Using Event-Based Method to Estimate Cybersecurity Equilibrium

Zhaofeng Liu, Ren Zheng, Wenlian Lu, and Shouhuai Xu

***Abstract*—Estimating the global state of a networked system is an important problem in many application domains. The classical approach to tackling this problem is the periodic (observation) method, which is inefficient because it often observes states at a very high frequency. This inefficiency has motivated the idea of event-based method, which leverages the evolution dynamics in question and makes observations only when some rules are triggered (i.e., only when certain conditions hold). This paper initiates the investigation of using the event-based method to estimate the equilibrium in the new application domain of cybersecurity, where equilibrium is an important metric that has no closed-form solutions. More specifically, the paper presents an event-based method for estimating cybersecurity equilibrium in the preventive and reactive cyber defense dynamics, which has been proven globally convergent. The presented study proves that the estimated equilibrium from our trigger rule i) indeed converges to the equilibrium of the dynamics and ii) is Zeno-free, which assures the usefulness of the event-based method. Numerical examples show that the event-based method can reduce 98% of the observation cost incurred by the periodic method. In order to use the event-based method in practice, this paper investigates how to bridge the gap between i) the continuous state in the dynamics model, which is dubbed probability-state because it measures the probability that a node is in the secure or compromised state, and ii) the discrete state that is often encountered in practice, dubbed sample-state because it is sampled from some nodes. This bridge may be of independent value because probability-state models have been widely used to approximate exponentially-many discrete state systems.**

***Index Terms*—Cybersecurity dynamics, cybersecurity equilibrium, event-based method, global state estimation, preventive and reactive cyber defense dynamics.**

Manuscript received March 8, 2020; revised August 6, 2020; accepted October 1, 2020. This work was supported in part by the National Natural Sciences Foundation of China (62072111). Recommended by Associate Editor Tengfei Liu. *(Corresponding author: Wenlian Lu.)*

Citation: Z. F. Liu, R. Zheng, W. L. Lu, and S. H. Xu, "Using event-based method to estimate cybersecurity equilibrium," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 2, pp. 455–467, Feb. 2021.

Z. F Liu is with the School of Mathematical Sciences, Fudan University, Shanghai 200433, China (e-mail: zhaofengliu@hotmail.com).

R. Zheng is with the Artificial Intelligence Laboratory, SAIC Motor Corporation Limited, Shanghai 200041, and also with SAIC Intelligent Technology (Shanghai) Corporation Limited, Shanghai 200433, China (e-mail: zhrkevin@gmail.com).

W. L. Lu is with the School of Mathematical Sciences, Fudan University, and Shanghai Center for Mathematical Sciences, Fudan University, and also with Shanghai Key Laboratory for Contemporary Applied Mathematics, Shanghai 200433, China (e-mail: wenlian@fudan.edu.cn).

S. H. Xu is with the Department of Computer Science, University of Texas at San Antonio, San Antonio TX 78249 USA (e-mail: shxu@cs.utsa.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2020.1003527

I. Introduction

ESTIMATING the global state of a networked system at any point in time is of fundamental importance in many application domains. This is because the real-time global state allows an engine (or administrator) to make prompt decisions. The classical approach to obtaining the global state of a networked system is the periodic method, which observes the state of every node in the networked system at every point in time (at an appropriate time resolution). Fig. 1 illustrates a networked system of n nodes and a time interval $[t_1, t_m]$ at a certain time resolution. In order to estimate the global state of the networked system at time $t_1,\ldots,t_m$, the periodic method requires the observation of every node's state at every point in time, leading to nm observations (or operations) in total.

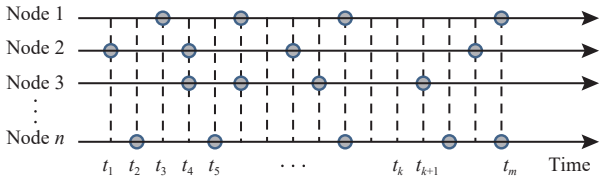


Fig. 1. Illustration of the advantage of the event-based method over the classical periodic (observation) method. The latter observes the state of every node at every point in time $t_1,\ldots,t_m$ (i.e., incurring nm observation events in total). The former only observes the state of some nodes at some points in time, which are highlighted with filled circles, meaning that the former incurs a much smaller (than nm) number of observations.

The nm complexity mentioned above has motivated the event-based method [1], [2]. The key idea underlying this method is to leverage the state evolution dynamics. As illustrated in Fig. 1, this method only observes the state of some nodes at some points in time, effectively achieving "observation on demand" and incurring a much smaller number (than nm) of observations. While intuitive, the event-based method is not always effective because it may fall victim to the so-called Zeno behavior [3], which renders it useless by incurring infinitely many observations within a finite period of time. Therefore, an event-based method must be proven Zeno-free.

A. Our Contributions

This paper initiates the investigation of adapting the event-based method to the cybersecurity domain. In this domain, the global cybersecurity state of a network is a basic input for making effective, if not optimal, cyber defense decisions, such as whether to impose new cybersecurity restrictions or not. The paper investigates how to estimate the cybersecurity

equilibrium in the context of preventive and reactive cyber defense dynamics, which is a particular kind of cybersecurity dynamics (and will be reviewed later). The dynamics have been proven globally convergent in the entire parameter universe (i.e., the dynamics always converge to a unique equilibrium for any possible initial state) [4]. Despite this exciting progress, one important problem is left unaddressed: How to estimate the equilibrium efficiently without knowing the value of every model parameter? Since the periodic observation method is inefficient (especially for large networks), the presented paper proposes adapting the event-based method to estimate the cybersecurity equilibrium in the preventive and reactive cyber defense dynamics.

Specifically, this paper proposes an active event-based method for estimating the cybersecurity equilibrium and proves that the method is Zeno-free (i.e., it does not fall victim to the Zeno behavior). Numerical examples show that our event-based method can reduce 98% of the observation cost when compared with the periodic method. In order to show how to use this event-based method in practice, we investigate how to bridge the gap between i) the continuous state in the dynamics model, which is dubbed probability-state because it measures the probability that a node is in the secure or compromised state, and ii) the discrete state that is often encountered in practice, dubbed sample-state because it is sampled from some nodes at some points in time. This bridge may be of independent value because probability-state models have been widely used to approximate discrete state systems with exponentially-many discrete states (incurred by a state-space explosion [5], [6]).

B. Related Work

The event-based method has been investigated in many application settings other than cybersecurity, such as sampling for stochastic systems [7], stabilizing control [8], self-triggered control [9], and set-membership filtering (SMF) [10]. A core research problem is to show that the method does not fall victim to the Zeno behavior (see, for example, [8], [11]–[19]), which can render the event-based method useless by imposing infinitely many observation events within a finite period of time and can prevent the estimated dynamics from converging [3].

To the best of the authors' knowledge, the presented study is the first to introduce the idea of event-based sampling into the cybersecurity domain. This is made possible by a recent breakthrough showing that a certain class of cybersecurity dynamics is globally convergent in the entire parameter universe [4], a characterization that was not proven until 10 years after the model was first introduced in [20]. The notion of cybersecurity dynamics [5], [6] was introduced to model and analyze cybersecurity from a whole-network perspective. This notion, as discussed in [5], [6], has roots in earlier studies in biological epidemiology (e.g., [21]–[25]) and its variants in cyber epidemiology (e.g., [26]–[36]), interacting particle systems [37], and microfoundation in economics [38]. This notion has opened the door to a new research field with many results (e.g., [39]–[50]).

However, the previous studies leave one important question unaddressed: How can one quantify the equilibrium in the real-world when the values of some model parameters are not known? This paper will fill the lacuna by showing that the event-based method can be naturally adapted to tackle this problem in the context of preventive and reactive cyber defense dynamics, which is globally convergent in the entire parameter universe [4]. Special cases of this dynamic are (partially) characterized in previous studies such as [33]–[36], [48], which mostly focus on the epidemic threshold, namely a condition under which the dynamics will converge to the equilibrium zero (i.e., a special equilibrium that does not need to be estimated). In the cybersecurity domain, the notion of epidemic threshold is less relevant because the dynamics rarely "die out", which is inherent to the nature of the dynamics (e.g., computers can become compromised by means other than infection, contrary to biological dynamics).

The estimation of equilibrium has been explored in a smaller parameter regime [48], within which the dynamics were known to be convergent while certain parameters were specified (i.e., the structure of the global attack-defense graph, which will be elaborated later). In contrast, the presented paper investigates how to estimate the cybersecurity equilibrium in the entire parameter universe, making results applicable to broader scenarios. This is made possible by the theoretical result that the dynamics are globally convergent in the entire parameter universe [4].

It is worth mentioning that the preventive and reactive cyber defense dynamics are particular kinds of cybersecurity dynamics for quantifying cybersecurity from a holistic perspective [51]–[55]. There are other kinds of cybersecurity dynamics, which aim to accommodate adaptive defenses [45], active defenses [56]–[58], and proactive defenses [43]. Adapting the event-based method to these kinds of dynamics is an important open problem for future research.

C. Paper Outline

In Section II, the paper briefly reviews the preventive and reactive cyber defense dynamics model and its global convergence in the entire parameter universe [4]. In Section III, an event-based method for estimating the equilibrium is presented. Section IV involves a discussion on how to apply this event-based method in practice by bridging the gap between the probability-state in the theoretical model and the sample-state in practice. Section V concludes the paper with open problems and further research topics.

II. Problem Statement

A. Review of Preventive and Reactive Defense Dynamics

The idea of a preventive and reactive cyber defense dynamics model was first introduced in [20] and partially analyzed in [48], while noting that its special cases were studied earlier in [33]–[35]. However, all these studies only contribute a partial understanding of the dynamics corresponding to a special parameter regime rather than the entire parameter universe. Very recently, it is proven that these dynamics are globally convergent in the entire parameter universe, meaning that there is always a unique equilibrium [4], whose exact value (or position) depends on the parameter values rather than the initial state of the dynamics.

In the dynamics model, the defender employs two classes of defenses:

1) Preventive Defenses: These correspond to the use of intrusion prevention tools to block cyber attacks before they reach a target or before they can cause any damage.

2) Reactive Defenses: These correspond to the use of anti-malware tools to detect compromised computers and then clean them up.

On the other hand, the attacker wages two kinds of attacks:

1) Push-based Attacks: These correspond to the use of computer malware to spread across the network.

2) Pull-based Attacks: These correspond to the use of compromised or malicious websites to attack browsers when vulnerable browsers visit those malicious websites.

The model abstracts the attack-defense interaction taking place over an attack-defense graph structure $G = (V, E)$, where V is the vertex set representing computers and $(u, v) \in E$ means computer u can wage push-based attacks against computer v directly (i.e., the communication from u to v is allowed by the security policy). This means that G is, in general, different from the underlying physical network structure because $(u, v) \in E$ may represents a variety of communication paths (rather than a single physical link), and that G can be derived from the security policy of a networked system and the physical network in question. The presented study does not make any restrictions on the structure of G; for example, G may be directed or undirected. Let $A = [a_{vu}]_{n\times n}$ denote the adjacency matrix of G, where $a_{vu} = 1$ if and only if $(u, v) \in E$. Since the model aims to describe the attacks between computers, we set $a_{vv} = 0$. Let $\deg(v)$ be the degree of node $v \in V$ when G is undirected or the in-degree of v when G is directed, where $\deg(v) = |N_v|$ with $N_v = \{u \in V : (u, v) \in E\}$.

The dynamics can equally be described with either a continuous-time model or a discrete-time model [4]. The presented paper focuses on the continuous-time model. At any point in time, a node $v \in V$ is in one of two states: "0" means secure but vulnerable, whereas "1" means compromised. Let $s_v(t)$ denote the probability that v is secure at time t and $i_v(t)$ denote the probability that v is compromised at time t. Note that $s_v(t) + i_v(t) = 1$ for $v \in V$ and for $t \geq 0$; thus, these terms interchangeably describe the probability-state of a given computer.

Fig. 2 describes the state-transition diagram for a node $v \in V$ at time t, where $\theta_{v,1\to0}(t)$ abstracts the effectiveness of the reactive defenses and $\theta_{v,0\to1}(t)$ abstracts the capability of attacks against the preventive defenses. Let $\beta \in (0, 1]$ be the probability that a compromised computer changes to the secure state because the attacks are detected and mitigated up by the reactive defenses. Then, $\theta_{v,1\to0}(t) = \beta$. On the other hand, $\theta_{v,0\to1}(t)$ is more inclusive because it accommodates both push-based and pull-based attacks. In order to model the power of pull-based attacks against the preventive defenses, let $\alpha \in [0, 1]$ denote the probability that a secure computer becomes compromised despite the presence of the preventive defenses (i.e., the preventive defenses are penetrated by the pull-based attacks). In order to model the power of push-based attacks against the preventive defenses, let $\gamma \in (0, 1]$ denote the probability that a compromised computer u wages a successful attack against a secure computer v despite the preventive defenses (i.e., the preventive defenses are penetrated by push-based attacks), where $(u, v) \in E$. Under the assumption that the attacks are waged independently of each other, it holds that

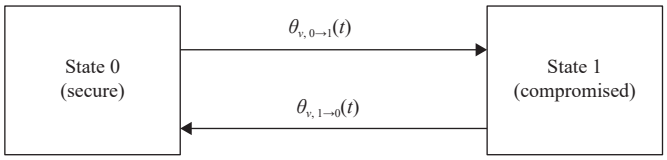


Fig. 2. The state-transition diagram of any $v \in V$ that leads to a nonlinear Dynamical System with the nonlinear term $\theta_{v,0\to1}(t)$, as shown in (1).

$$\theta_{v,0\to1}(t) = 1 - (1-\alpha)\prod_{u\in N_v}(1-\gamma i_u(t)). \tag{1}$$

The preceding discussion leads to the following continuous-time nonlinear dynamical system for $v \in V$:

$$\begin{cases} \dfrac{ds_v(t)}{dt} = \theta_{v,1\to0}(t)\times i_v(t) - \theta_{v,0\to1}(t)\times s_v(t) \\ \dfrac{di_v(t)}{dt} = \theta_{v,0\to1}(t)\times s_v(t) - \theta_{v,1\to0}(t)\times i_v(t). \end{cases}$$

The dynamics can be rewritten as a system of n nonlinear equations for $v \in V$

$$\begin{aligned} \frac{di_v(t)}{dt} &= f_v(i) \\ &= -\beta i_v(t) + \left[1 - (1-\alpha)\prod_{u\in N_v}(1-\gamma i_u(t))\right](1 - i_v(t)). \end{aligned} \tag{2}$$

The global convergence of system (2) presented in [4] can be summarized as follows:

1) If the attacker wages both push-based and pull-based attacks (i.e., $\alpha > 0$), system (2) is globally convergent in the entire parameter universe and the dynamics converge to a unique nonzero equilibrium exponentially.

2) If the attacker only wages push-based attacks (i.e., $\alpha = 0$), system (2) is still globally convergent in the parameter universe but the convergence speed depends on the model parameters and the largest eigenvalue $\lambda_{A,1}$ of adjacency matrix A is as follows:

a) If $\lambda_{A,1} < \beta/\gamma$, the dynamics converge to equilibrium 0 exponentially (see also [35], [48]).

b) If $\lambda_{A,1} = \beta/\gamma$, the dynamics converge to equilibrium 0 polynomially.

c) If $\lambda_{A,1} > \beta/\gamma$, the dynamics converge to a unique nonzero equilibrium exponentially.

This leads to:

Lemma 1 [4]: System (2) converges exponentially when $\alpha > 0$ and when $\alpha = 0$ and $\lambda_{A,1} \neq \beta/\gamma$.

It is worth mentioning that the results also hold for the more general setting with node-dependent parameters α_v and β_v and edge-dependent parameter γ_{uv} [4].

B. Problem Statement: Estimating Cybersecurity Equilibrium

Even though system (2) has been proven globally convergent in the entire parameter universe, there is no analytic result on the value of the equilibrium, which remains a hard

TABLE I
NOTATIONS USED THROUGHOUT THE PAPER

Notation	Description
$G=(V,E),A$	The attack-defense graph structure G with adjacency matrix $A=[a_{vu}]_{n\times n}$ where $a_{vu}=1$ if and only if $(u,v)\in E$
$\alpha\in[0,1]$	The probability that a secure computer becomes compromised because a pull-based attack penetrates a preventive defense
$\beta\in(0,1]$	The probability that a compromised computer becomes secure because a reactive defense detects and cleans the compromise
$\gamma\in(0,1]$	The probability that a compromised computer wages a successful push-based attack against a secure computer
N_v	$N_v=\{u\in V:(u,v)\in E\}$
$i_v(t)$, $i(t)$	The probability v is in the compromised state at time t; $i(t)=[i_1(t),\ldots,i_n(t)]$
i_v^*, i^*	The probability v is in the compromised state in the equilibrium; $i^*=[i_1^*,\ldots,i_n^*]$
$i_v^{[a]}(t)$, $i^{[a]}(t)$	The probability v is in the compromised state at time t w.r.t. the event-based method; $i^{[a]}(t)=[i_1^{[a]}(t),\ldots,i_n^{[a]}(t)]$
t_k^v	The time for the kth observation event at $v\in V$ in the event-based method; $t_0^v=0$
h	The constant time interval for periodic observations (as the reference setting)
$\chi_v(t)$	The sample-state of node v at time t; 0 means secure and 1 means compromised
$\widehat{i_v(t)}$, $\widehat{s_v(t)}$	The probability v is in the compromised (secure) state at time t as estimated from the sample-states
$\widehat{i_v^{[a]}(t)}$	The probability v is in the compromised state at time t as estimated from the sample-states w.r.t. the event-based method

problem (except for special cases, such as the aforementioned equilibrium 0). As discussed previously, the periodic method may be used to estimate the equilibrium, but in many cases, this is too costly. This observation reiterates the purpose of this paper, which is to investigate the use of an event-based method as an alternative. This paper focuses on estimating the equilibrium in the parameter regime where System (2) converges exponentially, namely when $\alpha>0$ (i.e., there are pull-based attacks) or when $\alpha=0$ (i.e., there are no pull-based attacks) but $\lambda_{A,1}\neq\beta/\gamma$, as shown in Lemma 1. The paper leaves it to future works to address the special parameter regime $\alpha=0$ and $\lambda_{A,1}=\beta/\gamma$, where the dynamics converge polynomially; as the techniques used in the presented paper are applicable to exponential convergence but not polynomial convergence.

C. Notations

Let $\mathbb{R}$ be the set of real numbers, $\mathbb{N}$ be the set of positive integers and zero. For an n-dimensional vector $i=[i_1,\ldots,i_n]\in\mathbb{R}^n$, the l_1-norm $\|i\|_1=\sum_{v=1}^n\xi_v|i_v|$ is adopted, where $\xi_v\in[0,1]$ is a positive constant subject to $\sum_{v=1}^n\xi_v=1$. Note that the result holds equally with respect to other norms. Table I summarizes the major notations used in the paper.

III. AN EVENT-BASED METHOD

In this section, the paper proposes an event-based method for estimating the cybersecurity equilibrium of system (2) and analyzes its properties, including Zeno-freeness. Then, the method is adapted to accommodate the practical case where state observations are not conducted arbitrarily but conducted at predetermined points in time.

A. Designing Event-based Trigger Rule

The presented work proposes using a linear dynamical system to approximate the original nonlinear dynamical system in the event-based method. In the linear system, the probability that a node is compromised evolves linearly between two consecutive state observation events. More specifically, a node actively probes its neighbors for their observed state information when certain conditions are satisfied. Note that this "active probing" strategy is sometimes called "pull-based" event-based method; here, the latter term is not adopted as it already refers to pull-based attacks. Suppose node v probes its neighbors $u\in N_v$ for u's observed state information at time t_k^v, which indicates node v's kth state observation event, where $k=0,1,\ldots$. Upon receiving the probe, u's current state, denoted by $i_u^{[a]}(t_k^v)$, is given to v, where superscript "[a]" highlights the difference from $i_u(\cdot)$ in the original dynamical system. However, it holds that $i_v^{[a]}(t_k^v)=i_v(t_k^v)$.

As discussed above, the presented work focuses on the parameter regime where the dynamics converge exponentially, namely $\alpha>0$ and $\alpha=0$ but $\lambda_{A,1}\neq\beta/\gamma$. In this parameter regime, system (2) becomes: for $v\in V$, $t\in[t_k^v,t_{k+1}^v)$,

$$\frac{di_v^{[a]}(t)}{dt}=-\beta i_v^{[a]}(t_k^v)+\left[1-(1-\alpha)\prod_{u\in N_v}\left(1-\gamma i_u^{[a]}(t_k^v)\right)\right]\left(1-i_v^{[a]}(t_k^v)\right)\quad(3)$$

where $\alpha>0$, or $\alpha=0$ but $\lambda_{A,1}\neq\beta/\gamma$.

For $u,v\in V$ where $u\in N_v$, define state errors as

$$\begin{cases}\varepsilon_v(t,t_k^v)=i_v(t)-i_v^{[a]}(t_k^v)\\ \varepsilon_u(t,t_k^v)=i_u(t)-i_u^{[a]}(t_k^v)\end{cases}$$

for $t\in[t_k^v,t_{k+1}^v)$ and $k=0,1,\ldots$. When system (2) converges exponentially, its convergence speed can be denoted by $e^{-\sigma t}$ for some appropriate σ. Let φ be a continuous function satisfying

$$\varphi(t)=M_0e^{-\nu t},\quad\forall t>0\quad(4)$$

where $0<\nu\leq\sigma$ and M_0 is a positive constant number. Then, the following event-based trigger rule defines a sequence of points in time at which state observation events occur.

Definition 1 (Event-based Trigger Rule): Let $t_0^v=0$ for $v\in V$. The trigger rule is defined as

$$t_{k+1}^v = \sup\left\{\tau \geq t_k^v : \max_{u\in N_v\cup\{v\}} \left|\varepsilon_u(\tau, t_k^v)\right| \leq \varphi(\tau)\right\} \tag{5}$$

which specifies a sequence of state observation events at time $\{t_k^v\}_{k=0}^{+\infty}$.

B. Analyzing the Event-based Method

In the following paragraphs, we demonstrate the effectiveness of the event-based method and prove that it is Zeno-free.

Theorem 1: Suppose the following conditions hold:

1) $(\alpha,\beta,\gamma) \notin \Theta$ for some set with zero measure $\Theta \subset \mathbb{R}^3$;

2) parameters satisfy the conditions required by Lemma 1;

3) there exists some $\zeta > 0$, so that

$$\max_{u\in N_v} |\varepsilon_u(t_{k+1}^v, t_k^v)| \leq \zeta |\varepsilon_v(t_{k+1}^v, t_k^v)|$$

holds for $\forall v \in V$, $k = 0, 1, \ldots$.

Then, system (3) under the event-based trigger rule in Definition 1 converges to the equilibrium of system (2) and is Zeno-free.

Proof: The presented study needs to show i) the sequence satisfies $\inf\{t_{k+1}^v - t_k^v\} > 0$ for all $v \in V$; ii) system (3) under the event-based trigger rule converges to the equilibrium of system (2) and system (3) is Zeno-free.

To prove part i), the first thing to note is that the global convergence of system (2) is proven in [4]. Let $i_v^* = \lim_{t\to+\infty} i_v(t)$ for all $v \in V$. Then

$$-\beta i_v^* + \left[1 - (1-\alpha)\prod_{u\in N_v}\left(1-\gamma i_u^*\right)\right](1 - i_v^*) = 0.$$

Let $z_v(t) = i_v(t) - i_v^*$ for all i_v^*. Then

$$\begin{aligned}\left|\frac{d}{dt} z_v(t)\right| = & \left| -\beta i_v(t) + \left[1 - (1-\alpha)\prod_{u\in N_v}\left(1-\gamma i_u(t)\right)\right] \right. \\ & \times \left(1 - i_v(t)\right) + \beta i_v^* - \left[1 - (1-\alpha)\prod_{u\in N_v}\left(1-\gamma i_u^*\right)\right] \\ & \left. \times (1 - i_v^*)\right| \\ = & \left| (\beta+1) z_v(t) - (1-\alpha)\prod_{u\in N_v}\left(1-\gamma i_u^*\right) z_v(t) \right. \\ & - (1-\alpha)\left[\prod_{u\in N_v}\left(1-\gamma i_u^*\right) - \prod_{u\in N_v}\left(1-\gamma i_u(t)\right)\right] \\ & \left. \times \left(1 - i_v(t)\right)\right|.\end{aligned}$$

Let u_- be the smallest index in N_v. Notice that

$$\begin{aligned}& \prod_{u\in N_v}\left(1-\gamma i_u^*\right) - \prod_{u\in N_v}\left(1-\gamma i_u(t)\right) \\ & = \left[\left(1-\gamma i_{u_-}(t)\right) + \left(\gamma i_{u_-}(t) - \gamma i_{u_-}^*\right)\right] \\ & \quad \times \prod_{u>u_-, u\in N_v}\left(1-\gamma i_u^*\right) - \prod_{u\in N_v}\left(1-\gamma i_u(t)\right) \\ & = \gamma z_{u_-} \prod_{u>u_-, u\in N_v}\left(1-\gamma i_u^*\right) + \left(1-\gamma i_{u_-}(t)\right) \\ & \quad \times \left[\prod_{u>u_-, u\in N_v}\left(1-\gamma i_u^*\right) - \prod_{u>u_-, u\in N_v}\left(1-\gamma i_u(t)\right)\right].\end{aligned}$$

This recurrent process will lead to

$$\begin{aligned}\left|\frac{d}{dt} z_v(t)\right| & \leq M_1 \left|z_v(t)\right| + \left|(1-\alpha)\gamma\left(1 - i_v(t)\right)\sum_{\omega\in N_v} z_\omega(t)\right. \\ & \quad \left. \times \prod_{u>\omega, u\in N_v}(1-\gamma i_u^*)\prod_{u<\omega, u\in N_v}\left(1-\gamma i_u(t)\right)\right| \\ & \leq M_1 \left|z_v(t)\right| + M_2 \sum_{\omega\in N_v}\left|z_\omega(t)\right|\end{aligned}$$

where M_1 and M_2 are positive constants. According to Lemma 1, when condition 2) holds, the system has an exponential convergence speed, which means

$$\forall v \in V,\ \exists\sigma,\ T_v > 0,\ \forall t > T_v,\ \left|z_v(t)\right| = \left|i_v(t) - i_v^*\right| \leq e^{-\sigma t}.$$

So

$$\begin{aligned}\left|\frac{d}{dt} z_v(t)\right| & \leq M_1 \left|z_v(t)\right| + M_2 \sum_{\omega\in N_v}\left|z_\omega(t)\right| \\ & \leq M e^{-\sigma t} \leq M e^{-\sigma t_k^v}\end{aligned} \tag{6}$$

where M is a positive constant. Since $\frac{d}{dt} z_v(t) = \frac{d}{dt} i_v(t)$, the following inequality holds:

$$\begin{aligned}\left|\varepsilon_v(t_{k+1}^v, t_k^v)\right| & = \left|i_v(t_{k+1}^v) - i_v^{[a]}(t_k^v)\right| = \left|i_v(t_{k+1}^v) - i_v(t_k^v)\right| \\ & \leq \int_{t_k^v}^{t_{k+1}^v}\left|\frac{d}{d\tau} i_v(\tau)\right| d\tau = \int_{t_k^v}^{t_{k+1}^v}\left|\frac{d}{d\tau} z_v(\tau)\right| d\tau \\ & \leq \int_{t_k^v}^{t_{k+1}^v} M e^{-\sigma t_k^v} d\tau = M e^{-\sigma t_k^v}(t_{k+1}^v - t_k^v).\end{aligned}$$

In the case $\varphi(t) = M_0 e^{-\nu t} = M_0 e^{-\sigma t}$ or $\nu = \sigma$, the event-based trigger rule in Definition 1 shows that v will not trigger a state observation event until time $t = t_{k+1}^v$, which means

$$\max_{u\in N_v\cup\{v\}} |\varepsilon_u(t_{k+1}^v, t_k^v)| = M_0 e^{-\sigma t_{k+1}^v}.$$

Under condition 3),

$$\begin{aligned}M_0 e^{-\sigma(t_{k+1}^v - t_k^v)} e^{-\sigma t_k^v} & = \max_{u\in N_v\cup\{v\}} |\varepsilon_u(t_{k+1}^v, t_k^v)| \\ & \leq \zeta |\varepsilon_v(t_{k+1}^v, t_k^v)| \\ & \leq \zeta M e^{-\sigma t_k^v}(t_{k+1}^v - t_k^v).\end{aligned} \tag{7}$$

It shows the existence of a positive number η_v, which is the root of the transcendental equation $M_0 e^{-\sigma\eta_v} = \zeta M \eta_v$ and satisfies $t_{k+1}^v - t_k^v \geq \eta_v$, which essentially means that for every $v \in V$, $\inf\{t_{k+1}^v - t_k^v\} > 0$.

In the case $\varphi(t) = M_0 e^{-\nu t} > M_0 e^{-\sigma t}$ or $\nu < \sigma$, with respect to the η_v mentioned above, we can easily get $t_{k+1}^v - t_k^v > \eta_v$. This completes the proof of part i).

In order to prove part ii), the presented study first shows that under condition 1), $t \to +\infty$ implies $k \to +\infty$ (i.e., there are infinitely many state observation events). Note that $\varphi(t) \to 0$ as $t \to +\infty$. For $\forall t_k^v > 0$, if $i_v(t_k^v) \neq i_v^*$, then there must exist a $t_{k+1}^v > t_k^v$ such that $|i_v(t_{k+1}^v) - i_v^{[a]}(t_k^v)| = \varphi(t_{k+1}^v)$, which means the $(k+1)$th state observation event for node v will occur within a finite time; if there exists some $t_k^v > 0$ such that $i_v(t_k^v) = i_v^*$, node v may not incur the $(k+1)$th state observation

event within a finite time, meaning $t_{k+1}^v = +\infty$. The latter situation can be addressed by using the Sard's lemma in [59]: $\forall v \in V$ and $\forall k = 0,1,\ldots$, this paper uses a set with zero measure, denoted by $\Theta_{v,k}$, to cover all of the parameter vectors $(\alpha,\beta,\gamma) \in \mathbb{R}^3$ corresponding to which $i_v(t_k^v) = i_v^*$ is true. Since $v \in V$ and $k = 0,1,\ldots$ are both countable, $\Theta = \cup_{v,k}\Theta_{v,k}$ is also a set with zero measure. Therefore, under condition (a), namely $(\alpha,\beta,\gamma) \notin \Theta$, $t \to +\infty$ implies $k \to +\infty$.

Then, the presented paper goes to part ii). For $v \in V$,

$$\begin{aligned}
&\frac{d}{dt}\left[i_v^{[a]}(t) - i_v(t)\right] \\
&\quad = \beta i_v(t) - \left[1 - (1-\alpha)\prod_{u\in N_v}(1-\gamma i_u(t))\right](1 - i_v(t)) \\
&\qquad - \beta i_v^{[a]}(t_k^v) + \left[1 - (1-\alpha)\prod_{u\in N_v}(1-\gamma i_u^{[a]}(t_k^v))\right] \\
&\qquad \times (1 - i_v^{[a]}(t_k^v)) \\
&\quad = (\beta+1)(i_v(t) - i_v^{[a]}(t_k^v)) \\
&\qquad + (1-\alpha)\Bigg[(1 - i_v(t))\prod_{u\in N_v}(1-\gamma i_u(t)) \\
&\qquad - (1 - i_v^{[a]}(t_k^v))\prod_{u\in N_v}(1-\gamma i_u^{[a]}(t_k^v))\Bigg] \\
&\quad = (\beta+1)\varepsilon_v(t,t_k^v) - (1-\alpha)\varepsilon_v(t,t_k^v)\prod_{u\in N_v}(1-\gamma i_u(t)) \\
&\qquad - (1-\alpha)\gamma(1 - i_v(t))\sum_{\omega\in N_v}\varepsilon_\omega(t,t_k^v) \\
&\qquad \times \prod_{u<\omega,u\in N_v}(1-\gamma i_u(t))\prod_{u>\omega,u\in N_v}(1-\gamma i_u^{[a]}(t_k^v)).
\end{aligned}$$

Under the event-based trigger rule in Definition 1, the following holds:

$$\begin{aligned}
&\left\|i^{[a]}(t) - i(t)\right\|_1 \\
&\quad \le \sum_{v\in V}\xi_v\int_{t_k^v}^t\left|\frac{d}{d\tau}\left[i_v^{[a]}(\tau) - i_v(\tau)\right]\right|d\tau \\
&\quad = \sum_{v\in V}\xi_v\int_{t_k^v}^t\Bigg|(\beta+1)\varepsilon_v(\tau,t_k^v) - (1-\alpha)\varepsilon_v(\tau,t_k^v) \\
&\qquad \times \prod_{u\in N_v}(1-\gamma i_u(\tau)) \\
&\qquad - (1-\alpha)\gamma(1 - i_v(\tau))\sum_{\omega\in N_v}\varepsilon_\omega(\tau,t_k^v) \\
&\qquad \times \prod_{u<\omega,u\in N_v}(1-\gamma i_u(\tau))\prod_{u>\omega,u\in N_v}(1-\gamma i_u^{[a]}(t_k^v))\Bigg|d\tau \\
&\quad \le C_1\sum_{v\in V}\xi_v\int_{t_k^v}^t\left[\left|\varepsilon_v(\tau,t_k^v)\right| + \sum_{\omega\in N_v}\left|\varepsilon_\omega(\tau,t_k^v)\right|\right]d\tau \\
&\quad \le C_2\sum_{v\in V}\xi_v\int_{t_k^v}^t e^{-\sigma\tau}d\tau \\
&\quad \le \frac{C}{2}\sum_{v\in V}\xi_v\left(e^{-\sigma t_k^v} - e^{-\sigma t}\right) \\
&\quad \le C\sum_{v\in V}\xi_v e^{-\sigma t_k^v}
\end{aligned}$$

where C_1, C_2 and C are some positive constants and $t \in [t_k^v, t_{k+1}^v)$ for all $v \in V$ and $k = 1,2,\ldots$.

It is proven in [4] that system (2) is globally convergent, confirming the existence of a unique equilibrium $i^* \in [0,1]^n$ such that $\lim_{t\to+\infty}\|i(t) - i^*\|_1 = 0$. From $\inf\{t_{k+1}^v - t_k^v\} > 0$ and $t \to +\infty$ implying $k \to +\infty$, it can be found that $t \to +\infty$ is equivalent to $t_k^v \to +\infty$. Therefore:

$$\begin{aligned}
\lim_{t\to+\infty}\left\|i^{[a]}(t) - i^*\right\|_1 &\le \lim_{t\to+\infty}\left\|i^{[a]}(t) - i(t)\right\|_1 \\
&\quad + \lim_{t\to+\infty}\left\|i(t) - i^*\right\|_1 \\
&\le \lim_{t\to+\infty} C\sum_{v\in V}\xi_v e^{-\sigma t_k^v} + 0 \\
&= 0
\end{aligned}$$

where $t \in [t_k^v, t_{k+1}^v)$.

Finally, it comes to the problem of Zeno-freeness. From inequality (7), it can be deduced that $t_{k+1}^v - t_k^v \ge \eta_v$ where η_v is a positive number. It indicates that for any finite period of time, there is only a finite number of state observation events. Furthermore, there is a positive lower bound in the time intervals between two consecutive state observation events, making the event-based method feasible in practice. In addition, the following holds:

$$t_\kappa^v = \sum_{k=1}^{\kappa}(t_k^v - t_{k-1}^v) = \sum_{k=0}^{\kappa-1}(t_{k+1}^v - t_k^v) < +\infty$$

for $\kappa = 1,2,\ldots$. It effectively shows that system (3) under the event-based trigger rule is Zeno-free, which completes the proof of part ii).

Putting the two pieces of proofs together, the presented work concludes that system (3) under event-based trigger rule in Definition 1 converges to the equilibrium of system (2) and is Zeno-free. ■

C. Adapting Theorem 1 to Accommodate Periodic Reference Setting

Theorem 1 requires that the trigger events occur precisely at sequential points in time t_k^v for $k = 0,1,\ldots$ as in Definition 1. In practice, observation events may occur at a predetermined sequence of points in time, say, with time interval h (e.g., the points highlighted with filled circles in Fig. 1). Since observations are made at points in time that are multiples of h, there can be delays in state observation events because the model-derived observation time may not be a multiple of h. Therefore, what the presented study needs to show is that Theorem 1 is still valid under the periodic reference setting as long as h is small enough, which can be achieved by Theorem 2 below with an adapted event-based trigger rule in Definition 2.

Definition 2 (Adapted Event-based Trigger Rule Accommdodating Discrete-time): Let $t_0^v = 0$ for $v \in V$. The adapted

trigger rule is defined as

$$t_{k+1}^v = \sup\left\{\tau \geq t_k^v, \frac{\tau}{h} \in \mathbb{N} : \max_{u\in N_v\cup\{v\}} \left|\varepsilon_u(\tau, t_k^v)\right| \leq \varphi(\tau)\right\}. \quad (8)$$

Theorem 2: Suppose system (2) submits to the periodic reference setting with a small enough time interval h (which will be specified), so that any actual state-observation event occurs at time t_k^v will be at a multiple of h where $v \in V$ and $k = 0, 1, \ldots$ as specified in Definition 2. Then, Theorem 1 still holds.

Proof: Remember that in the proof of Theorem 1, inequality (7) shows that for $\forall v \in V$ and $k = 0, 1, \ldots$, $t_{k+1}^v - t_k^v \geq \eta_v$ where η_v is a positive number, denoted by

$$\eta = \inf\{\eta_v : v \in V\}$$

a positive lower bound in the state observation time intervals with respect to $\forall v \in V$. Suppose h is small enough, which means $h < \eta$.

The next issue is the periodic reference setting. Without loss of generality, this paper assumes $t_k^v = l_k^v h$ where $l_k^v \in \mathbb{N}$. It executes the next state observation event at time $t_{k+1}^v = l_{k+1}^v h$ according to the adapted event-based trigger rule in Definition 2. Note that $l_{k+1}^v > l_k^v$ and $l_{k+1}^v \in \mathbb{N}$ because $h < \eta$. Regarding the time period $[l_k^v h, l_{k+1}^v h]$, the following can be proven in a similar fashion to the proof in Theorem 1 that

$$\begin{aligned}
&\left\|i^{[a]}(t) - i(t)\right\|_1 \\
&\leq \sum_{v\in V} \xi_v \int_{l_k^v h}^t \left|\frac{d}{d\tau}\left[i_v^{[a]}(\tau) - i_v(\tau)\right]\right| d\tau \\
&\leq C_1 \sum_{v\in V} \xi_v \int_{l_k^v h}^t \left[\left|\varepsilon_v(\tau, l_k^v h)\right| + \sum_{\omega\in N_v} \left|\varepsilon_\omega(\tau, l_k^v h)\right|\right] d\tau \\
&\leq C_2 \sum_{v\in V} \xi_v \int_{l_k^v h}^t e^{-\sigma\tau} d\tau \\
&\leq C \sum_{v\in V} \xi_v e^{-\sigma l_k^v h}
\end{aligned}$$

where C_1, C_2 and C are some positive constants and $t \in [l_k^v h, l_{k+1}^v h)$ for all $v \in V$ and $k = 1, 2, \ldots$.

Similarly to the proof of Theorem 1, regarding the unique equilibrium $i^* \in [0,1]^n$ satisfying $\lim_{t\to+\infty} \|i(t) - i^*\|_1 = 0$, $t \to +\infty$ is equivalent to $l_k^v h \to +\infty$. Then

$$\lim_{t\to+\infty} \left\|i^{[a]}(t) - i^*\right\|_1 \leq \lim_{t\to+\infty} C \sum_{v\in V} \xi_v e^{-\sigma l_k^v h} = 0$$

where $t \in [l_k^v h, l_{k+1}^v h)$.

As for Zeno-freeness, note that for the periodic reference setting, the time interval between two consecutive observation events must be not shorter than the period parameter $h > 0$, which implies Zeno-freeness. ■

In addition, note that Theorem 2 becomes Theorem 1 when $h \to 0$. In the numerical experiments, this study simulates the dynamics in the setting of Theorem 2 and in what follows it presents an algorithm to enforce the event-based trigger rule specified in Definition 2.

D. Translating Trigger Rule in Definition 2 to Algorithm

Here, the trigger rule in Definition 2 is adapted to design Algorithm 1 for estimating the cybersecurity equilibrium. To simplify notations, this paper defines, according to system (3)

$$\begin{aligned}
\mathcal{F}_v^{[a]}(t_k^v) = &-\beta i_v^{[a]}(t_k^v) \\
&+ \left[1 - (1-\alpha)\prod_{u\in N_v} (1 - \gamma i_u^{[a]}(t_k^v))\right](1 - i_v^{[a]}(t_k^v)). \quad (9)
\end{aligned}$$

Algorithm 1: Event-based trigger rule over probability-states as specified in Definition 2

input: $G = (V, E)$, $i_v(0)$ for $v \in V$, σ, h
output: $\{t_k^v\}_{k=0}^{+\infty}$ and $\{i_v(t)\}_{t=0}^{+\infty}$ for $v \in V$
initialize: $k \leftarrow 0$; $t_0^v \leftarrow 0$
while true **do**
  $t \leftarrow t_k^v$
  $Event \leftarrow 0$
  if v is observed with $i_u^{[a]}(t_k^v)$ for $u \in N_v$ **then**
    compute $\mathcal{F}_v^{[a]}(t_k^v)$ according to (9)
  end
  while $Event = 0$ **do**
    $i_v(t) \leftarrow i_v^{[a]}(t_k^v) + (t - t_k^v)\mathcal{F}_v^{[a]}(t_k^v)$
    if $\max_{u\in N_v\cup\{v\}} |i_u(t) - i_u^{[a]}(t_k^v)| \geq \varphi(t)$ **then**
      v probes its neighbors $u \in N_v$ for observing $i_v^{[a]}(t_k^v)$
      $Event \leftarrow 1$
      $t_{k+1}^v \leftarrow t$
      $i_v^{[a]}(t_{k+1}^v) \leftarrow i_v^{[a]}(t)$
    end
    $t \leftarrow t + h$
  end
  $k \leftarrow k + 1$
end

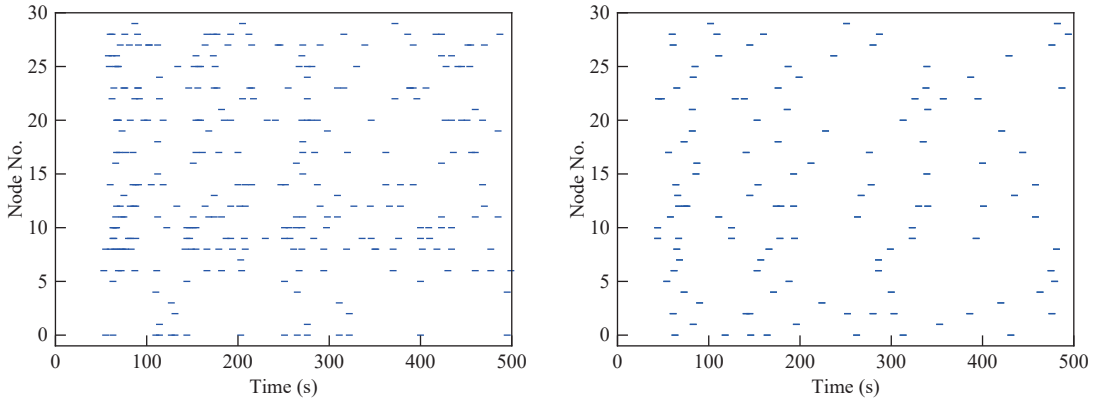
Algorithm 1 has four inputs: attack-defense graph $G = (V, E)$; initial values $i_v(0)$ for $v \in V$; a trigger function φ; and a step length parameter h (i.e., the constant time interval of the periodic reference setting). The presented study sets $\varphi(t) = e^{-\theta t}$, where $e^{-\sigma t}$ is the convergence speed of system (2) and $\theta < \sigma$.

E. Numerical Examples

The presented study uses numerical examples to confirm that the event-based method based on the event-based trigger rule specified in Definition 2 is correct as well as more efficient than the periodic observation method, where efficiency is exhibited by the reduced (or saved) number of observation events incurred by using the event-based method. For graph G in the dynamics model, the following network structures obtained from http://snap.stanford.edu/data/ are sufficient for illustration purposes. Note that the extraction of G in practice demands access to the enterprise's physical network topologies and security policies, which are usually confidential data unavailable to academic researchers.

i) Gnutella peer-to-peer network: This is a directed graph with $|V| = 8717$ nodes, $|E| = 31\,525$ links, maximal node in-degree 64 and $\lambda_{A,1} = 4.7395$. The other model parameters are set as: $\alpha = 0.2108$, $\beta = 0.6528$ and $\gamma = 0.1695$, which means $i(t)$ converges to a unique nonzero equilibrium exponentially.

ii) Enron email network: This is an undirected graph with $|V| = 5242$ nodes, $|E| = 28\,980$ edges, maximal node degree 81 and $\lambda_{A,1} = 45.6167$. The other model parameters are set as: $\alpha = 0.5268$, $\beta = 0.7856$ and $\gamma = 0.0212$, which means $i(t)$



(a) Gnutella; event-based method (b) Enron; event-based method

Fig. 3. Observation events at time $\{t_k^v\}_{k=0}^{+\infty}$ for nodes #0 − #30 in a network, where each blue line represents an observation event.

converges to a unique nonzero equilibrium exponentially.

The above network structures are suitable examples of G because cyber attacks on these networks must follow their topologies.

1) Numerical Method: In this paper's numerical examples, each node $v \in V$ is assigned with an initial compromise probability $i_v(0) \in_R [0,1]$ where $\in_R$ means sampling uniformly at random. This study considers $t \in [0,500]$ steps with a fixed step-length $h = 0.025$ and $\theta = 0.5$. The conditions in Theorem 1 hold in the settings. It is worth mentioning that the maximum value of ratio $\max_{u\in N_v} |\varepsilon_u(t_{k+1}^v, t_k^v)|/|\varepsilon_v(t_{k+1}^v, t_k^v)|$ appears in the early stage of the process with respect to condition 3). The execution of the periodic observation method directly keeps track of the $i_v(t)$ for $v \in V$. Corresponding to the event-based method, the execution of Algorithm 1 keeps track of the t_k^v and the $i_v(t)$ for $v \in V$.

2) Confirming the Correctness of the Event-based Method: In order to demonstrate that the event-based method indeed makes the global state converge to the equilibrium, the mean and standard deviation of $\frac{1}{n}\sum_{v\in V} |i_v(t) - i_v^{[a]}(t)|$ for $t \in [400, 500]$ are calculated. In principle, the mean and the standard deviation, denoted by m and sd, should satisfy $m \approx 0$ and $sd \approx 0$. For the presented experiment, the threshold of effectiveness is defined as $m + sd < 2\times 10^{-2}$. For the Gnutella network, when the dynamics converge to a unique nonzero equilibrium exponentially, we see that $m = 5.69\times 10^{-6}$ and $sd = 2.66\times 10^{-6}$ under the event-based method, with $m + sd = 8.35\times 10^{-6} < 2\times 10^{-2}$, which shows the effectiveness. For the Enron email network, when the dynamics converge to a unique nonzero equilibrium exponentially, we see that $m = 5.34\times 10^{-6}$ and $sd = 2.06\times 10^{-6}$ under the event-based method, with $m + sd = 7.40\times 10^{-6} < 2\times 10^{-2}$, which shows the effectiveness. These results show that the event-based method can estimate cybersecurity equilibrium effectively.

3) Measuring Efficiency of the Event-based Method: Having confirmed the correctness of the estimated cybersecurity equilibrium, the next step is to compare the numbers of observation events induced by the event-based method and by the periodic observation method. The threshold of efficiency is defined as 80% of the events induced by the periodic method (i.e., an event-based method should save at least 80% of the cost incurred by the periodic method).

Fig. 3 plots the observation events at $\{t_k^v\}_{k=0}^{+\infty}$ for nodes #0 − #30 during time interval $t \in [0,500]$, where each blue line represents an observation event. The following observations can be made. First, the event-based method incurs fewer observation events. Compared with the periodic observation method, the event-based method reduces 98.45% of the observation events in the case of the Gnutella network, and 99.08% in the case of the Enron email network. This demonstrates that the event-based method can reduce more than 98% of the observation cost compared with the periodic observation method. Second, the time intervals between observation events satisfy $t_{k+1}^v - t_k^v > 0$ for all $v \in V$ and $k = 1, 2, \ldots$. This confirms Zeno-freeness of the event-based method. Indeed, the time interval $t_{k+1}^v - t_k^v$ becomes larger and larger as the dynamics converge to the equilibrium.

Moreover, the authors discover an interesting empirical phenomenon: the convergence speed of the dynamics plays an important role in determining the cost of the associated observations. Specifically, slower convergence allows more observation cost to be reduced. The presented study leaves it to future investigations to rigorously prove whether the phenomenon is universally true or not.

IV. Putting the Event-based Method Into Practice

In order to utilize the aforementioned event-based method in practice, the following gap needs to be bridged. In the model, the state of node $v \in V$ at time t is represented by $i_v(t)$, namely the probability that v is in compromised state at time t. In practice, this state is often measured as a Boolean value, with "0" indicating v is secure but vulnerable and "1" indicating v is compromised. In other words, the sample-state of node $v \in V$ at time t can be denoted by

$$\chi_v(t) = \begin{cases} 0, & v \text{ is in the secures tate at time } t \\ 1, & v \text{ is in the compromised stateat time } t. \end{cases} \tag{10}$$

This difference underlines the gap between the probability-states in the model and the sample-states in practice.

A. Bridging the Gap via 0-1 State Ergodic Process

This paper proposes bridging the aforementioned gap by

obtaining an estimation $\widehat{i_v(t)}$ of probabilities $i_v(t)$ and an estimation $\widehat{s_v(t)}$ of probabilities $s_v(t)$ from a 0-1 state ergodic process over time as indicated by (10). For this purpose, the paper adopts the theorem of two-valued processes introduced in [59, Chapter 1], and uses the Lebesgue measure $\mathcal{M}$ to define

$$\begin{cases} \mathcal{T}_{v0}(t) = \mathcal{M}(\{\tau \le t : \chi_v(\tau) = 0\}) \\ \mathcal{T}_{v1}(t) = \mathcal{M}(\{\tau \le t : \chi_v(\tau) = 1\}). \end{cases} \tag{11}$$

Theorem 3 below shows how to generate probabilities $\widehat{i_v(t)}$ and $\widehat{s_v(t)}$ from a 0-1 state ergodic process over time.

Theorem 3 [59]: Let $\{\chi_v(t), t > 0\}$ for $v \in V$ be a 0-1 state ergodic process. Let

$$\begin{cases} \widehat{s_v(t)} = \dfrac{\mathcal{T}_{v0}(t)}{t} \\ \widehat{i_v(t)} = \dfrac{\mathcal{T}_{v1}(t)}{t}. \end{cases}$$

Then

$$\begin{cases} \lim\limits_{t\to+\infty} [\mathbb{P}(\chi_v(t) = 0) - \widehat{s_v(t)}] = 0 \\ \lim\limits_{t\to+\infty} [\mathbb{P}(\chi_v(t) = 1) - \widehat{i_v(t)}] = 0. \end{cases}$$

Based on Theorem 3, $\widehat{i_v(t)}$ can be used to estimate $i_v(t)$ and $\widehat{s_v(t)}$ to estimate $s_v(t)$ at sufficiently large time t. The following Algorithm 2 is designed for this estimation, where a stack data structure $\mathcal{S}$ is used with two standard stack operations in push (i.e., adding an element on the top of the stack) and pop (i.e., removing the element on the top of the stack). Let $|\mathcal{S}|$ be the number of elements in stack $\mathcal{S}$.

Algorithm 2: Estimating $\widehat{i_v(t)}$ and $\widehat{s_v(t)}$

input: h, $\{\chi_v(t)\}_{t=0}^{+\infty}$, $\mathcal{N}_v^1(0) = \chi_v(0)$, $\mathcal{N}_v^0(0) = 1 - \chi_v(0)$
output: $\{\widehat{s_v(t)}\}_{t=0}^{+\infty}$, $\{\widehat{i_v(t)}\}_{t=0}^{+\infty}$

for $t = 1$ **to** $+\infty$ **do**
  if $\chi_v(t) == 0$ **then**
    $\mathcal{N}_v^0(t) = \mathcal{N}_v^0(t-1) + 1$
    $\mathcal{N}_v^1(t) = 0$
  else if $\chi_v(t)$! $= 0$ **then**
    $\mathcal{N}_v^0(t) = 0$
    $\mathcal{N}_v^1(t) = \mathcal{N}_v^1(t-1) + 1$
  end
end
for $i = 0$ **to** 1 **do**
  Create Stack $\mathcal{S}_i$
  for $t = 0$ **to** $+\infty$ **do**
    if ($t == 0$ **and** $\mathcal{N}_v^i(t)$! $= 0$) **or** ($t > 0$ **and** $\mathcal{N}_v^i(t)$! $= 0$ **and** $\mathcal{N}_v^i(t-1) == 0$) **then**
      $\mathcal{S}_i.push(\mathcal{N}_v^i(t))$
    else if $t > 0$ **and** $\mathcal{N}_v^i(t)$! $= 0$ **and** $\mathcal{N}_v^i(t-1)$! $= 0$ **then**
      $\mathcal{S}_i.pop()$
      $\mathcal{S}_i.push(\mathcal{N}_v^i(t))$
    end
    if $|\mathcal{S}_i|$! $= 0$ **then**
      $\mathcal{T}_{vi}(t) = \frac{1}{|\mathcal{S}_i|} \sum_{e\in\mathcal{S}_i} e$
    else
      $\mathcal{T}_{vi}(t) = 0$
    end
  end
end
for $t = 0$ **to** $+\infty$ **do**
  $\widehat{s_v(t)} = \dfrac{\mathcal{T}_{v0}(t)}{\mathcal{T}_{v0}(t) + \mathcal{T}_{v1}(t)}$
  $\widehat{i_v(t)} = \dfrac{\mathcal{T}_{v0}(t)}{\mathcal{T}_{v0}(t) + \mathcal{T}_{v1}(t)}$
end
return $\{\widehat{s_v(t)}\}_{t=0}^{+\infty}$, $\{\widehat{i_v(t)}\}_{t=0}^{+\infty}$

Since undirected networks are a special case of directed networks, this study will only perform experiments on the directed Gnutella network. In order to simulate a 0-1 process for $\forall v \in V$, the paper samples node v at time t by its compromise probability $i_v(t)$

$$\chi_v(t) = H[i_v(t) - \mathrm{Rand}(0,1)] \tag{12}$$

where $\mathrm{Rand}(0,1)$ means drawing a random real number uniformly from $[0,1]$, and H is the discrete heaviside step function

$$H(x) = \begin{cases} 0, & x < 0 \\ 1, & x \ge 0. \end{cases} \tag{13}$$

Run Algorithm 2 until the state estimation curve converges to the probability-state curve. From the numerical result, it can be seen that the estimation curve indeed converges to the equilibrium of the underlying model as expected. Fig. 4 depicts the convergence processes of two arbitrarily-chosen nodes.

B. Using the Event-based Method in Practice

Having bridged the gap between probability-states and sample-states, this paper moves to use the event-based method in practice as follows. Fig. 5 plots the experimental result, where the red curve corresponds to the sample-state estimation curve $\widehat{i_v(t)}$ (which can also be regarded as the classic periodic observation method with a very high frequency), the green curve corresponds to the event-based method $\widehat{i_v^{[a]}(t)}$, and the blue curve corresponds to the under lying dynamic $i_v(t)$ (which can not be directly observed).

The study calculates the mean and standard deviation of $\frac{1}{n}\sum_{v\in V} |\widehat{i_v(t)} - \widehat{i_v^{[a]}(t)}|$, denoted by m_1 and sd_1. In principle, the mean and the standard deviation satisfy $m_1 \approx 0$ and $sd_1 \approx 0$. The results of $m_1 = 7.74\times10^{-3}$ and $sd_1 = 4.96\times10^{-3}$ for $t \in [400,500]$ prove the effectiveness of the event-based method. The mean and standard deviation of $\frac{1}{n}\sum_{v\in V} |i_v(t) - \widehat{i_v^{[a]}(t)}|$ are also calculated, denoted by m_0 and sd_0. The results are $m_0 = 1.81\times10^{-2}$ and $sd_0 = 1.10\times10^{-2}$ for $t \in [400,500]$. Notice that the sample-state estimation curve converges to the equilibrium relatively slowly, so the accuracy can be improved by prolonging the experiment time along with more observation events (i.e., higher cost). For example, we have $m_0 = 8.71\times10^{-3}$ and $sd_0 = 8.72\times10^{-3}$ for $t \in [900,1000]$,

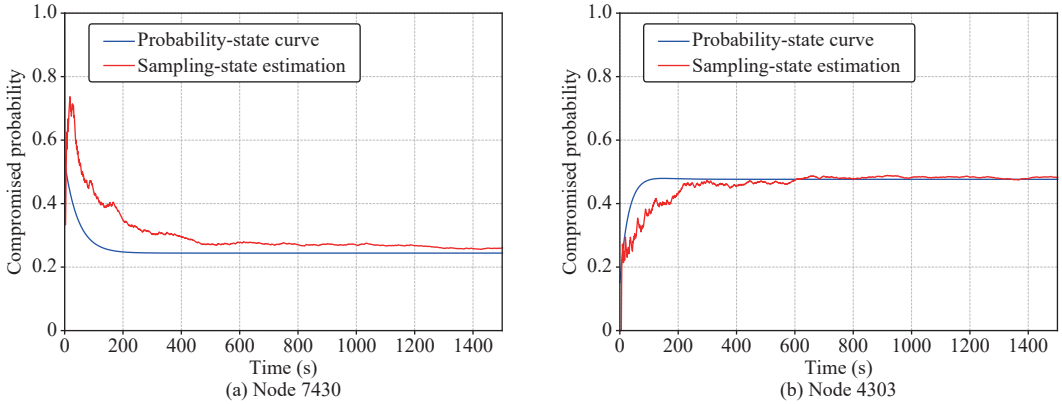


Fig. 4. The state estimation curve of a single node converges to the probability-state curve of that node.

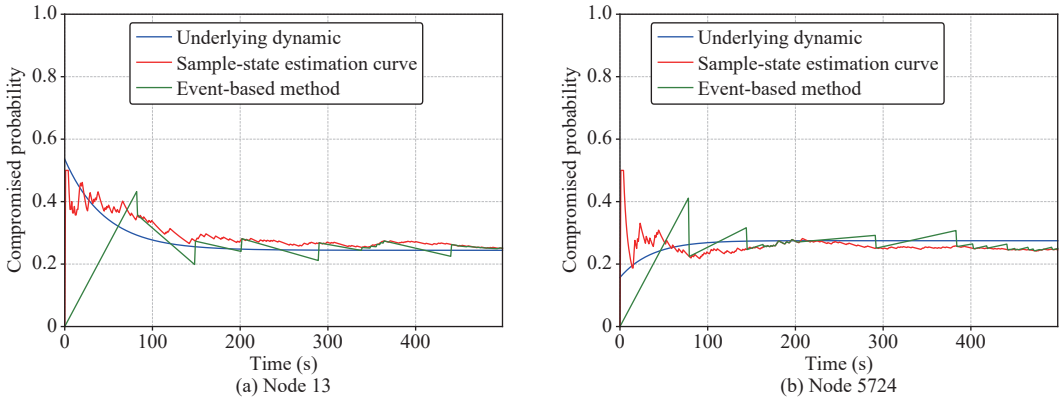


Fig. 5. Applying the event-based method to the sample-state estimation curve which approximates its underlying dynamic.

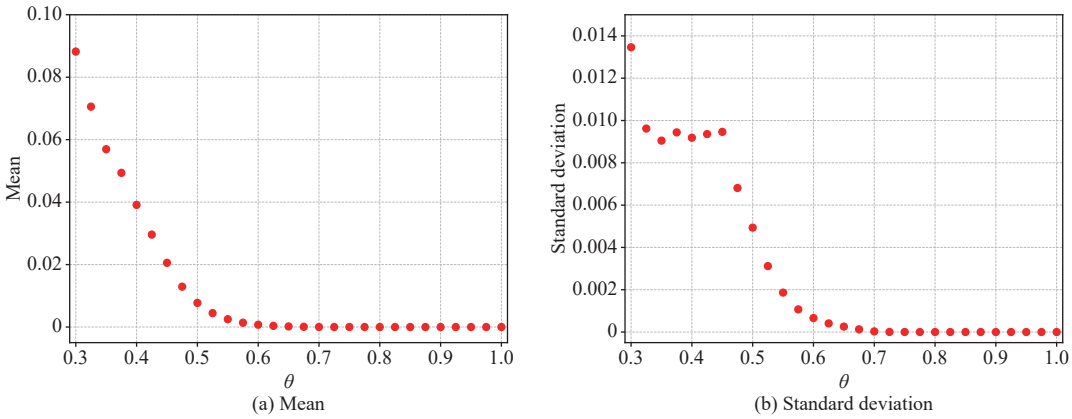


Fig. 6. The means and standard deviations with respect to various values of θ over the same time window in the event-based trigger function φ.

with section $m_0 + sd_0 = 1.743 \times 10^{-2} < 2 \times 10^{-2}$ (i.e., threshold defined in Section III-E), which shows effectiveness.

C. Impact of the Trigger Function Parameter

Note that trigger function (4) plays an important role in the event-based method. In the experiments herein, $\varphi(t) = e^{-\theta t}$ where $e^{-\sigma t}$ is the convergence speed of system (2) and $\theta < \sigma$. With respect to the trigger function, a smaller θ may be chosen to loosen the trigger rule. This paper therefore tests the impact of trigger functions with different values of θ. Fig. 6 plots the means and standard deviations of $\frac{1}{n}\sum_{v\in V}|\widehat{i_v(t)} - \widehat{i_v^{[a]}(t)}|$ for $t \in [400, 500]$ under different trigger functions.

Fig. 6 illustrates that with respect to a designated time interval, a larger θ does not necessarily achieve a better performance, which instead depends on whether or not system (3) under the event-based trigger rule in Definition 1 is able to converge during this time interval. If it converges, then a large θ results in extraneous observation events, while a small θ causes fewer events to be triggered.

D. Robustness Against False Negative Observations

When bridging the gap between sample-states observed in

practice and probability-states in the theoretical model, an underlying premise is that the 0-1 state can be precisely determined. However, this may not be true in practice because there might be false-negative observations when determining a computer's state (i.e., failures in detecting attacks). It is therefore important to accommodate such measurement errors. Since the dynamics converge to the equilibrium of the sample-state estimation ($\widehat{i_v(t)}$) for the event-based method, the only issue is the correlation between the false-negative rate in the state observation and the bias of the equilibrium estimation.

This paper conducts an experiment to evaluate the bias of the estimated equilibrium, which is the mean of $\frac{1}{n}\sum_{v\in V}\frac{|i_v(t)-\widehat{i_v(t)}|}{i_v(t)}$ for $t\in[1300,1500]$ and denoted by r. In principle, r should be linear. Regardless, it should hold that $r\approx 0$ when there are no false-negatives and $r=1$ when all compromised nodes are treated as secure (i.e., $\widehat{i_v(t)}=0$, $\forall v\in V$). Fig. 7 illustrates the correlation when varying the false-negative rate from 0 to 1, which is almost linear with a slope of 1. The practical meaning of this observation is that the estimated equilibrium needs to be adjusted to accommodate the false-negative rate (if applicable).

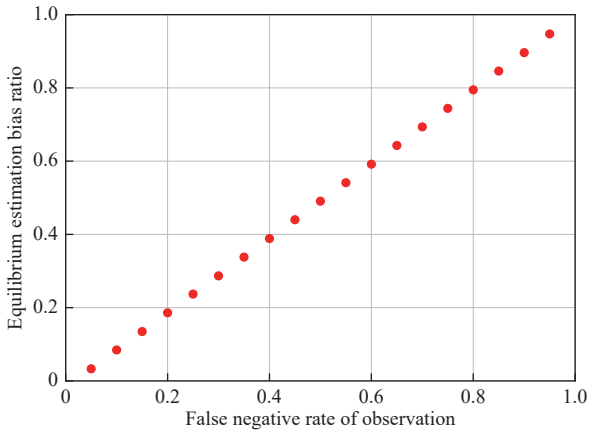


Fig. 7. Correlation between the false-negative rate in the sample-state observation and the bias of the equilibrium estimation.

V. Conclusion

This paper has shown how to use the event-based method to estimate the equilibrium of preventive and reactive cyber defense dynamics. Numerical examples confirmed that the event-based method can estimate the equilibrium while reducing 98% of the state observation cost incurred by the periodic method. The paper also spots an empirical phenomenon that the slower the convergence of the dynamics, the more observation cost is saved by the event-based method. Moreover, the presented study probed into the practical use of the event-based method, by bridging the gap between the probability-state in the theoretical model and the sample-state in practice, which may be of independent value.

There are many open problems for future research, such as: What is the lower-bound observation cost of an event-based method? Do there exist better, or even optimal, forms of event-based methods? How can the aforementioned empirical phenomenon (that the slower the convergence, the more observation cost is saved) be rigorously proven (or disproven)? Can other models cope with the case of polynomial convergence speed of a system (2)? Can other models handle situations where the observation errors are indeterminate (e.g., when only the upper or lower bound of the false negative rate are known)? Can the presented method be applied to other dynamics under different event-trigger scenarios? Can other event-based methods be designed for cybersecurity dynamics models [41], [44], [47] that do not make the current assumption of dynamics independence?

Acknowledgment

We thank Zongzong Lin for his constructive advice on improving the proof of this paper. We thank Eric Ficke and Yihan Xu for proofreading the paper.

References

[1] K. J. Åström and B. Bernhardsson, "Comparison of periodic and event based sampling for first-order stochastic systems," *IFAC Proc. Vol.*, vol. 32, no. 2, pp. 5006–5011, Jul. 1999.

[2] K. E. Årzén, "A simple event-based PID controller," *IFAC Proc. Vol.*, vol. 32, no. 2, pp. 8687–8692, Jul. 1999.

[3] K. H. Johansson, M. Egerstedt, J. Lygeros, and S. Sastry, "On the regularization of zeno hybrid automata," *Syst. Control Lett.*, vol. 38, no. 3, pp. 141–150, Oct. 1999.

[4] R. Zheng, W. L. Lu, and S. H. Xu, "Preventive and reactive cyber defense dynamics is globally stable," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 2, pp. 156–170, Apr. 2018.

[5] S. H. Xu, "Cybersecurity dynamics," in *Proc. Symp. and Bootcamp on the Science of Security*, Raleigh, USA, 2014, pp. 14.

[6] S. H. Xu, "Cybersecurity dynamics: A foundation for the science of cybersecurity," in *Proactive and Dynamic Network Defense*, C. Wang and Z. Lu, Eds. Cham, Switzerland: Springer, 2019, pp. 1–31.

[7] K. J. Astrom and B. M. Bernhardsson, "Comparison of riemann and lebesgue sampling for first order stochastic systems," in *Proc. 41st IEEE Conf. Decision and Control*, Las Vegas, USA, 2002, pp. 2011–2016.

[8] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Trans. Autom. Control*, vol. 52, no. 9, pp. 1680–1685, Sep. 2007.

[9] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Proc. 51st IEEE Conf. Decision and Control*, Maui, USA, 2012, pp. 3270–3285.

[10] D. R. Ding, Z. D. Wang, and Q. L. Han, "A set-membership approach to event-triggered filtering for general nonlinear systems over sensor networks," *IEEE Trans. Autom. Control*, vol. 65, no. 4, pp. 1792–1799, Apr. 2020.

[11] E. Johannesson, T. Henningsson, and A. Cervin, "Sporadic control of first-order linear stochastic systems," in *Hybrid Systems: Computation and Control*, A. Bemporad, A. Bicchi, and G. Buttazzo, Eds. Berlin, Heidelberg, Germany: Springer, 2007, pp. 301–314.

[12] X. F. Wang and M. D. Lemmon, "Event-triggering in distributed networked control systems," *IEEE Trans. Autom. Control*, vol. 56, no. 3, pp. 586–601, Mar. 2011.

[13] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson, "Distributed event-triggered control for multi-agent systems," *IEEE Trans. Autom. Control*, vol. 57, no. 5, pp. 1291–1297, May 2012.

[14] G. S. Seyboth, D. V. Dimarogonas, and K. H. Johansson, "Event-based broadcasting for multi-agent average consensus," *Automatica*, vol. 49, no. 1, pp. 245–252, Jan. 2013.

[15] W. L. Lu, Y. J. Han, and T. P. Chen, "Pinning networks of coupled dynamical systems with Markovian switching couplings and event-triggered diffusions," *J. Franklin Inst.*, vol. 352, no. 9, pp. 3526–3545, Sep. 2015.

[16] Y. J. Han, W. L. Lu, and T. P. Chen, "Consensus analysis of networks with time-varying topology and event-triggered diffusions," *Neural Netw.*, vol. 71, pp. 196–203, Nov. 2015.

[17] W. L. Lu, Y. J. Han, and T. P. Chen, "Synchronization in networks of linearly coupled dynamical systems via event-triggered diffusions," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 26, no. 12, pp. 3060–3069, Dec. 2015.

[18] R. Zheng, X. L. Yi, W. L. Lu, and T. P. Chen, "Stability of analytic neural networks with event-triggered synaptic feedbacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 2, pp. 483–494, Feb. 2016.

[19] W. L. Lu, R. Zheng, and T. P. Chen, "Centralized and decentralized global outer-synchronization of asymmetric recurrent time-varying neural network by data-sampling," *Neural Netw.*, vol. 75, pp. 22–31, Mar. 2016.

[20] X. H. Li, T. Parker, and S. H. Xu, "Towards quantifying the (in)security of networked systems," in *Proc. 21st Int. Conf. Advanced Information Networking and Applications*, Niagara Falls, Canada, 2007, pp. 420–427.

[21] A. G. M'Kendrick, "Applications of mathematics to medical problems," *Proc. Edinb. Math. Soc.*, vol. 44, pp. 98–130, Feb. 1925.

[22] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. Roy. Soc. A*: *Math.*, *Phys. Eng. Sci.*, vol. 115, no. 772, pp. 700–721, Aug. 1927.

[23] N. T. J. Bailey, *The Mathematical Theory of Infectious Diseases and Its Applications*. 2nd ed. London, UK: Hodder Arnold, 1975.

[24] R. M. Anderson and R. M. May, *Infectious Diseases of Humans*. Oxford, UK: Oxford University Press, 1991.

[25] H. W. Hethcote, "The mathematics of infectious diseases," *SIAM Rev.*, vol. 42, no. 4, pp. 599–653, Jan. 2000.

[26] J. O. Kephart and S. R. White, "Directed-graph epidemiological models of computer viruses," in *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, Oakland, USA, 1991, pp. 343–359.

[27] J. O. Kephart and S. R. White, "Measuring and modeling computer virus prevalence," in *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, Oakland, USA, 1993, pp. 2–15.

[28] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics and endemic states in complex networks," *Phys. Rev. E*, vol. 63, pp. 066117, May 2001.

[29] Y. Moreno, R. Pastor-Satorras, and A. Vespignani, "Epidemic outbreaks in complex heterogeneous networks," *Eur. Phys. J. B*, vol. 26, no. 4, pp. 521–529, Apr. 2002.

[30] R. Pastor-Satorras and A. Vespignani, "Epidemic dynamics in finite size scale-free networks," *Phys. Rev. E*, vol. 65, pp. 035108, Mar. 2002.

[31] M. E. J. Newman, "The structure and function of complex networks," *SIAM Rev.*, vol. 45, no. 2, pp. 167–256, Jan. 2003.

[32] A. Barrat, M. Barthélemy, and A. Vespignani, *Dynamical Processes on Complex Networks*. Cambridge, UK: Cambridge University Press, 2008.

[33] Y. Wang, D. Chakrabarti, C. X. Wang, and C. Faloutsos, "Epidemic spreading in real networks: An eigenvalue viewpoint," in *Proc. 22nd IEEE Int. Symp. Reliable Distributed Systems*, Florence, Italy, 2003, pp. 25–34.

[34] A. Ganesh, L. Massoulie, and D. Towsley, "The effect of network topology on the spread of epidemics," in *Proc. 24th IEEE Annu. Joint Conf. IEEE Computer and Communications Societies*, Miami, USA, 2005, pp. 1455–1466.

[35] D. Chakrabarti, Y. Wang, C. X. Wang, J. Leskovec, and C. Faloutsos, "Epidemic thresholds in real networks," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 4, pp. 13, Jan. 2008.

[36] P. Van Mieghem, J. Omic, and R. Kooij, "Virus spread in networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, Feb. 2009.

[37] T. M. Liggett, *Interacting Particle Systems*. New York: USA: Springer, 1985.

[38] K. D. Hoover, "Idealizing reduction: The microfoundations of macroeconomics," *Erkenntnis*, vol. 73, no. 3, pp. 329–347, Nov. 2010.

[39] Y. J. Han, W. L. Lu, and S. H. Xu, "Preventive and reactive cyber defense dynamics with ergodic time-dependent parameters is globally attractive," arXiv: 2001.07958, Jan. 2020.

[40] Z. Z. Lin, W. L. Lu, and S. H. Xu, "Unified preventive and reactive cyber defense dynamics is still globally convergent," *IEEE/ACM Trans. Netw.*, vol. 27, no. 3, pp. 1098–1111, Jun. 2019.

[41] M. C. Xu, G. F. Da, and S. H. Xu, "Cyber epidemic models with dependences," *Internet Math.*, vol. 11, no. 1, pp. 62–92, Jan. 2015.

[42] S. H. Xu, "Emergent behavior in cybersecurity," in *Proc. Symp. and Bootcamp on the Science of Security*, Raleigh, USA, 2014, pp. 13.

[43] Y. J. Han, W. L. Lu, and S. H. Xu, "Characterizing the power of moving target defense via cyber epidemic dynamics," in *Proc. Symp. and Bootcamp on the Science of Security*, Raleigh, USA, 2014, pp. 10.

[44] G. F. Da, M. C. Xu, and S. H. Xu, "A new approach to modeling and analyzing security of networked systems," in *Proc. Symp. and Bootcamp on the Science of Security*, Raleigh, USA, 2014, pp. 6.

[45] S. H. Xu, W. L. Lu, L. Xu, and Z. X. Zhan, "Adaptive epidemic dynamics in networks: Thresholds and control," *ACM Trans. Auton. Adapt. Syst.*, vol. 8, no. 4, pp. 19, Jan. 2014.

[46] S. H. Xu, W. L. Lu, and Z. X. Zhan, "A stochastic model of multivirus dynamics," *IEEE Trans. Depend. Secure Comput.*, vol. 9, no. 1, pp. 30–45, Jan.–Feb. 2012.

[47] M. C. Xu and S. H. Xu, "An extended stochastic model for quantitative security analysis of networked systems," *Internet Math.*, vol. 8, no. 3, pp. 288–320, Jul. 2012.

[48] S. H. Xu, W. L. Lu, and L. Xu, "Push- and pull-based epidemic spreading in networks: Thresholds and deeper insights," *ACM Trans. Auton. Adapt. Syst.*, vol. 7, no. 3, pp. 32, Oct. 2012.

[49] S. H. Xu, "The cybersecurity dynamics way of thinking and landscape," in *Proc. 7th ACM Workshop on Moving Target Defense (ACM MTD' 2020)*, Orlando, USA, pp. 69–80, Nov. 2020.

[50] X. H. Li, P. Parker, and S. H. Xu, "A stochastic model for quantitative security analyses of networked systems," *IEEE Trans. Depend. Secure Comput.*, vol. 8, no. 1, pp. 28–43, Jan.–Feb. 2011.

[51] J. D. Mireles, E. Ficke, J. H. Cho, P. Hurley, and S. H. Xu, "Metrics towards measuring cyber agility," *IEEE Trans. Inf. Foren. Secur.*, vol. 14, no. 12, pp. 3217–3232, Dec. 2019.

[52] J. H. Cho, S. H. Xu, P. M. Hurley, M. Mackay, T. Benjamin, and M. Beaumont, "STRAM: Measuring the trustworthiness of computer-based systems," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 128, Feb. 2019.

[53] M. Pendleton, R. Garcia-Lebron, J. H. Cho, and S. H. Xu, "A survey on systems security metrics," *ACM Comput. Surv.*, vol. 49, no. 4, pp. 62, Dec. 2016.

[54] H. S. Chen, J. H. Cho, and S. H. Xu, "Quantifying the security effectiveness of network diversity: Poster," in *Proc. 5th Annu. Symp. and Bootcamp on Hot Topics in the Science of Security*, Raleigh, USA, 2018, pp. 24.

[55] H. S. Chen, J. H. Cho, and S. H. Xu, "Quantifying the security effectiveness of firewalls and DMZs," in *Proc. 5th Annu. Symp. and Bootcamp on Hot Topics in the Science of Security*, Raleigh, USA, 2018, pp. 9.

[56] R. Zheng, W. L. Lu, and S. H. Xu, "Active cyber defense dynamics exhibiting rich phenomena," in *Proc. Symp. and Bootcamp on the Science of Security*, Urbana, USA, 2015, pp. 2.

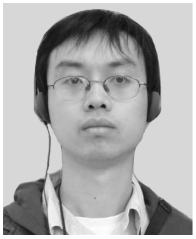
[57] S. H. Xu, W. L. Lu, and H. L. Li, "A stochastic model of active cyber defense dynamics," *Internet Math.*, vol. 11, no. 1, pp. 23–61, Jan. 2015.

[58] W. L. Lu, S. H. Xu, and X. L. Yi, "Optimizing active cyber defense," in *Proc. 4th Int. Conf. Decision and Game Theory for Security*, Fort Worth, USA, 2013, pp. 206–225.

[59] A. Sard, "The measure of the critical values of differentiable maps," *Bull. Am. Math. Soc.*, vol. 48, no. 12, pp. 883–890, 1999.

Zhaofeng Liu received the B.S. degree in mathematics and applied mathematics from Fudan University in 2016. Currently, he is pursuing the Ph.D. degree in applied mathematics at Fudan University. His research interests include cybersecurity dynamics, complex networks, and adversarial machine learning.

Ren Zheng received the Ph.D. degree in applied mathematics from Fudan University, in 2017. He is currently a Senior Researcher at the Artificial Intelligence Laboratory, SAIC Motor Corporation Limited, and also with SAIC Intelligent Technology (Shanghai) Corporation Limited. His research interests include deep reinforcement learning, optimization, complex networks, and cybersecurity dynamics.



Wenlian Lu (M'09–SM'15) received the B.S. degree in mathematics and the Ph.D. degree in applied mathematics from Fudan University, in 2000 and 2005, respectively. He was a Post-Doctoral Fellow with the Max Planck Institute for Mathematics in the Science, Leipzig, Germany, from 2005 to 2007, and a Marie-Curie International Incoming Research Fellow with the Department of Computer Sciences, University of Warwick, Coventry, UK, from 2012 to 2014. He is currently a Professor with the School of Mathematical Sciences and the Institute for Science and Technology of Brain-Inspired AI, Fudan University. His current research interests include neural networks, cybersecurity dynamics, computational systems biology, nonlinear dynamical systems, and complex systems. He served as an Associate Editor for the *IEEE Transactions on Neural Networks and Learning Systems* from 2013 to 2019 and *Neurocomputing* from 2010 to 2015.

Shouhuai Xu is a Full Professor in the Department of Computer Science, University of Texas at San Antonio. He received the Ph.D. degree in computer science from Fudan University. He is the Founding Director of the Laboratory for Cybersecurity Dynamics (http://www.cs.utsa.edu/~shxu/LCD/index.html). He coined the notion of cybersecurity dynamics as a foundation for the emerging science of cybersecurity, with three pillars: first-principle cybersecurity modeling and analysis (the *x*-axis, to which the present paper belongs); cybersecurity data analytics (the *y*-axis); and cybersecurity metrics (the *z*-axis). He co-initiated the International Conference on Science of Cyber Security and is serving as its Steering Committee Chair. He is/was an Associate Editor of *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, *IEEE Transactions on Information Forensics and Security (IEEE T-IFS)*, and *IEEE Transactions on Network Science and Engineering (IEEE TNSE)*.