

Stochastic Games for Security in Networks with Interdependent Nodes

Kien C. Nguyen, Tansu Alpcan, and Tamer Başar

Abstract—This paper studies a stochastic game theoretic approach to security and intrusion detection in communication and computer networks. Specifically, an *Attacker* and a *Defender* take part in a two-player game over a network of nodes whose security assets and vulnerabilities are correlated. Such a network can be modeled using weighted directed graphs with the edges representing the influence among the nodes. The game can be formulated as a non-cooperative zero-sum or nonzero-sum stochastic game. However, due to correlation among the nodes, if some nodes are compromised, the effective security assets and vulnerabilities of the remaining ones will not stay the same in general, which leads to complex system dynamics. We examine existence, uniqueness, and structure of the solution and also provide numerical examples to illustrate our model.

I. INTRODUCTION

Today, as computer networks become ubiquitous, network security and *intrusion detection* (ID) play a more and more important role. The main task of an *intrusion detection system* (IDS) is to detect intrusions and report them to a system administrator. Among various approaches, non-cooperative game theory has recently been employed extensively to study ID problems [1]–[6].

In a general setting, a security game is defined between two players: an Attacker and a Defender (the IDS). A formulation of security games as static games can be found in [1]. In [3], the authors consider security games with imperfect observations and use the finite-state Markov chain framework to analyze such games. The work in [4] employs the framework of Bayesian games to address the intrusion detection problem in wireless ad hoc networks, where a mobile node viewed as a player confronts an opponent whose *type* is unknown.

In [5], the author examines the intrusion detection problem in heterogeneous networks as a nonzero-sum static game. In a complex network, nodes are of different levels of importance to the Defender, and also appear variably attractive to the Attacker. Heterogeneity also stems from hierarchy and correlation among nodes. It is thus essential to consider scenarios where nodes have different security assets. Also, apart from a node's security asset, if we take into account the players' motivations, the cost of attacking, the cost of monitoring, and other factors, the game is no longer a zero-sum one. Using the *Nash Equilibrium* (NE) solution concept,

the analysis allows one to compute the Attacker's optimal strategy as a probability mass distribution on the nodes to attack. Similarly, the Defender's optimal strategy is a probability mass distribution on the nodes to monitor (to collect and process data and detect attacks). However, in this work [5], the security assets are still assumed to be independent. Also, the dynamics of the ID problem when nodes are compromised along the play have not been taken into account.

The work in [6] addresses this problem using the framework of zero-sum stochastic games [8]. The network is now modeled as a discrete-time or continuous-time Markov chain where the network states are defined by the states (compromised or not) of the constituent nodes. This formulation thus takes into account the dynamics of the problem and allows one to incorporate correlation among nodes in terms of vulnerability. The analysis is nonetheless limited to zero-sum games and again, the security assets are considered to be independent.

This paper attempts to extend these earlier works to construct a more comprehensive network security and intrusion detection model. We develop a network model based on *linear influence networks* proposed in [7]. This model, when used under the framework of stochastic games, permits us to take into consideration the correlation among the nodes in terms of both security assets and vulnerabilities.

The rest of this paper is organized as follows. In the remaining part of this section, we summarize the notations and variables used throughout this paper. Next, in Section II, we introduce two linear influence network models for security assets and vulnerabilities. In Section III, we formulate the security game based on these models as a zero-sum stochastic game and present results on existence, uniqueness, and structure of the solution. We then provide a numerical example in Section IV. Finally, some concluding remarks of Section V end the paper.

Summary of notations and variables used in this paper

- \mathcal{N} : Set of nodes in the network.
- n : Number of nodes in the network.
- \mathcal{E}_s : Set of edges representing the influence among node security assets.
- \mathcal{E}_v : Set of edges representing the influence among node vulnerabilities.
- e_{ij} : A directed edge from node i to node j , $e_{ij} \in \mathcal{E}_s$ or $e_{ij} \in \mathcal{E}_v$.
- \mathcal{G}_s : Weighted directed graph for node security assets, $\mathcal{G}_s = \{\mathcal{N}, \mathcal{E}_s\}$

This work was supported by Deutsche Telekom Laboratories and in part by the Boeing Company and the Vietnam Education Foundation.

Tansu Alpcan is with Deutsche Telekom Laboratories, Ernst-Reuter-Platz 7, D-10587 Berlin, Germany tansu.alpcan@telekom.de

Tamer Başar and Kien C. Nguyen are with the Department of Electrical and Computer Engineering and the Coordinated Science Laboratory, University of Illinois at Urbana-Champaign, 1308 W Main St., Urbana, IL 61801, USA basarl@illinois.edu, knguyen4@illinois.edu

- \mathcal{G}_v : Weighted directed graph for node vulnerabilities, $\mathcal{G}_v = \{\mathcal{N}, \mathcal{E}_v\}$
- I, I_{ij} : Influence matrix for security assets and its entries.
- w_{ij} : Influence of node i on node j in terms of security assets, where $i, j \in \mathcal{N}$
- $s = \{s_1, s_2, \dots, s_n\}$: Vector of independent security assets.
- $x = \{x_1, x_2, \dots, x_n\}$: Vector of effective security assets.
- H, h_{ij} : Support matrix and its entries, h_{ij} signifies the support that node i gives node j (against attacks), $0 \leq h_{ij} \leq 1 \forall i, j \in \mathcal{N}$.
- h_j : Support to node j , $j \in \mathcal{N}$, $h_j = \sum_{i=1}^n h_{ij}$.
- p_{n1}^j : Probability that node j is compromised when player 1 (the Attacker) attacks, player 2 (the Defender) does not defend the node, and the support to node j is equal to 1 (full support).
- p_{n0}^j : Probability that node j is compromised when the Attacker attacks, the Defender does not defend the node, and the support to node j is equal to 0 (no support).
- p_{d1}^j : Probability that node j is compromised when the Attacker attacks, the Defender defends the node, and the support to node j is equal to 1 (full support).
- p_{d0}^j : Probability that node j is compromised when the Attacker attacks, the Defender defends the node, and the support to node j is equal to 0 (no support).
- $\{S_1, S_2, \dots, S_p\}$: States in the state space of the system.
- $\{\Gamma_1, \Gamma_2, \dots, \Gamma_p\}$: Game elements of the stochastic game, each of which corresponds to a state of the system.
- p_r^k : Probability that the network goes back to state S_1 , given that it is currently in state S_k , the Attacker attacks one node and the attack fails.
- p_e^k : Probability that the game ends given that it is currently in state S_k , the Attacker attacks one node and the attack fails.
- p_{0r}^k : Probability that the network goes back to state S_1 , given that it is currently in state S_k and the Attacker does not attack any node.
- p_{0e}^k : Probability that the game ends given that it is currently in state S_k and the Attacker does not attack any node.
- a_{ij}^k : Instant amount that player 2 pays player 1 at game element Γ_k , if player 1 plays pure strategy i and player 2 plays pure strategy j .
- q_{ij}^{kl} : Probability that both players have to play game element Γ_l next, given that they are currently at game element Γ_k , if player 1 plays pure strategy i and player 2 plays pure strategy j .
- q_{ij}^{k0} : Probability that the game ends given that they are currently at game element Γ_k , if player 1 plays pure strategy i and player 2 plays pure strategy j .
- m_k : Number of pure strategies for player 1 at game element Γ_k .
- n_k : Number of pure strategies for player 2 at game element Γ_k .
- p ($p = 2^n$): Number of game elements of the stochastic game, or the number of states of the state space.

- α_{ij}^k : A collective entry that includes the instant payoff and the transition probabilities to all game elements, $\alpha_{ij}^k = a_{ij}^k + \sum_{l=1}^p q_{ij}^{kl} \Gamma_l$, given that the players are currently at game element Γ_k , player 1 plays pure strategy i , and player 2 plays pure strategy j .
- b_{ij}^k : Value of α_{ij}^k when we replace game elements Γ_l 's with their values. $b_{ij}^k = a_{ij}^k + \sum_{l=1}^p q_{ij}^{kl} v_l$.
- y_i^{kt} : Probability that player 1 plays pure strategy i when playing game element Γ_k at the t -th stage of the game. For stationary strategies [8], the superscript t will be omitted.
- z_j^{kt} : Probability that player 2 plays pure strategy j when playing game element Γ_k at the t -th stage of the game.
- y^{kt} , ($k = 1, \dots, p$, $t = 1, 2, \dots$): Strategy for player 1, a set of m_k -vectors each of which is a mixed strategy of player 1 at game element Γ_k and t -th stage of the game.
- z^{kt} , ($k = 1, \dots, p$, $t = 1, 2, \dots$): Strategy for player 2, a set of n_k -vectors each of which is a mixed strategy of player 2 at game element Γ_k and t -th stage of the game.
- c_i^k : Pure strategy i for the Attacker at game element Γ_k .
- d_j^k : Pure strategy j for the Defender at game element Γ_k .
- $p_s^k(c_i^k, d_j^k)$: Probability that the attack is successful given that the Attacker plays pure strategy c_i^k and the Defender plays pure strategy d_j^k at game element Γ_k .
- $v = (v_1, v_2, \dots, v_p)$: Value vector of the stochastic game.
- $val(B)$: Value of the zero-sum matrix game given by the matrix B .

II. LINEAR INFLUENCE NETWORK MODELS FOR SECURITY ASSETS AND FOR VULNERABILITIES

We present in this section a network model based on the concept of linear influence networks [7]. The network will be represented by two weighted directed graphs, one signifying the relationship of security assets and the other denoting vulnerability correlation among the nodes.

A. Linear influence network model for security assets

For a particular node, the general term *security asset* is used to signify how important the node is to the network. All the security assets of a network can be modeled as a weighted directed graph $\mathcal{G}_s = \{\mathcal{N}, \mathcal{E}_s\}$ where \mathcal{N} is the set of nodes, and the elements of set \mathcal{E}_s represent the influence among the nodes. Let n be the cardinality of \mathcal{N} . For each edge $e_{ij} \in \mathcal{E}_s$, we denote an associated scalar w_{ij} that signifies the influence of node i on node j , where $i, j \in \mathcal{N}$. The entries of the *influence matrix* I are then given as follows:

$$I_{ij} = \begin{cases} w_{ij} & \text{if } e_{ij} \in \mathcal{E}_s \\ 0 & \text{otherwise,} \end{cases} \quad (1)$$

where $0 < w_{ij} \leq 1 \forall i, j \in \mathcal{N}$ and $\sum_{i=1}^n w_{ij} = 1, \forall j \in \mathcal{N}$. Note that here we allow for the edges of the form $w_{jj} = 1 - \sum_{i=1, i \neq j}^n w_{ij}$, which signifies the portion of influence of a node on the independent security asset of itself.

Let $s = \{s_1, s_2, \dots, s_n\}$ be the vector of *independent security assets*. The vector of *effective security assets*, denoted

by $x = \{x_1, x_2, \dots, x_n\}$ can then be computed by the *influence equation*:

$$x = Is. \quad (2)$$

With the condition $\sum_{i=1}^n w_{ij} = 1, \forall j \in \mathcal{N}$, we have that

$$\begin{aligned} \sum_{i=1}^n x_i &= \sum_{i=1}^n \sum_{j=1}^n w_{ij} s_j = \sum_{j=1}^n \sum_{i=1}^n w_{ij} s_j \\ &= \sum_{j=1}^n s_j \sum_{i=1}^n w_{ij} = \sum_{j=1}^n s_j. \end{aligned} \quad (3)$$

Therefore, the sum of all the effective security assets is equal to the sum of all the independent security assets. The influence matrix thus signifies the redistribution of security assets. The independent security asset of a node i is redistributed to all the nodes in the network that have influence on i (including itself). When a node is down, the node itself and all the edges connected to it will be removed from the graph. Thus the security loss of the network will be the node's effective security asset (instead of its independent security asset). Conversely, if a node is brought back to the network, it regains its original influence on other nodes. In either case, the entries of the influence matrix have to be normalized to satisfy $\sum_{i=1}^n w_{ij} = 1, \forall j \in \mathcal{N}$. For a quick justification of this linear influence model, consider a GSM network, where a base station controller (BSC) i controls several base transceiver stations (BTS), including BTS j . If a BSC fails, all the BTSs connected to it will be out of service. On the contrary, if only one BTS is compromised, the communication among the subscribers under other BTSs should not be affected (provided that the rest of the network is up and running). In such a situation, we can have for example, $w_{jj} = 0.7$ and $w_{ij} = 0.3$. If the BSC is down, there is still an amount of security asset $0.7s_j$ left, even though the BTS is not in service anymore. The reason is that, if this BTS gets connected to another BSC (or if the original BSC is up again), they will together create an added security asset for the network. We present in what follows an example to illustrate the linear influence network model.

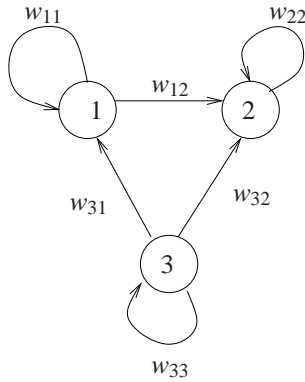


Fig. 1. A linear influence network for security assets of a three-node network.

Example 1: Suppose that we have a network of three nodes with correlations as shown in Fig. 1. As shown in Fig. 2, the states of the system are given as $\{S_1, S_2, \dots, S_p\}$ ($p =$

2^n) where $S_k \in \{0, 1\}^n, k = 1, \dots, p$. Here a node is said to be in state 1 if it is compromised and 0 otherwise. Note that we consider a discrete-time Markov chain where the system can transit from one state to any state of the state space (including the original state). The influence equation

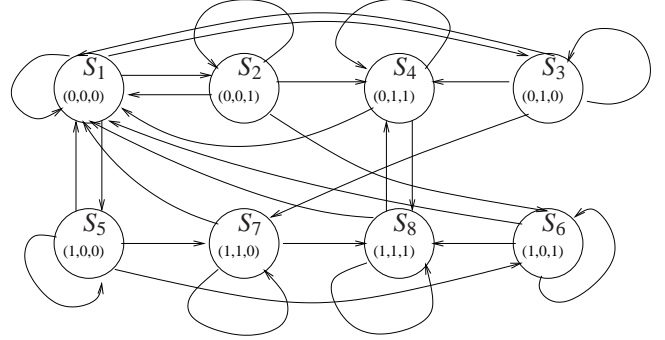


Fig. 2. An example state diagram for the network in Fig. 1.

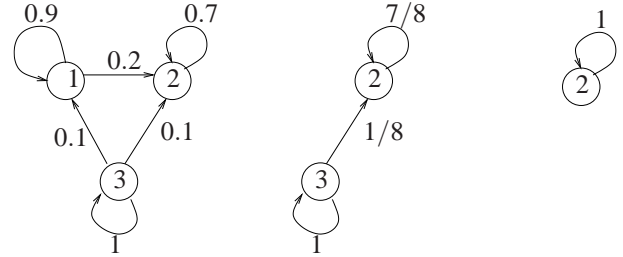


Fig. 3. Changes in a linear influence network for security assets when nodes are compromised (Example 1).

(2) can be written as:

$$\begin{pmatrix} x_1^{(1)} \\ x_2^{(1)} \\ x_3^{(1)} \end{pmatrix} = \begin{pmatrix} 0.9 & 0.2 & 0 \\ 0 & 0.7 & 0 \\ 0.1 & 0.1 & 1 \end{pmatrix} \begin{pmatrix} s_1^{(1)} \\ s_2^{(1)} \\ s_3^{(1)} \end{pmatrix} \quad (4)$$

Now suppose that node 1 is compromised; then the independent security asset of node 3 will remain the same, $s_3^{(2)} = s_3^{(1)}$. The independent security asset of node 2 will be decreased by an amount corresponding to the influence of node 1 on node 2: $s_2^{(2)} = s_2^{(1)} - 0.2s_2^{(1)} = 0.8s_2^{(1)}$. Also, the influences on each node have to be normalized to have $\sum_i w_{ij} = 1$. Thus we now have $w_{32} = 1/8$ and $w_{22} = 7/8$, and the influence equation becomes

$$\begin{pmatrix} x_2^{(2)} \\ x_3^{(2)} \end{pmatrix} = \begin{pmatrix} 7/8 & 0 \\ 1/8 & 1 \end{pmatrix} \begin{pmatrix} s_2^{(2)} \\ s_3^{(2)} \end{pmatrix} \quad (5)$$

Thus we can see

$$\begin{aligned} x_2^{(2)} &= (7/8)s_2^{(2)} = 0.7s_2^{(1)}, \\ x_3^{(2)} &= (1/8)s_2^{(2)} + s_3^{(2)} = 0.1s_2^{(1)} + s_3^{(1)}. \end{aligned}$$

After node 1 goes down, the effective security asset of node 2 remains the same, while that of node 3 is decreased by an amount representing its influence on node 1.

Now if node 3 is in turn compromised, we have a network with one node as in Fig. 3. We have

$$\begin{aligned} s_2^{(3)} &= s_2^{(2)} - s_2^{(2)}/8 = (7/8)s_2^{(2)} = 0.7s_2^{(1)}, \\ x_2^{(3)} &= s_2^{(3)}. \end{aligned}$$

B. Linear influence network model for vulnerabilities

In this subsection, we use the linear influence network model to represent the correlation of node vulnerabilities in a network. Beside the correlation of security assets, nodes also have influence on others' vulnerabilities. For example, within a corporate network, if a workstation is compromised, the data stored in this computer can be exploited in attacks against other workstations; these latter computers thus will become more vulnerable to intrusion. Under the framework of stochastic games, this kind of influence is readily incorporated. For instance, in the network of Example 1, if the Attacker attacks node 1, and the Defender decides not to defend this node, the probability that the system goes from $(0, 1, 0)$ to $(1, 1, 0)$ will be greater than the probability that the system goes from $(0, 0, 0)$ to $(1, 0, 0)$, if node 2 has some influence on node 1 in terms of vulnerability. For $e_{ij} \in \mathcal{E}_v$, we define the *support matrix* as follows

$$H = \begin{cases} h_{ij} & \text{if } e_{ij} \in \mathcal{E}_v \\ 0 & \text{otherwise,} \end{cases} \quad (6)$$

where h_{ij} signifies the support that node i gives node j (against attacks), $0 \leq h_{ij} \leq 1 \forall i, j \in \mathcal{N}$. The *support* to node j , $j \in \mathcal{N}$ is defined as

$$h_j = \sum_{i=1}^n h_{ij}, \quad (7)$$

where $0 \leq h_j \leq 1, \forall j \in \mathcal{N}$. Unlike the model for security assets, here we do not normalize h_j . When a node that supports node j is down, h_j will decrease, and thus the probability that node j is compromised under attack will increase. Let us denote by p_s^j the probability that node j is compromised at each state. We assume an affine relationship between p_s^j and h_j as follows:

- If node j is not attacked then $p_s^j = 0$.
- If node j is attacked, and the Defender is not defending this node, $p_s^j = p_{n0}^j - (p_{n0}^j - p_{n1}^j)h_j$, where p_{n1}^j and p_{n0}^j are the probabilities that the node is compromised given that the support is equal to 1 (full support) and 0 (no support), respectively ($p_{n1}^j < p_{n0}^j$).
- If node j is attacked, and the Defender is defending this node, $p_s^j = p_{d0}^j - (p_{d0}^j - p_{d1}^j)h_j$, where p_{d1}^j and p_{d0}^j are the probabilities that the node is compromised given that the support is equal to 1 and 0, respectively ($p_{d1}^j < p_{d0}^j$).
- Also, it is assumed that $p_{d1}^j < p_{n1}^j$ and $p_{d0}^j < p_{n0}^j$.

A weighted directed graph for network vulnerabilities is shown in Fig. 4.

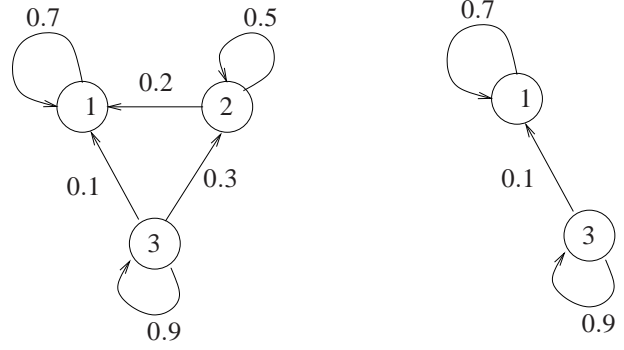


Fig. 4. A linear influence network for vulnerabilities and the changes of supports when one node is compromised.

III. THE NETWORK SECURITY PROBLEM AS A ZERO-SUM STOCHASTIC GAME

A. A brief overview of zero-sum stochastic games

In this subsection, we provide a brief overview of zero-sum stochastic games based on [8]. A stochastic game consists of p game elements $\Gamma_k, k = 1, \dots, p$. Each game element is associated with an $m_k \times n_k$ matrix, whose entries are given by

$$\alpha_{ij}^k = a_{ij}^k + \sum_{l=1}^p q_{ij}^{kl} \Gamma_l, \quad (8)$$

where $q_{ij}^{kl} \geq 0, l = 1, \dots, p, i = 1, \dots, m_k, j = 1, \dots, n_k$,

$$\sum_{l=1}^p q_{ij}^{kl} < 1, \forall k, i, j. \quad (9)$$

Expression (8) can be interpreted as follows. At game element Γ_k , if player 1 chooses pure strategy i and player 2 chooses pure strategy j , player 2 has to pay player 1 an amount a_{ij}^k . Furthermore, there is a probability q_{ij}^{kl} that both players have to play game element Γ_l next, and a probability

$$q_{ij}^{k0} = 1 - \sum_{l=1}^p q_{ij}^{kl} \quad (10)$$

that the game will end. With condition (9), the probability of infinite play is guaranteed to be zero, and the expected payoff of player 1 (or the expected loss of player 2), which is accumulated through all the stages of the game, is finite [8].

A strategy for player 1 is a set of m_k -vectors, denoted by $y^{kt}, k = 1, \dots, p, t = 1, 2, \dots$, each of which satisfies

$$\sum_{i=1}^{m_k} y_i^{kt} = 1, \quad (11)$$

$$y_i^{kt} \geq 0 \quad (12)$$

Here y_i^{kt} is the probability that player 1 plays pure strategy i if he is playing game element Γ_k at the t -th stage of the game. A strategy is said to be stationary if the vectors y^{kt} are independent of t for all k . In this case, the superscript t can be omitted. Similarly, a strategy for player 2 is a set of n_k -vectors, z^{kt} , where $\sum_{j=1}^{n_k} z_j^{kt} = 1$ and $z_j^{kt} \geq 0$. Given a pair

of strategies, we can compute the vector of expected payoffs $v = (v_1, v_2, \dots, v_p)$, where v_k , $k = 1, \dots, p$ is the expected payoff (to player 1) if the first stage of the game is Γ_k .

With the above settings, it is known [8], that we can replace the game element Γ_k by the value component

$$v_k = \text{val}(B_k), \quad (13)$$

where $\text{val}(B_k)$ is the value (in mixed strategies) of the matrix game B_k , and B_k is the $m_k \times n_k$ matrix whose entries are given by

$$b_{ij}^k = d_{ij}^k + \sum_{l=1}^p q_{ij}^{kl} v_l. \quad (14)$$

B. A zero-sum stochastic game model for network security

In this subsection we formulate the security problem as a zero-sum stochastic game. This is a modified version of the game presented in [6], applied to the linear influence network model proposed in Section II. At each state k , $k = 1, \dots, p$, the Attacker's pure strategies consist of $m_k = n + 1$ actions, where n is the number of nodes in the network:

- Attack one of n nodes, c_i^k , where $i = 1, \dots, n$.
- Do nothing, $c_{m_k}^k = \emptyset$.

Note that this strategy space is for use with more general payoff formulations. However, with the payoff formulation in this paper, the Attacker will not have motivation to attack a node that is already compromised, unless all the nodes have been compromised. For each k , the Defender's pure strategies are $\{d_i^k\}$, where

- Defend node i , d_i^k , $i = 1, \dots, n_k - 1$,
- Do nothing, $d_{n_k}^k = \emptyset$,

where $n_k = m_k = n + 1$. For each possible combination of the Attacker's and the Defender's pure strategies, the entries of the payoff matrix are:

$$\alpha_{ij}^k = a_{ij}^k + \sum_{l=1}^p q_{ij}^{kl} \Gamma_l, \quad (15)$$

where $a_{ij}^k = p_s^k(c_i^k, d_j^k) x^k(i)$, $p_s^k(c_i^k, d_j^k)$ is the probability that the attack is successful, and $x^k(i)$ is the effective security asset of the node being attacked, i . Note that once a node is compromised, the effective security assets and the supports of the remaining nodes have to be recalculated as in Example 1 and Fig. 4. As mentioned in Subsection II-B, the probabilities p_s^k , and thus q_{ij}^{kl} , are dependent on the supports to the nodes, and are therefore affected by the correlation in vulnerabilities of the nodes. It can be said that once we have incorporated node vulnerabilities into our model, we have already implicitly taken care of the cost of attacking/defending. For example, if a node is of high security asset but difficult to compromise (the transition probability to the compromise state is small), the Attacker may turn to another node with a smaller security asset, which is easier to attack.

At a state S_k , if the Attacker chooses to attack one node and the attack fails, there is a probability $p_r^k \in (0, 1)$ that the network will go back to state S_1 (which means the Defender has detected the Attacker and managed to restore

all the compromised nodes and the game restarts at S_1), and a probability $p_e^k \in (0, 1)$ that the game will end (which means the Defender has detected the Attacker and stopped him from further intruding). Note that $p_r^k + p_e^k \leq 1$ with equality only when $S_k = S_1(0, 0, \dots, 0)$. Similarly, at one point, if the Attacker chooses not to attack at all, there is a probability $p_{0r}^k \in (0, 1)$ that the network will go back to state S_1 , and a probability $p_{0e}^k \in (0, 1)$ that the game will end. Given $0 < p_{d1}^j, p_{n1}^j, p_{d0}^j, p_{n0}^j < 1$, $j \in \mathcal{N}$, p_r^k, p_e^k, p_{0r}^k , and p_{0e}^k , $k = 1, \dots, p$, and the support matrix H , p_s^k and q_{ij}^{kl} can be calculated using the equations in Subsection II-B. A numerical example is shown in Section IV.

C. Existence, uniqueness, and structure of the solution

We present in this subsection some analytical results for the game given in III-B, based on zero-sum stochastic game theory [8], [9].

Proposition 1: In the zero-sum stochastic game given in III-B, the probability of infinite play is zero and the expected payoff of the Attacker (which is also the expected cost of the Defender) is finite.

With the setup in III-B, we can show that $q_{ij}^{k0} = 1 - \sum_{l=1}^p q_{ij}^{kl} > 0$, $\forall k$ and $\forall i, j$ of each game element Γ_k . Thus the proposition is proved using the theory of stochastic games.

Proposition 2: (Theorem V.3.3 [8]) In the zero-sum stochastic game given in III-B, there exists exactly one vector $v = (v_1, v_2, \dots, v_p)$ that satisfies (13) and (14).

Using the results from III-A, we can then compute the NE of the game, which is a pair of stationary mixed strategies for the Attacker and for the Defender at each state.

Proposition 3: (Theorem V.3.3 [8]) The vector $v = (v_1, v_2, \dots, v_p)$ that satisfies (13) and (14) can be derived through the following recursive equations:

$$v^0 = (0, 0, \dots, 0), \quad (16)$$

$$b_{ij}^{kr} = a_{ij}^k + \sum_{l=1}^p q_{ij}^{kl} v_l^r, \quad (17)$$

$$v_k^{r+1} = \text{val}(B_k^r) = \text{val}(b_{ij}^{kr}). \quad (18)$$

We can stop the recursion at a desired level of accuracy and then use the current value of vector $v = (v_1, v_2, \dots, v_p)$ to compute B_k using (14). The mixed strategies of the players at each game element Γ_k are the NE in mixed strategies of the matrix game B_k . The strategies so obtained will converge to optimal stationary strategies of the stochastic game.

IV. A NUMERICAL EXAMPLE

In this section, we implement numerical simulation for a specific network with three nodes. The setup in III-B is carried over with some further assumptions as follows. First, we adopt a simplified state diagram as given in Fig. 1. Basically, after each time step, we only allow for transitions where one more node is compromised, the transition that returns to the same state, and the transition back to $S_1(0, 0, 0)$. Second, suppose that the influence equation is given as

follows (Example 1)

$$\begin{pmatrix} x_1^{(1)} \\ x_2^{(1)} \\ x_3^{(1)} \end{pmatrix} = \begin{pmatrix} 0.9 & 0.2 & 0 \\ 0 & 0.7 & 0 \\ 0.1 & 0.1 & 1 \end{pmatrix} \begin{pmatrix} 10 \\ 10 \\ 20 \end{pmatrix} = \begin{pmatrix} 11 \\ 7 \\ 22 \end{pmatrix}, \quad (19)$$

and the support matrix is given by (Fig. 4)

$$H = \begin{pmatrix} 0.7 & 0 & 0 \\ 0.2 & 0.5 & 0 \\ 0.1 & 0.3 & 0.9 \end{pmatrix}. \quad (20)$$

Finally, $p_{d1}^j = 0.2$, $p_{n1}^j = 0.4$, $p_{d0}^j = 0.5$, $p_{n0}^j = 0.7$, $\forall j \in \mathcal{N}$, $p_r^k = 0.2$, $\forall k \neq 1$, $p_r^1 = 0.7$, $p_e^k = 0.3$, $\forall k = 1, \dots, p$, $p_{0r}^k = 0.2$, $\forall k \neq 1$, $p_{0r}^1 = 0.7$, and $p_{0e}^k = 0.3$, $\forall k = 1, \dots, p$.

For example, suppose the system is at $S_1 (0,0,0)$. The next state could be one in $\{S_1 (0,0,0), S_2 (0,0,1), S_3 (0,1,0), S_5 (1,0,0)\}$. The Attacker's pure strategies include 1,2,3, and \emptyset , which mean to attack node 1, node 2, node 3, and do nothing, respectively. Similarly, the Defender's pure strategies include 1,2,3, and \emptyset . Using the above results, we have that

$$\begin{aligned} a_{11}^1 &= p_s^1(1,1)x_1^{(1)}, \\ q_{11}^{11} &= (1 - p_s^1(1,1))(1 - p^{1e}), \\ q_{11}^{15} &= p_s^1(1,1), \\ q_{11}^{1j} &= 0 \quad \forall j \neq 1,5, \end{aligned}$$

where $p_s^1(1,1) = p_{d0} - (p_{d0} - p_{d1})1 = p_{d1}$, as at this state, node 1 still has full support. Also, there is a probability $p_g^{1e} = (1 - p_s^1(1,1))p^{1e} > 0$ that the game will end. If the Attacker attacks node 1 and the Defender defends node 2, we have that

$$\begin{aligned} a_{12}^1 &= p_s^1(1,2)x_1^{(1)}, \\ q_{12}^{11} &= (1 - p_s^1(1,2))(1 - p^{1e}), \\ q_{12}^{15} &= p_s^1(1,2), \\ q_{12}^{1j} &= 0 \quad \forall j \neq 1,5, \end{aligned}$$

where $p_s^1(1,1) = p_{n0} - (p_{n0} - p_{n1})1 = p_{n1}$, again as at this state, node 1 still has full support. Also, there is a probability $p_g^{1e} = (1 - p_s^1(1,2))p^{1e} > 0$ that the game will end. Now, suppose that the system is at $S_5 (1,0,0)$. The next state could be one in $\{S_1 (0,0,0), S_5 (1,0,0), S_6 (1,0,1), S_7 (1,1,0)\}$. The Attacker's pure strategies include 2,3, and \emptyset , which mean to attack node 2, node 3, and do nothing, respectively. Similarly, the Defender's pure strategies include 2,3, and \emptyset . Now we have that

$$\begin{aligned} a_{22}^5 &= p_s^2(2,2)x_2^{(5)}, \\ q_{22}^{57} &= p_s^2(2,2), \\ q_{22}^{51} &= (1 - p_s^2(2,2))p_r^5, \\ q_{22}^{55} &= (1 - p_s^2(2,2))(1 - p_r^5 - p_e^5), \\ q_{22}^{5j} &= 0 \quad \forall j \neq 1,5,7, \end{aligned}$$

where $p_s^2(2,2) = p_{d0}^2 - (p_{d0}^2 - p_{d1}^2)0.8$, as at this state, node 2 has a support of 0.8. Also, there is a probability $p_g^{5e} =$

GE	Node 1	Node 2	Node 3	Do nothing
1 (0,0,0)	0.6126	0	0.3874	0
2 (0,0,1)	0.3817	0.6183	0	0
3 (0,1,0)	0.6415	0	0.3585	0
4 (0,1,1)	1	0	0	0
5 (1,0,0)	0	0.6568	0.3432	0
6 (1,0,1)	0	1	0	0
7 (1,1,0)	0	0	1	0
8 (1,1,1)	0.25	0.25	0.25	0.25

TABLE I

OPTIMAL STRATEGIES FOR THE ATTACKER AT EACH GAME ELEMENT (GE).

GE	Node 1	Node 2	Node 3	Do nothing
1 (0,0,0)	0.0702	0	0.9298	0
2 (0,0,1)	0.6614	0.3386	0	0
3 (0,1,0)	0.0869	0	0.9131	0
4 (0,1,1)	1	0	0	0
5 (1,0,0)	0	0.034	0.966	0
6 (1,0,1)	0	1	0	0
7 (1,1,0)	0	0	1	0
8 (1,1,1)	0.25	0.25	0.25	0.25

TABLE II

OPTIMAL STRATEGIES FOR THE DEFENDER AT EACH GAME ELEMENT.

$(1 - p_s^2(2,2))p^{5e} > 0$ that the game will end. The other entries of other game elements can be calculated in a similar way. Using the recursive procedure given in Proposition 3, we can then compute the optimal strategy of each player and the value of the game. The value vector converges to an accuracy of 10^{-4} after 56 iterations. The optimal strategies of the Attacker and the Defender, and the value vector are given in Tables I, III, and III. As can be seen from Table I, for example, when all the nodes are up and running, the Attacker wants to attack node 1 with probability 0.6126 and node 3 with probability 0.3874, while the Defender wants to defend node 1 with probability 0.0702 and node 3 with probability 0.9298. Recall that the effective security assets of nodes 1, 2, and 3 at this state are 11, 7, and 22, respectively. It is worth noting that the mixed strategies for the players can also be interpreted as the way to allocate their resources in the security game.

GE	1	2	3	4
Payoffs	19.6078	15.8301	17.9557	12.3392
GE	5	6	7	8
Payoffs	17.9659	13.0283	15.3228	7.8431

TABLE III

THE VALUE VECTOR (THE EXPECTED PAYOFFS OF THE ATTACKER, ALSO THE EXPECTED LOSSES OF THE DEFENDER AT EACH GAME ELEMENT).

V. CONCLUSION

In this paper we have proposed a new network model based on linear influence networks to represent the interdependence of nodes in terms of security assets and vulnerabilities. We took the first step to formulate the security game between an Attacker and a Defender over this network using the framework of zero-sum stochastic game theory. The optimal solution obtained allows one to comprehend the behavior of a rational attacker, as well as to provide IDSs with guidelines on how to allocate their resources. Moreover, modeling networks with linear influence network models helps facilitate solving the security games using software programs. As mentioned earlier, apart from a node's security asset, if we take into account the players' motivations, the cost of attacking, the cost of monitoring, and other factors, the game is no longer a zero-sum one. This work thus can be extended to nonzero-sum stochastic games, where we can address more flexible and practical payoff formulations. Furthermore, in many real-world scenarios, neither the Attacker nor the Defender has full knowledge of the network's nodes and their correlation. Thus studying stochastic security games with incomplete information is an intriguing research direction.

VI. ACKNOWLEDGMENTS

We would like to thank Deutsche Telekom Laboratories, the Boeing Company, and the Vietnam Education Foundation for their support. We are also grateful to four anonymous reviewers for their valuable comments.

REFERENCES

- [1] T. Alpcan and T. Başar, "A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection", *Proceedings of the 42nd IEEE Conference on Decision and Control*, Hawaii, USA, 2003, pp. 2595–2600.
- [2] T. Alpcan and T. Başar, "A game theoretic analysis of intrusion detection in access control systems," *Proceedings of the 43rd IEEE Conference on Decision and Control*, Paradise Island, Bahamas, 2004, pp. 1568–1573.
- [3] T. Alpcan and T. Başar, "An intrusion detection game with limited observations," *Proceedings of the 12th Int. Symp. on Dynamic Games and Applications*, Sophia Antipolis, France, 2006.
- [4] Y. Liu, C. Comaniciu, and H. Man, "A Bayesian game approach for intrusion detection in wireless ad hoc networks," *Proceedings of the Workshop on Game Theory for Networks (GameNets)*, Pisa, Italy, 2006.
- [5] L. Chen, "On Selfish and Malicious Behaviors in Wireless Networks - A Non-cooperative Game Theoretic Approach," Ph.D. thesis, Telecom ParisTech, 2008.
- [6] K. Sallhammar, "Stochastic Models for Combined Security and Dependability Evaluation," Ph.D. thesis, Norwegian University of Science and Technology, 2007.
- [7] R. A. Miura-Ko, B. Yolken, N. Bambos, and J. Mitchell, "Security Investment Games of Interdependent Organizations," *Proceedings of the 46th Allerton Conference*, Illinois, USA, Sep., 2008.
- [8] G. Owen, *Game Theory*, 3rd Ed., California: Academic Press, 2001.
- [9] L. Shapley, "Stochastic games," *Proc. Natl. Acad. Sci. USA* 39 (1953) 1095-1100.