A Moderate to Robust Game Theoretical Model for Intrusion Detection in MANETs

Hadi Otrok, Noman Mohammed, Lingyu Wang, Mourad Debbabi and Prabir Bhattacharya

Computer Security Laboratory
Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Quebec, Canada
Email:{h_otrok, no_moham, wang, debbabi, prabir}@ciise.concordia.ca

Abstract—One popular solution for reducing the resource consumption of Intrusion Detection System (IDS) in MANET is to elect a head-cluster (leader) to 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. Such a robust mode is, however, costly with respect to energy and leads nodes to die faster. Clearly, to reduce the resource consumption of IDSs and yet keep its effectiveness, a critical issue is: When should we shift from moderate to robust mode? In this paper, we formalize this issue as a nonzero-sum noncooperative game theoretical model that takes into consideration the tradeoff between security and IDS resource consumption. The game solution will guide the leader-IDS to find the right moment for notifying the victim node to launch its IDS once the security risk is high enough. 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, we are able to find the threshold value for notifying the victim node to launch its IDS once the probability of attack exceeds that value. Simulation results show that our scheme can effectively reduce the IDS resource consumption without sacrificing security.

Index Terms—Intrusion detection systems, MANET security, and leader election.

I. INTRODUCTION

The cooperation among nodes is a crucial requirement for intrusion detection in Mobile Ad hoc Networks (MANETs) due to their autonomous nature [2], [6]. The cooperation usually requires all the nodes to launch their own IDSs to increase the detection capability. Unacceptable resource consumption is the main obstacle faced by such a model since nodes in a MANET typically have only limited resources. A common approach for reducing the overall resource consumption of intrusion detection is for nodes to collaborate in electing a leader to serve as the intrusion detection system (IDS) for a cluster of one-hop nodes. The election process can be based on one of the following models: Random [3], connectivity index [4], or weight-based model [7]. Relying on leaders for providing IDS service by examining a portion of all nodes’ packets is suitable whenever the probability of attack is low. This is usually known as a moderate intrusion detection model. However, a robust model where the victim nodes launch their own IDSs will be more desirable when the probability of attack is high. To the best of our knowledge, the critical issue that has not been addressed so far is: When should we step from moderate to robust mode?

We discuss our approach within an efficient and truthful leader-IDS election framework based on mechanism design previously proposed in [10]. Our framework is able to elect the most cost efficient node to be the leader. The leader-IDS monitors the network according to a predefined sampling budget which is distributed over the protected list of nodes according to nodes’ reputation value. Thus, the IDS service is offered to nodes according to their reputation value. Running this model in a non-secure environment raises the need for more nodes to launch their IDS according to attack’s severity. Thus, more nodes should launch their own IDS according to node’s security risk. This will help to prolong the lifetime of nodes and increase nodes’ security. A question we did not address in [10] is: What is the optimal threshold value needed to inform the victim node to launch its own IDS in order to minimize both resource consumption and security risk? We tackle this important issue in this paper.

In this paper, we formalize the tradeoff between security and IDS resource consumption as a non-cooperative game between leader-IDS and attacker with incomplete information about the attacker. This game guides the leader-IDS and intruder to derive their optimal strategy against each other. For the leader-IDS, the game solution derives the threshold for informing the victim node to launch its own IDS once the probability of attack exceeds the derived threshold. The game will be repeated such that in every election round the leader-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. On the other hand, the attacker’s strategy will be to attack once the probability of stepping into the robust mode (that is, the victim node will be running its own IDS) is low. Empirical results indicate that our scheme can effectively reduce the resource consumption of IDSs without sacrificing security.

In summary, the contribution of this paper is a game theoretical solution to decide the optimal moment to switch from moderate mode to robust mode. The rest of the paper is organized as follows: Section II reviews related work. Section III shows our election mechanism. Section IV presents our moderate to robust IDS model. Section V presents empirical results. Finally, Section VI concludes the paper.
II. RELATED WORK

This section reviews related work on intrusion detection in MANET and the application of game theory to networks.

A. Intrusion Detection Systems in MANET

The difference between wired infrastructure networks and mobile ad hoc networks raises the needs for new IDS models that can handle new security challenges, such as attacks against routing protocols [6]. A cooperative intrusion detection model is proposed to allow all nodes in identifying possible attacks and escalating an identified anomaly to a global detection process [12]. An extended model is proposed in [3] to identify sources of attacks; the issue of run-time resource constraints is also addressed through a random leader-election scheme. Unlike our work [10], the random election scheme does not consider the remaining resources of nodes or the presence of selfish nodes. In [4], a modular IDS system based on mobile agents is proposed and the authors point out the impact of limited computational and battery power on the network monitoring tasks. Again, the solution ignores both the difference in remaining resources and the selfishness issue.

B. Game Theory

Game theory [8] 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 games with multi-players cooperating with each other in order to achieve the greatest possible total benefits. To predict the optimal strategy used by intruders to attack a network, the authors of [9] model a non-cooperative game-theoretic model to analyze the interaction between intruders and the IDS in a wired infrastructure network. They solve the problem using a zero-sum non-cooperative game with complete information about the intruder.

In complete information game, the type, strategy spaces, and payoff functions of both players are known. In [1], the authors aim at demonstrating the suitability of game theory for development of various decision, analysis, and control algorithms in intrusion detection. They address some of the fundamental network security tradeoffs, and give illustrative examples in different platforms. They propose two different schemes based on game theoretic techniques and consider a generic model of distributed IDSs equipped with a network of sensors. Bayesian Nash is used in [5] to analyze the interaction between the intruder and defender in static and dynamic scenarios. The authors provide a hybrid detection approach.

These existing studies clearly show that game theory is a strong candidate for providing the much-needed mathematical framework for analyzing the interaction between IDSs and intruders. To the best of our knowledge, our work is among the first efforts on improving the efficiency of intrusion detection in MANET. A nonzero-sum noncooperative game based on Bayesian Nash equilibrium is used to model the interaction between the leader and intruder, taking into consideration that the precise identity of the intruder is typically unknown. The solution of such a game guides the IDS to inform the victims to launch their IDS according to the game derived threshold.

III. LEADER-IDS ELECTION MECHANISM

Our discussion will be based upon our previous framework for electing leader-IDS. The detailed description of our previous model can be found in [7], [10]. To be self-contained, in this section, we briefly summarize this framework.

We consider the MANET as a collection of nodes. Each node has an IDS for detecting potential attacks targeting communication protocols. To reduce the performance overhead of intrusion detection, nodes in a cluster will cooperate to elect a leader node for handling the detection process for the whole cluster. To balance the IDS resource consumption among all nodes in the cluster, the most cost-efficient node who has the minimum cost-of-analysis should be elected as the leader. The cost-of-analysis is designed based on the reputation value, the expected number of alive-time slots that a node wants to stay alive in a cluster and energy level. The function is designed in this way to preserve the node’s privacy and ensure the contribution of all nodes in the election process (fairness).

A selfish node may choose to declare a fake value for its cost-of-analysis such that it can maximize its payoff during the election. We thus give incentives to nodes to motivate them in revealing truthfully their true cost-of-analysis. Incentives are given in the form of reputation and are computed based on the Vickrey, Clarke, and Groves (VCG) mechanism where truth telling is the node’s dominant strategy. The reputation is used by the leader to decide how much intrusion detection service each node is entitled to receive. All nodes are thus encouraged to reveal their true values of the cost-of-analysis during each election round.

In our model, nodes are asked to directly reveal their cost-of-analysis in order to find the most cost efficient IDS which is defined by the Social Choice Function $SCF = \min_{i \in N} C_i$ (i.e., the minimum cost-of-analysis). The $SCF$ is computed in a distributed manner where all the nodes make decisions about the leader node. This guarantees that the same leader is elected by all. Knowing that the election mechanism will be repeated every $T_{Elec}$ in order to ensure fairness and security. To achieve our mechanism, we also designed an election algorithm that minimizes the above SCF while not incurring too much of performance overhead.

IV. A MEDIUM TO ROBUST GAME MODEL

Leader election model is considered as a moderate intrusion detection since it only monitors and analyzes a portion of all events occurring in the network. This model can be used whenever the probability of attack is low. It will help to reduce the overall resource consumption of IDSs. Once the probability of attack against a node is high, the victim node should launch its own IDS to detect and thwart intrusions. Therefore, the
detection steps into the robust mode. A mechanism is needed to decide when to go from moderate mode to robust mode. To formally address this issue, we formulate a game with two players: Leader-IDS and intruder. The objective of the intruder is to attack a node without being detected, where that of the leader-IDS is to detect such intruders. In order to detect an intrusion, the leader-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 leader-IDS will notify the victim node to launch its own IDS.

A. The Game Definition

We model the game as a non-zero-sum noncooperative game with incomplete information about the players where each player has a private information about his/her preferences. In our case, the leader-IDS type is known to all the players while the sender type is selected from the type set $\Theta = \{\text{Malicious (M)}, \text{Normal (N)}\}$. Knowing that the sender type is a private information, Bayesian Equilibrium [11] dictates that sender’s action depends on his/her type $\theta$. By observing the behavior of the sender at time $t_k$, the leader-IDS can calculate the posterior belief evaluation function $\mu_{t_{k+1}}(\theta_i|a_i)$ using the following Bayes rule:

$$\mu_{t_{k+1}}(\theta_i|a_i) = \frac{\mu_{t_k}(\theta_i) P_{t_k}(a_i|\theta_i)}{\sum_{\theta_j \in \Theta} \mu_{t_k}(\theta_j) P_{t_k}(a_i|\theta_j)}$$  

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 stage of the game given the type $\theta$ of the node $i$. It is computed as follows:

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

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

where $O$ is the probability of attack determined by the IDS. $F_m$ is the false rate generated by the leader-IDS due to sampling and $E_m$ is the expected detection rate via sampling in moderate mode.

We define the intruder’s pure strategy as $A_i = \{\text{Attack, Not-Attack}\}$. On the other hand, leader-IDS strategy is selected from the strategy space $A_{IDS} = \{\text{Robust, Moderate}\}$. 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 robust mode and $p$ is the probability to attack by the attacker. In Table I, the game is defined where the utility function of the IDS by playing the Robust strategy while the attacker plays the Attack strategy is defined as $E_r V - C_r$. It represents the payoff of protecting the monitored node, which values $V$, from being compromised by the attacker, where $E_r V >> C_r$. On the other hand, the payoff of the attacker if the intrusion is not detected is defined as $E_m V - C_m$. It is considered as the gain of the attacker for compromising the victim node. Additionally, we define $E_m V - C_m$ as the payoff of IDS, if strategy Moderate is played while the attacker strategy remains unchanged. Conversely, the payoff of the attacker if the intrusion is not detected is defined as $E_m V - C_m$. Now, the cost of running the IDS strategy is Robust 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 Moderate is $0$ while the losses of the IDS is defined as $C_m$ which is the cost of running the IDS in moderate mode. Where,

- $E_r = 1 - E_r$, where $E_r$ is the expected detection of an intrusion in the robust mode. $E_r = E_{leader} + E_{victim}$, where $E_{leader}$ and $E_{victim}$ are the expected detection by leader-IDS and monitored node (victim) respectively.

We define the expected probability of detection as $E_r = \sum_{l \in L} x_l(\theta_l)$, where $x_l$ is the probability of detecting an intrusion via sampling and it is equal to $s_l|f_l$. On the other hand, $y_l$ is the probability of selecting link $l$ by an intruder to attack a victim node. Knowing that $s_l$ is the sampling rate at victim’s incoming link $l$ and $f_l$ is the flow at link $l$ where $L$ is the set of incoming links. We consider the link $l$ as the route link that connect the victim node with other nodes. In [10], we proposed a mechanism for finding the optimal value of $s_l$.

- $E_m = E_{leader}$ is the expected detection in the moderate mode, where only the leader-IDS is running the IDS to detect intrusions. On the other hand, $E_m$ is equal to $1 - E_m$.

- $C_r$ is the cost of running the IDS in robust mode. We define the cost as the aggregation of the cost of monitoring by the leader $C_{leader}$ and cost of monitoring by the victim $C_{victim}$.

- $C_m$ is the cost of running the IDS in moderate mode which is equal to $C_{leader}$.

- $C_c$ 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.

B. The Game solution

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 I, the IDS utility function $U_{IDS}$ is defined as follows:

$$U_{IDS} = [qq(E_r V - C_r) + p(1 - q)(E_m V - C_m) - q(1 - p)C_r]$$
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:

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

To achieve this goal, 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:

$$p^* = \frac{C_{s, t} - C_a}{\mu V |\theta - \theta_{p}}$$

and can be reduced to: $p^* = \frac{C_{s, t} - C_a}{\mu V E_{\text{victim}}}$.

The value of $p^*$ is used by the leader-IDS to decide whether to inform the victim node to launch its own IDS or not. Knowing that the leader-IDS is monitoring and analyzing traffic via sampling to detect an intrusion launched by an external attacker $i$. The IDS is computing the belief $\mu$, as in Equation 1, of 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 leader-IDS is $E_{\text{leader}}$. 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 $\frac{C_{s, t} - C_a}{\mu V E_{\text{victim}}}$.

On the other hand, the utility function $U_a$ of the attacker is defined as follows:

$$U_a = q p(\mu V - C_a) + (1 - q)(\mu V - C_a)$$

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 and leads to equilibrium where the following holds:

$$U_a((p^*|\theta = M), q^*) \geq U_a((p|\theta = M), q^*)$$

To maximize the utility function, it is sufficient to set the first derivative with respect to $p^*$ to zero which will be equal to: $q^* = \frac{\mu V C_a}{\mu V E_{\text{victim}} + \mu V C_a}$. This can be reduced to $\frac{\mu V C_a}{\mu V E_{\text{victim}} + \mu V C_a}$.

From the solution of the game, the attacker best strategy is to attack once the probability of running the IDS by the victim (robust mode) is less than $\frac{\mu V C_a}{\mu V E_{\text{victim}} + \mu V C_a}$. 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.

C. Illustrative Example

To illustrate the election scheme and the process for gradually adding more monitors, we consider a MANET of 10 nodes, as shown in Figure 1, with 3 external nodes with unknown identities. Since our model is repeatable, we present the election process at the 10th round. The reputation at the 9th round is given in the first row of Table II.

To elect a new leader in the 10th round, nodes reveal their cost-of-analysis [7] to the mechanism based on their type (Selfish or Normal). The corresponding cost-of-analysis is given in the second row of Table II. Then, node 7, 8, 9 and 10 vote for node 9 to be the leader as it has the least cost of analysis. Similarly, node 6 votes for node 5; node 3, 4 and 5 vote for node 3; node 1 and 2 vote for node 1. After getting the vote, leader node 1, 3, 5 and 9 will calculate their payment using our payment function [7]. The payment for elected leaders $N_1$, $N_3$, $N_5$ and $N_9$ will be 45, 95, 40 and 100 respectively. All the neighboring nodes increase the reputation of the elected leaders, as shown in the third row of Table II. After election, leaders distribute the IDS sampling budget over the protected nodes according to their reputation. For example, leader $N_9$ distributes its total budget $B$ over $N_7$, $N_8$, $N_3$ and $N_{10}$ as follows: $B = \{B_7 = \frac{210}{1100}, B_8 = \frac{540}{1100}, B_3 = \frac{100}{1100}, B_{10} = \frac{140}{1100}\}$. Here, we elected a set of leader-IDS and divided the network into a collection of protected clusters. Due to leader limited sampling budget and according to nodes’ security threat level, monitored nodes (victim) that are expected to receive an attack in the coming time slots should be notified to launch their own IDS. Thus, nodes’ resources are consumed according to the security needs.

After election is completed, nodes are in moderate intrusion detection mode where the leader is sampling and analyzing the packets. To demonstrate how nodes are notified according to the security needs, we show the interaction between leader-IDS $N_9$ and the 3 external nodes. As an example, we select node $N_7$ as the target node where an intruder is targeting to attack. Figure 1, describes an attack scenario where an intrusion could be directed to node $N_7$ either from node $N_{11}$, $N_{12}$ or $N_{13}$. Hence, the leader-IDS will use the belief function of Equation 1 to calculate the belief of each external node using the prior observed actions. For example, we assume that the leader’s belief regarding each external node connected to $N_7$ is $\mu = \{\mu_{11} = 0.7, \mu_{12} = 0.2, \mu_{13} = 0.1\}$. According
to node’s belief, the IDS will compute the threshold that determines the behavior of the external nodes (i.e., attack or not). If the probability of attack is greater than the computed threshold then the leader $N_0$ should inform the victim node $N_1$ to launch its own IDS. For example, if the threshold of attack by node $N_{11}$ is 0.18, assuming that $C_{\text{victim}} = 10$, $\mu = 100$ and $E_{\text{victim}} = 0.83$, then the victim node will more frequently launch its IDS. This is because the value of the node, with respect to the cluster, is much more than the cost of running the IDS. Hence, launching the IDS by the victim is affected by the ratio of the monitoring cost to the value of the node (gateway, normal, etc.).

V. SIMULATION RESULTS

To simulate our model, we assume the leader-IDS collects packets via sampling in each round to determine whether there is an attack or not. The output of the leader-IDS ranges between 0 and 1. If the computed output is less than 0.8 then it is classified as a normal behavior, otherwise it is abnormal (attack). Figure 2.a shows the behavior of an external node (node $N_{11}$ in the previous example) for two different attack scenarios for 40 consecutive rounds. To determine the type of the sender ($N_{11}$), the posterior belief function is calculated using Equation 1 with prior belief $\mu_0 = 0.5$, $F_m = 0.1$ and $E_m = 0.83$. Figure 2.b shows the posterior belief of the leader for these two attack scenarios. The belief for the first attack scenario converges to 1 faster than the second attack scenario. This is because in the first scenario the attacker starts to attack earlier compared to the second scenario. Once the belief reaches 1, it does not go down even if the attacker is not attacking since the type already been identified. After calculating the belief, the leader-IDS computes the attack threshold. The victim node launches its own IDS according to the notification of the leader-IDS. Figure 2.c illustrates the cumulative energy consumption by the victim node for the two attack scenarios. We assume that the victim node consumes 5 joules of energy for launching the IDS for one round. Thus, if the node is always monitoring it consumes $40 \times 5 = 200 J$ for the 40 rounds. On the other hand, in our model the victim node consumes $145 J$ and $100 J$ for the two attack scenarios respectively. This will prolong the IDS lifetime. Thus, the victim launches its IDS (robust mode) optimally depending on the frequency of attack and the ratio of the monitoring cost to its value.

VI. CONCLUSION

The tradeoff between security and the resource consumption of IDSs has motivated us to propose a game-theoretical solution for prolonging the lifetime of nodes and increasing their security. A nonzero-sum noncooperative game was formulated to analyze the interaction between the leader-IDS and intruder. The game guided the two players to know their optimal strategy against each other. The leader-IDS notifies the victim node to launch its own IDS once the probability of attack is greater than the game-derived threshold. Simulation results showed that our model is able to reduce IDS resource consumption according to the security risk.

REFERENCES