Sequential defense against random and intentional attacks in complex networks

Pin-Yu Chen[1] and Shin-Ming Cheng[2]

[1]*Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, Michigan 48109, USA*
[2]*Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology,*
Taipei 10607, Taiwan

Network robustness against attacks is one of the most fundamental researches in network science as it is closely associated with the reliability and functionality of various networking paradigms. However, despite the study on intrinsic topological vulnerabilities to node removals, little is known on the network robustness when network defense mechanisms are implemented, especially for networked engineering systems equipped with detection capabilities. In this paper, a sequential defense mechanism is first proposed in complex networks for attack inference and vulnerability assessment, where the data fusion center sequentially infers the presence of an attack based on the binary attack status reported from the nodes in the network. The network robustness is evaluated in terms of the ability to identify the attack prior to network disruption under two major attack schemes, i.e., random and intentional attacks. We provide a parametric plug-in model for performance evaluation on the proposed mechanism and validate its effectiveness and reliability via canonical complex network models and real-world large-scale network topology. The results show that the sequential defense mechanism greatly improves the network robustness and mitigates the possibility of network disruption by acquiring limited attack status information from a small subset of nodes in the network.

I. INTRODUCTION

In the past decade, with the advance of computation technology and the accessibility of real-world large-scale network data, the exploration and analysis of large-scale network attributes have received tremendous attention in network science [1] as they disclosed the mysterious masks in nature as well as manmade engineered systems and contrive to answer the fundamental networking problems such as network formulation, dependency, resilience, and evolution. Such networks, consisting of numerous nodes and intricate interconnections embedded with heterogeneous network structures in the graph-theoretic point of view, are renowned as *complex networks* [2–4]. Owing to large-scale network size, extreme volume of empirical network data, and potentially biased network sampling techniques [5], explicit analysis on the network structure turns out to be computationally infeasible and theoretically intractable. Consequently, collective network attributes instead of exact network topology are preferable for complex network analysis, and the developed measurement metrics (e.g., clustering coefficient and network centrality) play an essential role in network science and they have been applied to aid the design of communication systems [6]. Among all the network attributes, the degree distribution of the entire network is one of the most salient features that specifies the link characteristics since the degree distribution is defined as the probability distribution of the number of links of an arbitrarily selected node in the complex network, and it can be specified by a few network parameters.

What is of our particular interest in network science is the study of network resilience [7] (i.e., the extent of network tolerance to node removals) because of its kin relation and assessment to network robustness and connectivity in many networked engineering systems [8–12]. Typical examples include but are not limited to denial-of-service (DoS) attacks and jamming attacks. In particular, the U.S. Department of

Energy (DOE) has identified attack resistance to be one of the seven major properties required for the operation of smart grid [13]. From the bird's-eye view of the entire network, the giant connected component vanishes and the entire network is disintegrated into several small components when the fraction of the removed nodes exceeds certain critical value, which is known as the critical phenomenon of percolation theory in statistic physics [14]. More importantly, this critical phenomenon can be well mapped to the network robustness and connectivity of many practical networked engineering systems, owing to the network resilience protocols that the network retains its operations as long as a majority of nodes remain its functionality (i.e., most of the nodes are still connected). Throughout this paper, the critical phenomenon for network disruption caused by node removals are used to evaluate the performance of the proposed network defense mechanism and we denote the critical value for network disruption as the *percolation-based connectivity*.

Our physical model is built upon the structure of many practical networked engineering systems where a data fusion is responsible for data inference and decision making as illustrated in Fig. 1. Although a vast amount of research has been done in analyzing intrinsic network resilience in complex networks and devising efficient intrusion and anomaly detection techniques in practical networked engineering systems separately, a complete and interdisciplinary network robustness analysis, including both the intrinsic network resilience as well as the embedded attack detection capability, is still poorly understood. In this paper, a sequential defense mechanism is first proposed in complex networks where each node performs individual attack detection and sequentially reports binary attack status (i.e., under attack or not) to the data fusion center as shown in Fig. 1. The data fusion center then sequentially infers the presence of network attacks based on the feedback and makes a final decision when sufficient information has been collected. This mechanism is particularly applicable
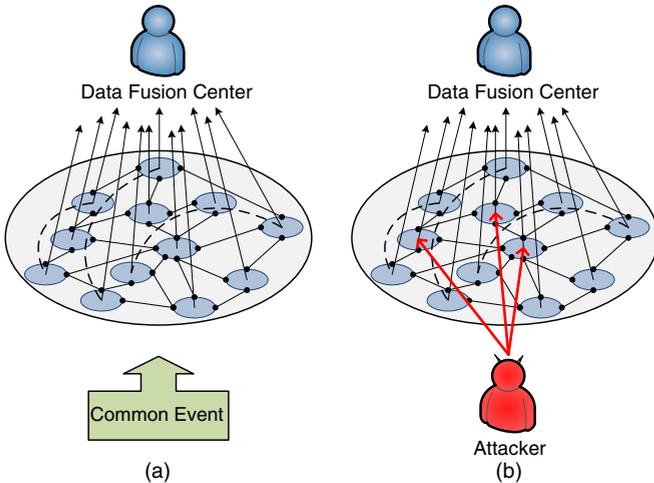
FIG. 1. (Color online) Structure of practical engineering system. A data fusion center is responsible for data inference and decision making based on the feedback data from the network. The solid lines represent localized connections (e.g., physical links in a power grid) and the dashed lines represent delocalized connections (e.g., friends in a social network) in the complex network. (a) Traditional data fusion scheme. Each node feedbacks its observation on a common event (e.g., channel vacancy or temperature) to the data fusion center for hypothesis test. (b) Intelligent targeted attack. Red solid arrows point to the targeted nodes. An intelligent adversary leverages the network topology to target the most vulnerable nodes to disrupt the entire network. As this targeted attack is not a common event to all the nodes, most of the nodes are unaware of the attack and therefore it is more difficult to be detected. Consequently, intelligent targeted attack hinders the attack inference precision and poses severe threats on the network robustness.

to networking paradigms with enormous number of nodes and stringent data transmission resources. It is also worth mentioning that the proposed sequential defense mechanism is quite distinct from the traditional data fusion scheme [15] due to the fact that the network attack may not be a common event to all the nodes in the network as illustrated in Fig. 1. In other words, an intelligent adversary can target at some crucial nodes instead of launching attacks on the entire network to efficiently disrupt the network and reduce the risks of being detected, which therefore hinders the attack inference precision and poses severe threats on the network robustness.

The performance of the proposed sequential defense mechanism is evaluated under random and intentional attacks, as random attack plays an identical role of temporal node disfunction and intentional attack refers to malicious attack caused by an adversary. We provide a parametric plug-in model for performance evaluation on the sequential defense mechanism, and we implement our mechanism in both canonical complex network models and empirical network data to validate its reliability and effectiveness. In addition to analyzing the critical value to sustain percolation-based connectivity via statistic physics approaches [14], we would like to point out that our defense mechanism is a general framework that does not depend on any underlying complex network models but is applicable to any network with arbitrary network structures, provided that the critical value of the

network can be realized at hand. The results show that our defense mechanism greatly enhances the network robustness and provides reliable protection against fatal attacks, even in the complex networks with fragile network structure and weak detection capability, which also offer new insights toward network robustness enhancement and robust network design.

The rest of this paper is organized as follows. The related works are summarized in Sec. II. Preliminaries on the percolation-based connectivity and the canonical complex network models are introduced in Sec. III. The system model and sequential defense mechanism are elucidated in Sec. IV. The critical values under random and intentional attacks are analyzed in Sec. V. The analysis on the sequential defense mechanism is derived in Sec. VI. The performance evaluation of the proposed defense mechanism in canonical complex network models and empirical network data are shown in Sec. VII. Section VIII provides discussions for robust network design. Finally, Sec. IX concludes this paper.

II. RELATED WORKS

The intrinsic topological vulnerabilities regarding different network structures under random and intentional attacks were first introduced in Ref. [7]. Compared with random attack, intentional attack is shown to be quite effective in disintegrating the entire network by removing a relatively small fraction of nodes with the highest degree in the network. As many real-world networks are observed to possess a heavy-tailed degree distribution, such as the webpage links on the world wide web (WWW) [16], router maps on the internet [17], and contacts in email networks [18], the existence of nodes with a relatively large number of links render such networks particularly vulnerable to intentional attack. Moreover, it has been demonstrated in Ref. [19] that intentional attack is the most effective attack strategy to disrupt the entire network when the network topology is known by the adversary, which suggests intentional attack to be an ever-increasing threat on the network robustness of many networked engineering systems.

With the aid of statistic physics and percolation theory [14], the critical values (i.e., the fraction of removed nodes) for a complex network to sustain random and intentional attacks prior to network disruption are investigated in Refs. [20] and [21], respectively, which offer analytically tractable tools for network robustness assessment. Please note that most of the existing research on network robustness against attacks mainly focus on intrinsic topological vulnerabilities while the impacts of implementing network defense mechanisms on the network robustness are still poorly understood. A naive perfect node protection scheme is proposed in Ref. [22] to prevent a subset of nodes in the network from being attacked, which can be shown as a degenerate case of our proposed model. A two-player, zero-sum attack and defense game is introduce in Refs. [10,23,24] to alleviate the damage caused by intentional attack by acquiring attack status from each node for attack inference and defense reaction, and the outcome of the game equilibrium is used to evaluate the network robustness. However, this mechanism is not suitable in networked systems with an enormous number of nodes and stringent data transmission resources as frequent data

transmissions may deteriorate the system performance and inevitably incur excessive energy consumption.

To provide efficient defense for complex networks, a sequential hypothesis test approach [25] is proposed to identify the attack while acquiring as little information from the network as possible. The data fusion center acquires the reports from each node in descending degree order, and therefore it is able to spare the transmissions of the unreported nodes once the process of sequential test terminates, which balances the goals of promptness and accuracy for attack inference.

III. PRELIMINARIES ON COMPLEX NETWORKS

A. Percolation-based connectivity in complex networks

In the realms of network science, the degree (the number of links of a node) distribution plays an essential role in characterizing the collective topological features. With the advance of computation capability and the accessibility of large-scale network data, the long-believed totally random link connections [26] have been overthrown by the extraordinary and ubiquitous degree distributions found in a variety of research areas, such as the power-law distribution in the internet router-level topological maps [17] and the small world phenomenon in social networks [27]. We denote the degree distribution of a complex network by $P(k)$, where $k \in [k_{\min}, k_{\max}]$ and $k_{\min}$ ($k_{\max}$) is the smallest (largest) degree of the complex network. From the bird's eye view, the network attack can be mapped to the node removal in the corresponding network graph (all links attached to the removed node are removed as well), and the network is said to be connected in percolation sense if the giant component (the connected component that includes a majority of nodes) still exists after node removal, which we refer to as the percolation-based connectivity. The physical interpretation of the percolation-based connectivity is that owing to the network resilience protocols [9], the network can continue its main operations under temporal node disfunction as long as most of the nodes are still connected.

According to the seminal work in Ref. [28], given the degree distribution $P(k)$ of an arbitrary network, a giant component containing the majority of the nodes exists in the network if $P(k)$ satisfies the criterion $\sum_k k(k-2)P(k) > 0$, which is equivalent to the condition

$$\tau \triangleq \frac{\mathbb{E}[\mathbf{K}^2]}{\mathbb{E}[\mathbf{K}]} > 2, \tag{1}$$

where $\mathbf{K} \in [k_{\min}, k_{\max}]$ is the random variable representing the degree of a randomly selected node. With the aid of percolation theory, the critical phenomenon of network disruption occurs if more than q_c fraction of nodes are removed from the network, where the critical value q_c can be estimated when the remaining degree distribution satisfies the criterion $\tau_c = 2$. In other words, the complex network transitions from the connected phase to the disconnected phase in percolation sense once more than q_c fraction of nodes are removed. Throughout this paper, the critical value q_c is used to evaluate the network robustness under different network structures and attack schemes. Please note that in the case of small-scale networks, the critical value can be obtained by performing exhaustive node removal

experiments (i.e., searching over all possible node removal strategies) instead of using statistic physics approaches (i.e., estimating q_c by degree distribution).

B. Canonical complex network models

In this paragraph, we introduce three canonical complex network models that serve as the platforms for performance evaluation of the proposed defense mechanism.

(1) ER network. In an ER network [26], a link between any arbitrarily selected node pair is present with probability p_{ER}. If the network size is large enough, the degree distribution approaches to the Poisson distribution $P(k) = e^{-\widehat{k}}\frac{\widehat{k}^k}{k!}$, where $\widehat{k} = N \cdot p_{\mathrm{ER}}$ is the mean degree of the network and N is the number of nodes in the network.

(2) Power-law network. A power-law network possesses a skewed degree distribution $P(k) \sim k^{-\alpha}$, where $\alpha > 0$ is the skewness parameter. The heavy tail of the degree distribution suggests the existence of the hub nodes that few nodes have a relatively high degree compared with most of the nodes in the network, which well explains the connectivity of the WWW [16] or the internet router maps [17].

(3) Exponential network. An exponential network has its degree distribution $P(k) \sim \frac{1}{\beta}e^{-\frac{k}{\beta}}$, where $\beta > 0$ is the mean degree of the network in the large scale network limit. It is demonstrated in Ref. [29] that the degree distribution of the power grid can be characterized by the exponential distribution, both in the national power grid scale and the European power grid scale.

IV. SYSTEM MODEL

A. Network model and sequential defense mechanism

Without loss of generality, we consider the complex network model consisting of N nodes characterized by its degree distribution $P(k)$ and the corresponding critical value q_c to sustain network connectivity against attacks. Each node is equipped with certain detection capability, for instance, intrusion detection techniques [30] or malicious activity filtering [31] for attack inference. The N nodes are sorted in descending degree order, i.e., $k_1 \geqslant k_2, \geqslant \cdots \geqslant k_N$. Let H_1 denote the hypothesis that the attack occurs in the complex network (either on one node or several nodes simultaneously), and H_0 denote the alternative hypothesis of a null attack (i.e., there is no attack in the network). Based on the nodal detection, every node sequentially reports its binary hypothesis testing decision to the data fusion center in descending degree order since intuitively the removal of nodes with higher degree results in more severe damage to the network robustness.

It is worth mentioning that although enabling local information exchange or cooperative detection among nodes may enhance the attack inference precision, these approaches inevitably increase the computation and data transmission overheads. Throughout this paper, we will concentrate on the degree-based sequential defense mechanism owing to its feasibility and simplicity. In practice, these local decisions can be transmitted in the header of data packets, or a node is regarded as being attacked if it fails to reply to the periodic beaconing from the data fusion center. If the attack is confirmed

by the data fusion center, network defense schemes, such as node quarantine or system renewal, will be launched to alleviate the damage, otherwise it keeps surveillance on the collected information.

The advantages of reporting binary attack status for sequential defense in complex networks reside in the feasibility of data transmission and computation complexity in the large-scale networked systems. The enormous network size (e.g., internet routers or wireless sensors) render simultaneous data transmissions infeasible, especially for wireless networks with scarce radio resources. Moreover, owing to the large network size and limited computational power, analyzing the collected information from all nodes incurs tremendous computation overheads and it may fail to provide timely defense. Consequently, sequential hypothesis test with minimum (one-bit) feedback information is an essential must for attack inference in complex networks because of its least additional communication overheads and timely defense. In other words, the sequential hypothesis test terminates once sufficient information is collected and a final decision is made by the data fusion center so that the system can spare the transmissions of the unreported nodes.

Let x_i denote the attack status reported by the ith node. $x_i = 1$ when the attack on the ith node is detected and $x_i = 0$ for null attack on the ith node. We assume that the detection capability of each node is identical with probability of detecting an attack P_D and probability of false alarm P_F. Each node performs an independent hypothesis test such that the joint probability distribution of the first $m \leqslant N$ reports when H_j is true can be represented as $P(x_1, \ldots, x_m | H_j) = \prod_{i=1}^{m} P(x_i | H_j)$. In general, we assume $P_D \geqslant P_F$, otherwise the sequential hypothesis test should be altered for attack inference.

B. Sequential probability ratio test (SPRT)

Using sequential analysis [25], let $P_{jm} = \prod_{i=1}^{m} P(x_i | H_j)$ denote the probability of obtaining a report sample $(x_1, \ldots, x_m)$, the sequential hypothesis test is carried out by performing the probability ratio test with two specified parameters A and B. After receiving the report from the mth node, if $\frac{P_{1m}}{P_{0m}} \geqslant A (\frac{P_{1m}}{P_{0m}} \leqslant B)$, then the data fusion center declares the presence of a (null) attack, otherwise it keeps surveillance on the next report for attack inference. Moreover, for purposes of practical computation, it is much more convenient to perform sequential probability ratio test by computing the logarithm of the ratio $\frac{P_{1m}}{P_{0m}}$ instead of the ratio itself as the product of individual tests can be decomposed into sum of the log likelihood ratios.

Let $z_i = \log \frac{P(x_i | H_1)}{P(x_i | H_0)}$ denote the log likelihood ratio of the ith report and $\Lambda_m = \sum_{i=1}^{m} z_i = \sum_{i=1}^{m} \log \frac{P(x_i | H_1)}{P(x_i | H_0)}$ denote the cumulative value of the first m reports for hypothesis testing. Consequently, the sequential hypothesis test is terminated with hypothesis $H_1 (H_0)$ if $\Lambda_m \geqslant \log A (\Lambda_m \leqslant \log B)$, otherwise the process is continued by taking an additional report. These two parameters A and B can be determined by setting $A = \frac{1-\theta}{\delta}$ and $B = \frac{\theta}{1-\delta}$, where $\delta = P(\text{say } H_1 \text{ when } H_0 \text{ is true})$ and $\theta = P(\text{say } H_0 \text{ when } H_1 \text{ is true})$ are the required false alarm and miss detection probabilities at the system level.

V. CRITICAL VALUES UNDER RANDOM AND INTENTIONAL ATTACKS

Incorporating the topological vulnerabilities of the complex network, the critical value q_c to sustain percolation-based connectivity under random and intentional attacks are analyzed with respect to distinct canonical complex network models. For comprehensive analysis and clear reading, only the results are displayed in this section and the mathematical derivations are placed in the appendices.

A. Random attack

Random attack on the q fraction of nodes in the network plays an identical role of random node removal. Given the original network degree $\mathbf{K_0}$ of a randomly selected node, the critical value for random attack becomes

$$q_c^{\text{ran}} = 1 - \frac{1}{\tau_0 - 1}, \tag{2}$$

where $\tau_0 \triangleq \frac{\mathbb{E}[\mathbf{K_0}^2]}{\mathbb{E}[\mathbf{K_0}]}$ is calculated from the original degree distribution. For ER network, $q_c^{\text{ran,ER}} = 1 - \frac{1}{k}$. For power-law network, $q_c^{\text{ran,POW}} = 1 - (\frac{2-\alpha}{3-\alpha} \frac{k_1^{3-\alpha} - k_N^{3-\alpha}}{k_1^{2-\alpha} - k_N^{2-\alpha}} - 1)^{-1}$. For exponential network, $q_c^{\text{ran,EXP}} = 1 - (\frac{k_N^2 + 2k_N\beta + 2\beta^2}{k_N + \beta} - 1)^{-1}$. Detailed derivations can be found in Appendix A.

B. Intentional attack

As demonstrated in Ref. [21], removing q fraction of nodes with the highest degree in the network is equivalent to randomly removing $\widetilde{q}$ fraction of nodes in the remaining network with new cutoff degree $\widetilde{k}_{\max} < k_{\max}$. With the continuous degree approximation and the relation $\sum_{k_{\max}}^{\infty} P(k) = \int_{k_{\max}}^{\infty} P(k) dk = \frac{1}{N}$, the new cutoff degree $\widetilde{k}_{\max}$ can be evaluated from

$$\int_{k=\widetilde{k}_{\max}}^{k_{\max}} P(k) dk = \int_{k=\widetilde{k}_{\max}}^{\infty} P(k) dk - \frac{1}{N} = q. \tag{3}$$

Moreover, $\widetilde{q}$ can be interpreted as the link deletion probability of a randomly selected link leading to a deleted node, which equals the ratio of the number of links belonging to the deleted nodes to the number of links [21,32], i.e., $\widetilde{q} = \sum_{k=\widetilde{k}_{\max}}^{k_{\max}} \frac{kP(k)}{\mathbb{E}[\mathbf{K_0}]}$. By specifying the relations between link deletion probability and targeted node removal in Eq. (3), the critical value q_c under intentional attack can be obtained by evaluating the critical link deletion probability $\widetilde{q}_c$ with the ubiquitous criterion for percolation-based connectivity in Eq. (2).

For ER network, $q_c^{\text{int,ER}} = \frac{1}{N} - e^{-\widehat{k}} \frac{\widehat{k}^{\widetilde{k}_{\max} - 1}}{(\widetilde{k}_{\max} - 1)!} + 1 - \frac{1}{k}$. For power-law network, $q_c^{\text{int,POW}} = (\frac{\widetilde{k}_{\max}}{k_N})^{1-\alpha}$. For exponential network, the critical value can be obtained by solving

$$\left[1 - \ln \left(q_c^{\text{int,EXP}} + \frac{1}{N} \right) \right] \left(q_c^{\text{int,EXP}} + \frac{1}{N} \right)$$

$$+ \frac{k_N + \beta}{k_N^2 + 2k_N\beta + 2\beta^2 - k_N - \beta} - 1 = 0. \tag{4}$$

Detailed derivations can be found in Appendix B.

C. Unified notations for attack schemes and SPRT

Since each node sequentially reports its one-bit detection result to the data fusion center for attack inference, let a_i denote the probability of attacking ith node, we introduce the unified notations for the aforementioned attack schemes as

$$P(x_i|H_j) = \begin{cases} \mathscr{B}(a_i P_D), & \text{if} \quad j = 1, \\ \mathscr{B}(P_F), & \text{if} \quad j = 0, \end{cases} \quad (5)$$

where $\mathscr{B}(p)$ is the Bernoulli trial with probability of success ($x_i = 1$) equals p. Incorporating the attack schemes, we have

$$a_i^{\text{ran}} = q^{\text{ran}}, \forall i; \quad (6)$$

$$a_i^{\text{int}} = \mathbf{1}_{i \leqslant \lceil Nq^{\text{int}} \rceil} + \frac{P_F}{P_D} \mathbf{1}_{i > \lceil Nq^{\text{int}} \rceil}$$

$$= \left(1 - \frac{P_F}{P_D}\right) \mathbf{1}_{i \leqslant \lceil Nq^{\text{int}} \rceil} + \frac{P_F}{P_D}, \quad (7)$$

where $\mathbf{1}_E$ denotes the indicator function of the event E and $\lceil x \rceil$ is the smallest integer that exceeds x.

VI. PERFORMANCE ANALYSIS OF SEQUENTIAL DEFENSE IN COMPLEX NETWORKS

Given the specified system parameters (δ, θ), we are interested in the effectiveness and the performance of the proposed sequential defense mechanism against random and intentional attacks in complex networks. Furthermore, knowing the critical value q_c, the data fusion center is required to infer the presence of the attack prior to the network disruption. In other words, a final decision has to be made according to the first $M_c = \lceil Nq_c \rceil$ reports for practical implementation purposes, which we refer to as the worst case scenario. Upon the reception of the M_cth report, if a final decision has not been reached, the data fusion center declares the presence of attack when $0 < \Lambda_{M_c} < \log A$ and declares a null attack when $\log B < \Lambda_{M_c} \leqslant 0$.

Let M_j denote the expected number of reports required for hypothesis testing when H_j is true. The proposed sequential defense mechanism is regarded as effective against attacks in the complex network if $M_1 \leqslant M_c$, i.e., the number of reports required for attack inference is less than the threshold of network disruption, otherwise the defense is in vain since it fails to provide timely defense reaction. We derive the closed-form expressions of M_1 for random and intentional attacks, and we prove that for intentional attack, taking additional reports from $m > M_c$ nodes does not improve the performance of the sequential defense mechanism.

A. Random attack

For random attack, with Eq. (5) we have

$$P_{1m} = \prod_{i=1}^{m} P(x_i|H_1)$$

$$= (q^{\text{ran}} P_D)^{d_m} (1 - q^{\text{ran}} P_D)^{m-d_m}, \quad (8)$$

$$P_{0m} = \prod_{i=1}^{m} P(x_i|H_0)$$

$$= (P_F)^{d_m} (1 - P_F)^{m-d_m}, \quad (9)$$

where d_m is the number of ones in the first m reports. Simple calculation on Λ_m yields

$$\Lambda_m = d_m \log \frac{q^{\text{ran}} P_D}{P_F} + (m - d_m) \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}. \quad (10)$$

Following the process of SPRT in Sec. IV B, the sequential defense criterion for random attack becomes

$$\begin{cases} \text{say } H_1, & \text{if } d_m \geqslant \dfrac{\log A}{\log \frac{q^{\text{ran}} P_D}{P_F} - \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}} \\ \qquad\qquad + m \dfrac{\log \frac{1 - P_F}{1 - q^{\text{ran}} P_D}}{\log \frac{q^{\text{ran}} P_D}{P_F} - \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}}, \\ \text{say } H_0, & \text{if } d_m \leqslant \dfrac{\log B}{\log \frac{q^{\text{ran}} P_D}{P_F} - \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}} \\ \qquad\qquad + m \dfrac{\log \frac{1 - P_F}{1 - q^{\text{ran}} P_D}}{\log \frac{q^{\text{ran}} P_D}{P_F} - \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}}, \\ \text{keep surveillance}, \text{otherwise}. \end{cases}$$

The expected number of reports to identify random attack when H_1 is true is

$$M_1^{\text{ran}} = \frac{\theta \log B + (1 - \theta) \log A}{\mathbb{E}[z_i|H_1]}$$

$$= \frac{\theta \log \frac{\theta}{1-\delta} + (1 - \theta) \log \frac{1-\theta}{\delta}}{q^{\text{ran}} P_D \log \frac{q^{\text{ran}} P_D}{P_F} + (1 - q^{\text{ran}} P_D) \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}}. \quad (11)$$

For the worst case scenario, if m is large enough, from central limit theorem we obtain the lower bounds of the probability that the SPRT will terminate by declaring attack or null attack with $m \leqslant M_c$ reports as [25]

$$P(\text{declare attack}) = P(\Lambda_m \geqslant \log A) \geqslant 1 - \Phi[y_1(M_c)], \quad (12)$$

$$P(\text{declare null attack}) = P(\Lambda_m \leqslant \log B) \geqslant \Phi[y_2(M_c)], \quad (13)$$

where $\Phi(x)$ is the cumulative density function (CDF) of a standard normal distribution, and

$$y_1(M_c) = \frac{\log A - M_c \mathbb{E}[z_i|H_1]}{\sqrt{M_c} \sigma(z_i|H_1)}, \quad (14)$$

$$y_2(M_c) = \frac{\log B - M_c \mathbb{E}[z_i|H_0]}{\sqrt{M_c} \sigma(z_i|H_0)}, \quad (15)$$

$$\mathbb{E}[z_i|H_0] = P_F \log \frac{q^{\text{ran}} P_D}{P_F} + (1 - P_F) \log \frac{1 - q^{\text{ran}} P_D}{1 - P_F}, \quad (16)$$

$$\sigma(z_i|H_1) = \sqrt{q^{\text{ran}} P_D(1 - q^{\text{ran}} P_D)} \log \frac{q^{\text{ran}} P_D(1 - P_F)}{P_F(1 - q^{\text{ran}} P_D)}, \quad (17)$$

$$\sigma(z_i|H_0) = \sqrt{P_F(1 - P_F)} \log \frac{q^{\text{ran}} P_D(1 - P_F)}{P_F(1 - q^{\text{ran}} P_D)}, \quad (18)$$

where $\sigma(z_i|H_1)$ and $\sigma(z_i|H_0)$ are the standard deviation of z_i under H_1 and H_0, respectively. Moreover, when a final decision

needs to be made upon the reception of M_cth report, the system level false alarm and miss detection probabilities (δ, θ) when taking M_c reports are bounded by [25]

$$\delta(M_c) \leqslant \delta + \Phi(y_3(M_c)) - \Phi[y_4(M_c)], \quad (19)$$

$$\theta(M_c) \leqslant \theta + \Phi(y_5(M_c)) - \Phi[y_6(M_c)], \quad (20)$$

where

$$y_3(M_c) = \frac{\log A - M_c \mathbb{E}[z_i | H_0]}{\sqrt{M_c} \sigma(z_i | H_0)}, \quad (21)$$

$$y_4(M_c) = -\sqrt{M_c} \frac{\mathbb{E}[z_i | H_0]}{\sigma(z_i | H_0)}, \quad (22)$$

$$y_5(M_c) = -\sqrt{M_c} \frac{\mathbb{E}[z_i | H_1]}{\sigma(z_i | H_1)}, \quad (23)$$

$$y_6(M_c) = \frac{\log B - M_c \mathbb{E}[z_i | H_1]}{\sqrt{M_c} \sigma(z_i | H_1)}. \quad (24)$$

The aforementioned equations are well-known results from Ref. [25] applied by the specified parameters q^{ran}, P_F, P_D, and M_c. Interested readers are referred to Ref. [25] for more details.

B. Intentional attack

Let d_m denote the number of nodes reporting attack for the first $M = \lceil Nq^{\mathrm{int}} \rceil$ reports and $d_{m'}$ denote the number of nodes reporting attack starting from the m'th node ($m' > M$). With Eq. (6), we obtain

$$
\begin{aligned}
P_{1m} &= P_D^{d_m} [(1 - P_D)^{m - d_m} \mathbf{1}_{m \leqslant M} + (1 - P_D)^{M - d_m} \mathbf{1}_{m > M}] \\
&\quad \times [\mathbf{1}_{m \leqslant M} + P_F^{d_{m'}} (1 - P_F)^{m - M - d_{m'}} \mathbf{1}_{m > M}] \\
&= P_D^{d_m} [(1 - P_D)^{m - d_m} \mathbf{1}_{m \leqslant M} + (1 - P_D)^{M - d_m} \\
&\quad \times P_F^{d_{m'}} (1 - P_F)^{m - M - d_{m'}} \mathbf{1}_{m > M}], \quad (25)
\end{aligned}
$$

$$
\begin{aligned}
P_{0m} &= P_F^{d_m} [(1 - P_F)^{m - d_m} \mathbf{1}_{m \leqslant M} + (1 - P_F)^{M - d_m} \\
&\quad \times P_F^{d_{m'}} (1 - P_F)^{m - M - d_{m'}} \mathbf{1}_{m > M}]. \quad (26)
\end{aligned}
$$

The cumulative log likelihood ratio becomes

$$
\begin{aligned}
\Lambda_m &= d_m \log \frac{P_D}{P_F} + \left[(m - d_m) \log \frac{1 - P_D}{1 - P_F} \right] \mathbf{1}_{m \leqslant M} \\
&\quad + \left[(M - d_m) \log \frac{1 - P_D}{1 - P_F} + d_{m'} \log \frac{P_F}{P_F} \right. \\
&\quad \left. + (m - M - d_{m'}) \log \frac{1 - P_F}{1 - P_F} \right] \mathbf{1}_{m > M} \\
&= d_m \log \frac{P_D}{P_F} + \left[(m - d_m) \log \frac{1 - P_D}{1 - P_F} \right] \mathbf{1}_{m \leqslant M} \\
&\quad + (M - d_m) \left[\log \frac{1 - P_D}{1 - P_F} \right] \mathbf{1}_{m > M} \\
&= d_m \left(\log \frac{P_D}{P_F} - \log \frac{1 - P_D}{1 - P_F} \right) \\
&\quad + (m \mathbf{1}_{m \leqslant M} + M \mathbf{1}_{m > M}) \log \frac{1 - P_D}{1 - P_F}, \quad (27)
\end{aligned}
$$

which suggests that taking additional reports starting from the m'th node does not help to improve the performance of the sequential defense mechanism as intuitively intentional attack targets only on the first M nodes. The sequential defense criterion for intentional attack is

$$
\begin{cases}
\text{say } H_1, & \text{if } d_m \geqslant \dfrac{\log A}{\log \frac{P_D}{P_F} - \log \frac{1 - P_D}{1 - P_F}} \\
& \quad + (m \mathbf{1}_{m \leqslant M} + M \mathbf{1}_{m > M}) \dfrac{\log \frac{1 - P_F}{1 - P_D}}{\log \frac{P_D}{P_F} - \log \frac{1 - P_D}{1 - P_F}}, \\
\text{say } H_0, & \text{if } d_m \leqslant \dfrac{\log B}{\log \frac{P_D}{P_F} - \log \frac{1 - P_D}{1 - P_F}} \\
& \quad + (m \mathbf{1}_{m \leqslant M} + M \mathbf{1}_{m > M}) \dfrac{\log \frac{1 - P_F}{1 - P_D}}{\log \frac{P_D}{P_F} - \log \frac{1 - P_D}{1 - P_F}}, \\
\text{keep surveillance,} & \text{otherwise.}
\end{cases}
$$

The expected number of reports required to identify intentional attack when H_1 is true is

$$M_1^{\mathrm{int}} = \frac{\theta \log \frac{\theta}{1 - \delta} + (1 - \theta) \log \frac{1 - \theta}{\delta}}{P_D \log \frac{P_D}{P_F} + (1 - P_D) \log \frac{1 - P_D}{1 - P_F}}. \quad (28)$$

Consequently, the sequential defense mechanism loses its appeals if $M_1 > M_c$ since the reports received are insufficient for attack inference before the adversary disrupts the entire network as proved in Eq. (27). Moreover, it is easy to show that the performance of worst case scenario ($M = M_c$) for intentional attack is identical to that of random attack by substituting $M_c = \lceil Nq_c^{\mathrm{int}} \rceil$ and a_i^{int} into Eqs. (12), (13), (19), and (20).

VII. PERFORMANCE EVALUATION

In this section, the proposed sequential defense mechanism is employed on canonical complex network models as well as empirical network data to evaluate the system performance and offer new insights on robust network design. The system parameters are set to be $N = 10\,000$, $k_1 = 1\,000$, $k_N = 1$, $\delta = 0.01$, and $\theta = 0.001$ without additional specifications.

A. Critical values of canonical complex network models

For fair comparisons between different canonical complex network models, we set the original mean degree to be identical such that $\widehat{k} = c_1 \frac{k_1^{2-\alpha} - k_N^{2-\alpha}}{2 - \alpha} = k_N + \beta$ and accordingly extract the network parameters $\widehat{k}$, α, and β for ER, power-law, and exponential networks. As shown in Fig. 2, the critical value q_c approaches to 0 as the mean degree decreases to 1 for all canonical complex network models since intuitively a network is prone to disruption if every node has only one link in average. On the other hand, the critical value increases with the mean degree as every node is able to connect to more nodes in the network in order to strengthen the network connectivity. Compared with random attack, intentional attack is shown to be more effective in disintegrating a network by sabotaging a small fraction of nodes with the highest degree. Moreover, despite the fact that the power-law network is resilient to random attack, the inherently skewed degree distribution render it quite vulnerable to intentional attack due to the existence of hub nodes with relatively high degree, which reveal the bottleneck of network robustness against intelligent attacks.
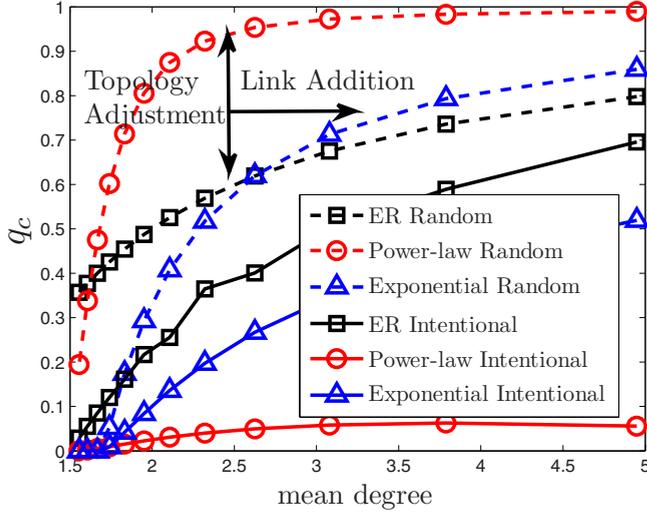
FIG. 2. (Color online) Vulnerabilities of different canonical complex network models under random and intentional attacks. Intentional attack is much more effective in disintegrating a complex network compared with random attack. Although power-law networks are resilient to random attack, they are very vulnerable to intentional attack due to the existence of hub nodes with relatively high degree.

B. Performance of sequential defense mechanism

By employing the proposed sequential defense mechanism in the complex networks, we select the number of reports required to identify an attack (M_1) as the performance measure for timely and efficient defense. As shown in Fig. 3, M_1^{ran} is shown to be a decreasing function of P_D because of better precision in attack inference, and M_1^{ran} increases with P_F in order to distinguish attack and null attack. In addition, since M_1^{ran} is also a decreasing function of q^{ran}, the optimal attack strategy for an intelligent adversary to disrupt the complex network
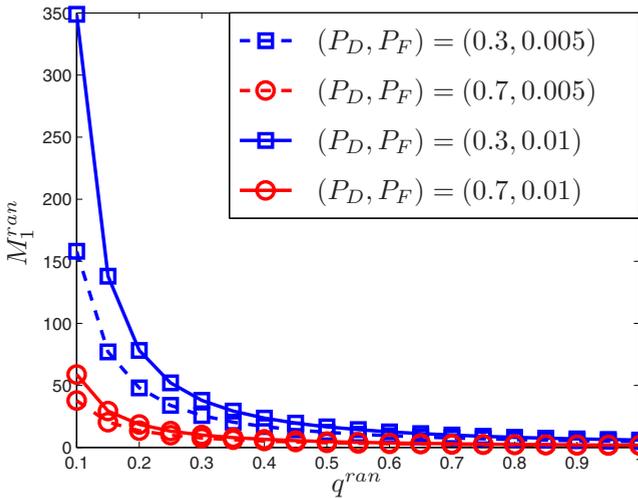
FIG. 3. (Color online) Number of reports required for attack detection (M_1^{ran}) with respect to q^{ran} under random attack. M_1^{ran} is shown to be a decreasing function of P_D due to better precision in attack inference. M_1^{ran} increases with P_F to distinguish between attack and null attack.
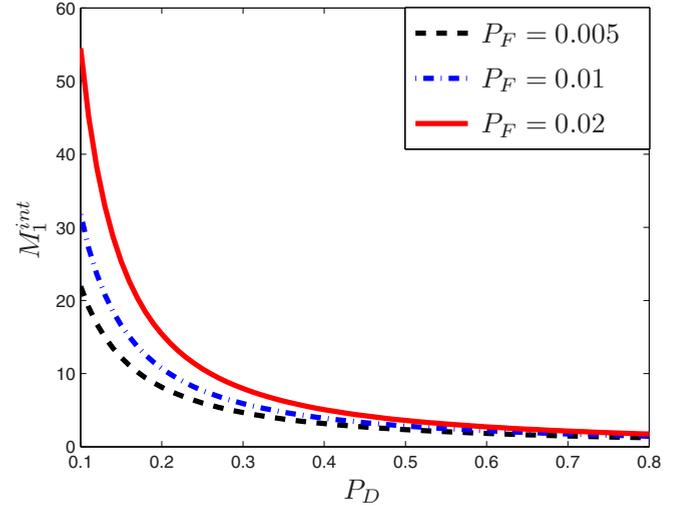
FIG. 4. (Color online) Number of reports required for attack detection (M_1^{int}) with respect to P_D under intentional attack. Compared with random attack, the proposed sequential defense mechanism requires only a few number of reports to target intentional attack, even in the low detection probability regime.

would be choosing $q^{\mathrm{ran}} = q_c^{\mathrm{ran}}$ in order to disrupt the network while minimizing the risks of being detected. The performance of sequential defense mechanism against intentional attack is shown in Fig. 4. Similar to random attack, M_1^{int} increases with P_F to validate the presence of attack. Compared with random attack, the proposed sequential defense mechanism requires only a few reports to target intentional attack, even in the low detection probability regime.

To gain clear insights on the performance of the proposed sequential defense mechanism, we plot M_1^{ran} and its contours with respect to the network parameters and P_D for ER, power-law, and exponential networks in Figs. 5, 6, and 7, respectively. The network parameters are associated with the critical values under random attack as discussed in Sec. V. For ER and exponential networks, M_1^{ran} increases with the decrease
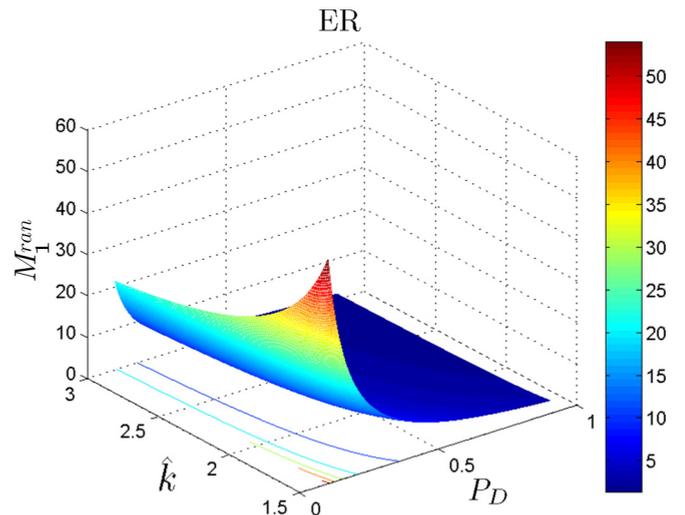
FIG. 5. (Color online) Performance of sequential defense against random attack in ER networks with $P_F = 0.001$.
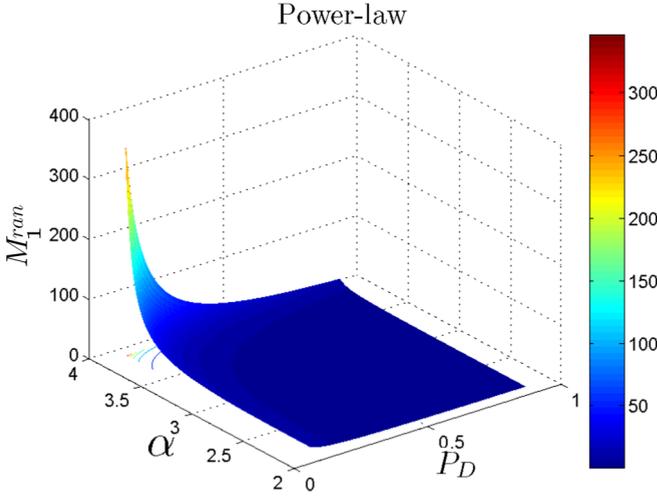
FIG. 6. (Color online) Performance of sequential defense against random attack in power-law networks with $P_F = 0.001$.
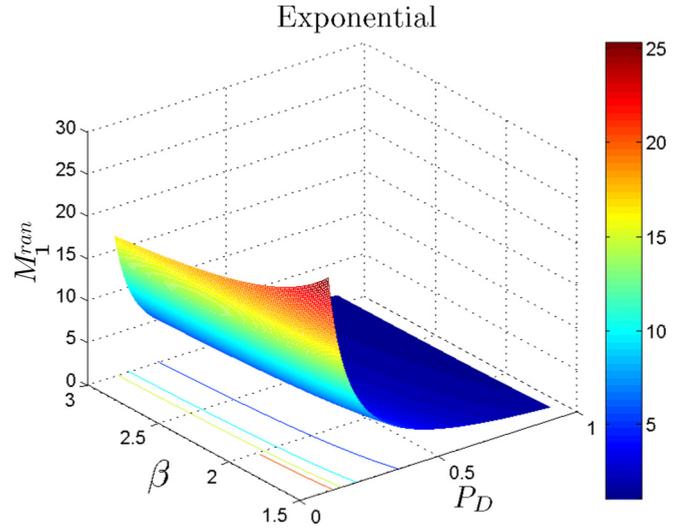
FIG. 7. (Color online) Performance of sequential defense against random attack in exponential networks with $P_F = 0.001$.

of $\widehat{k}(\beta)$ and P_D as the mean degree is proportional to $\widehat{k}(\beta)$ and low P_D hinders the process of SPRT. For power-law networks, more skewed degree distribution (larger α) incurs larger M_1^{ran} since the network is prone to disruption as α increases [20].

C. Reliability of sequential defense mechanism

To validate the reliability of the proposed sequential defense mechanism, the performance of worst-case scenario is investigated with respect to the critical values to sustain network connectivity. In view of practical implementations, an attack decision has to be made upon the reception of $M_c = \lceil Nq_c \rceil$ reports. The probability of acceptance (declaring attack) and the probability of rejection (declaring null attack) are displayed in Fig. 8. It is observed that the proposed sequential defense mechanism achieves high accuracy as the probability of acceptance (probability of rejection) approaches to 1 (0) at extremely small critical values, and higher P_D enhances the accuracy for attack inference, which validate that the proposed sequential defense mechanism is able to identify the attack with high precision. More importantly, given a critical value of a complex network, the probability of acceptance can be interpreted as the precision of identifying an attack prior to the network disruption, and the probability of rejection can be interpreted as the probability for an adversary to disrupt a complex network. The system level parameters $[\delta(q_c), \theta(q_c)]$ of the worst-case scenario are demonstrated in Figs. 9 and 10, respectively. These parameters converge to the desired system level parameters (δ, θ) at extremely small critical values, suggesting that the proposed sequential defense mechanism offers reliable and effective approaches against random and intentional attacks in complex networks.

D. Empirical network data

As a demonstration, the proposed sequential defense mechanism are implemented in real-world large-scale networks with network parameters extracted from empirical network data collected in Refs. [7,29]. The WWW contains 325 729 nodes (webpages) and 1 798 353 links with $\mathbb{E}[\mathbf{K}_0] = 4.6$.

The Internet router-level map contains 6 209 nodes (routers) and 12 200 links with $\mathbb{E}[\mathbf{K}_0] = 3.4$. The EU power grid contains 2 783 nodes (power stations) and 3 762 links with $\mathbb{E}[\mathbf{K}_0] = 3.4$. The WWW and the internet are power-law networks with network parameters $\alpha = 2.1$ and $\alpha = 2.5$, respectively. The EU power grid is an exponential network with network parameter $\beta = 1.63$. As shown in Fig. 11, the number of reports required to identify random attack (M_1^{ran}) is lower than the threshold M_c, even in the case of weak detection capability (low P_D). On the other hand, M_1^{ran} increases with P_F as the data fusion center requires more reports to distinguish between attack and null attack when the false alarm probability increases. Figure 12 displays the performance of the sequential defense mechanism with respect to P_D and P_F under intentional attack. A surge increase of
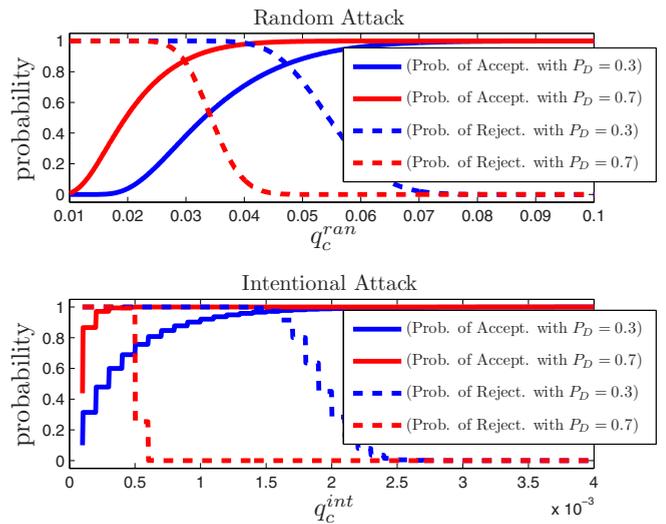
FIG. 8. (Color online) Probability of acceptance and rejection under worst-case scenario with $P_F = 0.001$. The probability of acceptance can be interpreted as the precision for attack inference, and the probability of rejection can be interpreted as the probability for an adversary to disrupt a network.
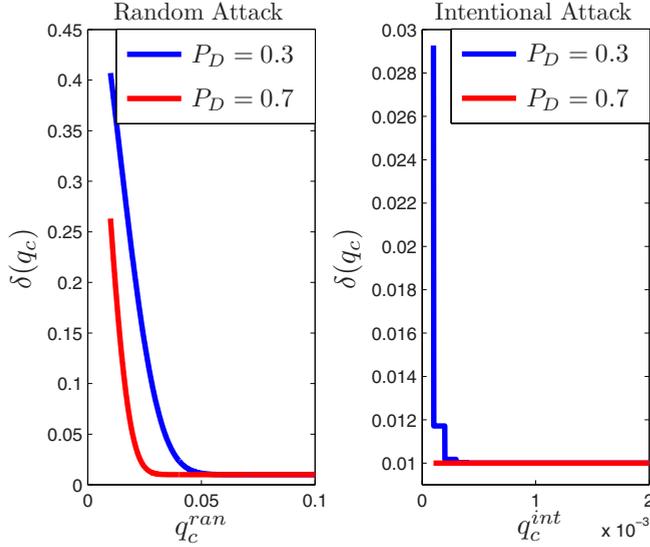
FIG. 9. (Color online) System level false alarm probability under worst case scenario with $P_F = 0.001$ and $\delta = 0.01$.

M_1^{int} is observed with the decrease of P_D and the increase of P_F, suggesting that the defense configurations have to be adjusted according to network characteristics in order to guarantee robust and reliable operations of the entire system, especially for the networks which are particularly vulnerable to intentional attack.

E. U.S. power grid

We implement the proposed sequential defense mechanism on the U.S. power grid topology collected in Ref. [27]. In addition to degree and random attacks, we also consider betweenness attack, where betweenness of a node is defined as the fraction of all shortest paths passing through the node among all shortest paths between each node pair in the
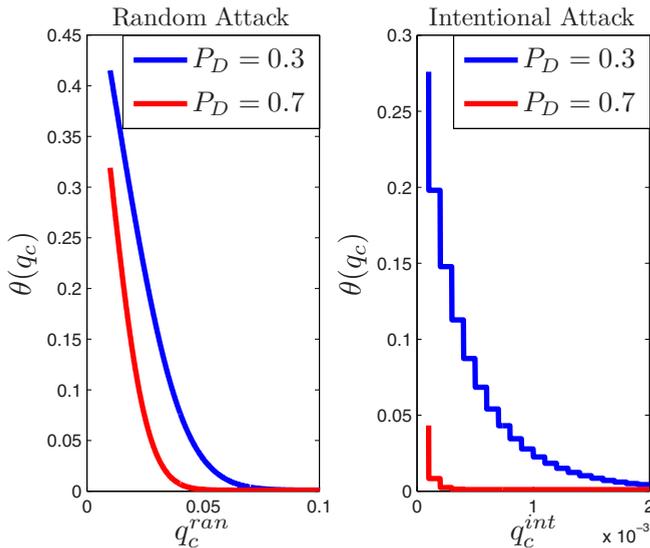
FIG. 10. (Color online) System level miss detection probability under worst-case scenario with $P_F = 0.001$ and $\theta = 0.001$.

network [33]. As shown in Fig. 13, the network resilience is evaluated in terms of the largest component size when a subset of nodes is removed from the network. Given the expected number of reports required for attack detection M_1, if an adversary attacks less than M_1 nodes in the network, then the attack will not be detected, which we refer to as the undetectable region. As shown in Fig. 13, M_1 decreases as P_D increases, and it is shown to be relatively small compared with the network size. Notably, in the undetectable region, most of the nodes are still connected, even with small P_D. The results indicate that the proposed sequential defense mechanism is quite effective in attack detection and the network suffers slight connectivity loss in the undetectable region. Note that the perfect protection defense strategy proposed in Ref. [22] is a degenerate case of our proposed mechanism when $P_D \to 1$ and $P_F \to 0$. It results in extremely small M_1 and suggests that a network can be robust to attacks if perfect protection is plausible.

VIII. DISCUSSIONS TOWARD ROBUST NETWORK DESIGN

Based on the performance analysis of a complex network empowered with the proposed sequential defense mechanism, we provide some insights on robust network design against attacks in complex networks. To guarantee that the process of SPRT terminates before an adversary paralyzes the entire system, the baseline requirement for the network disruption threshold is $M_c \geq \max\{M_1^{ran}, M_1^{int}\}$, which ensures that the data fusion center can acquire sufficient information for attack inference and make immediate reactions against the attacks prior to the network disruption. In other words, in the network operator's point of view, one has to enhance the critical values of a network under attacks to maintain the operations of the defense mechanism in the system, which can be achieved via different approaches in consideration of the network configurations and implementation costs. Consequently, this paper offers analytically tractable tools for robust network design and network defense performance assessment. Potential approaches to network robustness enhancement are discussed as follows.

(1) Link addition. As shown in Fig. 2, adding more links in the network (i.e., increasing the mean degree) strengthens the network connectivity and thereby offers more protection against attacks. Although link addition is a straightforward solution [34,35], the major drawback of link addition is that it may decrease the system revenue if the costs for link constructions are high, such as the transportation systems.

(2) Topology adjustment. As the network resilience varies from network parameters, the critical value of a network can be modified by topology adjustment while keeping the number of links in the network (i.e., the mean degree) unchanged [36], which is especially suitable for networks connected by logical configurations (e.g., the WWW). For an example, as demonstrated in Fig. 2, adjusting a power-law network to an exponential network enhances the resilience against intentional attack at the cost of decreasing the resilience against random attack, which offers tradeoffs between M_1^{ran} and M_1^{int}.

(3) Detection capability enhancement. In cases that link addition and topology adjustment are infeasible and thereby
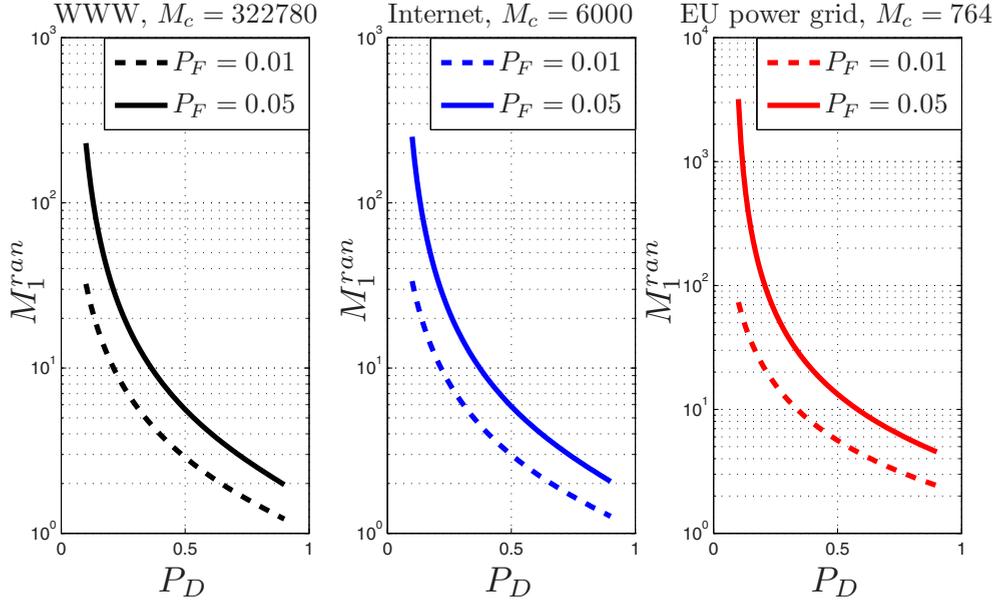
FIG. 11. (Color online) Performance of sequential defense mechanism under random attack with empirical network data. The critical values are $(q_c^{\text{ran}}, M_c) = (0.9909, 322\,780)$, $(q_c^{\text{ran}}, M_c) = (0.9673, 6\,000)$ and $(q_c^{\text{ran}}, M_c) = (0.629, 764)$ for the WWW, internet, and EU power grid, respectively.

the critical values cannot be modified, one has to enhance the detection capability to provide reliable network defense against attacks. Take sequential defense against intentional attack as a motivating example, the sequential defense mechanism is able to target intentional attack if the network disruption threshold M_c is no less than M_1^{int}. Applying this criterion to Eq. (28), the feasible parameters P_D and P_F for sequential defense mechanism need to satisfy the inequality

$$P_D \log \frac{P_D}{P_F} + (1 - P_D) \log \frac{1 - P_D}{1 - P_F}$$
$$\geqslant \frac{\theta \log \frac{\theta}{1-\delta} + (1 - \theta) \log \frac{1-\theta}{\delta}}{M_c}. \quad (29)$$

The operation curves when the equality in Eq. (29) holds given a specified network disruption threshold (M_c) are shown in Fig. 14, which can be interpreted as the minimum detection probability (P_D) required to perform sequential defense with respect to a false alarm probability P_F and M_c. The feasible operation region is composed of the parameters (P_D, P_F)
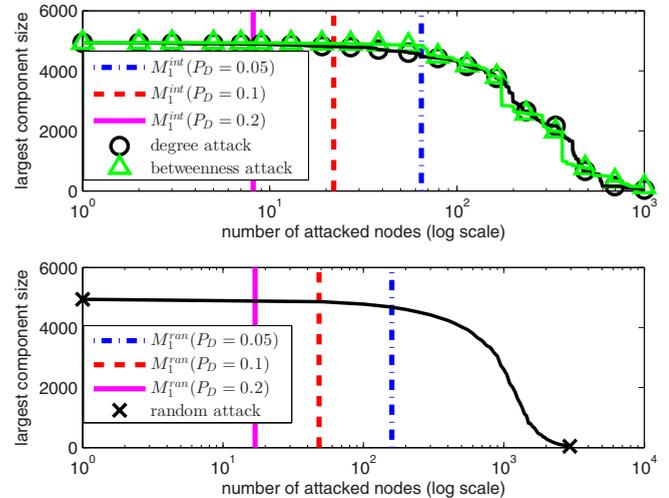
FIG. 13. (Color online) Performance of sequential defense mechanism on U.S. power grid topology [27] under different attack schemes with $P_F = 0.005$. The power grid topology contains 4 941 nodes (power stations) and 6 594 edges (power lines). For random attack, the results are averaged over 100 realizations. The expected number of reports (M_1) needed for attack detection is relatively small and it decreases as P_D increases. The proposed sequential defense mechanism is quite effective in the sense the network suffers slight connectivity loss when the number of attacked nodes is less than M_1 (i.e., the undetectable region), even for small P_D.

FIG. 12. (Color online) Performance of sequential defense mechanism under intentional attack with empirical network data. The critical values are $(q_c^{\text{int}}, M_c) = (0.067, 21\,824)$, $(q_c^{\text{int}}, M_c) = (0.03, 187)$, and $(q_c^{\text{int}}, M_c) = (0.275, 766)$ for the WWW, internet, and EU power grid, respectively.
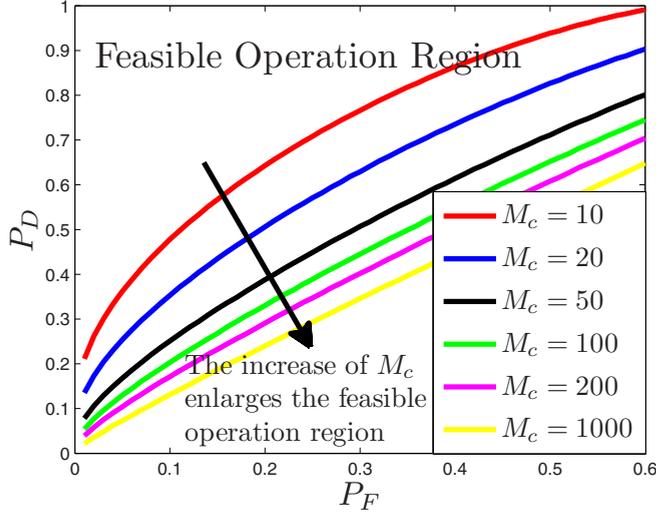
FIG. 14. (Color online) Operation curves of P_D and P_F with respect to a specified network disruption threshold M_c under intentional attack. The feasible operation region are composed of the feasible parameters (P_D, P_F) such that $M_c \geqslant M_1^{\text{int}}$ in order to guarantee network robustness.

satisfying the inequality in Eq. (29), and the increase of M_c enlarges the feasible operation region since the data fusion center can acquire more reports for attack inference prior to network disruption, even in the low P_D regime.

IX. CONCLUSION

In this paper, a sequential defense mechanism based on sequential hypothesis test is proposed in complex networks with an aim of enhancing the network robustness of networked engineering systems. This mechanism provides timely and efficient defense against random and intentional attacks by sequentially acquiring binary attack status of each node in descending degree order. The data collection process terminates once a final decision has been made by the data fusion center, which is particularly preferable in networking paradigms with stringent data transmission resources. Therefore, the low computation complexity and sequential transmission schemes render this defense mechanism compatible to practical networked engineering systems. A parametric plug-in model is proposed to evaluate the performance of the proposed sequential defense mechanism. By implementing this mechanism on the canonical complex network models as well as the empirical network data extracted from the WWW, the internet, the EU power grid, and the U.S. power grid topology, the results validate the effectiveness and reliability of this mechanism against fatal attacks. These attacks can be identified with high precision with limited binary attack status reported from a small subset of nodes in the network and thereby immediate defense reactions can be performed prior to the network disruption, even in the weak topological vulnerability and low detection capability regime. Based on the performance analysis and network configurations, several approaches including link addition, topology adjustment, and detection capability enhancement are elucidated to guarantee robust operations of the entire system. Consequently, this paper

provides profound theoretic framework of sequential defense in complex networks and offers new insights on robust network design in complex networks.

APPENDIX A: CRITICAL VALUE FOR RANDOM ATTACK

Following Ref. [20], given the original degree distribution $P_0(k_0)$, the new degree distribution of the network after randomly removing q fraction of nodes (the links emanating from the nodes are removed as well) is

$$P(k) = \sum_{k_0=k}^{k_{\max}} P_0(k_0) \binom{k_0}{k} (1-q)^k q^{k_0-k}. \quad \text{(A1)}$$

Applying Eq. (A1) to Eq. (1), the criterion for the percolation-based connectivity after random attack becomes

$$\frac{(1-q)^2 \mathbb{E}[\mathbf{K_0}^2] + q(1-q)\mathbb{E}[\mathbf{K_0}]}{(1-q)\mathbb{E}[\mathbf{K_0}]} = 2. \quad \text{(A2)}$$

Reorganizing Eq. (A2), we obtain the critical value $q_c^{\text{ran}} = 1 - \frac{1}{\tau_0 - 1}$ as in Eq. (2). For ER network, we have $\mathbb{E}[\mathbf{K_0}] = \widehat{k}$ and $\mathbb{E}[\mathbf{K_0}^2] = \widehat{k}^2 + \widehat{k}$, applying to Eq. (2), we have

$$q_c^{\text{ran,ER}} = 1 - \frac{1}{\widehat{k}}. \quad \text{(A3)}$$

For power-law network, the rth moment of the degree distribution is $\mathbb{E}[\mathbf{K}^r] = c_1 \cdot \frac{k_{\max}^{r-\alpha+1} - k_{\min}^{r-\alpha+1}}{r-\alpha+1}$, where $c_1 = \frac{1-\alpha}{k_{\max}^{1-\alpha} - k_{\min}^{1-\alpha}}$ is the normalization factor. Applying to Eq. (2), we obtain

$$q_c^{\text{ran,POW}} = 1 - \frac{1}{\frac{2-\alpha}{3-\alpha} \frac{k_1^{3-\alpha} - k_N^{3-\alpha}}{k_1^{2-\alpha} - k_N^{2-\alpha}} - 1}. \quad \text{(A4)}$$

For exponential network, $P(k) = c_2 \frac{1}{\beta} e^{-\frac{k}{\beta}}$, where $c_2 = \frac{1}{e^{-\frac{k_N}{\beta}} - e^{-\frac{k_1}{\beta}}}$ is the normalization factor. In the large-scale network limit (i.e., $k_1 \rightarrow \infty$), $c_2 = e^{\frac{k_N}{\beta}}$, $\mathbb{E}[\mathbf{K}] = k_N + \beta$, and $\mathbb{E}[\mathbf{K}^2] = k_N^2 + 2k_N\beta + 2\beta^2$. We obtain

$$q_c^{\text{ran,EXP}} = 1 - \frac{1}{\frac{k_N^2 + 2k_N\beta + 2\beta^2}{k_N + \beta} - 1}. \quad \text{(A5)}$$

APPENDIX B: CRITICAL VALUE FOR INTENTIONAL ATTACK

For simplicity, we derive the critical value under intentional attack in the large-scale network limit ($k_1 \rightarrow \infty$) as follows. It is also suggested in Ref. [21] the large-scale network limit assumption has negligible impacts on the accuracy of the critical value provided that the network size (N) is large enough. The methodology for deriving the critical value under intentional attack is to specify the relations between the cutoff degree $\widetilde{d}_{\max}$ and the fraction of removed nodes q using Eq. (3),

and then apply the cutoff degree to the deletion probability $\widetilde{q}$ and the criterion for percolation-based connectivity in Eq. (2) to obtain the critical value q_c^{int}.

For ER network, from Eq. (3) we have $e^{-\widehat{k}}\frac{\widehat{k}^{k_1}}{k_1!} = \frac{1}{N}$ and $q = \sum_{k=\widetilde{k}_{\max}}^{k_1} e^{-\widehat{k}}\frac{\widehat{k}^k}{k!} = 1 - \frac{\Gamma(\widetilde{k}_{\max}, \widehat{k})}{(\widetilde{k}_{\max}-1)!}$, where $\Gamma(s,x) = \int_x^\infty t^{s-1}e^{-t}dt$ is the upper incomplete γ function. The deletion probability becomes $\widetilde{q} = \sum_{k=\widetilde{k}_{\max}}^{k_1} \frac{kP(k)}{\mathbb{E}[\mathbf{K_0}]} = \sum_{k=\widetilde{k}_{\max}}^{k_1} e^{-\widehat{k}}\frac{\widehat{k}^{k-1}}{(k-1)!} = q - \frac{1}{N} + e^{-\widehat{k}}\frac{\widehat{k}^{\widetilde{k}_{\max}-1}}{(\widetilde{k}_{\max}-1)!}$, and the cutoff degree $\widetilde{k}_{\max}$ can be obtained by solving $\widetilde{q} = 1 - \frac{1}{\overline{k}}$. Consequently, the critical value under intentional attack is

$$q_c^{\text{int,ER}} = \frac{1}{N} - e^{-\widehat{k}}\frac{\widehat{k}^{\widetilde{k}_{\max}-1}}{(\widetilde{k}_{\text{maxmax}}-1)!} + 1 - \frac{1}{\overline{\overline{k}}}. \quad (B1)$$

For power-law network, from Eq. (3) we have $\widetilde{k}_{\max} = k_N(q + \frac{1}{N})^{\frac{1}{1-\alpha}}$ and $q \overset{N \to \infty}{=} (\frac{\widetilde{k}_{\max}}{k_N})^{1-\alpha}$ for all $\alpha > 1$. The relations between $\widetilde{q}$ and q are $\widetilde{q} = \int_{k=\widetilde{k}_{\max}}^{k_1} \frac{kP(k)}{\mathbb{E}[\mathbf{K_0}]}dk = (\frac{\widetilde{k}_{\max}}{k_N})^{2-\alpha} = q^{\frac{2-\alpha}{1-\alpha}}$. The cutoff degree $\widetilde{k}_{\text{man}}$ can be solved by applying the

link deletion probability to the criterion in Eq. (2), which yields the equation $(\frac{\widetilde{k}_{\max}}{k_N})^{2-\alpha} - k_N(\frac{2-\alpha}{3-\alpha})[(\frac{\widetilde{k}_{\max}}{k_N})^{3-\alpha} - 1] - 2 = 0$ [21], and we thereby obtain

$$q_c^{\text{int,POW}} = \left(\frac{\widetilde{k}_{\max}}{k_N}\right)^{1-\alpha}. \quad (B2)$$

For exponential network, the relations between the cutoff degree and the fraction of removed nodes are $\widetilde{k}_{\max} = -\beta \ln(q + \frac{1}{N}) + k_N$. The deletion probability becomes $\widetilde{q} = \int_{k=\widetilde{k}_{\max}}^{k_1} \frac{kP(k)}{\mathbb{E}[\mathbf{K_0}]}dk = \frac{\exp(\frac{k_N}{\beta})}{k_N+\beta} \cdot (\widetilde{k}_{\max} + \beta)\exp(-\frac{\widetilde{k}_{\max}}{\beta})$. If k_N is negligible (i.e., $k_N = 0$), we have $\widetilde{q} = [1 - \ln(q + \frac{1}{N})](q + \frac{1}{N})$. Applying the result to Eq. (A5), the critical value under intentional attack can be obtained by solving

$$\left[1 - \ln\left(q_c^{\text{int,EXP}} + \frac{1}{N}\right)\right]\left(q_c^{\text{int,EXP}} + \frac{1}{N}\right)$$
$$+ \frac{k_N + \beta}{k_N^2 + 2k_N\beta + 2\beta^2 - k_N - \beta} - 1 = 0. \quad (B3)$$

[1] T. G. Lewis, *Network Science: Theory and Practice* (John Wiley and Sons, Inc., New York, 2008).

[2] R. Albert and A.-L. Barabási, Statistical mechanics of complex networks, Rev. Mod. Phys. **74**, 47 (2002).

[3] M. E. J. Newman, The structure and function of complex networks, SIAM Rev. **45**, 167 (2003).

[4] X. F. Wang and G. Chen, Complex networks: small-world, scale-free and beyond, IEEE Circuits Syst. Mag. **3**, 6 (2003).

[5] M. Kurant, A. Markopoulou, and P. Thiran, Towards unbiased BFS sampling, IEEE J. Sel. Areas Commun. **29**, 1799 (2011).

[6] L. Cui, S. Kumara, and R. Albert, Complex networks: An engineering view, IEEE Circuits Syst. Mag. **10**, 10 (2010).

[7] R. Albert, H. Jeong, and A.-L. Barabási, Error and attack tolerance of complex networks, Nature **406**, 378 (2000).

[8] M. Menth, M. Duelli, R. Martin, and J. Milbrandt, Resilience analysis of packet-switched communication networks, IEEE/ACM Trans. Netw. **17**, 1950 (2009).

[9] P. Smith, D. Hutchison, J. P. G. Sterbenz, M. Schöandller, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, Network resilience: A systematic approach, IEEE Commun. Mag. **49**, 88 (2011).

[10] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, Smart attacks in smart grid communication networks, IEEE Commun. Mag. **50**, 24 (2012).

[11] P.-Y. Chen and A. O. Hero, Node removal vulnerability of the largest component of a network, in *Proc. IEEE GlobalSIP* (IEEE, Piscataway, New York, 2013), pp. 1–5.

[12] P.-Y. Chen and A. O. Hero, Assessing and safeguarding network resilience to nodal attacks, IEEE Commun. Mag. **52**, 138 (2014).

[13] *A System View of the Modern Grid*, National Energy Technology Laboratory (NETL), U.S. Department of Energy (DOE), 2007, https://www.smartgrid.gov/sites/default/files/pdfs/a_systems_view_of_the_modern_grid.pdf.

[14] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Network robustness and fragility:

Percolation on random graphs, Phys. Rev. Lett. **85**, 5468 (2000).

[15] P. K. Varshney, *Distributed Detection and Data Fusion* (Springer-Verlag, New York, 1996).

[16] A.-L. Barabási and R. Albert, Emergence of scaling in random networks, Science **286**, 509 (1999).

[17] M. Faloutsos, P. Faloutsos, and C. Faloutsos, On power-law relationships of the Internet topology, in *ACM SIG-COMM* (ACM, New York, NY, 1999), pp. 251–262.

[18] H. Ebel, L.-I. Mielsch, and S. Bornholdt, Scale-free topology of e-mail networks, Phys. Rev. E **66**, 035103 (2002).

[19] S. Xiao, G. Xiao, and T. H. Cheng, Tolerance of intentional attacks in complex communication networks, IEEE Commun. Mag. **45**, 146 (2008).

[20] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, Resilience of the Internet to random breakdowns, Phys. Rev. Lett. **85**, 4626 (2000).

[21] R. Cohen, K. Erez, D. Ben-Avraham, and S. Havlin, Breakdown of the Internet under intentional attack, Phys. Rev. Lett. **86**, 3682 (2001).

[22] S. Xiao and G. Xiao, Effects of node protections against intentional attack in complex communication networks, in *International Workshop on the Design of Reliable Communication Networks (DRCN)* (IEEE, Piscataway, New York, 2011), pp. 78–85.

[23] P.-Y. Chen and K.-C. Chen, Intentional attack and fusion-based defense strategy in complex networks, in *Proc. IEEE Globecom* (IEEE, Piscataway, New York, 2011), pp. 1–5.

[24] P.-Y. Chen, S.-M. Cheng, and K.-C. Chen, Information fusion to defend intentional attack in Internet of things, IEEE Internet Things J. **1**, 337 (2014).

[25] A. Wald, *Sequential Analysis* (Dover Phoenix Editions, New York, 2004).

[26] P. Erdös and A. Rényi, On random graphs, I, Publicationes Mathematicae (Debrecen) **6**, 290 (1959).

[27] D. J. Watts and S. H. Strogatz, Collective dynamics of 'small-world' networks, Nature **393**, 440 (1998).

[28] M. Molloy and B. Reed, A critical point for random graphs with a given degree sequence, Random Struct. Algorithms **6**, 161 (1995).

[29] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, Robustness of the European power grids under intentional attack, Phys. Rev. E **77**, 026102 (2008).

[30] B. Mukherjee, L. T. Heberlein, and K. N.Levitt, Network intrusion detection, IEEE Netw. **8**, 26 (1994).

[31] G. Androulidakis, V. Chatzigiannakis, and S. Papavassiliou, Network anomaly detection and classification via opportunistic sampling, IEEE Netw. **23**, 6 (2009).

[32] M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Random graphs with arbitrary degree distributions and theirapplications, Phys. Rev. E **64**, 026118 (2001).

[33] L. Freeman, A set of measures of centrality based on betweenness, Sociometry **40**, 35 (1977).

[34] A. Ghosh and S. Boyd, Growing well-connected graphs, in *Proc. IEEE Conference on Decision and Control* (IEEE, New York, 2006), pp. 6605–6611.

[35] A. Yehezkel and R. Cohen, Degree-based attacks and defense strategies in complex networks, Phys. Rev. E **86**, 066114 (2012).

[36] A. A. Moreira, J. S. Andrade, H. J. Herrmann, and J. O. Indekeu, How to make a fragile network robust and vice versa, Phys. Rev. Lett. **102**, 018701 (2009).