A Game Theoretic Approach to Detect Network Intrusions: The Cooperative Intruders Scenario

M. Mehrandish*, H. Otrak†, M. Debbabi‡, C. Assi§, P. Bhattacharya∥
Computer Security Laboratory
Concordia Institute for Information Systems Engineering
Concordia University, Montreal, Quebec, Canada
* Email: m_mehran@cs.concordia.ca
† Email:{h_otrok, debbabi, assi, prabir}@ciise.concordia.ca

Abstract—In this paper, we consider the problem of detecting intrusions initiated by cooperative malicious nodes in infrastructure-based networks. We achieve this objective by sampling a subset of the transmitted packets, between each intruder and the victim, over selected links or router interfaces. Here, the total sampling rate on all links must not exceed the sampling budget constraint. We build a game theoretic framework to model distributed network intrusions through multiple malicious nodes and a common victim node. To the best of our knowledge, there has not been any study for the case where the attack is distributed over cooperative intruders using game theory. Non-cooperative game theory is used to formally express the problem, where the two players are: (1) the intruders and (2) the intrusion detection system. Our game theoretic framework will guide the intruders to know their attack strategy and the IDS to have an optimal sampling strategy in order to detect these intrusion packets.

I. INTRODUCTION

Intrusion Detection Systems (IDSs) have become a critical important technology for protecting and defending networks and computer systems against malicious attacks. In order to address issues like attack modeling, analysis of detected threats, and decision on response actions, there is a need for a quantitative decision and control framework. Presently, a rich set of tools have been developed within the game theory discipline to address problems where multiple players with different objectives compete and interact with each other on the same system. These tools are successfully used in many disciplines including economics, political science, and control. Now, given the continuous struggle between attackers who aim to attack the networks and the intrusion detection system trying to detect intrusions, these interactions can be modeled as a non-cooperative game where the players are the intruders and the intrusion detection system. Therefore, game theory is a strong candidate to provide the much-needed mathematical framework for analysis, modeling, decision, and control process for information security and intrusion detection [4]. As a result, game theory has been lately proposed in several studies for a theoretical analysis of intrusion detection [1], [4], [5], [8]–[10].

In our previous study [10], we analyzed the problem of intrusion detection via multiple packets in a communication network. We built a game theoretic framework to model network intrusions. Detection was accomplished by sampling a portion of the packets transiting through selected network links while not exceeding a predefined sampling budget constraint to effectively reduce the chances of an intruder by finding the value of the game using a min-max strategy.

Unlike the other studies [8] [10] that considered only a single attacker, we investigate the case where we have a group of cooperating attackers, a more interesting scenario. The intruders initiate the attack by sending a series of malicious packets from different nodes. Our contribution in this paper is to build a game theoretic model in order to detect these network intrusions by sampling a subset of the transmitted packets over selected links or router interfaces. To the best of our knowledge, there has not been any study for the case where the attack is distributed over multiple intruders using game theory. Non-cooperative game theory will be used to formally express our problem, where the players are: (1) the cooperative intruders and (2) the intrusion detection system. This game theoretic model will guide the intruders to their attack strategy and the IDS to have an optimal sampling strategy in order to detect the malicious packets. The strategy for each intruder is the probability of choosing each possible path to send the malicious packet to the victim node. Consequently, the optimal strategy for the IDS is to assign the sampling rates to each link to maximize the probability of detection while not exceeding the total budget.

The rest of the paper is organized as follows. Section 2 discusses the related work. In Section 3, we present the problem statement. We first illustrate the assumptions, and then we introduce the game and talk about the constraints and objective of the game. Sections 4 and 5 discuss the game formulation and solution respectively. Furthermore, a case study is presented in order to show how the game formulation works in a practical network, which is followed by concluding remarks in Section 6.

II. RELATED WORK

Several proposals addressed the use of game theory in order to model and solve intrusion detection problems. The authors in [4], modeled the interaction between the attacker and the IDS as both finite and continuous-kernel non-cooperative security games to establish a quantitative mathematical framework. The interaction between the attacker and the IDS was
formulated as a non-cooperative non-zero sum game with the virtual sensor network as a third fictitious player. Existence of a unique Nash equilibrium and best-response strategies for players under specific cost functions was also investigated. Then, the authors extended the model to take the dynamic characteristics of the sensor network [3] into account. Finally, they discussed properties of the resulting dynamic system and repeated games both analytically and numerically.

In [5], the authors demonstrated the suitability of game theory for development of various decision, analysis, and control algorithms in intrusion detection. They accomplished this by addressing some of the basic network security tradeoffs, and giving illustrative examples in different platforms. Moreover, the authors devised a flexible scheme using intrusion warning levels with the IDS being able to operate in different modes at each security level, and to switch automatically between the different levels. To deal with this issue they used cooperative game theory and Shapley value [6]. Furthermore, the authors modeled the interaction between the attacker and the IDS as a two-person, non-zero sum, single act, finite game with dynamic information. They proposed two specific sub-games and Nash equilibrium solutions in closed forms were obtained for these specific sub-games.

In [1], Agah et al. pointed out the insufficiency of resources in sensor networks as the motivation of their study. They proposed a game theoretic framework for defending nodes in a sensor network in order to consume less resources. Their main concern was finding the most vulnerable node in a sensor network and protecting it. They applied three different schemes for defense; game theory, Markov Decision Process (MDP) and an intuitive metric (node’s traffic). Simulation results showed that using game theoretic framework significantly improved the chance of intrusion detection.

In [8], the authors considered the problem of detecting intruding packets in a network by means of network packet sampling. They take into consideration the scenario where the adversary has significant information about the network. The attack is accomplished when the adversary sends a malicious packet via a path to the victim node and the packet is not sampled. They have formulated the problem in a game-theoretic framework and the solution to this problem was a max-flow problem from which the stable operating points were obtained.

In [10], we considered the problem of intrusion via multi packets, where the intruder splits the attack over multiple packets. Knowing that, a single packet that belongs to the attack may look normal if sampled alone, while a series of these packets could be marked as an intrusion. We then built our game-theoretic framework and formulated the sampling problem. We solved the game using min-max approach to find the strategy for the service provider to increase the chance of detecting attack over multiple packets.

III. PROBLEM STATEMENT

The problem set-up is outlined in four steps. First, we discuss the assumptions in the network. Then, we introduce the game defining the adversaries in a game theoretic framework. Afterward, we describe the objective of the game that is played between the intruders and the IDS. Finally we introduce the strategies for the cooperative intruders and the IDS.

A. Assumptions

The network is modeled as a directed graph, \( G = (N, E) \) where \( N \) is the set of nodes and \( E \) is the set of unidirectional links in the network. It is also assumed that there are \( k \) nodes and \( l \) links in the network. The capacity of link \( e \in E \) denoted by \( c_e \) and the amount of traffic flowing on link \( e \) is represented by \( f_e \). Given two nodes \( u \) and \( v \) in the network, let \( \rho_u^e \) represent the set of paths from \( u \) to \( v \) in \( G \). We present the maximum flow between \( u \) and \( v \) with \( MF_u^v(c) \), where \( c \) is the capacity vector. Corresponding to the maximum flow between nodes \( u \) and \( v \), there is a minimum cut consisting of a set of links in the network. The set of links in this minimum cut will be represented by \( MinCut_{u,v}^e \). We also introduce the maximum flow among all links in all paths in \( \rho_u^e \) by \( max_{u,v}^e(f) = Max\{f_e | \forall e \in P, \forall P \in \rho_u^v(c)\} \). Moreover, we introduce \( \Omega \) to be the set of cooperating intruders, each sending a packet to node \( t \), the target node, in order to initiate the attack, where \( |\Omega| \) is the number of intruders. Furthermore, we introduce \( s_e \) to be the sampling rate on link \( e \). Since we consider this problem in a practical network with significant flows, without loss of generality, we assume that the following holds: \( s_e < f_e - 1 \).

B. Introducing the Game

The game is played on the infrastructure network between the IDS and the cooperating intruders. Assuming the set of cooperative intruders as one player, we model the game as a zero-sum game: the IDS and the intruders. The objective of each intruder \( x \in \Omega \) is to send a malicious packet to the target node \( t \). An intrusion is successful when at least \( m \) malicious packets out of the \( |\Omega| \) packets reach the desired target node \( t \) without detection. In order to detect the intrusion, the IDS samples packets in the network via its agents. Furthermore, the agents sample the traffic on each link in the network as shown in Figure 1.

C. Game objectives and constraints

Sampling the packets flowing on a link and examining the packets can be fairly expensive operations to perform in real time. Therefore, we assume that the IDS has a sampling bound of \( B_s \) packets per second over the entire network. This sampling effort can be distributed arbitrarily over the links in the network. Here, we have a distributed agent based IDS. The IDS samples the packets on each link via the agents while not exceeding the sampling budget, \( B_s \). The sampling bound can be viewed as the maximum rate at which the intrusion detection system can process packets in real time. If a link \( e \), with traffic \( f_e \) flowing on it, is sampled at rate \( s_e \), then the probability of sampling a malicious fragment on this link is given by \( p_e = s_e/f_e \). Therefore, we have the sampling constraint \( \sum_{e \in E} s_e \leq B_s \). The game theoretic problem that
we are going to discuss in sections 4 and 5, is formulated in terms of $p_e$. We assume that all the players have complete information about the topology of the network and all the link flows in the network.

D. Strategies for the Two Players

In the case of the intruder, a pure strategy would be to pick a path $P \in \rho_x$ for the malicious packet to traverse from $x$ to $t$. The intruders, in our case, can use a mixed strategy. In the case of a mixed strategy, the intruders have a probability vector $q_x = (q(P_1), ..., q(P_{z_x}))$ over the set of paths in $\rho_x = \{P_1, P_2, ..., P_{z_x}\}$ such that $\sum_{P \in \rho_x} q(P) = 1$. Moreover, let $V_x = \{q : \sum_{P \in \rho_x} q(P) = 1\}$ represent the set of feasible probability allocations over the set of paths between $x$ and $t$. Each intruder, $x$, then picks a path $P \in \rho_x$ with probability $q_x(P)$ for each malicious packet. The strategy for the IDS is to choose the sampling rate $s_e$ on link $e$ such that $\sum_{e \in E} s_e \leq B_s$. We also introduce $U = \{p : \sum_{e \in E} f_e p_e \leq B_s\}$ to represent the set of detection probability vectors $p = (p_{e_1}, ..., p_{e_i})$ that satisfy the sampling budget constraint. The strategy for the IDS is to pick a set of detection probabilities at the links which belongs to the set $U$.

IV. MODELING THE COOPERATIVE INTRUDERS AND THE IDS GAME

The intruders and the intrusion detection system (IDS) each should choose their strategies, which are the probability distributions: $q_x$ over the set of paths in $\rho_x$, and $p$ a set of detection probabilities at the links for the intruders and the IDS respectively. Then, the payoff for both the IDS and the intruders depends on the probability of the intrusion being detected as it goes from the intruding nodes to the target node $t$. For any node $x \in \Omega$, the probability of sampling a packet traversing from node $x$ to node $t$ is the sum of probability of taking each path times the probability of sampling the packet on that particular path over all possible routes from $x$ to $t$. We introduce $\alpha_x$ to be the probability of detecting the intrusion, when intruder $x$ is attacking node $t$, which is given by:

$$\alpha_x = \sum_{P \in \rho_x} q(P)[1 - \prod_{e \in P} (1 - p_e)]$$  \hspace{1cm} (1)

Next, we define the function $\Phi$ to be the mean value of detecting the intrusion through sampling:

$$\Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (2)

The main goal of the IDS is to maximize $\Phi$. In other words, the IDS aims at maximizing the following:

$$\max_{p_e \in U} \min_{q \in V_x} \Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (3)

where:

$$U = \{p : \sum_{e \in E} f_e p_e \leq B_s\}$$  \hspace{1cm} (4)

On the other hand, the cooperative intruders aim at minimizing Equation (3). The intruders will fulfill this objective by assigning probabilities for all possible routes to the target node:

$$\min_{q \in V_x} \max_{p \in U} \Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (5)

where:

$$V_x = \{q : \sum_{P \in \rho_x} q(P) = 1\}$$  \hspace{1cm} (6)

Using a similar argument, the objective of the IDS becomes:

$$\max_{p \in U} \min_{q \in V_x} \Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (7)

This is a mixed strategy zero-sum game, for which the following min-max theorem holds:

$$\beta = \max_{p \in U} \min_{q \in V_x} \Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (8)

where $\beta$ is the value of the game.

V. SOLUTION OF THE GAME BETWEEN COOPERATIVE INTRUDERS AND THE IDS

In this section, we propose our solution to the min-max problem formulated in section 4. First, we consider the intruders’ problem:

$$\min_{q \in V_x} \max_{p \in U} \Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (9)

For a fixed $q$ the problem reduces to the following:

$$\max_{p \in U} \Phi = \frac{1}{|\Omega|} \sum_{x \in \Omega} \alpha_x$$  \hspace{1cm} (10)

In order to maximize the previous equation, it is sufficient to maximize all the terms. Therefore, the problem simplifies to the following:

$$\max_{p \in U} \alpha_x$$  \hspace{1cm} (11)
From the model in section 4, we know that each node is sending one packet to the target node. Therefore, we can divide the budget, $B_s$, among the $|\Omega|$ intruders. Thus, each intruder, $x$, will have the budget constraint $\frac{B_s}{|\Omega|}$ or $B_s|\Omega|^{-1}$. Replacing $\alpha_x$, using Equation (1) and rewriting Equation (11) the problem can be written as follows:

$$\max_{\pi^x \in U_x} \sum_{P \in \rho_x} q(P)[1 - \prod_{e \in P}(1 - \pi^x_e)]$$ \hspace{1cm} (12)

where,

$$\sum_{x \in \Omega} \pi^x_e = p_e,$$ \hspace{1cm} (13)

$$U_x = \{\pi^x : \sum_{e \in E} f_e \pi^x_e \leq B_s|\Omega|^{-1}\}$$ \hspace{1cm} (14)

Having the sampling constraint:

$$\sum_{e \in E} f_e \pi^x_e \leq B_s|\Omega|^{-1}$$ \hspace{1cm} (15)

Knowing (6), Equation (12) reduces to the following:

$$\min_{\pi^x \in U_x} \sum_{P \in \rho_x} [q(P) \prod_{e \in P}(1 - \pi^x_e)]$$ \hspace{1cm} (16)

Note that for any positive function, $f(x)$, in order to minimize that function, it is sufficient to minimize $\ln f(x)$. This follows from the strictly increasing characteristic of the logarithmic function. Since we are solving for a fixed $q$, we can now minimize the following:

$$\min_{\pi^x \in U_x} \sum_{P \in \rho_x} [q(P) \ln \prod_{e \in P}(1 - \pi^x_e)]$$ \hspace{1cm} (17)

which is equal to:

$$\min_{\pi^x \in U_x} \sum_{P \in \rho_x} [q(P) \sum_{e \in P} \ln(1 - \pi^x_e)]$$ \hspace{1cm} (18)

It is evident that $\ln(1 - \pi^x_e) \leq 0$, since $0 \leq \pi^x_e \leq 1$. We introduce $v^x_e$ to be $-\ln(1 - \pi^x_e)$ and rewrite the minimization problem in terms of $v^x_e$:

$$\min_{\pi^x \in U_x} \sum_{P \in \rho_x} [q(P) \sum_{e \in P} -v^x_e]$$ \hspace{1cm} (19)

Or alternatively:

$$\max_{\pi^x \in U_x} \sum_{P \in \rho_x} [q(P) \sum_{e \in P} v^x_e]$$ \hspace{1cm} (20)

Similarly, we have to rewrite the constraints in terms of the new variable, $\pi^x_e$. The sampling constraint is:

$$\sum_{e \in E} f_e \pi^x_e \leq B_s|\Omega|^{-1}$$ \hspace{1cm} (21)

Replacing $\pi^x_e$ with $1 - e^{-v^x_e}$, we get:

$$\sum_{e \in E} f_e (1 - e^{-v^x_e}) \leq B_s|\Omega|^{-1},$$ \hspace{1cm} (22)

which is:

$$\sum_{e \in E} f_e - B_s|\Omega|^{-1} \leq \sum_{e \in E} f_e e^{-v^x_e}$$ \hspace{1cm} (23)

We use the following inequality to simplify the constraint:

$$\prod_{e \in E} f_e (1 - \pi^x_e) \geq \sum_{e \in E} f_e (1 - \pi^x_e)$$ \hspace{1cm} (24)

In order to prove (24), we know from the assumption in Section 3 that $f_e > s_e + 1$. Given that $\pi^x_e = \frac{f_e}{s_e}$, we replace $s_e$ by $\pi^x_e f_e$, which can be written as $f_e > \pi^x_e f_e + 1$. Rephrasing it, we will have $f_e (1 - \pi^x_e) > 1$. Notice that the sum of any number of variables each greater than one is less than or equal to the product of them. Knowing that for all the links $f_e (1 - p_e) > 1$, inequality (24) holds. Now, we substitute $\pi^x_e$ for $1 - e^{-v^x_e}$ in (24):

$$\prod_{e \in E} f_e e^{-v^x_e} \geq \sum_{e \in E} f_e e^{-v^x_e}$$ \hspace{1cm} (25)

Therefore, applying log to both sides of inequality (23), we get:

$$\ln (\sum_{e \in E} f_e - B_s|\Omega|^{-1}) \leq \sum_{e \in E} f_e e^{-v^x_e}$$ \hspace{1cm} (26)

and, using (24) we get:

$$\ln (\sum_{e \in E} f_e - B_s|\Omega|^{-1}) \leq \sum_{e \in E} \ln (f_e e^{-v^x_e})$$ \hspace{1cm} (27)

Or alternatively:

$$\sum_{e \in E} \ln f_e - \sum_{e \in E} v^x_e \geq \ln (\sum_{e \in E} f_e - B_s|\Omega|^{-1})$$ \hspace{1cm} (28)

Consequently, the game will reduce to the following:

$$\max_{\pi^x \in U_x} \sum_{P \in \rho_x} [v^x_e \sum_{e \in P} q(P)]$$ \hspace{1cm} (29)

having the constraints:

$$\sum_{e \in E} v^x_e \leq \sum_{e \in E} \ln f_e - \ln (\sum_{e \in E} f_e - B_s|\Omega|^{-1})$$ \hspace{1cm} (30)

$$v^x_e \geq 0$$

Associating a dual variable $\lambda$ [7], we obtain the following dual optimization problem with the corresponding constraints:

$$\min (\sum_{e \in E} \ln f_e - \ln (\sum_{e \in E} f_e - B_s|\Omega|^{-1}))\lambda$$ \hspace{1cm} (31)

$$\lambda \geq \sum_{P \in \rho_x, e \in P} q(P), \forall x \in \omega, \forall e \in E$$ \hspace{1cm} (32)

$$\lambda \geq 0$$ \hspace{1cm} (33)

$$\sum_{P \in \rho_x} q(P) = 1$$ \hspace{1cm} (34)

Next, we calculate the maximum flow from $x$ to $t$, $MF^x_t(f)$. Knowing that the maximum flow is equal to the summation of the flows on all the paths from $x$ to $t$, we then normalize the flows in the network (with respect to the $MF^x_t(f)$). Therefore, the normalized flow on each path can be interpreted as $q(P)$ and constraints (34) hold. Furthermore, interpreting $q(P)$ as the flow on path $P$ suggests $\sum_{P \in \rho_x, e \in P} q(P)$ to be the normalized flow on link $e$. Hence, in order to minimize $\lambda$,
sends the malicious packet through path $AGCI$, with probability $7/33$.

The game would guide us to the following strategies satisfying the budget constraint. Hence, the intruder $x$'s strategy is:

- Calculate the maximum flow from $x$ to $t$ using $f_e$ as the capacity of the link $e$.
- Use the standard flow decomposition techniques [2] to decompose the maximum flow into flows on paths $P_1, P_2, ..., P_s$ from node $x$ to node $t$ with flows of $m_1, m_2, ..., m_s$ respectively, knowing that $\sum_{i=1}^{s} m_i = MF_x^!(f)$ and $|\rho_x^e| = l_x$.
- Transmit the malicious packet along the path $P_t$ with probability $m_i MF_x^!(f)$.

Consequently, the IDS’s strategy is:

- For each node $x \in \Omega$ find the minimum cut.
- Let $\text{Mincut}_x^t$ denote the set of arcs in the corresponding minimum cut.
- Sample link $e$ at rate:

$$\sum_{x \in \Omega, e \in \text{Mincut}_x^t} B_x |\Omega|^{-1} MF_x^t(f)^{-1} f_e$$

Note that, $\sum_{e \in E} \sum_{x \in \Omega, e \in \text{Mincut}_x^t} B_x |\Omega|^{-1} MF_x^t(f)^{-1} f_e = B_s$ and therefore, satisfying the budget constraint. Now, we illustrate the game with an example as shown in Figure 2, where nodes $A$ and $E$ are the cooperative intruders and node $I$ is the target. In other words, $\Omega = \{A, E\}$ and $|\Omega| = 2$. The budget constraint, $B_s$, is 20. Therefore, $B_s |\Omega|^{-1} = 10$. The maximum flow from $A$ to $I$ is 33 and the maximum flow from $E$ to $I$ is 18 as shown in Figure 2 in bold links. $\text{Mincut}_A^t = \{AB, DG, EG, EF\}$ and $\text{Mincut}_E^t = \{EG, EF\}$. Hence the IDS will sample the links as follows:

- Node $A$ sends the malicious packet through path $ABCI$ with probability $10/33$.
- Node $A$ sends the malicious packet through path $ADGI$ with probability $5/33$.
- Node $A$ sends the malicious packet through path $ADEGCI$ with probability $7/33$.
- Node $A$ sends the malicious packet through path $AEGCI$ with probability $6/33$.
- Node $A$ sends the malicious packet through path $AEFHI$ with probability $5/33$.
- Node $E$ sends the malicious packet through path $EGCI$ with probability $13/18$.
- Node $E$ sends the malicious packet through path $EFHI$ with probability $5/18$.

VI. CONCLUSION

We considered the problem of multiple cooperating intruders attacking a target node by means of network packet sampling. Given a total sampling budget, we developed a network packet sampling strategy to effectively reduce the success chances of the intruders. We considered the scenario where the attackers select paths to minimize the chances of detection. Moreover, we formulated the intrusion detection problem as a zero-sum non-cooperative game between the IDS and the set of attackers. Furthermore, we solved the game to bring up the strategies for both the IDS and the set of intruders. Finally, we illustrated the game with a case study to gain more insights about the solution of the game.

REFERENCES