Scientific Research and Essays Vol. 6(31), pp. 6535-6539, 16 December, 2011
Available online at http://www.academicjournals.org/SRE
DOI: 10.5897/SRE11.1479
ISSN 1992-2248 ©2011 Academic Journals

*Full Length Research Paper*

# Game theory approaches for improving intrusion detection in MANETs

**Mohammad Masoud Javidi* and Laya Aliahmadipour**

Department of Computer Science, Shahid Bahonar University of Kerman, Kerman, Iran.

Accepted 20 September, 2011

**Mobile Ad Hoc Networks (MANETs) are wireless networks in which the mobile nodes exchange information without the help of any predefined infrastructure. In such networks also called spontaneous networks, the nodes collaborate to provide the basic network services. Due to their communication type and resources constraint, MANETs are vulnerable to diverse types of attacks and intrusions. One of the security mechanisms for MANETs is intrusion detection that consists in taking action on demand to mitigate intrusions. In this paper, we investigate intrusion detection in MANETs and some different solutions of this problem based on the approach of game theory. Game theory is a theory of decision making under conditions of uncertainty and interdependence. Game theory is a powerful mathematical tool that analyzes the strategic interactions among multiple decision makers and the results of researches show that this subject improves the network performance. The aim of this paper is comparing some of existing methods that can be used to gain optimal intrusion detection for MANETs.**

**Key words:** Mobile ad hoc network, intrusion detection system, game theory, life time.

## INTRODUCTION

Mobile ad hoc network (MANET) is a network formed by a set of mobile hosts which communicate among themselves by means of the air. Those hosts establish dynamically own network without relaying on a support infrastructure or a central administration and cooperate to forward data in a multi-hop mode. MANETs were initially proposed for military applications and currently their use has been enlarged. Examples of application include emergency disaster relief, digital sensors positioned to take measurements in a region, battle-field communication, sharing information during a lecture or conference and so on (Lima et al., 2009). The unique characteristics of MANETs, such as arbitrary node movement and lack of centralized control and resource constrain, make them vulnerable to a wide variety of external and internal attackers (Zhang and Lee, 2000). Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the network and external ones. Unlike firewalls which are the first line of defense, IDSs come into the picture only after an intrusion has occurred and a node or network has been compromised. That is why IDSs are aptly called the second line of defense (Mishra et al., 2004). Game theory has been used extensively in computer and communication networks to model a variety of problems. Game theory provides a wealth of tools that can be applied to the design and operation of communication systems. The applications of game theory, especially non-cooperative game theory are usually studied based on power control, random access and energy minimization in wireless networks (Miao et al., 2010). 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. 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.

*Corresponding author. E-mail: javidi@mail.uk.ac.ir. Tel: +98 341 320 2251.

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 et al., 2010). There are many methods about using game theory approaches in the field of intrusion detection. In this study we review and investigate some methods about this area for MANETs, then we compare these approaches and finally we conclude this paper.

## INTRUSION DETECTION BY GAME THEORY APPROACHES FOR MANETS

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

### First game theory approach

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.

### Second game theory approach

The second method is proposed by Otrok et al. (2008a). Authors 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, Otrok et al. (2008a) 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

**Table 1.** Comparing discussed methods.

| Metric method | Game type | Game solution | Clustering | IDS | Detecting misbehaving node | Energy efficiency |
|---|---|---|---|---|---|---|
| First approach | Non cooperative<br>Non zero sum | Nash equilibrium<br>Mixed strategy | No | On all nodes | NO | Yes |
| Second approach | Step 2: cooperative<br>Step 3: non cooprative<br>Zero sum | Bayesian game | Yes | On cluster head | Leader | Yes |
| Third approach | Non-cooperative | Bayesian game | Yes | Cluster members and leader | Leader | Some deal |
| Fourth approach | Non-cooperative | Phase 1: Bayesian nash equilibrium<br>Phase 3: Bayesian game | Yes | Cluster members and leader | Cluster members and leader | Yes |

**Table 2.** Advantage and disadvantage of each method.

| Methods | Advantages | Disadvantages |
|---|---|---|
| First approach | This approach is optimal because of energy efficiency and also it considers perfect and imperfect IDS. | This approach can not detect misbehaving nodes and does not distinct difference between internal and external attackers. |
| Second approach | Energy efficiency due to clustering, electing honest, most cost efficient cluster leader with enough remaining resource and detection of external intruder. | In this approach due to using VCG mechanism and checker nodes, the network overhead will be increased and also it does not detect internal attackers and misbehaving nodes except the leader node. |
| Third approach | Improving the advantage of second approach and increasing the network security because of each victim node besides the cluster head cooperate in intrusion detection. | Similar to second approach. |
| Fourth approach | This approach has the advantages of the third approach also decreasing the network overhead as well as it can detect internal and external intruders and find misbehaving nodes in a cluster. | - |

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.

### Third game theory approach: A moderate to robust game theoretical model

Otrok et al. (2008b) 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 an 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. Otrok et al. (2008b) 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 have been presented in Otrok et al. (2008b).

### Fourth game theory approach: An optimal intrusion detection system

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. (2008b). 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.

## COMPARISON AND PERFORMANCE EVALUATION OF THE APPROCHES

We have investigated different methods of using game theory for intrusion detection in MANETs. Here, we compare these methods. There is comparison of the methods based on different metrics in Table 1 and also advantages and disadvantages of each method have been illustrated in Table 2.

## CONCLUSION

We reviewed four approaches of intrusion detection systems in MANET that are based on game theory. After investigation of the methods, we found that in the first approach by using a simple game, it is not essential that the IDS be always running. Then a framework by using game theory and mechanism design in a cluster of nodes to improve security in MANET is introduced, but this method increased the network overhead. In the third method, network security is improved by using game and switch between moderate mode and robust mode. In the last method an optimal method is proposed that is able to detect misbehaving nodes and prevent internal intruders, then elect an honest, most cost efficient cluster-head with enough remaining resource to detect external intruder. This method has the advantages of other methods and also it reduces the network overhead efficiently.

### REFERENCES

Kuchaki RM, Aliahmadipour L, Javidi MM (2010). An optimal method for detecting internal and external intrusion in MANET, Proceeding of the Int. Conf. on Future Generation Communication and Networking (FGCN 2010) held at Jeju Island. Korea. pp. 71-82.

Lima M, Santos A, Pujolle G (2009). A survey of survivability in Mobile Ad Hoc Networks. IEEE. J. Communications surv. tutor., 11(1): 66-77.

Marchang N, Tripathi R (2007). A game theoretical approach for efficient deployment of intrusion detection system in Mobile Ad Hoc Networks. Proceeding of the 15th Int. Conf. on Advanced Computing and Communications Held at Guwahati. Assam, pp. 460-464.

Miao X, Zhou X, Yi Wu H (2010). A cooperative differential game model based on transmission rate in wireless networks. J. Operat. Res. Lett., 38(1): 292-295.

Mishra A, Nadkarni K, Patcha A, Tech V (2004). intrusion detection in wireless ad hoc networks, IEEE . J. Wireless Commun., 11(1): 48-60.

Otrok H, Mohammed N, Wang L, Debbabi M, Bhattacharya P(2008a). A game-theoretic intrusion detection model for Mobile Ad Hoc Networks. J. Comput. Commun., 31(4): 708-721.

Otrok H, Mohammed N, Wang L, Debbabi M, Bhattacharya P (2008b). A moderate to robust game theoretical model for intrusion detection in MANETs. Proceeding of the IEEE Int. Conf. on Wireless & Mobile Computing, Networking & Communication held at Avignon. pp. 608-612.

Zhang Y, Lee W (2000). Intrusion Detection in Wireless Ad Hoc Networks. Proceeding of the 6th Annual Int. Conf. on Mobile Computing and Networking (ACM MobiCom'00) held at Boston , pp. 275-283.