ad hoc networks.

A game theoretic platform is suitable for modeling security issues such as intrusion prevention and intrusion detection. There are many researches on applying game theory in intrusion detection systems. In this paper we investigated some of these studies about capability of game theory approaches to enhance performance of IDS.

## 4. Application of Game Theory in Intrusion Detection for MANET

This section is review and investigation of the some proposed game theory approaches in various branches of intrusion detection for MANET. At the first we illustrate overview of game theoretic approaches on branch of IDS, in figure 2. Then introduce and survey these game models also their goal and performance. In addition we pointed out that each proposed game model in a branch in figure 2 are various approaches of game theory whereas as all of them in different ways lead to increase the efficiency of intrusion detection.

A. Host based IDS by applying game theory:

For this branch of intrusion detection system researchers proposed different game model that consider various parameter to increase performance of IDS.

**Patcha and Park** (2004) 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 offer optimal strategy for host based IDS and either intruder. Also 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. 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. As long as they believed their model is theoretically consistent and this game-theoretic modeling technique models intrusion detection in a more realistic way compared to previous approaches.

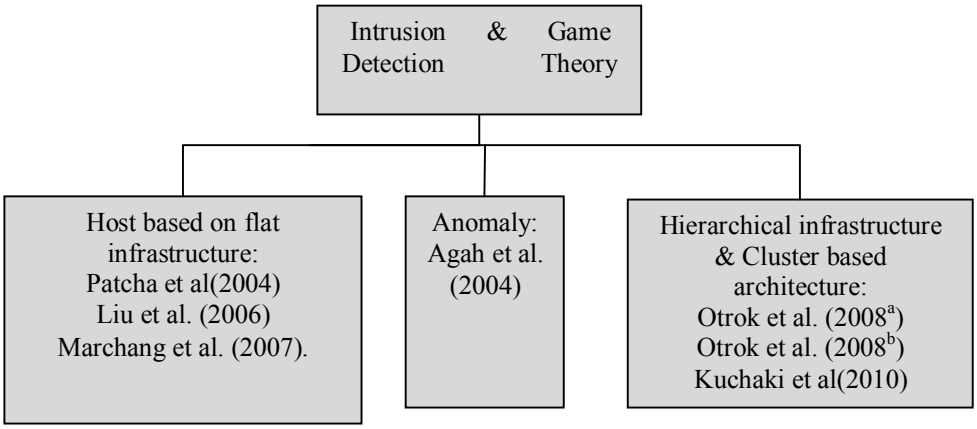


Figure 2. Game theory approaches in intrusion detection

- **Liu et al** (2006). Proposed a game theoretic framework to analyze the interactions between pairs of attacker/defending (is equipped with an IDS ) nodes using a Bayesian formulation although they considered resource and energy limitation in MANET They study the achievable Nash equilibrium for the attacker/host based IDS game in both static and dynamic scenarios. The dynamic Bayesian game is a more realistic model, since it allows the IDS to consistently update his belief on his opponent's maliciousness as the game evolves. A new Bayesian hybrid detection approach is suggested for the IDS, in which a lightweight monitoring system is used to estimate his opponent's actions, and a heavyweight monitoring system acts as a last resort of defense. We show that the dynamic game produces energy-efficient monitoring strategies for the defender, while improving the overall hybrid detection power.

In the static game model they consider a flat ad hoc network with a fixed number of *N* nodes in the network and apply host based IDS due to they assumed that any defending node is equipped with an IDS. Depending on the capability of the IDS, the defending node can detect an attacking node in the neighborhood or any node in the network. In Static mode considered a two-player static Bayesian game. One player is a *potential* attacking node, it can be malicious or normal that has private information about its type. Another player is defending node (IDS). The type of defender *is* common knowledge to the two players. The malicious type of player has two pure strategies: *Attack* and *Not attack*. The normal type of player has one pure strategy: *Not attack*. Defender has two pure strategies: *Monitor* and *Not monitor*. The two players choose their strategies simultaneously at the beginning of the game, assuming common knowledge about the game (costs and beliefs). This static non cooperative game has Bayesian Nash Equilibrium solution (BNE) (Liu et al, 2006) Authors represent the advantage of using a static Bayesian game model instead of applying an always-on IDS monitoring strategy is the defender can implement an efficient monitoring strategy according to his BNE solution that maximizes his expected payoff.

In the dynamic game model they extend the static Bayesian game to a multi-stage dynamic Bayesian game, where the defender updates his beliefs according to the game evolution. So they assume that the static Bayesian game is repeatedly played in each time period $t_k$, where k = 0, 1,... An interval of T seconds may be selected for each stage game. They consider that the game has an infinite horizon because in general any node will not have the information about when his neighboring node leaves the network. The payoff of the players in each stage game is the same as in the preceding static game, and we assume that there is no discount factor with respect to the payoffs of the players. They showed that the dynamic game has a mixed-strategy perfect Bayesian equilibrium solution.

Finally Liu et al (2006) have shown that the equilibrium strategies can preserve energy expenditure, and improve the performance of the hybrid detection approach. Also have shown that, while the equilibrium depends on the malicious node's knowledge on the defender's utility for different actions, and depends on what he thinks about the defender's updated belief, it is fairly robust to the malicious node's imperfect knowledge on the performance of the defender's lightweight monitoring system.

- **Marchang and Tripathi** (2007) have presented a game-theoretic model for efficient deployment of intrusion detection systems (IDSs) in MANETs. They declare that most of the existing intrusion detection systems in MANETs, a detection system sits on every node which runs all the time. So, there is a costly overhead for a battery powered mobile device. 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. In this game model, an IDS attempts to detect intrusion from an attacker; hence, they may look at this as a game between two players, the IDS and the attacker. The attacker's intent is to attack the network without getting caught, whereas that of the IDS is to detect when the attacker attacks. So, the model is constructed for a two-player non-cooperative non-zero sum game. The assumptions are: an IDS sits at every node and monitors some data to detect intrusion and need not be running on the node 100% of the time during which the MANET is up. The strategy profile for both the players consists of two strategies. Hence, the pure strategy space of the IDS is: monitor t% time, no monitor. Thus, the pure strategy space of the attacker is: attack s% time, not attack. The authors were considered both perfect and imperfect IDS. So, they established two game models, first, the game between perfect IDS and attacker then imperfect IDS and attacker. The game solution for both is a Nash equilibrium mixed strategy pair, where neither player has unilateral incentive to change its strategy. There are game models detail and players' payoff table in (Marchang and Tripathi, 2007) the results of their analysis show that one does not need to keep an IDS running all the time while maintaining its effectiveness. They claim the analysis helps in determining the optimal defense strategies that the network administrator must deploy.

In this section we survey three researches in intrusion detection field by using game approaches in host based IDS.

B. Anomaly detection by applying game theory

The state-of-the-art techniques of anomaly detection in ad hoc network are systematically can be introduced, according to network architectures (Hierarchical/Flat) and detection technique categories (statistical techniques, rule based, data mining, computational intelligence, game theory, graph based, and hybrid, etc.) in this section we investigate a method about this area.

- **Agah et al**. (2004) introduced a game theory based scheme for finding out the vulnerable areas in a WSN, based on many risk factors such as reliability of a sensor node, different types of attack, and past behaviors of the attacker. Only these identified areas are provided with the protection of detection, In order to save the energy cost. Intrusion detection is modeled as a game played between detection system and adversary. Each player is allowed to select a strategy from a set of strategies once. Given a fixed cluster in the network, says *K*, these strategies are available to adversary: attack cluster K, not attack cluster *K*, and attack a different cluster. Detection system responds to either defend cluster *K*, or defend a different cluster. The strategies a remarked with1 to 3 and 1 to 2 for adversary and detection system respectively, where two 2 × 3 payoff matrixes A and B can be established. The problem is to find out the optimized strategy that maximizes the profit for both players, namely achieving Nash equilibrium. Measuring the pay off depends on a couple of factors, including attack type, density of sensor nodes, and the number of previous attacks. Nash equilibrium is achieved when both players selected their own first strategy. In other words, protecting the cluster which has the highest value of $U(t)$-$C_k$ brings about a reliable rate of successful detection, where $U(t)$ indicates the utility of the network' s on-going sessions, and $C_k$ indicates the average cost of protecting cluster *K*.

C. Hierarchical infrastructure & Cluster based architecture by applying game theory Of course there are many studies about using game theory approaches in hierarchical intrusion detection system, here, we

investigate four methods that have employed different game theory approaches to enhance the performance of intrusion detection systems in MANET.

- **Otrok et al** (2008[a]) address the problem of increasing the effectiveness of an intrusion detection system (IDS) for a cluster of nodes in ad hoc networks. To reduce the overhead of IDS, a leader node is usually elected to handle the intrusion detection service on behalf of the whole cluster. However, most of current solutions elect a leader randomly without considering the resource level of nodes. Such a solution will cause that the nodes with less remaining resources to die faster and also 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. Their experiments show that the presence of selfish nodes can significantly reduces the effectiveness of an IDS because fewer packets are inspected over time. So, authors have proposed a framework to improve the performance of MANET security; their framework has multi goal that we briefly describe them and ways to achieve the desire goals as follows:

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 to truthfully reveal their cost of analysis during a leader election. This is achieved by a mechanism designed using the truth-telling mechanism Vickrey, Clarke, and Groves (VCG) and by binding the reputation of a node to the amount of services the node is entitled to. Mechanism design is a sub-field of microeconomics and game theory. It uses game theory tools to achieve a desired goal. The main difference between game theory and mechanism design is that the former is used to study what could happen when independent players act selfishly, whereas mechanism design allows us to define the game in such a way that the outcome of the game, known as the social choice function (SCF) will be played by independent players according to the rules set by the mechanism designer.

iii. Catch and punish a misbehaving leader; 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. Due to un-control problems such as channel collision, the leader-IDS could not be able to monitor and analyze the traffic of some protected nodes for a specific period of time. Hence, a checker that is monitoring the behavior of the leader-IDS could report a misbehaving event and therefore the leader-IDS is punished and a new leader is elected.

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.

v. Increase probability of intrusion detection; 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.

- **Otrok et al**. (2008[b]) improved security in the framework that was introduced in previously. They take into consideration the tradeoff between security and IDS resource consumption by a nonzero-sum non cooperative game theoretical model in the cluster. Authors considered IDS in two mode: moderate and robust. In moderate mode, cluster leader should provide intrusion detection service to other nodes in the same cluster. However, such a moderate mode is only suitable when the probability of attack is low. Once the probability of attack is high, victim nodes should launch their own IDSs to detect and thwart intrusions that is called robust mode. They found the threshold value for notifying the victim node to launch its IDS once the probability of attack exceeds that threshold value, thus shift from moderate to robust mode. To achieve this goal, the Bayesian game theory is used to analyze the interaction between the leader-IDS and intruder with incomplete information about the intruder. By solving such a game, the threshold values are found. In this game, strategy space of the leader-IDS is moderate, robust and also strategy space of the intruder is attack, not attack. The table of game and solution has been presented in (Otrok et al, 2008[b]).

- **Kuchaki et al** (2010) with combination of game theory approaches proposed an optimal solution to attain the security for a cluster of nodes in MANETs. This hybrid method has the benefits of previous methods, so that it increases security despite the resource efficiency. This optimal method has three phases:

i. The first phase building trust relationship between nodes and estimation trust value for each node to prevent internal intrusion; for achieving this goal, they have employed Bayesian game. Therefore, 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; with this way, internal intrusions are prevented. So, if node be malicious or selfish then

its neighbors estimate low trust value about it and it is denied of the network services or is removed.

ii. In the second phase, an optimal mechanism for holding cluster head election is presented. This elected cluster head is ideal, because it is not misbehaving node and it has enough energy resource for intrusions detection in its cluster and also has the lowest cost for packet analyzing.

iii. In the third phase, to detect external intruder, authors employed Bayesian game that is proposed by (Otrok et al, 2008[b])Authors assert that their hybrid method due to using game theory, trust value and honest cluster head can effectively improve the network security, performance and reduce resource consumption.

## 5. Conclusion

Intrusion detection based upon game theory is currently attracting considerable interest from the research community. So due to vital role of intrusion detection in security issue, many various studies were proposed in this area which all of them lead to enhance performance of intrusion detection in MANETs. In this paper, we review some the game theory approaches which were proposed for branches of intrusion detection; and researchers aim that in their game model was considered MANET's features. We presented taxonomy and investigated these game models and their goal.

**Acknowledgements:**

The authors have been supported by Mahani Mathematical Research Center of Shahid Bahonar University of Kerman, Iran**.**

**Corresponding Author:**
Dr. Mohammad Masoud Javidi
Department of Computer Science
Shahid Bahonar University of Kerman
Kerman, Iran
E-mail: javidi@uk.ac.ir

**References**

1. Kuchaki Rafsanjani M, Aliahmadipour L, Javidi M. M. A hybrid intrusion detection by game theory approaches in MANET. Indian Journal of Science and Technology 2011: 5 (2): 2123-2131.
2. Lima M, Santos A, Pujolle G. A survey of survivability in mobile ad hoc networks. IEEE Communication Surveys & Tutorials 2009: 11(1): 66-77.
3. Mitrokotsa A, Komninos N, Douligeris C. Intrusion detection with neural network and watermarking techniques for MANET. IEEE conf, Turkey 2007.
4. Mishra A, Nadkarni K. M. Security in wireless ad hoc networks. Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
5. Kuchaki Rafsanjani M. Evaluating intrusion detection system and comparison of intrusion detection and detecting misbehaving nodes for MANET", INTECH: advanced technologies, Ch.6, 2009.
6. Hodge VJ, Justin J. A survey of outlier detection methodologies. Artificial Intelligence Review 2004: 22(1): 85–126.
7. Chebrolu S, Abraham A, Thomas J. P. Feature deduction and ensemble design of intrusion detection systems. Computers & Security 2005: 24 (4): 295–307.
8. Anantvalee T, Wu J. A survey on intrusion detection in mobile ad hoc networks. Book Series Wireless Network Security, Springer, 2007.
9. Mandala S, Asri Ngadi Md., Abdullah H. A survey on manet intrusion detection international journal of computer science and security2007: 2(1): 1-11.
10. Morris P. Introduction to game theory. Springer, 1st edition, 1994.
11. Ganchev A, Narayanan L, Shende S. Games to induce specified equilibria. Elsevier Theoretical Comput. Sci 2008: 409(3): 341-350.
12. Paramasivan B, Mohaideen Pitchai K. Comprehensive survey on game theory based intrusion detection system for mobile ad hoc networks. IJCA Network Security and Cryptography 2011 NSC(5): 23-29.
13. Charilas DE, Panagopoulos AD. A survey on game theory applications in wireless networks. Computer Networks 2010: 54(18: 3421–3430.
14. Patchay A, J. Park. A game theoretic approach to modeling intrusion detection in mobile ad hoc networks. Proceedings of the IEEE Workshop on Information Assurance and Security United States Military Academy, 2004.
15. Liu Y, Comaniciu C, Man H. A Bayesian game approach for intrusion detection in wireless ad hoc networks. GameNets'06, ACM, 2006.
16. Marchang N, Tripathi R. A game theoretical approach for efficient deployment of intrusion detection system in mobile ad hoc networks. proceeding of the IEEE 15th International Conference on Advanced Computing and Communications, 2007.
17. Afgah A, Das, Basu K. A non-cooperative game approach for intrusion detection in sensor networks. Proceeding of the VTC, 2004.

18. Otrok H, Mohammed N, Wang L, Debbabi M, Bhattacharya P. A game-theoretic intrusion detection model for mobile ad hoc networks. Algorithmic and Theoretical Aspects of Wireless ad hoc and Sensor Networks 2008[a]:31(4): 708-721.
19. Otrok H, Mohammed N, Wang L, Debbabi M, Bhattacharya P. A moderate to robust game theoretical model for intrusion detection in MANETs. proceeding of the IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, 2008[b].
20. Kuchaki Rafsanjani M, Aliahmadipour L, Javidi M. M. An optimal method for detecting internal and external intrusion in MANET. Proceeding of the Communications in Computer and Information Science, Springer, Korea, 2010.

2/25/2017