Modeling Stepping Stone Attacks with Constraints in Cyber Infrastructure

Marco A. Gamarra, Sachin Shetty, Oscar R. Gonzalez
Old Dominion University
Norfolk, VA 23529
Email: [mgama002, sshetty, ogonzale]@odu.edu

David M. Nicol
University of Illinois at Urbana-Champaign
Urbana, IL 61801
Email: dmnicol@illinois.edu

Laurent Njilla
U.S. Air Force Research Laboratory
Rome, NY
E-mail: laurent.njilla@us.af.mil

***Abstract*—Most cyber attacks involve an attacker launching a multi-stage attack by exploiting a sequence of hosts. This multi-stage attack generates a chain of "stepping stones" from the origin to target. The choice of stepping stones is a function of the degree of exploitability, the impact, attacker's capability, masking origin location, and intent. In this paper, we model and analyze scenarios wherein an attacker employs multiple strategies to choose stepping stones. The problem is modeled as an Adjacency Quadratic Shortest Path using dynamic vulnerability graphs with multi-agent dynamic system approach. Using this approach, the shortest stepping stone attack with maximum node degree and the shortest stepping stone attack with maximum impact are modeled and analyzed.**

I. Introduction

Stepping stone attack is a sophisticated technique used by adversaries to launch multi-stage attacks on computer networks. The choice of stepping stones is influenced by the attacker's goal, the increased difficulty of attribution, the exertion of minimum effort, etc. Security risk assessment of critical infrastructure hinges on the ability to quantify the probability of lateral propagation of attackers [1], [2], [3], [4]. The identification of attacker stepping stones is essential for security administrators to aid the mitigation process.

Stepping stone attacks have been modeled and estimated the most vulnerable paths corresponding to stepping stone attacks using **Montecarlo** simulations [5]. In [6], the analysis of stepping stone attacks with fixed and switching topology with a dynamic multi-agent system approach has been proposed. In this approach, the authors have introduced a *dynamic vulnerability graph*, which is a network of dynamic multi-agent systems [7], and the Biased min-consensus protocol introduced in [8] has been discretized for the calculation of the shortest stepping stone path between source and target nodes when the vulnerability graph is static (fixed topology), and when the vulnerability graph evolves in the time (switching topology). The switching topology network is modeled as a switched dynamical system where the vulnerability graph changes according to a switching signal.

In [5] and [6], the models have assumed that the attackers exert the minimum effort in the selection of the stepping stone attack as a unique criteria, and the most vulnerable stepping stone path is calculated as the shortest path. However, according to the experience attackers are not limited to one criterion in the selection of the stepping stones, for mention a few examples of other criteria in the stepping stone selection we have:

- *Stepping stone path with maximum node degree:* To design an efficient method for searching a specific file in peer-to-peer networks, the so-called *maximum degree strategy* has been proposed [9], [10], this approach is based on the assumption that a node has information on its neighbors' degree. In the context of stepping stone attacks, an attacker that is resident in a node searching a specific file may move whenever is possible to the neighbor node having the highest degree, because of the highest-degree nodes are connected to a significant fraction of all nodes in the network and the attacker would need only a few steps to find a node that is a neighbor of the target. Then, the attacker wishes to minimize the attack cost but also move to the highest-degree node.
- *Stepping stone path with maximum impact:* Attackers may cause several kinds of damages according to the knowledge they have on organizations configuration and of systems vulnerabilities. In a stepping stone attack, the attacker's damage in every step is according to the knowledge they have on the portion of the network configuration and vulnerabilities that they can see from his current position. Usually, damage evaluation activities are estimated in two ways. First, directly by searching the specific damages caused by the attack on the technological environment, which might be a complex task to perform due to destroyed by the attacker. Second, indirectly by comparing after-attack systems integrity to before-attack integrity, in this approach, a quantification of the damage is performed, focusing on estimating the integrity impacts which is a metric used by security scoring models. An attacker may wish to minimize the attack cost but also look to maximize the impact.
- *Stepping stone path with variance constraint:* The attackers are *risk-averse*, and they will not attack unless their perceived risk to be detected below some threshold [11],

DISTRIBUTION A. Approved for public release: distribution unlimited. Case Number: 88ABW-2019-2269. Dated 15 May 2019

978-1-7281-0962-6/19/$31.00 ©2019 IEEE

in this context, the attacker wishes to minimize the cost and probability of detection simultaneously.

The problems described above involve variants of the classic Shortest Path Problem (SPP) in which additional costs are considered with the presence of pairs of edges in the solution. In other words, the objective function takes into account not only the cost of each edge but also the cost of the interactions among the edges. In the literature, this kind of problems is called Quadratic Shortest Path Problem (QSPP) [12], [13], [14], [15], because can be modeled by a quadratic objective function on binary variables associated with each edge [13]. The QSPP is the problem of finding a path in a directed graph from the source vertex a to the target vertex b such that the sum of costs of the edges and the sum of interaction costs overall distinct pairs of edges on the path is minimized. In stepping stone attacks, an attacker that is resident in a host is *constrained* to exploit vulnerabilities of an adjacent host, that is that the vulnerabilities of the host that are not adjacent to the attackers' current position does not influence the selection of its next stepping stone. This is a variant of the QSPP called *Adjacent QSPP* (AQSPP) [13], [15]. In this paper, we will develop mathematical models for the analysis and simulation of stepping stone attacks with a maximum degree and with maximum impact, respectively.

To represent *potentially-conflicting criteria* in the selection of the path in every step, multiple edge cost can be introduced, and the cost of the constraints is incorporated into the objective function, yielding an AQSPP problem [12], [13]. In this venue, we will introduce more than one score to the same edge for modeling, and analysis of the most vulnerable stepping stone path. In correspondence with the related literature, we will call this problem as *Adjacent Quadratic Stepping Stone Attack*.

This paper is a generalization of, [6] and attempts to calculate the most vulnerable stepping stone path when the attacker use more that one criterion in the selection of the stepping stones. The main contribution of this paper is twofold:

First. A mathematical model for the propagation of stepping stone attacks in a dynamic vulnerability graph with multi-agent dynamic system approach when the attacker use more of one criterion in the selection of the stepping stones is proposed as an AQSPP, where an interplay between min-consensus and min-plus algebra is used for modeling and analysis.

Second. The AQSPP is solved as an SPP, providing an necessary and sufficient conditions for finite-time convergence to the shortest path.

The rest of the paper is organized as follows: Section 2 discusses the background, Section 3 is devoted to developing the model of the adjacent Quadratic stepping stone attack in a dynamic vulnerability graph with a multi-agent dynamic systems approach. Section 4 discusses the paper's results, and Section 5 provides the paper's conclusions.

II. Background

A. Vulnerability Graph and Stepping Stones

Consider as network $\mathcal{N}$ with m host $\{h_1, \ldots, h_m\}$. Each host h_i has a set of applications, and each application has a set of well-known vulnerabilities (eventually empty), and an open port through an authorized, or an unauthorized user may gain access to h_i.

Definition II.1. *A **Vulnerability graph** $G = (V, E)$ associated with the network $\mathcal{N}$ is a directed graph that represents ways in which an adversary can exploit sequentially different vulnerabilities to disrupt the system. The set of nodes $V = \{v_1, \ldots, v_n\}$ represent all the vulnerabilities of the network $\mathcal{N}$ and $E \subseteq V \times V$ is the set of directed edges of G that represent the vulnerability relations.*

If v_i and v_j are vulnerabilities of applications running in hosts h_k and h_l of $\mathcal{N}$ respectively, the directed edge (v_i, v_j) on G, means that the system rules allow accessing host h_l from host h_k trough the vulnerability v_j. In other words, the edge (v_i, v_j) on G will enable an attacker that is resident in h_k trough the vulnerability v_i, to reach h_l trough the vulnerability v_j.

Definition II.2. *The **edge cost** is a function ζ over the set of edges E that quantifies any property related to exploiting a vulnerability, formally*

$$\zeta : E \longrightarrow A \subseteq \mathbb{R}; \quad (v_i, v_j) \longrightarrow \zeta[(v_i, v_j)] \tag{1}$$

An edge cost function that is used in this paper is the *exploit complexity score* [5], defined as $\zeta_c : E \longrightarrow [0 \quad 10]$; $\zeta_c[(v_i, v_j)] = \epsilon_{ij} = 10 - \varepsilon_{ij}/A_v$, which has a range between 0 and 10, where ε_{ij} is the *exploitability subscore* of the vulnerability v_j and A_v is its *accessibility vector* that is provided by the Common Vulnerability Scoring System (CVSS) [16], [17]. The smaller ϵ_{ij}, the easier it is to exploit the vulnerability. See [5] for more details on the construction of this score.

Definition II.3. *A **stepping stone path** is a path through a vulnerability graph. The **cost** of a stepping stone path is defined as the sum of the costs of the edges of the path.*

B. Dynamic Graph

Let $G = (V, E)$ be a directed graph with a vertex set $V = \{v_1, \cdots, v_n\}$ and edge set E. Let $x_i \in \mathbb{R}$ denote the value of vertex v_i. Definition II.4 and Definition II.5 are introduced according to [7].

Definition II.4. *[7] The pair (G, x) with $x = [x_1 \cdots x_n]^T$ is called an **algebraic graph** with value $x \in \mathbb{R}^n$ and topology (or information flow) G. The value x_i of a vertex v_i represents any physical quantities or any other attribute of the network.*

If x_i in the algebraic graph (G, x) is a dynamic agent with dynamics $\frac{dx}{dt} = \dot{x}_i(t) = f_i(x(t), u_i)$, $i \in I = \{1, \cdots, n\}$.

Definition II.5. *[7] A **dynamic graph** is a dynamical system with a state (G,x) in which the value $x = [x_1 \cdots x_n]^T$ evolves according to the network dynamics*

$$\dot{x}_i = f_i(x, u_i), \quad \forall i = 1, 2, \ldots, n \tag{2}$$

*where $u_i = g_i(x)$ is called a **distributed protocol** with topology G.*

An algebraic graph is called **algebraic network**, and a dynamical graph is called a **dynamic network**. In the rest of the paper, a simple case of the dynamical network (2) when $f_i(x, u_i) = u_i$ is considered, that is,

$$\dot{x}_i(t) = u_i(t), \quad \forall i = 1, 2, \ldots, n \tag{3}$$

We denote with N_i the set of all the vertex x_j neighbors of x_i, that is $N_i = \{x_j : (x_i, x_j) \quad \text{is an edge in } G\}$. All edge cost defined over an edge (x_i, x_j) is denoted with a lower case letter with subscripts ij.

C. Biased Min-Consensus

The following nonlinear distribute protocol

$$\dot{x}_i = -x_i + \min_{j \in N_i}(x_j + w_{ij}) \tag{4}$$

where w_{ij} is the edge cost of (x_i, x_j), is called *biased min-consensus protocol* [8] that asymptotically converges to the equilibrium point x_i^* [8], that is, $\lim_{t\to\infty} x_i(t) = x_i^*$ which satisfies the equation $x_i^* = \min_{j\in N_i}(x_j^* + w_{ij})$, with $i = 1, \ldots, n$.

D. Leader-Follower Strategy

In many applications of multi-agent systems, a leader-follower strategy is considered. In this approach, a subset of agents is called *leader set* N_l, and the remaining agents are called *follower set* N_f. In this context, the biased min-consensus is

$$\begin{cases} \dot{x}_i = \mu_i & \text{if } i \in N_l \\ \dot{x}_i = -x_i + \min_{j\in N_i}(x_j + w_{ij}) & \text{if } i \in N_f \end{cases} \tag{5}$$

respectively, where μ_i is an exogenous input. If $\mu_i = 0$, the systems are called *static leaders*. The following theorem has been stated and proven in [8].

Theorem II.1. *[8] Let G be an undirected connected graph and suppose that the dynamical network (G, x) evolves according to the protocol* (5) *with static leaders. Then the system asymptotically converges to the equilibrium point x^* of* (5)*, which satisfies the following equation:*

$$\begin{cases} x_i^* = x_i(0) & \textit{if } i \in N_l \\ x_i^* = \min_{j\in N_i}(x_j^* + w_{ij}) & \textit{if } i \in N_f \end{cases} \tag{6}$$

E. Biased Min-Consensus and Shortest Patch

The relationship between the biased min-consensus protocol in a dynamical network (G, x) and the shortest path in G has been developed in [8] as follows: ***First***, the leader agents are static, that is $\dot{x}_i(t) = 0, \forall x_i \in N_l$, and are called *destination nodes*. The follower agents are called *source nodes*. ***Second***, if there is an edge between x_i and x_j, the weight w_{ij} of this edge is the *length* between these agents. ***Third***, the system evolves according to the protocol (5) with static leaders. Note that according to the optimality principle of Bellman's dynamic programming [18], the solution of the considered shortest path problem satisfies the following nonlinear equations:

$$\begin{cases} x_i^* = 0 & \text{if } i \in N_l \\ x_i^* = \min_{j\in N_i}(x_j^* + w_{ij}) & \text{if } i \in N_f \end{cases} \tag{7}$$

which are the equilibrium points of (5) with static leaders and $x_i(0) = 0, \quad \forall x_i \in N_l$.

The following theorem has bee stated and proven in [8].

Theorem II.2. *[8] If $x_i(0) = 0, \quad \forall x_i \in N_l$, then the equilibrium of the system* (5) *with statics leaders is given by* (7)*, which forms a solution to the corresponding shortest path problem.*

Remark II.1. ***1)*** *When the estates have reached the equilibrium point* (7)*, the shortest path can be found by recursively finding the parent nodes [8].* ***2)*** *According to Theorem II.1 and Theorem II.2, all the states values of the system globally converges to the lengths of the corresponding shortest path independently of the initial state values [8].*

The following subsections has been proposed in [6].

F. Stepping stone Dynamics

1) Fixed Topology Case: Given a vulnerability graph G with m hosts $\{h_1, \ldots, h_m\}$, and n vulnerabilities, a dynamic graph (G, x) is assigned such that for every vulnerability v_i there is a state $x_i \in \mathbb{R}$ and the weight of the edge (x_i, x_j) is its exploit complexity score ϵ_{ij}. A leader-follower strategy is used where the states x_i evolves according to biased min-consensus dynamics (5) with static leaders; in this model, the leaders are called *valuable targets*, and the followers are called *source nodes*. Given a valuable target x_l, the state of the source x_i is defined as the minimum stepping stone cost from x_i to x_l, that is, the minimum length of the path from x_i to x_l. Mathematically, the stepping stone dynamics can be written as

$$\begin{cases} \dot{x}_i(t) = 0, \quad x_i(0) = 0 & \text{if } i \in N_l \\ \dot{x}_i(t) = -x_i(t) + \min_{j\in N_i}(x_j(t) + \epsilon_{ij}) & \text{if } i \in N_f \end{cases} \tag{8}$$

then, according to Theorem II.2, in the equilibrium $x_i^* \in N_f$ is the minimum stepping stone cost from x_i to any valuable target x_l, then by remark II.1, the shortest path from x_i to x_l has been calculated which represent the most vulnerable stepping stone path and can be interpreted as the most probable stepping stone attack from host x_i to the valuable target x_l. As has claimed in [5], according to experience, as an attacker penetrates more deeply into a system, the *exploit complexity score* should change, as a consequence the graph topology change as well. A more realistic model where the *exploit complexity score* change as the attack penetrates more deeply in the system is developed in the following subsection.

2) Switching Topology Case: Let $\{G_1, \ldots, G_m\}$ be a finite collection of vulnerability graphs with the same hosts and $s : \mathbb{R} \longrightarrow \{1, \ldots, m\}$ a switching signal. For every $s(t) = l$, a vulnerability graph $G_l \in \{G_1, \ldots, G_m\}$ and its associated dynamic graph (G_l, x) are well defined, then the stepping

stone dynamics *with switching topology* is equivalent to the *hybrid system*

$$\begin{cases} \dot{x}_i(t) = 0, \quad x_i(0) = 0 & \text{if } i \in N_l \\ \quad l = s(t) & \\ \dot{x}_i(t) = -x_i(t) + \min_{j \in N_i}(x_j(t) + \epsilon_{ij}(l)) & \text{if } i \in N_f \end{cases} \tag{9}$$

where $\epsilon_{ij}(l)$ is the exploit complexity score of (x_i, x_j) in the dynamic vulnerability graph (G_l, x).

The progress of the stepping stone dynamics is monitored at δ time intervals; hence, the stepping stone dynamics at a discrete time for the fixed topology case is

$$\begin{cases} x_i[k+1] = x_i[k], \quad x_i[0] = 0 & \text{if } i \in N_l \\ x_i[k+1] = \min_{j \in N_i}(x_j[k] + \epsilon_{ij}) & \text{if } i \in N_f \end{cases} \tag{10}$$

where

$$x[k] \stackrel{\text{def}}{=} x(\delta k), \quad \delta > 0 \quad \text{and} \quad k \in \mathbb{Z}_0^+ \tag{11}$$

and for the switching-topology case is

$$\begin{cases} x_i[k+1] = x_i[k], \quad x_i[0] = 0 & \text{if } i \in N_l \\ \quad l = s[k] & \\ x_i[k+1] = \min_{j \in N_i}(x_j[k] + \epsilon_{ij}(l)) & \text{if } i \in N_f \end{cases} \tag{12}$$

Min-Plus Algebra: Min-plus algebra consists of two binary operations, $\oplus$ and $\otimes$, on the set $\mathbb{R}_{min} = \mathbb{R} \cup \{+\infty\}$, defined as follows

$$a \oplus b = \min\{a, b\} \tag{13}$$

$$a \otimes b = a + b \tag{14}$$

The neutral element for the min-plus addition $\oplus$ is $+\infty$, and for the min-plus multiplication $\otimes$ is 0. Both operations are associative and commutative, and the multiplication is distributive over the addition. Both operations are extended to matrices as follows. Given $A, B \in \mathbb{R}_{min}^{m \times n}$,

$$[A \oplus B]_{ij} = a_{ij} \oplus b_{ij}, \quad i = 1, \ldots, m \quad j = 1, \ldots, n$$

Given $A \in \mathbb{R}_{min}^{m \times q}$, $B \in \mathbb{R}_{min}^{q \times n}$,

$$[A \otimes B]_{ij} = \min_{k=1}^{q}\{a_{ik} + b_{kj}\} = \bigoplus_{k=1}^{q}(a_{ik} \otimes b_{kj})$$

The identity matrix of size n is a square matrix denoted by I_n and given by $[I_n]_{ij} = 0$ for $i = j$ and $[I_n]_{ij} = +\infty$ for $i \neq j$.

If $A \in \mathbb{R}_{min}^{n \times n}$, for any integer $k \geq 1$,

$$A^k = \underbrace{A \otimes A \otimes \cdots \otimes A}_{k-1 \quad \text{multiplications}}$$

and $A^0 = I_n$. For more properties and application of min-plus algebra, see [19], [20] and the references therein. If G is a vulnerability graph with n nodes $\{1, \ldots n\}$, a Modified Weighted Adjacency Matrix (MWAM) $A \in \mathbb{R}_{min}^{n \times n}$ is associated with G defined as

$$A = \begin{cases} [A]_{ii} = 0, \quad \text{if } i \text{ is a target node} \\ [A]_{ij} = \epsilon_{ij}, \quad \text{if } (i,j) \text{ is and edge} \\ [A]_{ij} = +\infty, \quad \text{in other cases} \end{cases} \tag{15}$$

Using the min-plus formalism, the stepping stone dynamics with fixed topology (10) can be rewritten as

$$\begin{cases} x_i[k+1] = x_i[k] = x_i[0] = 0 & \text{if } i \in N_l \\ x_i[k+1] = \bigoplus_{j \in N_i}(x_j[k] \otimes \epsilon_{ij}) & \text{if } i \in N_f \end{cases}$$

or in matrix form as

$$x[k+1] = A \otimes x[k] = A^{k+1} \otimes x[0] \tag{16}$$

and the stepping stone dynamics with switched topology (12) can be written as

$$\begin{cases} x_i[k+1] = x_i[k] = 0 & \text{if } i \in N_l \\ \quad l = s[k] & \\ x_i[k+1] = \bigoplus_{j \in N_i}(x_j[k] \otimes \epsilon_{ij}(l)) & \text{if } i \in N_f \end{cases}$$

or in matrix form

$$x[k+1] = A_l \otimes x[k], \quad l = s[k] \tag{17}$$

where A_l is the matrix associated with the vulnerability graph $G_l \in \{G_1, \ldots, G_m\}$.

Theorem II.3, Corollary II.1 and Theorem (II.4) have been proposed and proved in [6].

Theorem II.3. *A necessary and sufficient condition for which the stepping stone dynamics* (10) *converge to equilibrium* (6) *is that $A^{k+1} = A^k$ for any integer $k \geq 1$.*

Corollary II.1. *If $A \in \mathbb{R}_{min}^{n \times n}$ is the matrix associated with the vulnerability graph G and there is an integer $k \geq 1$ such that $A^{k+1} = A^k$, then $k \leq n - 1$.*

Remark II.2. *Corollary II.1 implies that the stepping stone dynamics* (10) *converge to equilibrium in finite time $\tau = k\delta$ with $k \leq n - 1$ instant communications.*

Theorem II.4. *The stepping stone dynamics with switching topology* (12) *converge to equilibrium if the time interval between two consecutive switching signals is slow enough, as $k = n - 1$ instant communication.*

III. Stepping stone attack with constraints

Given the dynamic vulnerability graph (G, x), where $x = [x_1 \quad \cdots \quad x_n]^T$.

A. Stepping stone path with maximum out-degree node constraint

As was mentioned before, according to the *maximum degree strategy* [9], [10], the attacker may wish to minimize the attack cost but also move to the highest-degree node. We will model this scenario as follow:

For every edge (x_i, x_j) we introduce a *node degree complexity score* σ_{ij}^2 defined as

$$\sigma_{ij}^2 = 10 - \frac{10}{n}\delta_{out}(x_j) \tag{18}$$

where $\delta_{out}(x_j)$ is the number of outgoing edges from node x_j, called in the literature as the *out-degree* of the node. σ_{ij}^2 ranges between 0 and 10 and is classified as a node-centrality metric that is proportional to the out-degree of the node x_j, as closer to 0 is this score, as higher out-degree of x_j. Since an attacker that is resident in a node x_i can scan the information of the neighbors' nodes x_j ($j \in N_i$), and because of the maximum degree strategy assumption, he knows the out-degrees of the neighbors' nodes x_l of x_j and may select the one with maximum out-degree. Then in the context of our model, for an attacker that is in node x_i, the following edge score is well known:

$$y_j = \begin{cases} \min_{l\in N_j}(\sigma_{jl}) & \text{if there is} \quad l \in N_j \\ 0 & \text{if } j \text{ is a target} \\ 10 & \text{if there is not} \quad l \in N_j \end{cases} \tag{19}$$

and its interaction over the edge (x_i, x_j) is modeled by the score

$$y_{ij} = \sigma_{ij} y_j \tag{20}$$

Then by (10) the stepping stone dynamic with maximum out-degree constraint influenced by the neighbor's edges (AQSPP) is given by

$$\begin{cases} x_i[k+1] = x_i[k] = x_i[0] = 0 & \text{if } i \in N_l \\ x_i[k+1] = \min_{j\in N_i}(x_j[k] + \epsilon_{ij} + \sigma_{ij}^2 + y_{ij}) & \text{if } i \in N_f \end{cases} \tag{21}$$

Using the min-plus formalism yields

$$\begin{cases} x_i[k+1] = x_i[k] = x_i[0] = 0 & \text{if } i \in N_l \\ x_i[k+1] = \bigoplus_{j\in N_i}(x_j[k] \otimes \gamma_{ij}) & \text{if } i \in N_f \end{cases} \tag{22}$$

where

$$\gamma_{ij} = \epsilon_{ij} + \sigma_{ij}^2 + y_{ij} \tag{23}$$

is a new complexity score for (x_i, x_j) that combines the properties described by ϵ_{ij} and σ_{ij}^2, but also the influence of the neighbors' paths described by y_{ij}. Let's denote with $\Gamma = [\gamma_{ij}]_{n\times n}$ the MWAM that encodes the complexity scores $\gamma_{i,j}$, then equation (22) in matrix form is

$$x[k+1] = \Gamma \otimes x[k] = \Gamma^{k+1} \otimes x[0] \tag{24}$$

From Theorem II.3, Corollary II.1, and Remark II.1 equation (24) converges to the equilibrium if and only if $\Gamma^{k+1} = \Gamma^k$ for any $k \geq 1$, and the following theorem has been proved.

Theorem III.1. *Equation* (24) *converges to the shortest path with maximum node-degree if and only if* $\Gamma^{k+1} = \Gamma^k$ *for any* $1 \leq k \leq n-1$.

An immediate consequence of Theorem III.1 is stated in the following result.

Corollary III.1. *The AQSPP defined by equation* (18)-(23) *can be solved as the SPP with* (24)

B. Stepping stone attack with maximum impact constraint

For every edge (x_i, x_j) we introduce the *impact complexity score* $\hat{\sigma}_{ij}^2$ defined as

$$\hat{\sigma}_{ij}^2 = 10 - \psi(x_j) \tag{25}$$

where $\psi(x_j)$ is the impact subscore of v_j provided by CVSS, and assuming that every node has information about the vulnerabilities of the neighbors' nodes, then in the context of our model, if an attacker is a resident in a node x_i scanning a neighbors node x_j, because of our assumption, x_j has the vulnerabilities information about its neighbors' nodes x_l, then the scores $\hat{y}_l$ and $\hat{y}_{ij}$ for (x_i, x_j) defined by equations (19) and (20) respectively with $\hat{\sigma}_{ij}$ instead of σ_{ij} are well known for the attacker. Then the shortest path with maximum impact influenced by its adjacent edges is given by equation (22) with the new complexity score $\hat{\gamma}_{ij} = \epsilon_{ij} + \hat{\sigma}_{ij}^2 + \hat{y}_{ij}$ instead of γ_{ij}. Denoting with $\hat{\Gamma} = [\hat{\gamma}_{ij}]_{n\times n}$ the MWAM that encodes the complexity scores $\hat{\gamma}_{ij}$, then the following result can be stated.

Theorem III.2. *Equation* (24) *with* $\hat{\Gamma}$ *instead of* Γ*, converges to the shortest path with maximum impact if and only if* $\hat{\Gamma}^{k+1} = \hat{\Gamma}^k$ *for any* $1 \leq k \leq n-1$.

An immediate consequence of Theorem III.2 is a result identical to Corollary III.1 , with $\hat{\gamma}_{ij}$ instead of γ_{ij}.

Remark III.1. *In general, the costs* ϵ_{ij} *and* σ_{ij}^2 *(or* $\hat{\sigma}_{ij}^2$*) can be multiplied by constants* α *and* β *respectively, to describe the influence of the constraint in the attackers' strategy, the estimation of this constants may be according to modelers' experience or historical data.*

Node ID	Device	Vulnerability	ε	A_v	ϵ	ψ	NVD Last Modified
1	SCADA Server	CVE-2010-2772	3.4	0.395	1.4	10	08/16/2017
2	F& P Server	CVE-2008-0405	10	1	0	10	10/15/2018
3	CISCO ASA	CVE-2002-1278	10	1	0	6.4	09/10/2018
4	Active Directory	CVE-1999-0504	10	1	0	6.4	09/09/2008
5	Payment Gateway	CVE-2015-0075	3.9	0.395	0.1	10	10/12/2018
6	Mail Server	CVE-2002-1278	10	1	0	6.4	09/10/2008
7	LAN User	CVE-2017-11783	3.4	0.395	1.4	10	11/03/2017
8	LAN User	CVE-2013-0640	8.6	1	1.4	10	09/18/2017
9	Building Management System	CVE-2012-4701	8.6	1	1.4	10	02/15/2013
10	Solar Farm Inverter	CVE-2017-9859	3.9	1	6.1	5.9	08/21/2017
11	Solar Array Management Module	CVE-2017-9861	3.9	1	6.1	5.9	08/21/2017
12	Attacker	Source					

TABLE I: Vulnerabilities of the devices corresponding to the IIOT network presented in figure 1, where ε is the exploitability subscore, A_v is the accessibility subscore, and ψ is the impact subscore, provided by CVSS, and ϵ is the exploit complexity score.

IV. Results and Discussion

For an illustration of our approach, a portion of a solar network integrated with an industrial plant control network like that one presented in [21] is considered as a strategic space for attackers potential propagation [22]. Its vulnerability

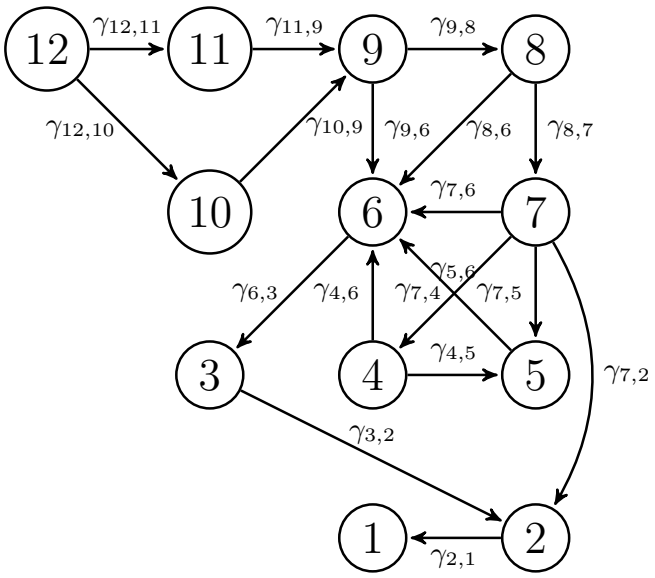

Fig. 1: Vulnerability graph of a portion of an Industrial Internet of Things (IIOT). The edges are labeled with the complexity scores γ_{ij}.

graph is presented in figure 1. In Table I, the information of the nodes IDs and its vulnerabilities are presented, the source of the attack is node 12, and the target is node 1 (SCADA server). Table II summarizes the simulation using our approach, and are described in more detail as following:

First, using only the exploit complexity score ϵ_{ij} that encode a unique attackers' strategy, the most vulnerable stepping stone path is calculated with the equation (8) as the SPP from the source node 12 to the target, giving as results any path between both of them, because all have the same cost 8.89. Some of the shortest paths have a minimum impact cost of 48.7 and others have a maximum of 55.9, the out-degree cost for some of them is 6 (the minimum) and for others is 10 (the maximum). This result is a usual shortcoming of the use of only one edge cost with the shortest path metric, in general, the shortest path metric does not indicate the number of shortest paths that may exist in a network, and in consequence, a network administrator may arrive at an erroneous result.

Second, using the complexity scores γ_{ij}, that encodes two attackers strategies, equation (24) give us two shortest paths, then most vulnerable stepping stone path with maximum out-degree node (Shortest path with maximum out-degree node) from node 12 to the target are given by $12 \rightarrow 11(or 10) \rightarrow 9 \rightarrow 8 \rightarrow 7 \rightarrow 2 \rightarrow 1$ with cost 104.91, both paths has the maximum out-degree cost of 10, and impact cost of 55.9.

edge score	Stepping stone path	cost	Impact cost	Out-degree cost
ϵ_{ij}	Any from 12 to 1	8.89	48.7-55.9	6-10
γ_{ij}	$12 \rightarrow 11 \rightarrow 9 \rightarrow 8 \rightarrow 7 \rightarrow 2 \rightarrow 1$ $12 \rightarrow 10 \rightarrow 9 \rightarrow 8 \rightarrow 7 \rightarrow 2 \rightarrow 1$	104.91	55.9	10
$\hat{\gamma}_{ij}$	$12 \rightarrow 11 \rightarrow 9 \rightarrow 8 \rightarrow 7 \rightarrow 2 \rightarrow 1$ $12 \rightarrow 10 \rightarrow 9 \rightarrow 8 \rightarrow 7 \rightarrow 2 \rightarrow 1$	21.63	55.9	10

TABLE II: Simulation results.

Third, using the exploit complexity score $\hat{\gamma}_{ij}$ that encodes two attackers strategies, equation (24) with $\hat{\Gamma}$ instead of Γ provides two shortest paths, then the most vulnerable stepping stone path with maximum impact (Shortest path with maximum impact) from node 12 to the target are $12 \rightarrow 11 \rightarrow 9 \rightarrow 8 \rightarrow 7 \rightarrow 2 \rightarrow 1$ with cost 21.63, out-degree cost of 10 and impact cost of 55.9.

The effort exerted by an attacker to exploit vulnerabilities has been represented by assigning the exploit complexity score ϵ_{ij}. The intuition underlying the Shortest Path is that from the perspective of the attacker, given the option of different stepping stones, the attacker will choose the series of stepping stones that require the least amount of effort. Resources of an attacker may include but are not limited to, tenacity, skills, and money. Our simulation results described in the second an third part, show that if an attacker is not constrained to the minimum effort (attacker with full resources), that is, if the attacker wants to use more the one criteria in the selection of the stepping stones, the most vulnerable paths may be different from the paths with only one strategy. More elaborated scores can be introduced to describe more multiple criteria in the selection of the stepping stone by the attackers; our model provides one way to use one strategy and take any other as a constraint.

V. Conclusion

This paper has presented a mathematical model for the analysis and simulation of the stepping stone attacks when attackers employ multiple strategies to choose stepping stones as an AQSPP in a dynamic vulnerability graph with a multi-agent system approach. This approach allows modeling the scenario when the attacker uses one strategy constrained by another. As a result, the most vulnerable stepping stone path that satisfies both conditions is calculated, which can be interpreted as the stepping stone path most likely to succeed.

Theorem III.1 and Theorem III.2 provide a necessary and sufficient condition for a finite time convergence to the shortest path for the stepping stone attack models with a maximum degree and maximum impact respectively and show that can be solved as the SPP. The models can be expanded easily for the case of vulnerability graphs with switching topology [6], using equation (12) with $\gamma_{ij}(l)$ or $\hat{\gamma}_{ij}(i)$ instead of $\epsilon_{ij}(l)$ for every vulnerability graph G_l.

Acknowledgement

We thank Dr. David Myers (Air Force Research Laboratory) for his contributions to the research and review of the paper.

This material is based upon work supported by the Department of Energy under award number DE-OE0000780, Department of Homeland Security Grant 2015-ST-061-CIRC01 and Office of the Assistant Secretary of Defense for Research and Engineering agreement FA8750-15-2-0120. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

REFERENCES

[1] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, "Defending critical infrastructure," *Interfaces*, vol. 36, no. 6, pp. 530–544, 2006.

[2] P. A. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," *ISA Transactions*, vol. 46, no. 4, pp. 583–594, 2007.

[3] C. Ten, G. Manimaran, and C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 4, pp. 853–865, 2010.

[4] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem, and J. Chen, "Modeling cost of countermeasures in software defined networking-enabled energy delivery systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–9.

[5] D. M. Nicol and V. Mallapura, "Modeling and analysis of stepping stone attacks," in *Proceedings of the Winter Simulation Conference 2014*, Dec 2014, pp. 3036–3047.

[6] M. Gamarra, S. Shetty, D. M. Nicol, O. Gonzalez, C. A. Kamhoua, and L. Njilla, "Analysis of stepping stone attacks in dynamic vulnerability graphs," in *2018 IEEE International Conference on Communications (ICC)*, May 2018, pp. 1–7.

[7] R. Olfati-Saber and R. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *Automatic Control, IEEE Transactions on*, vol. 49, no. 9, pp. 1520–1533, Sept 2004.

[8] Y. Zhang and S. Li, "Distributed biased min-consensus with applications to shortest path planning," *IEEE Transactions on Automatic Control*, vol. PP, no. 99, pp. 1–1, 2017.

[9] S. Bornholdt and H. G. Schuster, *Handbook of Graphs and Networks: From the Genome to the Internet*. John Wiley & Sons, 2006.

[10] M. Boguná, R. Pastor-Satorras, A. Díaz-Guilera, and A. Arenas, "Models of social networks based on social distance attachment," *Physical review E*, vol. 70, no. 5, p. 056122, 2004.

[11] G. Schudel and B. Wood, "Adversary work factor as a metric for information assurance," in *Proceedings of the 2000 workshop on New security paradigms*. ACM, 2001, pp. 23–30.

[12] B. Rostami, F. Malucelli, D. Frey, and C. Buchheim, "On the Quadratic Shortest Path Problem," in *14th International Symposium on Experimental Algorithms*, ser. 14th International Symposium on Experimental Algorithms, Paris, France, Jun. 2015. [Online]. Available: https://hal.inria.fr/hal-01251438

[13] B. Rostami, A. Chassein, M. Hopf, D. Frey, C. Buchheim, F. Malucelli, and M. Goerigk, "The quadratic shortest path problem: complexity, approximability, and solution methods," *European Journal of Operational Research*, vol. 268, no. 2, pp. 473–485, 2018.

[14] H. Hu and R. Sotirov, "Special cases of the quadratic shortest path problem," *Journal of Combinatorial Optimization*, vol. 35, no. 3, pp. 754–777, 2018.

[15] H. Hu and R. Sotirov, "On solving the quadratic shortest path problem," *arXiv preprint arXiv:1708.06580*, 2017.

[16] P. Mell, K. Scarfone, and S. Romanosky, "The Common Vulnerability Scoring System (CVSS) and its Applicability to Federal Agency Systems," National Institute of Standards and Technology, Tech. Rep., 2007.

[17] P. Mell, K. Scarfone, and S. Romanosky, "Common Vulnerability Scoring System," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, Nov 2006.

[18] R. Bellman, "On a routing problem," *Quart. Appl. Math.*, vol. 16, no. 1, pp. 87–90, 1958.

[19] G. C. F. Baccelli, G. Olsder, and J. Quadrat, *Synchronization and Linearity: An algebra for discrete event systems*. http://www-rocq.inria.fr/metalau/cohen/DES/book-online.html.: Wiley, Web edition., 2001.

[20] S. Watanabe and Y. Watanabe, "Min-plus algebra and networks," in *Novel Development of Nonlinear Discrete Integrable Systems*. RIMS Kkyroku Bessatsu B47, 2014.

[21] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43 586–43 601, 2018.

[22] S. Ullah, S. Shetty, and A. Hassanzadeh, "Towards modeling attackers opportunity for improving cyber resilience in energy delivery systems," in *2018 Resilience Week (RWS)*. IEEE, 2018, pp. 100–107.