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 estimation of 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—global state estimation, event-based method, preventive and reactive cyber defense dynamics, cybersecurity dynamics, cybersecurity equilibrium

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). Figure 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 Figure 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 [3, 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], 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, [3, 11, 12, 13, 14, 15, 16, 17, 18, 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, 22, 23, 24, 25]) and its variants in cyber epidemiology (e.g., [26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36], interacting particle systems [37], and microfoundations in economics [38]). This notion has opened the door to a new research field with many results (e.g., [39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 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, 34, 35, 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 (in [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, 52, 53, 54, 55]. There are other kinds of cybersecurity dynamics, which aim to accommodate adaptive defenses [45], active defenses [56, 57, 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, 34, 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:
- **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.
- **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:

- **Push-based attacks**: These correspond to the use of computer malware to spread across the network.
- **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 $A = [a_{uv}]_{n \times n}$ denote the adjacency matrix of $G$, where $a_{uv} = 1$ if and only if $(u, v) \in E$. Since the model aims to describe the attacks between computers, we set $a_{uv} = 0$. Let $\text{deg}(v)$ be the degree of node $v \in V$ when $G$ is undirected or the in-degree of $v$ when $G$ is directed, where $\text{deg}(v) = |N_v|$ 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. 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.

![State-transition diagram](image)

Figure 2 describes the state-transition diagram for a node $v \in V$ at time $t$, where $\theta_{v,1\rightarrow0}(t)$ abstracts the effectiveness of the reactive defenses and $\theta_{v,0\rightarrow1}(t)$ 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, $\theta_{v,1\rightarrow0}(t) = \beta$. On the other hand, $\theta_{v,0\rightarrow1}(t)$ 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

$$\theta_{v,0\rightarrow1}(t) = 1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i_u(t)).$$

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

$$\begin{cases}
\frac{ds_v(t)}{dt} = \theta_{v,1\rightarrow0}(t) \cdot i_v(t) - \theta_{v,0\rightarrow1}(t) \cdot s_v(t)
\frac{di_v(t)}{dt} = \theta_{v,0\rightarrow1}(t) \cdot s_v(t) - \theta_{v,1\rightarrow0}(t) \cdot i_v(t).
\end{cases}$$

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

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

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

- 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.
- 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.

- If $\lambda_{A,1} < \beta/\gamma$, the dynamics converge to equilibrium $0$ exponentially (see also [35], [48]).
- If $\lambda_{A,1} = \beta/\gamma$, the dynamics converge to equilibrium $0$ polynomially.
- 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 $\alpha_e$ and $\beta_v$, and edge-dependent parameter $\gamma_{uv}$ [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 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 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 \( ||i||_1 = \sum_{i=1}^{n} \xi_i |i_i| \) is adopted, where \( \xi_i \in [0, 1] \) is a positive constant subject to \( \sum_{i=1}^{n} \xi_i = 1 \). 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 \( t_k \), which indicates node \( v \)'s \( k \)-th state observation event, where \( k = 0, 1, \ldots \). Upon receiving the probe, \( u \)'s current state, denoted by \( i_u^{[a]}(t_k) \), is given to \( v \), where superscript \( “[a]” \) highlights the difference from \( i_u(t) \) in the original dynamical system. However, it holds that \( i_u^{[a]}(t_k) = i_v(t_k) \).

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 \( v \in V, t \in [t_k, t_{k+1}) \),

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

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

\[
\begin{align*}
\varepsilon_v(t, t_k) &= i_v(t) - i_v^{[a]}(t_k) \\
\varepsilon_u(t, t_k) &= i_u(t) - i_u^{[a]}(t_k)
\end{align*}
\]

for \( t \in [t_k, t_{k+1}) \) and \( k = 0, 1, \ldots \). When system (2) converges exponentially, its convergence speed can be denoted by \( e^{-\sigma t} \) for some appropriate \( \sigma \). Let \( \varphi \) be a continuous
function satisfying:
\[ \varphi(t) = M_0 e^{-\nu t}, \forall t > 0, \tag{4} \]
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 \( t^v_0 = 0 \) for \( v \in V \). The trigger rule is defined as:
\[ t^v_{k+1} = \sup \left\{ \tau \geq t^v_k : \max_{u \in N_v \cup \{v\}} |\varepsilon_u(\tau, t^v_k)| \leq \varphi(\tau) \right\}, \tag{5} \]
which specifies a sequence of state observation events at time \( \{t^v_k\}_{k=0}^{+\infty} \).

**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:
(a) \((\alpha, \beta, \gamma) \notin \Theta\) for some set with zero measure \( \Theta \subset \mathbb{R}^3 \);
(b) parameters satisfy the conditions required by Lemma 7;
(c) there exists some \( \zeta > 0 \), so that:
\[ \max_{u \in N_v} |\varepsilon_u(t^v_k + 1, t^v_k)| \leq \zeta |\varepsilon_v(t^v_k + 1, t^v_k)| \]
holds for \( \forall v \in V, k = 0, 1, \cdots \). 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 \( \inf \{t^v_{k+1} - t^v_k\} > 0 \) 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:
\[ -\beta i^*_v + \left[ 1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i^*_u) \right] (1 - i^*_v) = 0 \]
Let \( z_v(t) = i_v(t) - i^*_v \) for all \( i^*_v \). Then:
\[ \left| \frac{d}{dt} z_v(t) \right| \]
\[ = \left| -\beta i_v(t) + \left[ 1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i_u(t)) \right] \left( 1 - i_v(t) \right) + \beta i^*_v - \left[ 1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i^*_u) \right] \right| \]
\[ = \left| (\beta + 1)z_v(t) - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i_u(t)) z_v(t) \right| \]
\[ - \left( 1 - \alpha \right) \left[ \prod_{u \in N_v} (1 - \gamma i^*_u) - \prod_{u \in N_v} (1 - \gamma i_u(t)) \right] \]
\[ \left( 1 - i_v(t) \right) \right| \]
Let \( u_- \) be the smallest index in \( N_v \). Notice that
\[ \prod_{u \in N_v} \left( 1 - \gamma i^*_u \right) - \prod_{u \in N_v} \left( 1 - \gamma i_u(t) \right) \]
\[ = \left[ (1 - \gamma i_u(t)) + (\gamma i_u - \gamma i^*_u) \right] \]
\[ \prod_{u > u, u \in N_v} (1 - \gamma i_u(t)) - \prod_{u > u, u \in N_v} (1 - \gamma i_u(t)) \]
\[ = \gamma z_{u-} \prod_{u > u, u \in N_v} (1 - \gamma i^*_u) + \prod_{u > u, u \in N_v} (1 - \gamma i_u(t)) \]
\[ \left[ \prod_{u > u, u \in N_v} (1 - \gamma i^*_u) - \prod_{u > u, u \in N_v} (1 - \gamma i_u(t)) \right]. \]
This recurrent process will lead to
\[ \left| \frac{d}{dt} z_v(t) \right| \]
\[ \leq M_1 |z_v(t)| + \left( 1 - \alpha \right) \gamma \left( 1 - i_v(t) \right) \sum_{\omega \in N_v} z_{\omega}(t) \]
\[ \prod_{u > u, u \in N_v} (1 - \gamma i^*_u) \prod_{u < u, u \in N_v} (1 - \gamma i_u(t)) \]
\[ \leq M_1 |z_v(t)| + M_2 \sum_{\omega \in N_v} z_{\omega}(t), \]
where \( M_1 \) and \( M_2 \) are positive constants. According to Lemma 7 when condition (b) holds, the system has an exponential convergence speed, which means
\[ \forall v \in V, \exists \sigma, T_v > 0, \forall t > T_v, |z_v(t)| \leq |i_v(t) - i_v(t)| \leq e^{-\sigma t}. \]
So:
\[ \left| \frac{d}{dt} z_v(t) \right| \leq M_1 |z_v(t)| + M_2 \sum_{\omega \in N_v} |z_{\omega}(t)| \]
\[ \leq M e^{-\sigma t} \leq M e^{-\sigma t}, \]
where \( M \) is a positive constant. Since \( \frac{d}{dt} z_v(t) = \frac{d}{dt} i_v(t) \), the following inequality holds:
\[ \left| \frac{d}{dt} z_v(t) \right| \]
\[ = \left| i_v(t_{k+1}) - i_v(t_k) \right| = \left| i_v(t_{k+1}) - i_v(t_k) \right| \]
\[ \leq \int_{t_k}^{t_{k+1}} \left| \frac{d}{d\tau} z_v(\tau) \right| d\tau = \int_{t_k}^{t_{k+1}} \left| \frac{d}{d\tau} z_v(\tau) \right| d\tau \]
\[ \leq \int_{t_k}^{t_{k+1}} M e^{-\sigma t} d\tau = Me^{-\sigma t_k} \]
In the case \( \varphi(t) = M_0 e^{-\nu t} = M_0 e^{-\nu t} = M_0 e^{-\nu t} \) or \( \nu = \sigma \), the event-based trigger rule in Definition 1 shows that \( v \) will not trigger a state observation event until time \( t = t^v_{k+1} \), which means
\[ \max_{u \in N_v \cup \{v\}} |\varepsilon_u(t^v_{k+1}, t^v_k)| = M_0 e^{-\sigma t^v_{k+1}}. \]
Under condition (c):
\[ M_0 e^{-\sigma (t^v_{k+1} - t^v_k)} e^{-\sigma t^v_k} = \max_{u \in N_v \cup \{v\}} |\varepsilon_u(t^v_{k+1}, t^v_k)| \]
\[ \leq \zeta |\varepsilon_v(t^v_{k+1}, t^v_k)| \leq \zeta Me^{-\sigma t^v_k} (t^v_{k+1} - t^v_k). \]
It shows the existence of a positive number $\eta_0$, which is the root of the transcendental equation $M_0e^{-\sigma\eta_0} = \zeta M\eta_0$ and satisfies $t^u_{k+1} - t^u_k \geq \eta_0$, which essentially means that for every $v \in V$, $\inf\{t^u_{k+1} - t^u_k\} > 0$.

In the case $\varphi(t) = M_0e^{-\sigma t} > M_0e^{-\sigma t}$ or $\nu < \sigma$, with respect to the $\eta_0$ mentioned above, we can easily get $t^u_{k+1} - t^u_k > \eta_0$. This completes the proof of part (i).

In order to prove part (ii), the presented study first shows that under condition (a), $t \to +\infty$ implies $k \to +\infty$ (i.e., there are infinitely many state observation events). Note that $\varphi(t) \to 0$ as $t \to +\infty$. For $\forall t^u_k > 0$, if $i_v(t^u_k) \neq i^*_v$, then there must exist a $t^u_{k+1} > t^u_k$ such that $i_v(t^u_{k+1}) = i^*_v(t^u_k)$, which means the $(k+1)$-th state observation event for node $v$ will occur within a finite time; if there exists some $t^u_k > 0$ such that $i_v(t^u_k) = i^*_v$, node $v$ may not incur the $(k+1)$-th state observation event within a finite time, meaning $t^u_{k+1} = +\infty$. The latter situation can be addressed by using the Sard’s Lemma in [59]. For $v \in V$ and $k = 0, 1, \ldots$, 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 $i_v(t^u_k) = i^*_v$ is true. Since $v \in V$ and $k = 0, 1, \ldots$ are both countable, $\Theta = \bigcup_{v,k} \Theta_{v,k}$ 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 $v \in V$, \[
\frac{d}{dt}\left[i^a_v(t) - i_v(t)\right] = \beta i_v(t) - \left[1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i_u(t))\right] (1 - i_v(t)) - \beta i^a_v(t^u_k) + \left[1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma i^a_u(t^u_k))\right] (1 - i^a_v(t^u_k)) = (\beta + 1)(i_v(t) - i^a_v(t^u_k)) + (1 - \alpha) \left[1 - \beta i_v(t)\right] \prod_{u \in N_v} (1 - \gamma i_u(t)) - (1 - \alpha) \gamma (1 - i_v(t)) \sum_{u \in N_v} \varepsilon_\omega(t, t^u_k) - (1 - \alpha) \gamma \prod_{u \in N_v} (1 - \gamma i^a_u(t^u_k)).\]

Under the event-based trigger rule in Definition 3, the following holds:
\[
\left\|i^a(t) - i(t)\right\|_1 \leq \sum_{v \in V} \xi_v \int_{t^u_k}^{t} \frac{d}{dt}\left|i^a_v(\tau) - i_v(\tau)\right| d\tau = \sum_{v \in V} \xi_v \int_{t^u_k}^{t} \left((\beta + 1)\varepsilon_\sigma(\tau, t^u_k) - (1 - \alpha)\varepsilon_\sigma(\tau, t^u_k)\right) \prod_{u \in N_v} (1 - \gamma i^a_u(t^u_k)).\]

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 $\lim_{t \to +\infty} \left\|i(t) - i^*\right\|_1 = 0$. From $\inf\{t^u_{k+1} - t^u_k\} > 0$ and $t \to +\infty$ implying $k \to +\infty$, it can be found that $t \to +\infty$ is equivalent to $t^u_k \to +\infty$. Therefore:
\[
\lim_{t \to +\infty} \left\|i^a(t) - i^*(t)\right\|_1 \leq \lim_{t \to +\infty} \left\|i^a(t) - i(t)\right\|_1 + \lim_{t \to +\infty} \left\|i(t) - i^*(t)\right\|_1 \leq \lim_{t \to +\infty} C \sum_{v \in V} \xi_v e^{-\sigma t^u_k} + 0 = 0,
\]

where $t \in [t^u_k, t^u_{k+1})$.

Finally, it comes to the problem of Zeno-freeness. From inequality (7), it can be deduced that $t^u_{k+1} - t^u_k \geq \eta_0$, where $\eta_0$ 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:
\[
t^u_k = \sum_{k=1}^{\infty} (t^u_{k+1} - t^u_k) = \sum_{k=0}^{\infty} (t^u_{k+1} - t^u_k) < +\infty
\]
for $k = 1, 2, \ldots$. It effectively shows that system (5) 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 7 to Accommodate Periodic Reference Setting

Theorem 1 requires that the trigger events occur precisely at sequential points in time $t^u_k$ 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 Figure 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 accommodating discrete-time). Let \( t^*_v = 0 \) for \( v \in V \). The adapted trigger rule is defined as

\[
t^*_v = \sup \left\{ \tau \geq t^*_v, \tau \in \mathbb{N} : \max_{u \in N_v \cup \{v\}} |\varepsilon_u(\tau, t^*_v)| \leq \varphi(\tau) \right\}.
\]

**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 \( t^*_v \) 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 all \( v \in V \) and \( k = 0, 1, \ldots, t^*_v - t^*_v \geq \eta_v \) where \( \eta_v \) is a positive number, denoted by

\[
\eta = \inf \left\{ \eta_v : v \in V \right\},
\]

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

The next issue is the periodic reference setting. Without loss of generality, this paper assumes \( t^*_v = l^*_v h \) where \( l^*_v \in \mathbb{N} \). It executes the next state-observation event at time \( t^*_{v+1} = l^*_{v+1} h \) according to the adapted event-based trigger rule in Definition 2.

Note that \( l^*_{v+1} > l^*_v \) and \( l^*_{v+1} \in \mathbb{N} \) because \( h \) is small enough. Regarding the time period \([l^*_v h, l^*_{v+1} h] \), the following can be proven in a similar fashion to the proof in Theorem 1 that

\[
\|i^{[a]}(t) - i^*(t)\|_1 \leq \sum_{v \in V} \int_t^t \frac{d}{dt} \left| j^{[a]}_v(\tau) - i^*(\tau) \right| d\tau
\]

\[
\leq C_1 \sum_{v \in V} \int_t^t \left[ \varepsilon_v(\tau, l^*_v h) + \sum_{\omega \in N_v} |\varepsilon_\omega(\tau, l^*_v h)| \right] d\tau
\]

\[
\leq C_2 \sum_{v \in V} \int_t^t e^{-\sigma \tau} d\tau
\]

\[
\leq C_3 \sum_{v \in V} \varepsilon_v e^{-\sigma l^*_v h},
\]

where \( C_1, C_2 \) and \( C_3 \) are some positive constants and \( t \in [l^*_v h, l^*_{v+1} h] \) 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 \( l^*_v h \to +\infty \). Then,

\[
\lim_{t \to +\infty} \|i^{[a]}(t) - i^*(t)\|_1 \leq \lim_{t \to +\infty} C \sum_{v \in V} \varepsilon_v e^{-\sigma l^*_v h} = 0,
\]

where \( t \in [l^*_v h, l^*_{v+1} h] \).

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),

\[
F^{[a]}(t^*_v) = -\beta^{[a]}(t^*_v) + \left[ 1 - (1 - \alpha) \prod_{u \in N_v} (1 - \gamma^{[a]}(t^*_v)) \right] \left( 1 - i^{[a]}(t^*_v) \right).
\]

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

1. input: \( G = (V, E) \), \( i_v(0) \) for \( v \in V \), \( \varphi, h \)
2. output: \( \{t^*_v\}_{k=0}^{\infty} \) and \( \{i_v(t)\}_{t=0}^{\infty} \) for \( v \in V \)
3. initialize: \( k \leftarrow 0 \), \( t^*_v \leftarrow 0 \)
4. while true do
5. \( t \leftarrow t^*_v \)
6. Event \( \leftarrow 0 \)
7. if \( v \) is observed with \( i_v^{[a]}(t^*_v) \) for \( v \in N_v \) then
8. compute \( F^{[a]}(t^*_v) \) according to Eq. (9)
9. end
10. while Event = 0 do
11. \( i_v(t) \leftarrow i_v^{[a]}(t^*_v) + (t^*_v - t) F^{[a]}(t^*_v) \);
12. if \( \max_{u \in N_v \cup \{v\}} |i_v(t) - i_u^{[a]}(t^*_v)| \geq \varphi(t) \) then
13. \( v \) probes its neighbors \( u \in N_v \) for observing \( i_u^{[a]}(t^*_v) \)
14. \( i_v^{[a]}(t^*_v) \)
15. \( Event \leftarrow 1 \)
16. \( t^*_v \leftarrow t \)
17. \( t^*_v \leftarrow t^*_v + t \)
18. \( i_v^{[a]}(t^*_v) \leftarrow i_v(t) \)
19. end
20. \( t \leftarrow t + h \)
21. \( k \leftarrow k + 1 \)

Algorithm 1 has four inputs: attack-defense graph \( G = (V, E) \); initial values \( i_v(0) \) for \( v \in V \); a trigger function \( \varphi \); 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 \( e^{-\theta t} \) 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/](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.

- Gnutella peer-to-peer network: This is a directed graph with $|V| = 8,717$ nodes, $|E| = 31,525$ links, maximal node in-degree 64 and $\lambda_{A1} = 4.7395$. 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.

- Enron email network: This is an undirected graph with $|V| = 5242$ nodes, $|E| = 28980$ edges, maximal node degree 81 and $\lambda_{A1} = 45.6167$. The other model parameters are set as: $\alpha = 0.5268$, $\beta = 0.7856$ and $\gamma = 0.0212$, which means $i(t)$ 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 $i_v(0) \in [0, 1]$ 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 $\max_{v \in V} \frac{|i_v(t_k + 1) - i_v(t_k)|}{|i_v(t_k)|}$ appears in the early stage of the process with respect to condition (c). 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 $\frac{1}{n}\sum_{v \in V} |i_v(t) - \bar{i}^{[n]}(t)|$ 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.** Observation events at time $i(t)\in [0, 500]$ for nodes $0–30$ in a network, where each blue line represents an observation event.

Figure 3 plots the observation events at $i(t)\in [0, 500]$ 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 $k = 1, 2, \cdots$. 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

$$\chi_v(t) = \begin{cases} 0 & v \text{ is in the secure state at time } t \\ 1 & v \text{ is in the compromised state at time } t. \end{cases} \quad (10)$$

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 $\tilde{\chi_v}(t)$ of probabilities $\hat{\chi}_v(t)$ and an estimation $\tilde{s}_v(t)$ of probabilities $s_v(t)$ from a 0-1 state ergodic process over time as indicated by Eq. (10). For this purpose, the paper adopts the theorem of two-valued processes introduced in [60] Chapter 1, and uses the Lebesgue measure $\mathcal{M}$ to define

$$\mathcal{T}_{\chi_0}(t) = \mathcal{M}(\{\tau \leq t : \chi_v(\tau) = 0\})$$
$$\mathcal{T}_{\chi_1}(t) = \mathcal{M}(\{\tau \leq t : \chi_v(\tau) = 1\}). \quad (11)$$

Theorem 3 below shows how to generate probabilities $\tilde{\chi_v}(t)$ and $\tilde{s}_v(t)$ from a 0-1 state ergodic process over time.

**Theorem 3** ([60]). Let $\{\chi_v(t), t > 0\}$ for $v \in V$ be a 0-1 state ergodic process. Let

$$\tilde{s}_v(t) = \frac{\mathcal{T}_{\chi_0}(t)}{t}$$
$$\tilde{\chi_v}(t) = \frac{\mathcal{T}_{\chi_1}(t)}{t}. \quad (12)$$

Then

$$\lim_{t \to +\infty} [\mathbb{P}(\chi_v(t) = 0) - \tilde{s}_v(t)] = 0$$
$$\lim_{t \to +\infty} [\mathbb{P}(\chi_v(t) = 1) - \tilde{\chi_v}(t)] = 0. \quad (13)$$

Based on Theorem 3, $\tilde{\chi_v}(t)$ can be used to estimate $\hat{\chi}_v(t)$ and $\tilde{s}_v(t)$ to estimate $s_v(t)$ at sufficiently large time $t$. The following Algorithm 2 is designed for this estimation, where a stack data structure $S$ 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 $|S|$ be the number of elements in stack $S$.

Since undirected networks are a special case of directed networks, this study will only perform experiments on the directed Gnutella Network. To maintain a 0-1 process for $\forall v \in V$, the paper samples node $v$ at time $t$ by its compromise probability $\hat{\chi}_v(t)$:

$$\chi_v(t) = H[\hat{\chi}_v(t) - \text{Rand}(0,1)] \quad (12)$$

where $\text{Rand}(0,1)$ means drawing a random real number uniformly from $[0,1]$, and $H$ is the Discrete Heaviside step function:

$$H(x) = \begin{cases} 0 & x < 0 \\ 1 & x \geq 0. \end{cases} \quad (13)$$

Run Algorithm 2 until the state estimation curve converges to the probability-state curve. From the numerical result, it

**Algorithm 2:** Estimating $\hat{\chi}_v(t)$ and $\tilde{s}_v(t)$

1. **input:** $h$, $\{\chi_v(t)\}_{t=0}^{+\infty}$, $\mathcal{N}_v^i(0) = \chi_v(0)$,
   $\mathcal{N}_v^0(0) = 1 - \chi_v(0)$
2. **output:** $\{\tilde{s}_v(t)\}_{t=0}^{+\infty}$, $\{\tilde{\chi_v}(t)\}_{t=0}^{+\infty}$

for $t = 1$ to $+\infty$ do
   if $\chi_v(t) == 0$ then
      $\mathcal{N}_v^0(t) = \mathcal{N}_v^0(t-1) + 1$
      $\mathcal{N}_v^i(t) = 0$
   else if $\chi_v(t) == 0$ then
      $\mathcal{N}_v^0(t) = 0$
      $\mathcal{N}_v^i(t) = \mathcal{N}_v^i(t-1) + 1$
   end
end

for $i = 0$ to $1$ do
   Create Stack $S_i$
   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
         $S_i, \text{push}(\mathcal{N}_v^i(t))$
      else if $t > 0$ and $\mathcal{N}_v^i(t) ! = 0$ and
      $\mathcal{N}_v^i(t-1) ! = 0$ then
         $S_i, \text{pop}()$
         $S_i, \text{push}(\mathcal{N}_v^i(t))$
      end
   if $|S_i| ! = 0$ then
      $\mathcal{T}_{\chi_v}(t) = \frac{1}{|S_i|} \sum_{e \in S_i} e$
   else
      $\mathcal{T}_{\chi_v}(t) = 0$
   end
end

for $t = 0$ to $+\infty$ do
   $\tilde{s}_v(t) = \frac{\mathcal{T}_{\chi_0}(t)}{\mathcal{T}_{\chi_0}(t) + \mathcal{T}_{\chi_1}(t)}$
   $\tilde{\chi_v}(t) = \frac{\mathcal{T}_{\chi_0}(t)}{\mathcal{T}_{\chi_0}(t) + \mathcal{T}_{\chi_1}(t)}$
   return $\{\tilde{s}_v(t)\}_{t=0}^{+\infty}$, $\{\tilde{\chi_v}(t)\}_{t=0}^{+\infty}$
can be seen that the estimation curve indeed converges to the equilibrium of the underlying model as expected. Figure 4 depicts the convergence processes of two arbitrarily-chosen nodes.

![Convergence Processes](image)

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

### 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. Figure 5 illustrates the experimental result, where the red curve corresponds to the sample-state estimation curve \( i_v(t) \) (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 \( \hat{i}_v(t) \), and the blue curve corresponds to the underlying dynamic \( i_v(t) \) (which can not be directly observed).

![Event-based Method](image)

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

The study calculates the mean and standard deviation of \( \frac{1}{n} \sum_{v \in V} |i_v(t) - \hat{i}_v(t)| \), 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 \( m_1 = 7.74 \times 10^{-3} \) and \( sd_1 = 4.96 \times 10^{-3} \) for \( t \in [400, 500] \) prove the effectiveness of the event-based method. The mean and standard deviation of \( \frac{1}{n} \sum_{v \in V} (i_v(t) - \hat{i}_v(t)) \) are also calculated, denoted by \( m_0 \) and \( sd_0 \). The results are \( m_0 = 1.81 \times 10^{-2} \) and \( sd_0 = 1.10 \times 10^{-2} \) 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).

### 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 \( e^{-\theta t} \) is the convergence speed of system (2) and \( \theta < \sigma \). With respect to the trigger function, a smaller \( \theta \) may be chosen to loosen the trigger rule. This paper therefore tests the impact of trigger functions with different values of \( \theta \). Figure 6 plots the means and standard deviations of \( \frac{1}{n} \sum_{v \in V} |i_v(t) - \hat{i}_v(t)| \) for \( t \in [400, 500] \) under different trigger functions.

![Trigger Function Impact](image)

**Fig. 6.** The means and standard deviations with respect to various values of \( \theta \) over the same time window in the event-based trigger function \( \varphi \).

Figure 6 illustrates that with respect to a designated time interval, a larger \( \theta \) 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 \( \theta \) results in extraneous observation events, while a small \( \theta \) 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 \( (\hat{i}_v(t)) \) 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 \( \frac{1}{n} \sum_{v \in V} (i_v(t) - \hat{i}_v(t)) \) 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., \( \hat{i}_v(t) = 0 \), \( \forall v \in V \)). Figure 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).

V. CONCLUSION

This paper has shown how to use the event-based method to estimate the equilibrium of preventive and reactive cyber de-
fense 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 [3]? 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 [47], [44], [41] that do not make the current assumption of dynamics independence?

ACKNOWLEDGMENT

We thank the anonymous reviewers for their comments that guided us in revising the paper. 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. Wenlian Lu was supported by National Natural Sciences Foundation of China under Grant (No. 62072111).

REFERENCES


Fig. 7. Correlation between the false-negative rate in the sample-state observation and the bias of the equilibrium estimation.
Shouhuai Xu is a Full Professor in the Department of Computer Science, University of Texas at San Antonio. 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 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). He received his PhD in Computer Science from Fudan University.