Safeguarding the IoT From Malware Epidemics: A Percolation Theory Approach

Ainur Zhaikhan, Mustafa A. Kishk, *Member, IEEE*, Hesham ElSawy, *Senior Member, IEEE*, and Mohamed-Slim Alouini, *Fellow, IEEE*

***Abstract*—The upcoming Internet of Things (IoT) is foreseen to encompass massive numbers of connected devices, smart objects, and cyber–physical systems. Due to the large scale and massive deployment of devices, it is deemed infeasible to safeguard 100% of the devices with state-of-the-art security countermeasures. Hence, large-scale IoT has inevitable loopholes for network intrusion and malware infiltration. Even worse, exploiting the high density of devices and direct wireless connectivity, malware infection can stealthily propagate through susceptible (i.e., unsecured) devices and form an epidemic outbreak without being noticed to security administration. A malware outbreak enables adversaries to compromise a large population of devices, which can be exploited to launch versatile cyber and physical malicious attacks. In this context, we utilize *spatial firewalls*, to safeguard the IoT from malware outbreak. In particular, spatial firewalls are computationally capable devices equipped with state-of-the-art security and anti-malware programs that are spatially deployed across the network to filter the wireless traffic in order to detect and thwart malware propagation. Using tools from percolation theory, we prove that there exists a critical density of spatial firewalls beyond which malware outbreak is impossible. This, in turn, safeguards the IoT from malware epidemics regardless of the infection/treatment rates. To this end, a tractable upper bound for the critical density of spatial firewalls is obtained. Furthermore, we characterize the relative communications ranges of the spatial firewalls and IoT devices to ensure secure network connectivity. The percentage of devices secured by the firewalls is also characterized.**

***Index Terms*—Boolean model, network epidemics, percolation theory, random geometric graphs (RGGs).**

I. Introduction

THE SURGING Internet of Things (IoT) and cyber–physical systems (CPSs) are extending wireless connectivity to billions of new devices of multitude heterogeneity [1]. In addition to phones, tablets, and laptops, the IoT and CPS integrate appliances, sensors, actuators, machines, robots, vehicles, and many other smart objects to the wireless infrastructure. It is speculated that the numbers of IoT devices per square kilometers will be in the order of millions [2]. Such ubiquitous, large-scale, diverse, and massive wireless connectivity is essential for big data aggregation and smart world automation, which is expected to improve almost every aspect in our lives [1]. For instance, healthcare providers can access real-time vital signals for patients through connected body sensors, which improves diagnostics, enables early disease detection, and decreases infection risks. Smart power grids utilize wireless connectivity of smart meters and field devices to improve energy generation and distribution. Intelligent transportation systems with connected/autonomous vehicles exploit wireless connectivity to improve road safety and reduce traffic congestion. Large-scale massive connectivity is also foundational for process automation in the next industrial revolution (i.e., industry 4.0). In addition to the aforementioned examples, IoT/CPS can bring unlimited potentials to many other verticals, such as crowd management, public safety, agriculture, retail, etc.

The aforementioned benefits of IoT/CPS come at the cost of a plenty of new and challenging security threats [3]–[7]. The IoT and CPS devices are mainly installed and controlled via consumers who have a limited knowledge about security threats and countermeasures. The imposed high competition between IoT vendors leads to overlooking cybersecurity aspects in order to accelerate the production of devices and reduce their prices. Furthermore, many of the IoT and CPS devices do not have sufficient energy, storage, or computational power to implement up-to-date anti-malware programs and/or sophisticated intrusion defense mechanisms [8]–[11]. In large-scale IoT/CPS networks, there is no distinct boundary between secured and public (i.e., unsecured) domains to enforce security policies on the incoming/outgoing traffic. The lack of per-device defense mechanisms and network-wide security administration open several loopholes for network intrusion and malware infiltration. Even worse, exploiting the high spatial density of devices and direct wireless connectivity (e.g., machine-to-machine and device-to-device communications), the malware infection can stealthily propagate from one device to another and form an *epidemic outbreak* without being noticed to security administration [8], [12]–[14]. Malware diffusion through the devices can be further accelerated via emerging beyond 5G technologies, such as nonorthogonal multiple access (NOMA) and ultrareliable low-latency communications (URLLCs), which are meant to enhance information dissemination.

Manuscript received September 25, 2020; accepted October 21, 2020. Date of publication October 27, 2020; date of current version March 24, 2021. The work of Hesham ElSawy was supported by the Deanship of Scientific Research (DSR) at King Fahd University of Petroleum and Minerals (KFUPM) under Grant DF191052. *(Corresponding author: Hesham ElSawy.)*

Ainur Zhaikhan was with the Computer, Electrical, and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia. She is now with the Department of Electrical Engineering, École Polytechnique Fédérale de Lausanne, CH-1015 Lausanne, Switzerland (e-mail: ainur.zhaikhan@kaust.edu.sa).

Mustafa A. Kishk, and Mohamed-Slim Alouini are with the Computer, Electrical, and Mathematical Sciences and Engineering Division, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia (e-mail: mustafa.kishk@kaust.edu.sa; slim.alouini@kaust.edu.sa).

Hesham ElSawy is with the Electrical Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran 31261, Saudi Arabia (e-mail: hesham.elsawy@kfupm.edu.sa).

Digital Object Identifier 10.1109/JIOT.2020.3034111

A malware outbreak gives adversaries the opportunity to compromise a large population of IoT/CPS devices, which can then be used to launch versatile criminal and hostile attacks. Examples of generic IoT/CPS attacks are network-jamming, colluded eavesdropping, spoofing, denial of service, and data falsification [15]. The negative impact of any of the aforementioned attacks is proportional to the number of compromised devices. It is worth noting that, in IoT/CPS systems, adversaries can compromise, control, and manipulate physical equipment, which may lead to physical consequences, such as equipment sabotage, power outage, vehicles collisions, or workers injury [3]. The aforementioned security risks call for resilient, robust, and ubiquitous security countermeasures to safeguard IoT/CPS networks from large-scale malware attacks.

II. Prior Art and Contributions

One major research direction is to develop lightweight security countermeasures for IoT/CPS devices. Per-device IoT/CPS security can be implemented either in hardware [16] or in software [17], [18]. However, many IoT/CPS devices are too constrained (e.g., storage, energy, and computational power) to implement such per-device countermeasures. Furthermore, due to the massive number of devices, implementation of hardware solutions, and licensing of software countermeasures may impose overwhelming monetary costs. Hence, it is infeasible to ubiquitously safeguard 100% of the devices against malware intrusion/infection [9], [10], [19]. Articulated differently, interim infection of some devices is inevitable in large-scale massive IoT/CPS systems. Hence, timely detection and treatment of malware is the security challenge in large-scale IoT/CPS networks such that malware outbreak is prevented. Otherwise, the malware infection goes out of control and large populations of devices are compromised.

To detect compromised devices, Asokan *et al.* [20] and Yan *et al.* [21] proposed software attestation schemes to ensure the integrity of the running software and configuration of IoT devices. However, the attestation schemes in [20] and [21] are centralized, which may impose overwhelming overhead traffic and delay to detect compromised devices. The work in [9] proposes a game-theoretic approach to select the devices that install anti-malware programs such that an epidemic outbreak is prevented. However, the proposed mechanism in [9] is based on a fully mixed epidemic model,[1] which is not adequate for wireless IoT networks. Accounting for the physical layer parameters of wireless networks, Farooq and Zhu [10] proposed periodic software patching for IoT/CPS devices to eliminate potential malicious codes to combat botnet formation. However, the technique proposed in [10] is oblivious to the device status, which may lead to unnecessary disruption for the IoT/CPS operation as a price for patching healthy devices. Furthermore, compromising a device shortly after being attested and/or patched may grant adversaries enough time to launch malicious attacks. Such scheduled software attestation/patching problems are more acute when employing wireless technologies, such as NOMA and URLLC due to the accelerated epidemic infection rate.

To overcome the aforementioned problems, ElSawy *et al.* [22] proposed a novel countermeasure denoted as *spatial firewalls*. The spatial firewalls are wireless devices, with sufficient computational power, energy resources, and memory, to store, execute, and frequently update anti-malware and intrusion detection programs. Spatial firewalls can be edge servers, access points, or capable IoT/CPS devices, which are randomly deployed in the network to analyze the wireless traffic in order to detect and thwart emerging-malware infections. However, the exposition in [22] is based on simulations, which lacks the mathematical details that are necessary to prove the concept, assess, and design spatial firewalls. In this context, we develop a rigorous mathematical framework to assess and design spatial firewalls. In order to account for the underlying limited-range wireless connectivity for the firewalls and IoT/CPS devices, we utilize percolation theory on random geometric graphs (RGGs) for the developed mathematical framework.

It is worth noting that percolation theory on RGG is widely used to assess information dissemination and global network connectivity in wireless sensors networks [23], [24], robot swarms [25], high altitude platforms [26], and connected unmanned aerial vehicles [27]. Percolation models are also used to study information dissemination in cognitive networks [28], [29]. Note that the models in [23]–[29] assume proximity-based wireless communications, which does not account for the aggregated network interference. Interference-aware percolation models are developed in [30] and [31], where nodes communicate if and only if the signal-to-interference-plus-noise ratio exceeds a certain threshold. Percolation theory is also used in [32] and [33] to study private information dissemination in the presence of eavesdroppers.

In this article, we utilize percolation theory on RGG to characterize wireless malware propagation in IoT/CPS networks, and hence, prove the concept and assess the spatial firewalls solution. That is, we mathematically prove the existence of a critical density of firewalls beyond which malware outbreak becomes impossible. To this end, we find a tractable upper bound on the critical density of firewalls that is required to safeguard large-scale IoT/CPS networks against malware epidemics. In addition, we present several insights for the design of spatial firewalls. The contributions of this article can be summarized in the following points.

1) We define the infection susceptible graph (ISG) to characterize the risk malware propagation in large-scale IoT/CPS networks.
2) Using percolation theory along with the ISG, we prove that properly designed firewalls are capable to safeguard large-scale IoT/CPS networks from malware outbreak irrespective of the infection propagation rate.
3) We derive a tractable upper bound for the critical density of spatial firewalls that is required to safeguard large-scale IoT/CPS networks against malware epidemics.
4) We analytically characterize the IoT/CPS communications range that allows network connectivity while prohibiting malware epidemics.

[1] A fully mixed epidemic model assumes that an infection (e.g., malware) can be directly transmitted from any node in the network to any other node in the network.

TABLE I
TABLE OF NOTATIONS

Notation	Description
Φ; λ_r; r_r	the set of IoT/CPS devices locations; their intensity; their communication range
Ψ; λ_f; r_f	the set of firewalls locations; their intensity; their communication range
$\Xi = \Phi \setminus \Theta$	the set of susceptible devices locations
$\Theta = \Phi \setminus \Xi$	the set of protected devices locations
$G = (\Phi, E)$	the RGG representation of IoT/CPS network with vertex set Φ and edge set E
$\mathcal{I} = \{\Xi, \mathcal{E}\}$	the infection susceptible graph with vertex set Ξ and edge set $\mathcal{E}$
$\theta_G(\lambda_r, r_r)$	probability of percolation in G
$\theta_{\mathcal{I}}(\lambda_f, r_f, \lambda_r, r_r)$	probability of percolation in $\mathcal{I}$
λ_f^c	critical density of firewalls
$\mathcal{L}_h$; $\mathcal{L}_s$; $\mathcal{L}_s^d$	hexagonal lattice; square lattice; dual of square lattice
K, $K_{\mathcal{L}_h}$, $K_{\mathcal{L}_s}$, $K_{\mathcal{L}_s^d}$, $K_{\mathcal{I}}$	connected component in G, $\mathcal{L}_h$, $\mathcal{L}_s$, $\mathcal{L}_s^d$ and $\mathcal{I}$, respectively
δ_{sec}; δ_{sec}^c	the percentage of protected devices; critical percentage of protected devices

5) We provide several insights on the percentage of IoT/CPS devices that are protected via the spatial firewalls.

It is worth noting that the spatial firewalls represent one layer of the IoT cybersecurity countermeasures. In the IoT era, specially when the devices are simple, ultradense, and managed by general public, the security problem is not a single-sided IT problem. Instead, cybersecurity in IoT is a multidimensional problem that should be collaboratively solved by wireless communication experts, machine learning experts, hardware designers, software developers, and IT experts, in addition to IoT consumers by raising awareness regarding cybersecurity threats. This article focuses on the wireless communications and networking aspect of the IoT and provides a proactive countermeasure that eliminates the risk of large-scale diffusion of malware epidemics.

A. Article Organization

The remainder of this article is organized as follows. Section III presents the system model and formulates the large-scale malware epidemic problem in terms of graph and percolation theory. Section IV proves the concept of spatial firewalls and shows the existence of a critical density for the spatial firewalls that safeguards large-scale IoT/CPS from malware epidemics. Section V discusses different design schemes for the spatial firewalls. Simulation and numerical results are presented in Section VI. Finally, concluding remarks are given in Section VII. For the ease of mathematical exposition, frequently used symbols are summarized in Table I.

III. SYSTEM MODEL

We consider a large-scale IoT/CPS network with *ad hoc* topology. In particular, the IoT/CPS devices are assumed to be scattered in $\mathbb{R}^2$ according to a homogeneous Poisson point process (PPP) $\Phi \equiv \{x_0, x_1, \ldots, x_k, \ldots\} \subset \mathbb{R}^2$ with intensity λ_r. We model the locations of the IoT devices as a PPP with density λ_r. Note that the PPP is commonly utilized and widely accepted in the literature to model wireless networks due to its tractability and practical significance [10], [34]–[38]. The IoT/CPS devices can establish bidirectional device-to-device (D2D) links if they are within the wireless communication ranges of each other. It is assumed that all devices have the same wireless communication range of r_r meters. All IoT/CPS devices are assumed to be too constrained to install and execute anti-malware programs. Hence, the D2D links can be used for legitimate code dissemination or exploited for malware infection propagation. We assume autonomous malware worms in which compromised devices are infection threats for all of their connected neighbors [12], [13]. Exploiting multihop D2D connectivity, the malware infection may diffuse to a large population of devices and create an epidemic outbreak.

To secure such large-scale IoT/CPS network from malware epidemic outbreak, spatial firewalls are randomly deployed according to an independent PPP $\Psi \equiv \{a_0, a_1, \ldots, a_k, \ldots\} \subset \mathbb{R}^2$ with intensity λ_f. Firewalls are computationally capable devices (e.g., edge computing device, access point, and high-end IoT/CPS devices) that are equipped with the state-of-the-art anti-malware programs [39]–[41]. Each firewall is assumed to have a communication range of r_f meters, and hence, each firewall creates a *secured zone* of radius r_f around itself. Due to the higher transmit power and better signal capture capabilities of firewalls, it is assumed that the firewalls have larger communication and detection ranges than the IoT/CPS devices (i.e., $r_f \geq r_r$). IoT/CPS devices within secured zones inquire the firewall about software codes received from the wireless interface. The firewalls scan inquired codes for security threats. If the code is legitimate and free from malware threats, the firewalls approve it. Otherwise, the code is disapproved and reported to the security administration for further action.[2] Consequently, IoT/CPS devices within secured zones are protected from malware infection and do not participate in malware propagation. On the other hand, devices outside secured zones have no direct

[2]For instance, the security administration may need to launch a patching campaign to recover compromised devices and prevent further propagation of the malware to other vulnerable devices.

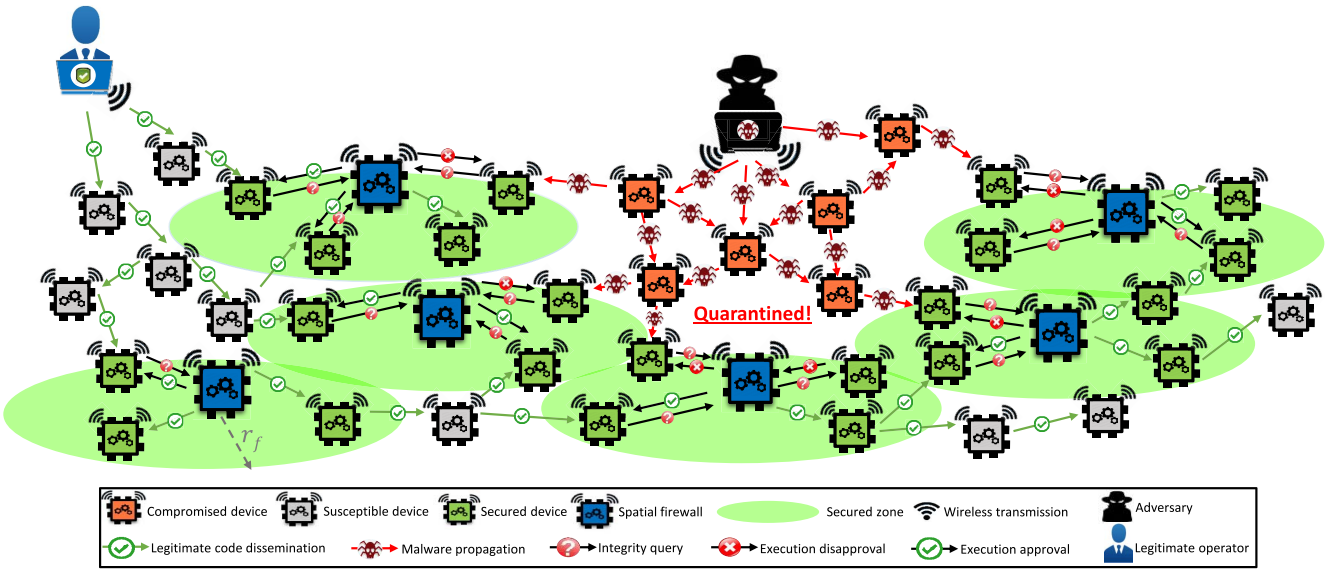


Fig. 1. Illustration of spatial firewalls operation.

connectivity with firewalls, and hence, they opt to directly execute and relay the codes received from the wireless interface. Hence, devices that are outside secured zones are susceptible to malware infection and may participate to malware propagation. In practice, we can expect that spatial firewalls are continuously updated, monitored and maintained with highly skilled personnel. Hence, in analysis, we assume that spatial firewalls are never compromised with attackers and can ensure almost 100% security. The operation of the spatial firewalls in large-scale IoT/CPS is depicted in Fig. 1. As shown in the figure, if the firewalls are dense enough, the collective impact of secured zones can thwart malware outbreak by spatially quarantining malware infections within a finite region. The firewalls can then report to the security administration about detected malware for localized patching and the treatment of compromised devices. As shown in Fig. 1, the IoT/CPS network is composed of three types of devices.

1) *Spatial firewalls* are capable devices, equipped with the state-of-the-art anti-malware programs, that are spatially distributed across the network.
2) *Protected devices* are IoT/CPS devices that fall within the secured zone of a firewall, and hence, cannot be infected with malware and do not participate in malware propagation.
3) *Susceptible devices* are IoT/CPS devices that fall outside the secured zone of a firewall, and hence, can be compromised and may participate in malware propagation.

A. Mapping to Graph and Percolation Theory

To study and characterize malware propagation in IoT/CPS networks and assess the impact of spatial firewalls, we utilize graph and percolation theory. In particular, the IoT/CPS network is mapped to an RGG, denoted as $G = \{\Phi, E\}$, where the devices Φ are mapped to the graph vertices. Accounting for the limited wireless D2D communications range of r_r, the set of edges E is defined as

$$E = \left\{\overline{x_i x_j} : \left\|x_i - x_j\right\| \leq r_r,\ x_i, x_j \in \Phi\right\} \tag{1}$$

where $\|\cdot\|$ denotes the Euclidean norm and $\overline{x_i x_j}$ is the edge connecting x_i and x_j. The edges defined in (1) represent bidirectional direct (i.e., one hop) D2D connectivity between devices. The bidirectional links in E can be used for legitimate traffic dissemination or malware propagation. An infection from a device in G can reach its direct D2D neighbor devices in one hop. Furthermore, an infection from a device in G can also reach nonneighbor distant devices through multihop connectivity if there exists a route in E that connects the compromised device to the distant device. However, due to the random devices locations and limited wireless D2D range, a compromised device does not imply an infection threat to all other devices in G. This is because there might not be a multihop route in E that connects the compromised device to all other devices in G. The mutual infection threat between devices in G is specified through the connected components, which are defined as follows.

Definition 1 (Connected Component): A connected component is a subgraph $K \subseteq G(\Phi, E)$ with the largest possible devices such that, within K, any device $x_i \in K$ can always find a multihop route through a set of consecutive edges in E to any other device $x_j \in K$, $i \neq j$. Consequently, a malware infiltration to any device $x_i \in K$ represents an infection threat for all devices $x_j \in K$ for $i \neq j$.

Based on Definition 1 and the ability of malware infection to exploit multihop connectivity, a compromised device is an infection threat to all devices within its own connected component. Hence, the infection threat is directly proportional to the size of the connected components. Small values of λ_r and/or r_r lead to sparse vertices in Φ, and hence, the graph G will be consisting of several disjoint small connected components. In such a case, there is no risk of an epidemic outbreak due to the lack of multihop wireless connectivity that connects a large population of devices. Increasing λ_r and/or r_r, the connected components start to merge together into larger components and an infection becomes threatening to a larger number of devices. Sufficiently high λ_r and/or r_r create a *giant*

component that connects infinite number of devices [42], [43]. The existence of a giant component implies the risk of an epidemic outbreak that gets out of control and compromise large population of IoT/CPS devices. Characterizing the network parameters that lead to the existence/absence of the giant component is the core focus of *percolation* theory. Formally, the percolation probability on the graph G, as a function of λ_r and/or r_r, is defined as follows.

Definition 2 (Percolation Probability): Percolation probability defines the probability of existence of infinitely large connected component $K \subseteq G$, defined as

$$\theta_G(\lambda_r, r_r) = \mathbb{P}\{|K| = \infty\} \tag{2}$$

where $|\cdot|$ denotes the set cardinality. A nonzero percolation probability $\theta_G(\lambda_r, r_r) > 0$ defines the super-critical regime in which the network percolates and a giant component exists. On the other hand, a zero percolation probability $\theta_G(\lambda_r, r_r) = 0$ defines the subcritical regime with no percolation and no giant components.

In the context of the malware infection in IoT/CPS network, the super-critical regime implies the risk of having a large connected population of devices that are vulnerable to an epidemic outbreak if a single device is compromised. The relative values of λ_r and r_r that lead to super-critical regime operation and raise the risk of malware epidemic in the depicted IoT/CPS network is defined in the following proposition.

Lemma 1: The IoT/CPS network operates in the super-critical regime $\theta_G(\lambda_r, r_r) > 0$, and hence, is susceptible to malware epidemic if and only if

$$\lambda_r \geq \frac{\lambda_c(1)}{r_r^2} \tag{3}$$

where $\lambda_c(1) \approx 1.44$.

Proof: The proof is similar to [44, Ch. 2] which characterizes continuum percolation on PPP networks with homogeneous communication ranges. ∎

If (3) is not satisfied, the IoT/CPS network is physically immune to malware epidemics. That is because if the defence mechanism of an IoT device is beaten by the attacker, the largest infected region will still be finite.

Remark 1: $\lambda_c(1)$ defined in Lemma 1 is the critical (i.e., minimum) intensity of nodes required for continuum percolation in homogeneous PPP network with a normalized communication range 1. There is no known exact value for $\lambda_c(1)$ in the literature. However, there exists some useful approximations in the literature, such as $\lambda_c(1) \approx 1.44$ [45]. There are also analytically derived lower and upper bounds: $0.768 < \lambda_c(1) < 3.37$ [44], [46].

If the condition defined in (3) of Lemma 1 is not satisfied, then the IoT/CPS network is physically immune to malware epidemics due to the lack of multihop D2D connectivity that can be exploited to transfer malware infection to large-population of devices. Otherwise, the IoT/CPS network is at risk of malware epidemic and the spatial firewalls countermeasure is required. Note that in dense IoT/CPS networks, the condition in (3) is usually satisfied.

As discussed earlier, the spatial firewalls introduce spatial secured zones that protect some IoT/CPS devices and thwart malware propagation.[3] To incorporate the impact of spatial firewalls to the mathematical framework, the vertices Φ in the RGG G are further divided into susceptible devices $\Xi \subseteq \Phi$ and protected devices $\Theta \subseteq \Phi$ such that $\Xi \cup \Theta = \Phi$ and $\Xi \cap \Theta = \emptyset$. The protected set $\Theta = \{x_i \in \Phi : \min_{a_j \in \Psi} \|x_i - a_j\| \leq r_f\}$, where $\min_{a_j \in \Psi} \|x_i - a_j\|$ is the minimum distance between x_i and all firewalls in Ψ. Hence, Θ contains all the devices that are located within the secured zones of the firewalls, i.e., the devices that can neither be infected nor participate in malware propagation. On the other hand, the susceptible set $\Xi = \{x_i \in \Phi : \min_{a_j \in \Psi} \|x_i - a_j\| > r_f\}$ contains the devices that are located outside the secured zones of all firewalls. A pictorial illustration for a realization of $G = (\Phi, E)$ before and after deploying spatial firewalls is shown in Fig. 2.

To characterize the impact of spatial firewalls, we define the ISG $\mathcal{I} = \{\Xi, \mathcal{E}\}$, with all susceptible devices in Ξ and set of edges $\mathcal{E}$, which contains all the D2D links that can be exploited for malware infection propagation. The set $\mathcal{E}$ is defined as

$$\mathcal{E} = \left\{\overline{x_i x_j} : \left\|x_i - x_j\right\| \leq r_r,\ x_i, x_j \in \Xi\right\}. \tag{4}$$

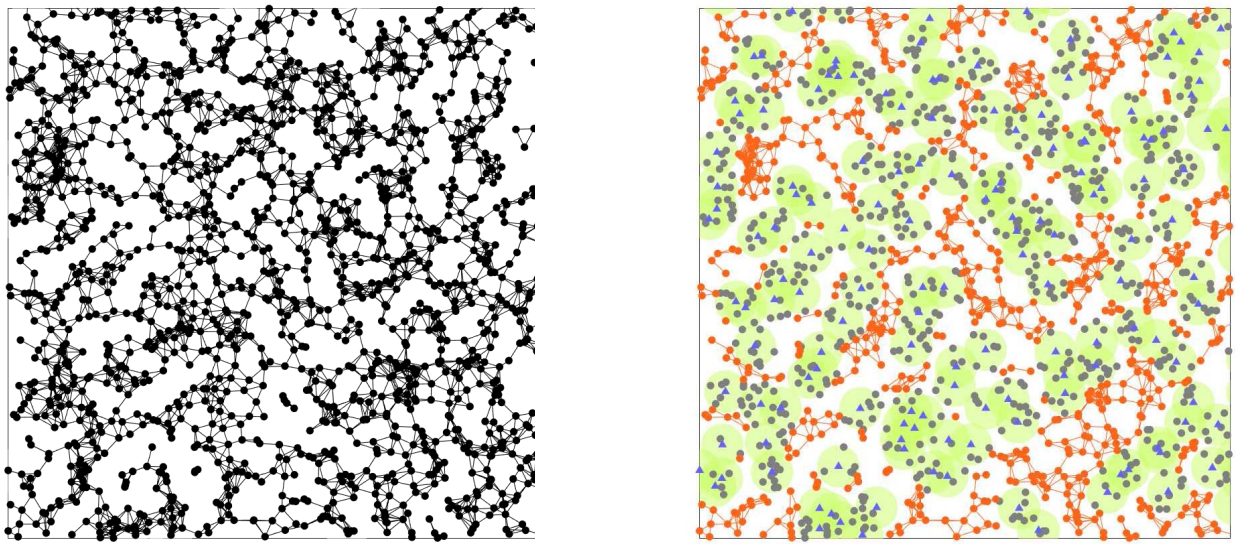
The ISG is illustrated in Fig. 2(b), which highlights all susceptible deceives and their D2D connectivity. It is worth noting that an infection cannot propagate from a device in Ξ to a device in Θ, or vice versa, due to the firewall protection for all devices in Θ. Hence, the definition in (4) for the edges in $\mathcal{E}$ is restricted to the susceptible devices in Ξ.

It is clear that the ISG is a subset of the IoT/CPS network graph $\mathcal{I} \subseteq G$. At the absence of spatial firewalls (i.e., $\lambda_f = 0$), all the devices are susceptible to infection, and hence, the ISG coincides with the IoT/CPS network graph $\mathcal{I} = G(\Phi, E)$. Deploying spatial firewalls splits the set Φ into protected Θ and susceptible Ξ devices. The ISG $\mathcal{I}$ can be constructed by removing the vertices in Θ and their associated edges from $G(\Phi, E)$. Given that G operates in the super-critical regime, the objective is to deploy sufficiently dense spatial firewalls (i.e., λ_f) such that the ISG $\mathcal{I} \subseteq G$ operates in the subcritical regime. Note that the subcritical regime operation of $\mathcal{I} \subseteq G$ implies that the risk of malware epidemic is eliminated. Consequently, the IoT/CPS network is safeguarded from malware epidemics regardless of the malware infection rate. Let $K_{\mathcal{I}} \subseteq \mathcal{I}$ be the largest connected component in the ISG $\mathcal{I}$ and let $\theta_{\mathcal{I}}(\lambda_f, r_f, \lambda_r, r_r) = \mathbb{P}\{|K_{\mathcal{I}}| = \infty\}$ be the percolation probability of the ISG $\mathcal{I}$. Then, the design objective of the spatial firewalls is formally defined as

$$\begin{aligned} &\text{minimize} \quad \lambda_f \\ &\text{subject to} \quad \theta_{\mathcal{I}}\left(\lambda_f, r_f, \lambda_r, r_r\right) = 0. \end{aligned} \tag{5}$$

To minimize the monetary cost (e.g., deployment and/or anti-malware licensing) of spatial firewalls, it is desirable to find the minimum intensity of firewalls that safeguards the IoT/CPS network against malware epidemics. In the notion of

[3]Different from traditional reactive cybersecurity countermeasures, the proposed spatial firewall solution is a proactive networking solution that eliminates network-wide malware infection risks rather than reacting to local attacks. To defend against local attacks (i.e., within single or multiple proximate susceptible devices), there should be complementing reactive security countermeasure.



(a) (b)

Fig. 2. (a) Realization of $G(\Phi, E)$ before the deployment of spatial firewalls. (b) Impact of spatial firewalls (blue triangles with green secured zones), which splits $G(\Phi, E)$ into the ISG $\mathcal{I} = \{\Xi, \mathcal{E}\}$ (orange connected nodes) and protected deceives Θ (gray nodes).

percolation theory, the optimal λ_f^* is denoted as the critical density for percolation.

IV. Proof of Concept

This section proves the concept of spatial firewalls by showing that there exists a phase transition for the percolation probability of the ISG. In particular, there is a critical intensity of spatial firewall λ_f^c below which the ISG operates in the super-critical regime. Hence, if the firewalls are not dense enough, the percolation probability is nonzero and the risk of malware epidemic exists. If the intensity of firewalls is above the critical intensity λ_f^c, the ISG operates in the subcritical regime, which eliminates the risk of malware epidemic by enforcing a zero percolation probability. To complete the proof of concept, we show that the percolation probability is monotonically decreasing in λ_f, which proves the phase transition at a critical intensity λ_f^c. Hence, the critical intensity λ_f^c is the optimal density that minimizes (5).

For the sake of organized presentation, Section IV-A presents the subcritical regime operation for the ISG, which proves the effectiveness of the spatial firewalls. Then, Section IV-B presents the super-critical regime operation for the ISG, which proves the need for dense enough spatial firewalls. Last but not least, Section IV-C completes the proof of concept by showing the monotonicity of the percolation probability in λ_f.

A. Subcritical Regime

This section proves that sufficiently dense firewalls enforce a subcritical regime operation for the ISG, which safeguards the IoT/CPS networks against malware epidemics. To find sufficient conditions for spatial firewalls intensity that enforces subcritical regime operation for the ISG, a worst case scenario of $r_f = r_r$ is assumed. Such sufficient firewalls intensity would also enforce subcritical regime for the general case of $r_f \geq r_r$. For tractable analysis, the common practice in percolation theory is to study continuum percolation in RGG by mapping them to discrete lattices. Inspired by [32], we prove the subcritical regime operation by mapping the ISG to the hexagonal lattice as defined in the sequel.

Mapping to a Hexagonal Lattice: Let $\mathcal{L}_h$ be a hexagonal lattice with a side equal to the D2D communication range r_r, which is also equal to the secured zone radius (i.e., $r_f = r_r$). Let $\mathcal{H}$ denote a randomly selected hexagon, also denoted as a face, in $\mathcal{L}_h$. Depending on the firewalls occupancy, a face $\mathcal{H}$ can be either open or closed, as explained next.

Definition 3 (Closed/Open Face in $\mathcal{L}_h$): Let $\{T_i\}_{i=1}^3$ denote three nonadjacent equilateral triangles within a face $\mathcal{H}$ as shown in Fig. 3(a). Then, the face $\mathcal{H}$ is said to be closed if each of these triangles is occupied with at least one firewall. Otherwise, the face $\mathcal{H}$ is denoted as *an open face*.

Definition 3 is chosen such that the absence of open face percolation in $\mathcal{L}_h$ assures no continuum percolation in the ISG $\mathcal{I} = (\Xi, \mathcal{E})$. In particular, open face percolation is obstructed by closed faces. In our setup, a closed face defines a protected geographical region (i.e., by secured zones of firewalls) that cannot be crossed by a malware infection. More precisely, due to the union of the secured zones of the firewalls within the triangles $\{T_i\}_{i=1}^3$, an infected device within the vicinity of a closed face will not have any susceptible device within its D2D reach through the closed face. Articulated differently, there could not be susceptible edges in $\mathcal{E}$ of the ISG that passes through a closed face in $\mathcal{L}_h$. A sequence of connected closed faces form *a closed path*, which further extends the firewalls spatial protection to larger connected (i.e., no gaps for malware propagation) geographical region. A path that starts and ends at the same face is denoted as a *closed circuit*. A closed circuit on $\mathcal{L}_h$ implies no open face percolation on $\mathcal{L}_h$, which also implies finite connected component in $\mathcal{I} = (\Xi, \mathcal{E})$.

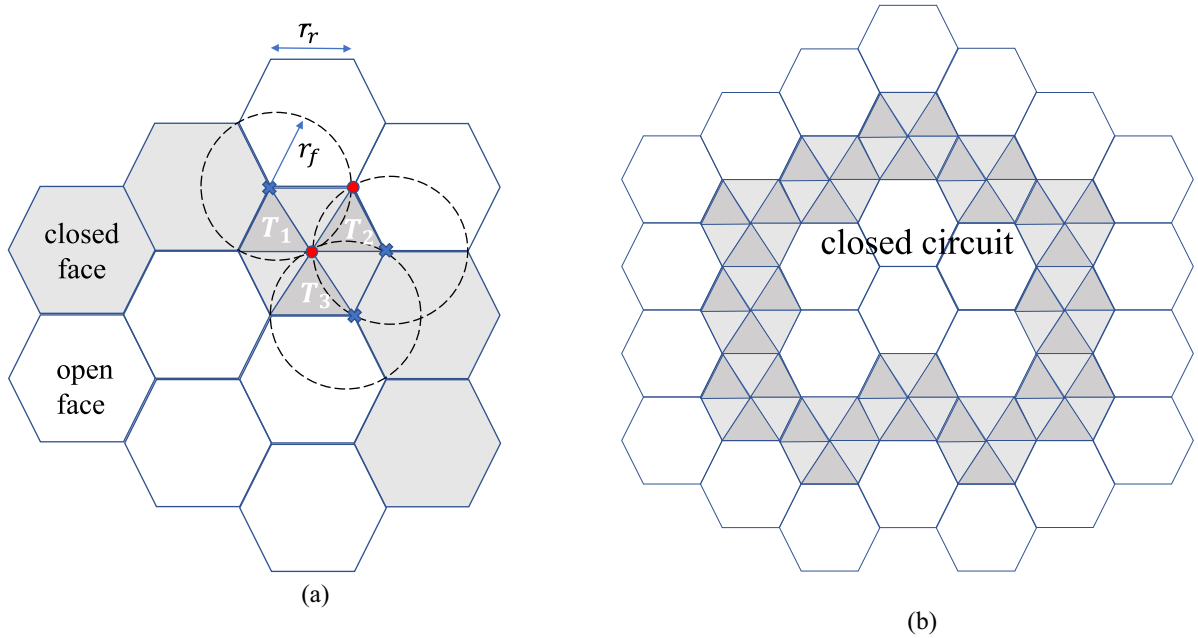


Fig. 3. Illustrating the concept of (a) closed face and (b) closed circuit in the hexagonal lattice $\mathcal{L}_h$.

Hence, a closed circuit on $\mathcal{L}_h$ means spatially quarantined (i.e., surrounded) malware. pictorial illustrations of a closed face and a closed circuit are shown in Fig. 3(b).

As illustrated above, malware infection is obstructed by closed faces. Hence, an infection that originated within a closed circuit is spatially quarantined within the connected component of the infected device. Due to the stationarity of the PPP, there is no loss of generality to assume that the infection originates at the device located at the origin. Hence, it is sufficient to prove that the origin is surrounded by a closed circuit to prove that the ISG operates in the subcritical regime. The coupling between the hexagonal lattice $\mathcal{L}_h$ and the ISG $\mathcal{I}$ is formally stated and proved in the following lemma.

Lemma 2 (Hexagonal Lattice Coupling): Let $K_{\mathcal{I}}(0) \subseteq \mathcal{I}(\Xi, \mathcal{E})$ and $K_{\mathcal{L}_h}(0) \subseteq \mathcal{L}_h$ denote connected components around the origin in, respectively, the ISG $\mathcal{I}$ and the hexagonal lattice $\mathcal{L}_h$. If $K_{\mathcal{L}_h}(0)$ is surrounded with closed circuit $\mathcal{C}(0)$ in $\mathcal{L}_h$, then $K_{\mathcal{I}}(0)$ is finite.

Proof: A closed circuit around the origin implies a finite number of open faces on the inner side of the circuit. Consequently, $|K_{\mathcal{L}_h}(0)| < \infty$ and the region covered by $K_{\mathcal{L}_h}(0)$ involves a finite number of vertices of $\mathcal{I}(\Xi, \mathcal{E})$. Hence, to prove that $K_{\mathcal{I}}(0)$ is finite, it is sufficient to prove that no edge of $\mathcal{I}(\Xi, \mathcal{E})$ crosses $\mathcal{C}(0)$. Let us consider an extreme scenario for the closed face with the worst spatial setup for the three firewalls and IoT/CPS devices, shown in Fig. 3(a). In particular, assume each of the triangles $\{T_i\}_{i=1}^3$ has only one firewall in the shown worst case locations such that their secured zones provide minimum protection (i.e., coverage) of the closed face. Furthermore, let us consider the most advantageous location for the IoT/CPS devices for malware infection propagation as shown in Fig. 3(a). Recall that the side of each equilateral triangle is r_r, then we have one of the following two scenarios: 1) if the two devices are within the D2D communication range of each other, then one of them should be in Θ (i.e., within the secured zone of one or more of the three spatial firewalls) and 2) if both devices are in Ξ (i.e., both of them are out of the range of the three firewalls), then they are out of the D2D communication range of each other [i.e., the condition in (4) is not satisfied]. The example shown in Fig. 3(a) shows that even in the worst case spatial setup of firewalls, an infection cannot bypass the closed face. Therefore, no edge in $\mathcal{E}$ can cross $\mathcal{C}(0)$, and hence we conclude that a finite $|K_{\mathcal{L}_h}(0)|$ leads to a finite $|K_{\mathcal{I}}(0)|$. ■

Exploiting the mapping to the hexagonal lattice and the coupling introduced in Lemma 2, we can state the main result of this section in the following proposition.

Proposition 1 (Sufficient Condition for Zero Percolation on ISG): For given $\lambda_r > 0$ and $r_r > 0$, the ISG operates in the subcritical regime (i.e., $\theta_{\mathcal{I}}(\lambda_f, r_f, \lambda_r, r_r) = 0$) if

$$\lambda_f > \frac{3.65}{r_r^2}. \tag{6}$$

Proof: Referring to the results in Lemma 2, a closed circuit $\mathcal{C}(0)$ on the hexagonal lattice $\mathcal{L}_h$ implies subcritical regime operation of the ISG $\mathcal{I}$. Based on the results in [47], the origin is almost surely (a.s.) surrounded with the closed circuit $\mathcal{C}(0)$ in $\mathcal{L}_h$ if

$$P(\mathcal{H} \text{ is closed}) > \frac{1}{2}. \tag{7}$$

From the PPP properties of the spatial firewalls, we have

$$\begin{aligned} P(\mathcal{H} \text{ is closed}) &= \mathrm{P}\left(\bigcap_{i=1,2,3} |T_i \cap \Psi| \geq 1 \right) \\ &= (1 - \mathrm{P}(|T_1 \cap \Psi| = 0))^3 \\ &= \left(1 - e^{-\lambda_f \frac{\sqrt{3}}{4} r_r^2}\right)^3. \end{aligned} \tag{8}$$

Substituting (8) back in (7), we conclude that the origin is a.s. surrounded with the closed circuit $\mathcal{C}(0)$ in $\mathcal{L}_h$ if

$$\left(1 - e^{-\lambda_f \frac{\sqrt{3}}{4} r_r^2}\right)^3 > \frac{1}{2}. \tag{9}$$

Rearranging the terms of (9) and following to the statement of Lemma 2 we conclude that there is a closed circuit $\mathcal{C}(0)$ in $\mathcal{L}_h$ if $\lambda_f > 3.65/r_r^2$. Meanwhile, the existence of $\mathcal{C}(0)$ assures $K_{\mathcal{L}_h}(0) < \infty$. Hence, $\lambda_f > 3.65/r_r^2$ is the condition that guarantees that the ISG $\mathcal{I}(\Xi, \mathcal{E})$ does not percolate, which concludes the proof of Proposition 1. ■

Before switching the discussion to the super-critical regime operation of the ISG, it is worth stating the following two important remarks.

Remark 2: It is important to note that the condition in (6) that enforces subcritical regime operation of the ISG is independent of the IoT/CPS devices intensity λ_r. This is because the proof of Proposition 1 is based on the collective ability of the secured zones to spatially quarantine malware infection within finite region. That is, the condition in (6) implies that the spatial firewalls are dense enough to construct continuous secured zones that surround any malware infection to safeguard the IoT/CPS from malware epidemic regardless of the IoT/CPS devices intensity.

Remark 3: The proof of Proposition 1 is based on the assumption that $r_r = r_f$. The case of $r_f > r_r$ also satisfies Definition 3 for the closed face. In fact, increasing r_f expands the secured zone of $\mathcal{H}$. Hence, the expression for λ_f that satisfies (7) is also sufficient for no percolation when $r_f \geq r_r$. Therefore, the proof of Proposition 1 is also valid for the case of $r_f \geq r_r$.

B. Super-Critical Regime

This section shows that insufficient deployment of spatial firewalls leads to a super-critical regime operation for the ISG, which implies that the IoT/CPS network is at a risk of malware epidemics. For a tractable analysis for the super-critical regime operation, we map the ISG to a square lattice as defined in the sequel.

Mapping to a Square Lattice: Let $\mathcal{L}_s$ be a square lattice with side $s = (r_r/\sqrt{5})$. The dual lattice $\mathcal{L}_s^d$ is a translated version of $\mathcal{L}_s$ with the translation magnitude $((s/2), (s/2))$. That is, $\mathcal{L}_s^d = \mathcal{L}_s + ((s/2), (s/2))$. Without loss of generality, it is assumed that one of the vertices of $\mathcal{L}_s^d$ is the origin. Let e denote an edge common to two adjacent squares $S_1(e)$ and $S_2(e)$ in $\mathcal{L}_s$ and e^d is the corresponding dual edge in $\mathcal{L}_s^d$. According to the spatial firewalls and IoT/CPS devices locations, the edge e can be either *open* or *closed* as defined below.

Definition 4 (Open/Closed Edge): Let $\{v_k\}_{k=1}^4$ denote vertices of a rectangle formed by the union $S_1(e) \cup S_2(e)$. Also, let $A(e)$ be the smallest square containing circles $\{C(v_k, r_f)\}_{k=1}^4$. where $C(a, r)$ denotes a circle of radius r centered at a. Then, an edge e is defined to be open if 1) each of $S_1(e)$ and $S_2(e)$ has at least one IoT/CPS device and 2) there are no firewalls within $A(e)$. Otherwise, the edge is said to be closed.

A pictorial illustration of the square lattice mapping with an open edge e is shown in Fig. 4. The rectangular lattice

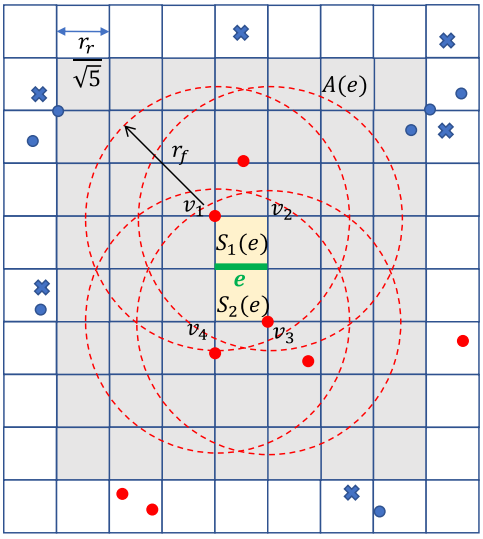


Fig. 4. Illustration of the open edge e in the square lattice $\mathcal{L}_s$, where red dots denote susceptible devices, blue dots denote protected devices, and crosses denote spatial firewalls.

mapping is chosen to define a geographical region that contains a connected component of susceptible devices in the ISG $\mathcal{I} = \{\Xi, \mathcal{E}\}$. Since $A(e)$ is free from firewalls, then the region covered by $S_1(e) \cup S_2(e)$ is located outside the secured zones of all firewalls. Furthermore, since each of $S_1(e)$ and $S_2(e)$ has at least one IoT/CPS device, then the region $S_1(e) \cup S_2(e)$ contains some vertices of Ξ. Finally, since the largest distance (i.e., the diagonal) within the region $S_1(e) \cup S_2(e)$ equals to r_r, all devices that are located within $S_1(e) \cup S_2(e)$ are within the D2D range of each other. Hence, the region defined by $S_1(e) \cup S_2(e)$ contains devices in Ξ that are all connected to each other with edges in $\mathcal{E}$. The connectivity within $S_1(e) \cup S_2(e)$ (i.e., open edge in $\mathcal{L}_s$) is also represented via an open edge in the dual lattice $\mathcal{L}_s^d$. Hence, bond percolation on the square lattice $\mathcal{L}_s^d$ implies infinite connected component in $\mathcal{I} = \{\Xi, \mathcal{E}\}$. To study bond percolation of $\mathcal{L}_s^d$, we focus on the connected component that contains the origin. As mentioned before, there is no loss in generality to focus on the origin due to the stationarity of the PPP. The coupling between the square lattice $\mathcal{L}_s^d$ and the ISG $\mathcal{I} = \{\Xi, \mathcal{E}\}$ is formally stated in the following lemma.

Lemma 3 (Square Lattice Coupling): Let $K_{\mathcal{L}_s^d}(0)$ denote a connected component in $\mathcal{L}_s^d$ containing the origin. If $K_{\mathcal{L}_s^d}(0)$ is infinite, then $K_{\mathcal{I}}(0)$ is also infinite.

Proof: Let a path $\mathcal{P}_{\mathcal{L}_s^d}$ denote a sequence of connected open edges in $\mathcal{L}_s^d$. Since there is a one-to-one mapping between dual and prime edges, $\mathcal{P}_{\mathcal{L}_s^d}$ is uniquely associated with another path $\mathcal{P}_{\mathcal{L}_s} \in \mathcal{L}_s$, in which all edges are also open. Furthermore, $\mathcal{P}_{\mathcal{L}_s}$ is associated with a unique sequence of $\{S_1(e_i), S_2(e_i)\}_{e_i \in \mathcal{P}_{\mathcal{L}_s}}$ pairs, where each pair is composed of single connected component within the ISG $\mathcal{I}$. Hence, an infinite-length path in $\mathcal{L}_s^d$ implies that there is an infinite sequence of connected susceptible devices that are members of the same connected component in $\mathcal{I}(\Xi, \mathcal{E})$. ■

By virtue of Lemma 3, it is sufficient to characterize percolation in $\mathcal{L}_s^d$ to prove the super-critical regime of the ISG $\mathcal{I}(\Xi, \mathcal{E})$. However, before delving into the analysis, it is

important to note the dependency between proximate edges, as stated in the following remark.

Remark 4 (Edge Dependencies): Since an open edge e ensures that firewalls are absent from the region $A(e)$, then the status of proximate edges are correlated. The status of two edges is independent if they do not share a common spatial region that requires the absence of spatial firewalls. Hence, the smallest distance that ensures independent edges is $2s\lceil(r_f/s)\rceil$ horizontally and $2s\lceil(r_f/s)\rceil + 2s$ vertically.

Now, we are in a position to study the super-critical regime of the ISG, which is characterized in the following proposition.

Proposition 2 (Sufficient Condition for Nonzero Percolation on ISG): For given $r_r > 0$ and $\lambda_r > 0$, the ISG operates in the super-critical regime (i.e., $\theta_{\mathcal{I}}(\lambda_f, r_f, \lambda_r, r_r) > 0$) if

$$\lambda_f < \frac{10}{N_A r_r^2} \ln\left(\frac{1 - \exp\left(-\frac{\lambda_r r_r^2}{5}\right)}{\sqrt{1-\beta}}\right) \tag{10}$$

where $\beta = ([11 - 2\sqrt{10}]/27)^N$, $N = 8ab - 2a - 6b + 1$, $N_A = ab$, $a = 2\lceil(\sqrt{5}r_f/r_r)\rceil + 2$ and $b = 2\lceil(\sqrt{5}r_f/r_r)\rceil + 1$.

Proof: To prove the proposition, we characterize the conditions which ensure that the probability of no percolation is strictly less than one. Hence, the probability of the complement event (i.e., percolation) is strictly greater than zero. As mentioned in Lemma 3, a finite $K_{\mathcal{L}_s^d}(0)$ implies no percolation on $\mathcal{L}_s^d$, which in turns implies subcritical regime of the ISG. In the following, we find the conditions that ensures that $\mathbb{P}\{|K_{\mathcal{L}_s^d}(0)| < \infty\} < 1$. Hence, such conditions also imply a nonzero probability of the complement event $\mathbb{P}\{|K_{\mathcal{L}_s^d}(0)| = \infty\} = (1 - \mathbb{P}\{|K_{\mathcal{L}_s^d}(0)| < \infty\}) > 0$. Hence, the ISG has a nonzero probability to operate in the super-critical regime.

Let $\mathcal{P}_{\mathcal{L}_s}(n)$ denote a path of length n edges $\{e_i\}_{i=1}^n \in \mathcal{L}_s$. From the coupling between the dual and primal square lattices, it can be inferred that $K_{\mathcal{L}_s^d}(0)$ is finite iff there is a closed circuit path in $\mathcal{L}_s$ around the origin. To account for the edge dependencies within the path $\mathcal{P}_{\mathcal{L}_s}(n)$, we recall from Definition 4 that the edges e_i and e_j are independent if $(A(e_i) \cap A(e_j)) = \emptyset$. Let N denote the number of edges in $A_0(e)$ and let $S_I \subseteq \mathcal{P}_{\mathcal{L}_s}(n)$ denote the subset of all independent edges in $\mathcal{P}_{\mathcal{L}_s}(n)$. Then, the set S_I has a cardinality of at least n/N. The construction of $A_0(e)$ and the computation of N are illustrated in the Appendix.

It is shown in [48] that there are $4n3^{n-2}$ possible ways to construct a circuit of length n around the origin. Therefore, the probability that a closed path exists around the origin is expressed as

$$\begin{aligned} P_c &= \sum_n 4n3^{n-2}\mathbb{P}\left\{\mathcal{P}_{\mathcal{L}_s}(n) \text{ is closed}\right\} \\ &\leq \sum_{n=1}^{\infty} 4n3^{n-2}q^{\frac{n}{N}} = \frac{4q^{\frac{1}{N}}}{3\left(1 - 3q^{\frac{1}{N}}\right)^2} \end{aligned} \tag{11}$$

where $q \equiv \mathbb{P}\{e \text{ is closed}\}$ and the last equality in (11) is obtained by treating the sum as a derivative of geometric series with respect to $q^{1/N}$. To ensure that P_c is strictly less than 1, the following condition must be satisfied:

$$q < \left(\frac{11 - 2\sqrt{10}}{27}\right)^N. \tag{12}$$

Based on Definition 4, an explicit expression for q can be found as follows:

$$\begin{aligned} q &= 1 - \mathbb{P}\{\Phi \cap S_1(e) \neq \emptyset \ \ \& \ \ \Phi \cap S_2(e) \neq \emptyset \\ &\qquad \& \ \ \Psi \cap A(e) = \emptyset\} \\ &= 1 - \left(1 - e^{-\lambda_r s^2}\right)^2 e^{-\lambda_f N_A s^2} \end{aligned} \tag{13}$$

where N_A is the number of squares covered by $A(e)$. From Fig. 4, $N_A = (2\lceil(\sqrt{5}r_f/r_r)\rceil + 2) \times (2\lceil(\sqrt{5}r_f/r_r)\rceil + 1)$. The condition in (12) ensures that $\mathbb{P}\{|K_{\mathcal{L}_s^d}(0)| < \infty\} < 1$, which implies nonzero probability of percolation. Hence, substituting (13) into (12) and after some basic algebraic manipulations, we can finally get the result in (10). ■

Remark 5: Proposition 2 shows that the super-critical regime operation, which raises the risk of malware epidemic requires both: 1) sufficiently dense IoT devices and 2) sufficiently sparse firewall deployment. More precisely, (10) shows an inverse relationship between λ_r and λ_f to allow long-range malware propagation. Hence, it may be apparent that a higher intensity of IoT/CPS devices requires a higher intensity of firewalls to spatially quarantine malware infections. However, this is only true up to the threshold shown in Proposition 1. This is because the intensity shown in Proposition 1 implies that the firewalls are dense enough such that the union of their secured zones forms continuous circles in the spatial domain that surrounds and thwarts any emerging-malware infection. Hence, the intensity of spatial firewalls shown in Proposition 1 safeguards the IoT/CPS network from malware epidemics irrespective of the IoT/CPS devices intensity.

C. Phase Transition

This section shows that the percolation probability of the ISG exhibits a phase transition property in the intensity of firewalls λ_f. Hence, the percolation critical intensity of firewalls is the unique intensity that minimizes (5). Such phase transition behavior is formally stated in the following theorem.

Theorem 1 (Phase Transition): Let $\theta_{\mathcal{I}}(\lambda_f, r_f, \lambda_r, r_r)$ denote the percolation probability of the ISG $\mathcal{I}(\Xi, \mathcal{E})$, then $\forall \lambda_r > 0$ there exists a critical value $\lambda_f^c < \infty$ for the density of firewalls such that

$$\begin{aligned} &\theta_{\mathcal{I}}\left(\lambda_f, r_f, \lambda_r, r_r\right) > 0, \quad \text{for } \lambda_f < \lambda_f^c \\ &\theta_{\mathcal{I}}\left(\lambda_f, r_f, \lambda_r, r_r\right) = 0, \quad \text{for } \lambda_f > \lambda_f^c. \end{aligned} \tag{14}$$

Proof: We start the proof by showing that the percolation probability $\theta_{\mathcal{I}}(\lambda_f, r_f, \lambda_r, r_r)$ is nonincreasing function in λ_f. Consider two sets of firewalls Ψ_1 and Ψ_2 with intensities $\lambda_{f_1} < \lambda_{f_2}$, respectively. Owing to the fact that both Ψ_1 and Ψ_2 are PPPs and that $\lambda_{f_1} < \lambda_{f_2}$, then Ψ_1 can be constructed by thinning Ψ_2 with probability $\frac{\lambda_{f_1}}{\lambda_{f_2}}$ [49, Ch. 2]. As thinning implies random removal of nodes, then $|\Psi_1 \cap \mathcal{A}| \leq |\Psi_2 \cap \mathcal{A}|$ for any $\mathcal{A} \in \mathbb{R}^2$. For the set of IoT devices Φ, the set of protected

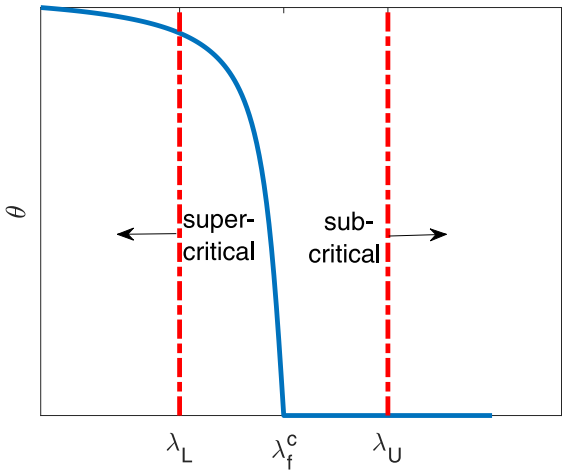


Fig. 5. Existence of critical density of firewalls.

devices is defined as $\Theta_i = \{x_k \in \Phi: \min_{a_j \in \Psi_i} \|x_k - a_j\| \leq r_f\}$ for $i \in \{1, 2\}$, and hence, $|\Theta_1 \cap \mathcal{A}| \leq |\Theta_2 \cap \mathcal{A}|$ for any $\mathcal{A} \in \mathbb{R}^2$. Now, consider two ISGs $\mathcal{I}_1 = (\Xi_1, \mathcal{E}_1)$ and $\mathcal{I}_2 = (\Xi_2, \mathcal{E}_2)$ constructed with the same parameters λ_r, r_r, and r_f but with the different sets of firewalls Ψ_1 and Ψ_2. Since $\Xi_i = \Phi \setminus \Theta_i$ for $i \in \{1, 2\}$, then $|\Xi_1 \cap \mathcal{A}| \geq |\Xi_2 \cap \mathcal{A}|$ for any $\mathcal{A} \in \mathbb{R}^2$. So, it is valid to state that $K_{\mathcal{I}_1}(0) \supseteq K_{\mathcal{I}_2}(0)$. Therefore, the condition $0 < \lambda_{f_1} < \lambda_{f_2}$ implies that $\theta_{\mathcal{I}}(\lambda_{f_1}, r_f, \lambda_r, r_r) \geq \theta_{\mathcal{I}}(\lambda_{f_2}, r_f, \lambda_r, r_r)$, and hence, $\theta_{\mathcal{I}}(\lambda_f)$ is a nonincreasing function of λ_f.

Recall that $\theta_{\mathcal{I}}(\lambda_{f_1}, r_f, \lambda_r, r_r) > 0$ for $\lambda_f < \lambda_L$ as shown in Proposition 2. Also, $\theta_{\mathcal{I}}(\lambda_{f_1}, r_f, \lambda_r, r_r) = 0$ for $\lambda_f > \lambda_U$ as shown in Proposition 1. Since $\theta_{\mathcal{I}}(\lambda_{f_1}, r_f, \lambda_r, r_r)$ is nonincreasing in λ_f, there should be a critical value λ_f^c that exhibit the phase transition indicated in (14) and depicted in Fig. 5. ■

V. Secured IoT/CPS Network Design

Section IV proves the concept of spatial firewalls. In particular, Theorem 1 shows that the phase transition critical intensity λ_f^c is the minimum intensity of firewalls that safeguards the IoT/CPS from malware epidemics. Hence, λ_f^c implies minimum deployment and licensing cost for spatial firewalls. However, as in the majority of continuum percolation models, there is no exact expression for λ_f^c. Hence, approximations and bounds are always sought. Proposition 1 shows sufficient conditions for the firewalls intensity to safeguards IoT/CPS networks from malware epidemic. However, the sufficient condition of Proposition 1 can be regarded as a loose upper bound on λ_f^c as it assumes a worst case scenario of $r_f = r_f$. Furthermore, Proposition 1 restricts the vulnerable and secured regions to hexagonal shapes. Relaxing the assumptions of Proposition 1, the following theorem presents a tight upper bound for λ_f^c, which provides an economical design of spatial firewalls. In addition, Theorem 2 gives extra parameter for manipulation of λ_f^c upper bound.

Theorem 2: Consider an IoT/CPS network with devices intensity $\lambda_r > 0$ and D2D communications range $r_r > 0$. To secure such IoT/CPS network, spatial firewalls with communication/detection range of $r_f \geq r_r$ are deployed. Then, the critical intensity of firewalls that safeguards such IoT/CPS network from malware epidemics is bounded by

$$\lambda_f^c \leq \frac{\lambda_c(1)}{4r_f^2 - r_r^2} \tag{15}$$

where $\lambda_c(1)$ is given in Remark 1.

Proof: The construction of the ISG graph is based on the interaction between the IoT/CPS devices in Φ and the firewalls in Ψ. Particularly, the devices in the ISG $\Xi = \Phi \setminus \Theta$ are the IoT/CPS devices in Φ that exists outside the secured zones of the firewalls in Ψ. Hence, Ξ and Ψ can be treated as an overlay of two nonintersecting networks: a network of firewalls and a network of susceptible devices. Let us define the vacant space $\mathcal{V} = \{x \in \mathbb{R}^2: \min_{a_j \in \Psi} \|x_k - a_j\| > r_f\}$ as all spatial regions in $\mathbb{R}^2$ that are not covered by the secured zones of the firewalls in Ψ. By virtue of the exclusive relation between $\mathcal{I} = \{\Xi, \mathcal{E}\}$ and Ψ, an infinite connected component in $\mathcal{I}$ necessitates an infinite vacant component within $\mathcal{V}$. Hence, to prove Theorem 2, we analyze the condition for the existence of an infinite vacant component (i.e., infinite continuous space) in $\mathcal{V}$. Let us consider the worst case arrangement shown in Fig. 6. The figure shows two IoT/CPS devices that are exactly r_f away from the nearest firewall and r_r away from each other. Such setup depicts the minimum vacant space W that allows for malware propagation between two IoT/CPS devices in Φ, where r_o is the minimum distance from any firewall in Ψ and W. Therefore, the minimum requirement for the existence of an infinite path in $\mathcal{I}$ corresponds to the case of having an infinite vacant component in the Poisson Boolean model [42] with the intensity λ_f and radius $r_o \equiv \sqrt{r_f^2 - (r_r^2/4)} - (\epsilon_2/2)$. Following [28], it can be shown that the critical intensity for coverage percolation of a Boolean model with secured zones of radius r is

$$\frac{\lambda_c(1)}{(2r)^2}. \tag{16}$$

Substituting the value for r_o in (16), we conclude that there is no infinite vacant component in $\mathcal{V}$ if

$$\lambda_f \geq \frac{\lambda_c(1)}{\left(2\sqrt{r_f^2 - \frac{r_r^2}{4}} - \epsilon_2\right)^2}. \tag{17}$$

Hence, the firewall intensity in (17) prohibits percolation in $\mathcal{I}$. Owing to the fact that the critical intensity is the minimum intensity of firewalls that prohibit percolation in $\mathcal{I}$ and taking the limit $\epsilon_2 \longrightarrow 0$, we finally get the upper bound in (15). ■

The results in Theorem 2 show that any firewall intensity equal to or above the threshold shown in (15) is ensured to safeguard the IoT/CPS networks from malware epidemics. Different from Theorem 1, the threshold shown in (15) accounts for the larger communication/detection range of firewalls when compared to the IoT/CPS devices. Capitalizing on Theorem 2, it is possible to prohibit malware epidemics through the design of the communication range of the IoT/CPS devices as an alternative to deploying more spatial firewalls. However, it should be noted that the communication range of the IoT/CPS devices should ensure global network connectivity. The D2D communication range that ensures both

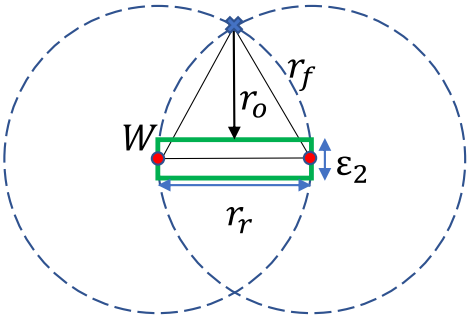


Fig. 6. Worst case scenario for existence of infinite path.

global network connectivity and prohibits malware epidemics is stated in the following corollary.

Corollary 1: For a given λ_f, r_f, and λ_r, a safeguarded wide range connectivity for the IoT/CPS network can be ensured if the D2D range satisfies the following condition:

$$\sqrt{\frac{\lambda_c(1)}{\lambda_r}} \leq r_r \leq \sqrt{4r_f^2 - \frac{\lambda_c(1)}{\lambda_f}}. \tag{18}$$

Proof: The corollary can be directly proved from Theorem 2 and IoT/CPS connectivity condition in (3). ■

The conditions in (18) ensure that the D2D communication range is sufficient for legitimate information dissemination within $G = \{\Phi, E\}$ but not for a malware epidemic outbreak on $\mathcal{I}(\Xi, \mathcal{E})$. Hence, Theorem 2 and Corollary 1 allow alternative techniques for safeguarding IoT/CPS networks, namely, through the firewalls intensity λ_f, the firewalls communication/detection range r_f, or the IoT/CPS D2D range r_r. Note that the ranges r_f and r_r can be controlled through the transmit powers and receivers sensitivities.

The results in Theorem 2 and Corollary 1 safeguard the IoT/CPS networks from malware epidemics. However, Theorem 2 and Corollary 1 do not give insights about the percentages of susceptible and secured IoT devices. Hence, an alternative design objective is to ensure that a required percentage, denoted as δ_{sec}, of the devices are secured as shown in the following corollary.

Corollary 2: The percentage of IoT/CPS devices that are protected from malware infiltration/infection is given by

$$\delta_{\text{sec}} = 1 - \exp\left(-\pi \lambda_f r_f^2\right). \tag{19}$$

Proof: By definition, a device is protected from malware infection if it falls within the secured zones of firewalls. Hence, the corollary can be directly proved from the void probability of the PPP. ■

Combining the results of Theorem 2 and Corollary 2, it can be shown that using the critical intensity of firewalls in (15) corresponds to securing the following critical percentage of IoT/CPS devices:

$$\delta_{\text{sec}}^c = 1 - \exp\left\{-\frac{\pi \lambda_c(1)}{4 - \left(\frac{r_r}{r_f}\right)^2}\right\}. \tag{20}$$

Owing to the fact that $r_f \geq r_r$ and using $\lambda_c(1) \approx 1.44$, it can be shown that δ_{sec}^c is a decreasing function in r_f which is bounded within the following range:

$$0.67 \leq \delta_{\text{sec}}^c \leq 0.78 \tag{21}$$

where the upper limit corresponds to $r_f = r_r$ and the lower limit corresponds to the $r_f \gg r_r$. Note that δ_{sec} approaches the lower limit rapidly with increasing r_f, which appears within a quadratic term inside the exponential function.

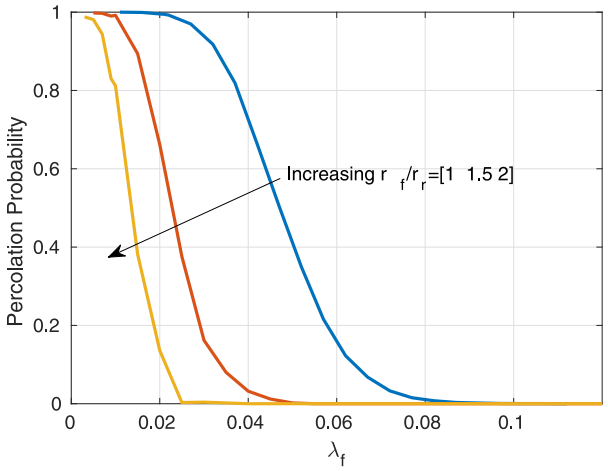


Fig. 7. Phase transition.

Remark 6: The results in Theorems 2 and (21) show that lower values of r_f necessitate higher intensity of firewalls to safeguard the IoT/CPS network. That is, lower values of r_f requires protecting at most 10% more IoT/CPS devices to safeguard the IoT/CPS network from malware epidemics.

The results in (20) and (21) also show the percentage of devices that are required to be secured by spatial firewalls to safeguard the IoT/CPS networks from malware epidemics.

VI. Numerical and Simulation Results

The simulation of the IoT/CPS network is implemented in MATLAB. In each simulation run, two independent PPPs with intensities λ_f device/m^2 for firewalls and λ_r device/m^2 for IoT/CPS devices are scattered over a square region of size 100×100 m^2. The set of protected devices Θ and the set of susceptible devices Ξ are first identified based on the distances between the IoT/CPS devices and firewalls. The ISG $\mathcal{I}(\Xi, \mathcal{E})$ is then constructed based on the D2D communication range among the susceptible devices in Ξ. Percolation is declared on $\mathcal{I}(\Xi, \mathcal{E})$ if it contains a connected component that spans the simulation region from left to right and from bottom to top. Percolation probability is then calculated by averaging over several realizations of the Monte Carlo simulations. The unit of λ_r, λ_f, and λ_f^c in all the figures is device per square meter.

Fig. 7 shows the percolation probability versus the intensity of firewalls for $r_r = 2$ m and $\lambda_r = 0.8$ device/m^2. Recall that the critical density, λ_f^c appears at the point where percolation probability drops to 0 for the first time. The figure shows a phase transition in the percolation probability, which verifies Theorem 1. The figure also highlights the positive impact of firewall communication/detection range r_f. Increasing r_f reduces the critical intensity that is required to safeguard the IoT/CPS network from malware epidemics.

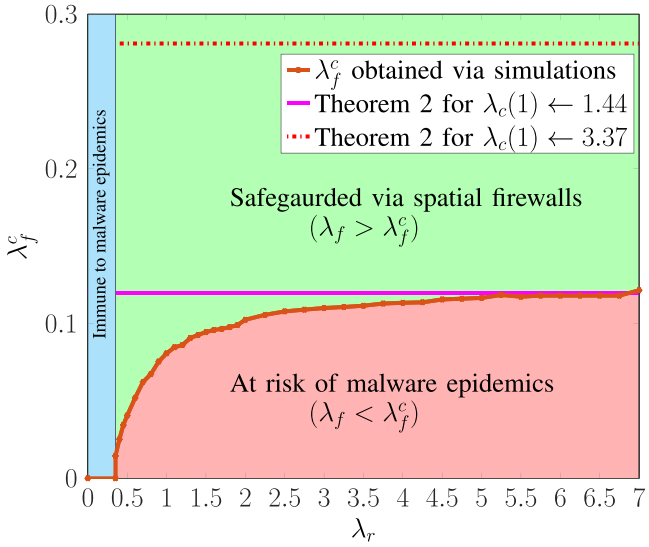


Fig. 8. Critical intensity of firewalls versus the intensity of IoT/CPS devices.

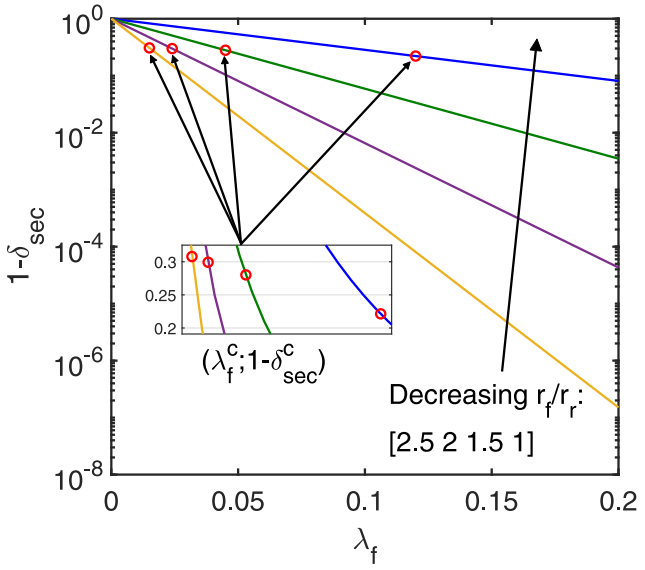


Fig. 9. Percentage of susceptible devices versus different values of λ_f [using $\lambda_c(1) \approx 1.44$].

Fig. 8 plots the critical intensity of firewalls λ_f^c (obtained via simulations) versus the intensity of IoT/CPS devices. The figure also depicts the upper bounds in Theorem 2 for different values of $\lambda_c(1)$. The figure clearly shows the three regions of operation for the IoT/CPS network. The first region is characterized by small values of λ_r such that the network lacks long range multihop wireless connectivity, and hence, is physically immune to malware epidemics. The second region is when the intensity of IoT/CPS is sufficiently high for global network connectivity while the intensity of firewalls is not sufficient (i.e., $\lambda_f < \lambda_f^c$), and hence, the network is at risk of malware epidemics. The last region is where sufficiently dense spatial firewalls are deployed (i.e., $\lambda_f \geq \lambda_f^c$), and hence, the network is safeguarded from malware epidemics.

Fig. 8 also shows that as the intensity of IoT/CPS devices increase, denser firewalls deployment is required to prohibit malware epidemics. However, the required intensity for firewalls saturates at the upper bound indicated in Theorem 2, which validates our analysis. That is, the figure confirms that there exists a finite intensity of firewalls λ_f that safeguards the IoT/CPS network from malware epidemics regardless of the intensity of IoT/CPS devices. It is worth noting that the upper bound in (15) depends on the approximate value of $\lambda_c(1)$. Hence, the figure also shows (15) when using the upper bound on $\lambda_c(1)$ provided in Remark 1, which provides a safety margin against malware epidemics. Note that operating with such safety margin increases the critical percentage of protected devices from the range shown in (21) to $0.92 \leq \delta_{\text{sec}}^c \leq 0.97$ depending on the relative value of r_f compared to r_r.

Fig. 9 shows the percentage of susceptible devices, i.e., $(1-\delta_{\text{sec}})$, for different values of λ_f and r_f/r_r. On the same figure, we also highlight the critical percentage $1-\delta_{\text{sec}}^c$, i.e., the complement of (20), which shows the percentage of susceptible devices when operating at the critical intensity λ_f^c derived in Theorem 2. First, the figure illustrates the range of δ_{sec}^c presented in (21) and shows the fast convergence of δ_{sec}^c to the upper limit 0.78. The figure also depicts the high impact of r_f on the network design and performance. For instance, at $\lambda_f = 0.1$ device/m^2 increasing r_f to twice r_r leads to more than tenfold decrease in the percentage of susceptible devices. Furthermore, doubling r_f also leads to around 4 times reduction in the critical intensity of firewalls required to safeguard the IoT/CPS devices. The figure also shows the costs, in terms of λ_f and r_f, that are required to protect more devices beyond the required critical percentage δ_{sec}^c.

VII. Summary and Conclusion

The IoT is intrinsically vulnerable to large-scale malware attacks, where malware infiltrated to one device represents an infection threat to a large population of devices. To safeguard the IoT from malware epidemics, spatial firewalls are randomly deployed in the network to detect and thwart emerging-malware infections. Each firewall imposes a secured zone, determined by its wireless connectivity, that protects its proximate devices from malware infection. Mapping the network to an RGG and using tools from percolation theory, we develop a novel mathematical framework to assess and design spatial firewalls. In particular, we define the ISG to assess the risk of a malware outbreak (i.e., epidemic). We prove that the connectivity of the ISG exhibits a phase transition, where there exists a critical intensity of firewalls that prohibit the formation of a giant-connected component within the ISG. From the security perspective, the absence of a giant-connected component within the ISG eliminates the risk of long-range propagation of malware infection, and hence, safeguards the IoT from malware epidemics.

To this end, we present a flexible design paradigm for the firewalls to safeguard the IoT. For instance, we find a tight upper bound for the critical intensity of spatial firewalls required to safeguard the IoT from malware epidemics. We also characterize the relative communications ranges of the firewalls and the IoT devices that allow secure global network connectivity. In addition, we specify the percentage

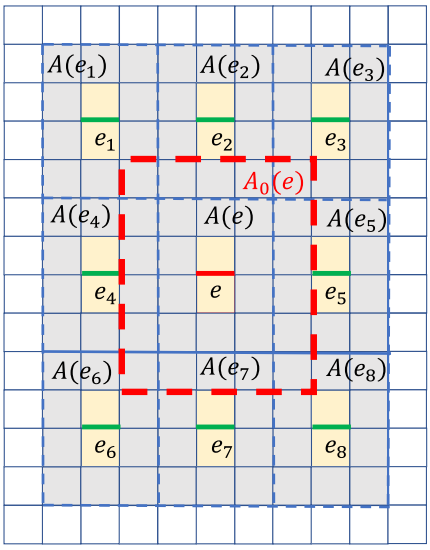


Fig. 10. Example of edge dependency region $A(e)$: $a = 4$ and $b = 3$.

of secured devices that corresponds to the critical intensity of spatial firewalls. The results show that the required density of spatial firewalls significantly decreases as we increase the relative communication range of the spatial firewalls when compared to the IoT devices. It is also shown that securing 67%–78% of the IoT devices via firewalls is sufficient to safeguard the IoT network from malware epidemics, where the required percentage of secured IoT devices decreases as the communication range of the spatial firewalls increases.

APPENDIX

MAXIMUM NUMBER OF DEPENDENT EDGES

This appendix illustrates how to find general expression for the maximum number of edges N that are dependent of some arbitrary edge e. We assume that all edges in the lattice have dependency region $A(\cdot)$ of general size $a \times b$ squares. According to the definition of dependency region, any two edges e_i and e_j are considered independent iff $(A(e_i) \cap A(e_j)) = \emptyset$. Therefore, let $\{e_n\}_{n=1}^{8}$ be the eight closest edges which dependency regions $\{A(e_i)\}_{i=1}^{8}$ do not overlap with $A(e)$. Next, we should construct maximal rectangle around e such that created region $A_0(e)$ does not include $\{e_i\}_{i=1}^{8}$. Hence, we can be sure that $A_0(e)$ covers maximal number of edges that are dependent of e. For illustrative purposes, a toy example of edge dependency problem is given in Fig. 10. By construction, the size of $A_0(e)$ is $(2a-2) \times (2b-1)$. Hence, the number of edges in $A_0(e)$ is

$$N = (2a-1)(2b-1) + (2a-2)2b = 8ab - 2a - 6b + 1. \tag{22}$$

For the scenario in Proposition 2, the dimensions of $A(e)$ are

$$a = 2\left\lceil \frac{\sqrt{5} r_f}{r_r} \right\rceil + 2 \quad \text{and} \quad b = 2\left\lceil \frac{\sqrt{5} r_f}{r_r} \right\rceil + 1.$$

Substituting these values in (22) leads to the final result of N.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[2] A. Hoglund *et al.*, "Overview of 3GPP release 14 enhanced NB-IoT," *IEEE Netw.*, vol. 31, no. 6, pp. 16–22, Nov./Dec. 2017.

[3] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[4] K. S. Ali, H. ElSawy, M. Haenggi, and M. Alouini, "The effect of spatial interference correlation and jamming on secrecy in cellular networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 4, pp. 530–533, Aug. 2017.

[5] M. A. Kishk and H. S. Dhillon, "Stochastic geometry-based comparison of secrecy enhancement techniques in D2D networks," *IEEE Wireless Commun. Lett.*, vol. 6, no. 3, pp. 394–397, Jun. 2017.

[6] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2734–2771, 3rd Quart., 2019.

[7] M. A. Kishk and H. S. Dhillon, "Coexistence of RF-powered IoT and a primary wireless network with secrecy guard zones," *IEEE Trans. Wireless Commun.*, vol. 17, no. 3, pp. 1460–1473, Mar. 2018.

[8] I. Agadakos *et al.*, "Jumping the air gap: Modeling cyber-physical attack paths in the Internet-of-Things," in *Proc. Workshop Cyber Phys. Syst. Security Privacy*, 2017, pp. 37–48.

[9] Y. Hayel and Q. Zhu, "Epidemic protection over heterogeneous networks using evolutionary Poisson games," *IEEE Trans. Inf. Forensics Security*, vol. 12, pp. 1786–1800, 2017.

[10] M. J. Farooq and Q. Zhu, "Modeling, analysis, and mitigation of dynamic botnet formation in wireless IoT networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 2412–2426, 2019.

[11] X. Liu, M. Zhao, S. Li, F. Zhang, and W. Trappe, "A security framework for the Internet of Things in the future Internet architecture," *Future Internet*, vol. 9, no. 3, p. 27, 2017.

[12] M. Nekovee, "Worm epidemics in wireless ad hoc networks," *New J. Phys.*, vol. 9, no. 6, p. 189, 2007.

[13] J. Kleinberg, "Computing: The wireless epidemic," *Nature*, vol. 449, no. 7160, pp. 287–288, 2007.

[14] M. Nekovee, "Modeling the spread of worm epidemics in vehicular ad hoc networks," in *Proc. IEEE 63rd Veh. Technol. Conf.*, vol. 2. Melbourne, VIC, Australia May 2006, pp. 841–845.

[15] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[16] M. Hasan and S. Mohan, "Protecting actuators in safety-critical IoT systems from control spoofing attacks," in *Proc. 2nd Int. ACM Workshop Security Privacy Internet Things*, 2019, pp. 8–14.

[17] H. Darabian, A. Dehghantanha, S. Hashemi, S. Homayoun, and K.-K. R. Choo, "An opcode-based technique for polymorphic Internet of Things malware detection," *Concurrency Comput. Pract. Exp.*, vol. 32, no. 6, p. e5173, 2020.

[18] H.-T. Nguyen, Q.-D. Ngo, D.-H. Nguyen, and V.-H. Le, "PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms," *ICT Exp.*, vol. 6, no. 2, pp. 128–138, 2020.

[19] F. Abdi, C. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Preserving physical safety under cyber attacks," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6285–6300, Aug. 2019.

[20] N. Asokan *et al.*, "SEDA: Scalable embedded device attestation," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Security*, 2015, pp. 964–975.

[21] W. Yan, A. Fu, Y. Mu, X. Zhe, S. Yu, and B. Kuang, "EAPA: Efficient attestation resilient to physical attacks for IoT devices," in *Proc. 2nd Int. ACM Workshop Security Privacy Internet Things*, 2019, pp. 2–7.

[22] H. ElSawy, M. A. Kishk, and M.-S. Alouini, "Spatial firewalls: Quarantining malware epidemics in large-scale massive wireless networks," *IEEE Commun. Mag.*, vol. 58, no. 9, pp. 32–38, Sep. 2019.

[23] L. Liu, X. Zhang, and H. Ma, "Optimal density estimation for exposure-path prevention in wireless sensor networks using percolation theory," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, Mar. 2012, pp. 2601–2605.

[24] J. Wang and X. Zhang, "3D percolation theory-based exposure-path prevention for optimal power-coverage tradeoff in clustered wireless camera sensor networks," in *Proc. IEEE Global Commun. Conf.*, Austin, TX, USA, Dec. 2014, pp. 305–310.

[25] Y. Katada, "Connectivity of swarm robot networks for communication range and the number of robots based on percolation theory," in *Proc. IEEE/SICE Int. Symp. Syst. Integr.*, Tokyo, Japan, Dec. 2014, pp. 93–98.
[26] N. Anjum, H. Wang, and H. Fang, "Percolation analysis of large-scale wireless balloon networks," *Digit. Commun. Netw.*, vol. 5, pp. 84–93, Mar. 2019.
[27] M. N. Anjum, H. Wang, and H. Fang, "Coverage analysis of random UAV networks using percolation theory," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Big Island, HI, USA, 2020, pp. 667–673.
[28] W. Ren, Q. Zhao, and A. Swami, "Connectivity of heterogeneous wireless networks," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 4315–4332, Jul. 2011.
[29] M. Yemini, A. Somekh-Baruch, R. Cohen, and A. Leshem, "The simultaneous connectivity of cognitive networks," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 6911–6930, Nov. 2019.
[30] O. Dousse, F. Baccelli, and P. Thiran, "Impact of interferences on connectivity in ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 13, no. 2, pp. 425–436, Apr. 2005.
[31] O. Dousse, M. Franceschetti, N. Macris, R. Meester, and P. Thiran, "Percolation in the signal to interference ratio graph," *J. Appl. Probab.*, vol. 43, no. 2, pp. 552–562, 2006.
[32] P. C. Pinto and M. Z. Win, "Percolation and connectivity in the intrinsically secure communications graph," *IEEE Trans. Inf. Theory*, vol. 58, no. 3, pp. 1716–1730, Mar. 2012.
[33] R. Vaze and S. Iyer, "Percolation on the information theoretic secure SINR graph: Upper and lower bounds," in *Proc. 12th Int. Symp. Model. Optim. Mobile Ad Hoc Wireless Netw. (WiOpt)*, Hammamet, Tunisia, 2014, pp. 620–627.
[34] A. Guo and M. Haenggi, "Spatial stochastic models and metrics for the structure of base stations in cellular networks," *IEEE Trans. Wireless Commun.*, vol. 12, no. 11, pp. 5800–5812, Nov. 2013.
[35] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.
[36] W. Bao and B. Liang, "Stochastic geometric analysis of user mobility in heterogeneous wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 10, pp. 2212–2225, Oct. 2015.
[37] W. Lu and M. Di Renzo, "Stochastic geometry modeling of mmWave cellular networks: Analysis and experimental validation," in *Proc. IEEE Int. Workshop Meas. Netw. (M N)*, Coimbra, Portugal, 2015, pp. 1–4.
[38] W. Lu and M. Di Renzo, "Stochastic geometry modeling of cellular networks: Analysis, simulation and experimental validation," in *Proc. 18th ACM Int. Conf. Model. Anal. Simulat. Wireless Mobile Syst.*, 2015, pp. 179–188.
[39] H. El Merabet and A. Hajraoui, "A survey of malware detection techniques based on machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, pp. 1–6, Jan. 2019.
[40] N. C. Idika and A. P. Mathur, "A survey of malware detection techniques," Dept. Comput. Sci., Purdue Univ., West Lafayette, IN, USA, Rep., 2007.
[41] A. Souri and R. Hosseini, "A state-of-the-art survey of malware detection approaches using data mining techniques," *Hum. Centric Comput. Inf. Sci.*, vol. 8, pp. 1–22, Dec. 2018.
[42] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[43] M. Haenggi, J. G. Andrews, F. Baccelli, O. Dousse, and M. Franceschetti, "Stochastic geometry and random graphs for the analysis and design of wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 7, pp. 1029–1046, Sep. 2009.
[44] R. Meester and R. Roy, *Continuum Percolation*. New York, NY, USA: Cambridge Univ. Press, 1996.
[45] J. Quintanilla, S. Torquato, and R. M. Ziff, "Efficient measurement of the percolation threshold for fully penetrable discs," *J. Phys. A, Math. Gen.*, vol. 33, no. 42, pp. L399–L407, Oct. 2000.
[46] Z. Kong and E. M. Yeh, "Characterization of the critical density for percolation in random geometric graphs," in *Proc. IEEE Int. Symp. Inf. Theory*, Nice, France, Jun. 2007, pp. 151–155.
[47] B. Bollobas and O. Riordan, *Percolation*. Cambridge, U.K.: Cambridge Univ. Press, 2006.
[48] G. Grimmett, *Percolation*. Heidelberg, Germany: Springer, 1980.
[49] M. Haenggi, *Stochastic Geometry for Wireless Networks*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

Ainur Zhaikhan received the B.Sc. degree in electrical and electronics engineering from Nazarbayev University, Nur-Sultan, Kazakhstan, in 2018, and the M.Sc. degree in electrical engineering from the King Abdullah University of Science and Technology, Thuwal, Saudi Arabia, in 2020. She is currently pursuing the Ph.D. degree in electrical engineering with the École polytechnique fédérale de Lausanne, Lausanne, Switzerland.

Her research interests include network epidemics, percolation theory, and reinforcement learning.

Mustafa A. Kishk (Member, IEEE) received the B.Sc. and M.Sc. degrees from Cairo University, Giza, Egypt, in 2013 and 2015, respectively, and the Ph.D. degree from Virginia Tech, Blacksburg, VA, USA, in 2018.

He is a Postdoctoral Research Fellow with the Communication Theory Laboratory, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia. His current research interests include stochastic geometry, energy harvesting wireless networks, UAV-enabled communication systems, and satellite communications.

Hesham ElSawy (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Winnipeg, MB, Canada, in 2014.

He is an Assistant Professor with the Electrical Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. His research interests include statistical modeling of wireless networks, cybersecurity for the Internet of Things, stochastic geometry, and queueing analysis for wireless communication networks.

Dr. ElSawy is a recipient of the IEEE ComSoc Outstanding Young Researcher Award for Europe, Middle East, and Africa Region, in 2018. He received several academic awards during his Ph.D., including the NSERC Industrial Postgraduate Scholarship from 2010 to 2013 and the TRTech Graduate Students Fellowship from 2010 to 2014. His research is recognized by several awards, including the IEEE COMSOC Best Survey Paper Award in 2017 and the IEEE COMSOC Best Tutorial Paper Award in 2020. He is recognized as an Exemplary Reviewer by IEEE TRANSACTIONS ON COMMUNICATIONS from 2014 to 2016, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS in 2017 and 2018, and IEEE WIRELESS COMMUNICATIONS LETTERS in 2018.

Mohamed-Slim Alouini (Fellow, IEEE) was born in Tunis, Tunisia. He received the Ph.D. degree in electrical engineering from the California Institute of Technology, Pasadena, CA, USA, in 1998.

He served as a Faculty Member with the University of Minnesota, Minneapolis, MN, USA, and then with Texas A&M University at Qatar, Education City, Doha, Qatar, before joining King Abdullah University of Science and Technology, Thuwal, Saudi Arabia, as a Professor of Electrical Engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.