IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 5 May 2022, accepted 3 June 2022, date of publication 13 June 2022, date of current version 16 June 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3182243

Malware Spreading Model for Routers in Wi-Fi Networks

DUC TRAN LE[1], THONG TRUNG TRAN[2], KHANH QUOC DANG[2], REEM ALKANHEL[3], (Member, IEEE), AND AMMAR MUTHANNA[4], (Member, IEEE)

[1]NetSecITDUT Laboratory, Faculty of Information Technology, University of Science and Technology–The University of Danang, Da Nang 55000, Vietnam
[2]Faculty of Information Technology, University of Science and Technology–The University of Danang, Da Nang 55000, Vietnam
[3]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[4]Department of Applied Probability and Informatics, Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia

Corresponding author: Duc Tran Le (letranduc@dut.udn.vn)

This work was supported in part by The University of Danang, University of Science and Technology, under Project T2021-02-06; in part by the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

ABSTRACT Malware attacks have become very common in recent years. The variety and continuous improvement of malware capabilities threaten any network. Wi-Fi is also not an exception in that context. This paper proposes a model describing the spreading of malware in Wi-Fi networks using an epidemiological mathematical model. This model is built on the characteristics of encryption and authentication in Wi-Fi networks. In addition, we also consider state transitions of devices based on some assumptions about modern malware capabilities. We calculate the basic reproduction number $\boldsymbol{R}_0$ and thereby indicate the condition to limit the spread of malware. This spreading model is analyzed through numerical simulation. Besides, for the readers to have an overview of the main threats and the security capabilities of the Wi-Fi devices, we also briefly present security threats and encryption methods used in Wi-Fi.

INDEX TERMS Basic reproduction number, Wi-Fi, mathematical models, SIR model.

I. INTRODUCTION

Today, Wi-Fi, which is one type of Wireless Local Area Network (WLAN), has become a ubiquitous wireless technology widely used everywhere for data transmission and connection to the Internet [1]. Since 1997, Wi-Fi has evolved with many different features and services. The first version of Wi-Fi (also called Wi-Fi 0) based on the IEEE 802.11 family of standards provided up to 2 Mbps link speeds. Then, in turn, other versions were introduced, such as Wi-Fi 1 (IEEE 802.11b), Wi-Fi 2 (IEEE 802.11a), Wi-Fi 3 (IEEE 802.11g), Wi-Fi 4 (IEEE 802.11n), Wi-Fi 5 (IEEE 802.11ac), Wi-Fi 6 (IEEE 802.11ax with 2.4/5GHz frequencies), Wi-Fi 6E (IEEE 802.11ax with 6 GHz frequency). Many Wi-Fi standards are being used in many different fields such as 802.11h, 802.11i, 802.11ad, 802.11af, 802.11-2016, 802.11ah, 802.11ai 802.11aj, 802.11aq. IEEE 802.11 standard organization is currently developing a new amendment standard called IEEE 802.11be Extremely High Throughput (EHT) or Wi-Fi 7. This standard promises to meet the increasing requirements of services provided on the Wi-Fi platform, especially video traffic [2]–[4].

Recent statistics also show that the number of Wi-Fi users has increased very quickly, and the traffic over Wi-Fi is also forecasted to reach an impressive indicator soon. Here are some information from the Cisco Annual Internet Report for the period of 2018 - 2023 [5] and Cisco Visual Networking Index (VNI) - Forecast and Trends for the period of 2017 - 2022 [6]:

- From 2018 to 2023, the number of Wi-Fi hotspots will quadruple. By 2023, there will be almost 628 million public Wi-Fi hotspots worldwide. This figure in 2018 was 169 million.
- From 2020 to 2023, Wi-Fi 6 hotspots will increase and account for 11% of all public Wi-Fi hotspots.
- By 2023, mobile device Wi-Fi speeds will triple. The average Wi-Fi speed worldwide will increase from 30.3 Mbps in 2018 to 92 Mbps in 2023.
- By 2022, conventional networks will account for only 29% of IP traffic, while 71% will come from mobile and Wi-Fi networks.

While Wi-Fi enables convenient network connectivity, it also exposes significant security risks. Wi-Fi networks in

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

public places such as airports, amusement parks, supermarkets, or shopping malls have become the target of attackers [7]. In these locations, most Wi-Fi networks have a very low-security level. They use weak passwords or do not use any security. Some Wi-Fi owners even openly share passwords with everyone. Despite widespread awareness of public Wi-Fi's potential vulnerabilities, most people connect to it in public places [8]–[11].

In addition to the security issues that come from the user side, Wi-Fi devices themselves have many vulnerabilities [12]–[14]. Attackers can control Wi-Fi routers by leveraging vulnerabilities in configurations [15]–[17] and protocols used in routers [18]–[20].

A. WIRELESS AUTHENTICATION AND ENCRYPTION METHODS

When constructing a Wi-Fi network, it is essential to employ strong authentication and encryption mechanisms to ensure that the network may be used only by authorized users and devices.

In Wi-Fi, three primary methods of authentication are used:

- **Open authentication:** This is the most straightforward option. The end device only needs Service-Set Identifier (SSID) information used on the network. The device will be able to connect to the network as long as the SSID is known. In this process, any wireless client that attempts to access a Wi-Fi network sends a request containing the identity of the sending client for authentication and connection to the wireless access point (AP). The AP then returns an authentication frame to confirm access to the requested client, thereby completing the authentication process. The disadvantage of this approach is that the SSID is often broadcast, and the passive capturing techniques can easily reveal it.
- **Shared authentication:** It is frequently utilized in wireless LAN deployments for individuals and small businesses. This approach employs a shared key (Pre-Shared Key - PSK). This key is shared between the two parties of the connection. If they match, the device is permitted to connect to the network.
- **Extensible Authentication Protocol (EAP) authentication:** It is the most frequently employed approach by businesses. The EAP technique employs an authentication server (RADIUS - Remote Authentication Dial-in User Service) that is contacted for authentication using some credential settings.

Along with the authentication, selecting an encryption method is critical while constructing a WLAN. Wireless encryption is a procedure that secures a wireless network from attackers that try to steal sensitive data by intercepting Radio-Frequency (RF) communication. It is critical to understand the difference between authenticating onto a network and sending the encrypted traffic in that network. It is possible to connect to a network, be authenticated, and then transmit unencrypted data. There are different wireless encryption techniques available for securing a WLAN. Each wireless encryption method offers several benefits and drawbacks.

- **Wired Equivalent Privacy (WEP):** WEP became an early attempt to secure Wi-Fi networks, but as technology developed, it is clear that WEP-encrypted data is susceptible to attack. WEP employs an encryption method at the data-link layer to protect Wi-Fi from illegal access. It is performed using the symmetric Rivest Cipher 4 (RC4) algorithm to encrypt data. However, WEP has some serious weaknesses and architectural flaws: (i) There is no standard technique of distributing encryption keys: Pre-shared keys are initially configured upon installation and are rarely modified; and (ii) RC4 was designed to function in a more random environment than WEP does.
- **Wi-Fi Protected Access (WPA):** WPA is defined by IEEE as an enhancement to the 802.11 protocols that enable greater security. WPA provides stronger data encryption security than WEP because data are passed through a Message Integrity Check (MIC) with the Temporal Key Integrity Protocol (TKIP), which employs the RC4 with 128-bit keys and a 64-bit MIC to provide robust authentication and encryption.
- **Wi-Fi Protected Access 2 (WPA2):** WPA2 uses the Advanced Encryption Standard (AES), a robust wireless encryption method, and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It provides better data security and network access control than WPA. Additionally, it secures Wi-Fi connections, ensuring that only authorized users access the network.
- **Wi-Fi Protected Access 3 (WPA3):** WPA3 provides cutting-edge features to simplify Wi-Fi security and provides the capabilities necessary to support different network deployments ranging from corporate networks to home networks. It also ensures cryptographic consistency using encryption algorithms such as AES and TKIP to defend against network attacks. Additionally, it enhances network resilience by utilizing Protected Management Frames (PMF), which give an additional layer of security against forging and eavesdropping attacks. There are some important features of WPA3: secured handshake, unauthenticated encryption with Opportunistic Wireless Encryption (OWE), bigger session keys.
- **Wi-Fi Protected Setup (WPS):** WPS is a security standard used to provide access to a Wi-Fi network. While WPS supports a variety of alternative techniques, the most prevalent is the "*push button*" option. However, when used in home networks, this security standard is quite susceptible to brute force attacks.

B. WIRELESS THREATS

Numerous encryption methods used in older WLAN standards have been demonstrated to be unsafe and have been superseded by more contemporary approaches. It is certain to

happen with all encryption systems over time, as they become more widely used and as processing capacity continues to increase.

There are many issues in existing encryption methods as follows:

- Prone to password cracking attacks [21], [22]
- Associate/disassociate messages are not authenticated
- The pre-shared key is vulnerable to eavesdropping and dictionary attacks [23]
- WPA-TKIP is vulnerable to packet spoofing and decryption attacks [24]–[26]
- Vulnerabilities in TKIP allow attackers to guess the IP address of the subnet
- Hole96 vulnerability [27] makes WPA2 vulnerable to some attacks such as Denial of Service (DoS), Man-in-the-Middle (MITM)
- Weakness of 4-way handshake process in WPA2/PSK [28], [29]
- Insecure WPS Personal Identification Number (PIN) recovery [30]
- WPS flaws [18] and so on.

New encryption methods such as WPA2 and WPA3 also face several other attacks, such as Active Dictionary Attack on WPA3 [31], [32], Key Reinstallation Attack on WPA2 [33]. In addition, firmware vulnerabilities [34] are also vulnerable to weaknesses of Wi-Fi routers.

Besides the issues in encryption methods, the wireless network can also be at risk to various types of attacks, including authentication attacks, access-control attacks, availability attacks, confidentiality attacks, and integrity attacks.

- **Access Control Attacks** are launched to compromise a network by defeating WLAN access-control mechanisms such as Wi-Fi port access restrictions and AP MAC filters. Access-control attacks come in a variety of types: *WarDriving* [35] (WLANs are identified by transmitting probing requests or by monitoring web beacons); *Rogue Access Points* [36]–[38] (an attacker may install an unsecured AP or fake AP inside a firewall); *MAC spoofing* [39] (an attacker modifies a MAC address so that it seems to be an authorized access point (AP) to a host on a trusted network); *AP misconfiguration* [40]; *Ad-hoc associations* [41] (an attacker connects the host to an untrusted client to attack that client or to bypass AP security).
- **Integrity Attacks** involve changing or altering data during transmission. Wireless integrity attacks involve the transmission of forged control or data frames through a wireless network to cause wireless devices to communicate incorrectly and launch another attack, such as a denial-of-service attack. Some different types of integrity attacks are *Data-Frame Injection* [13] (constructing and transmitting bogus 802.11 frames); *WEP Injection* [42] (constructing and sending forged WEP encryption keys); *Data Replay* [43] (catching 802.11 data packets to replay them (modified) afterward); *Bit-Flipping Attacks* [44] (grabbing the packet and randomly flipping bits in the payload, then altering and delivering the payload to the user).
- **Confidentiality Attacks** attempt to capture confidential information transmitted via a wireless network, regardless of whether the system transmits data in cleartext or an encrypted format. Some different types of confidentiality attacks are *Eavesdropping* [45], [46] (eavesdropping on and decoding unsecured application traffic to get potentially sensitive data); *Evil Twin AP* [47]–[49] (spoofing an authorized AP by broadcasting the WLAN's SSID to entice users); *Honeypot AP* [50], [51] (setting an AP's SSID to be the same as that of a legitimate AP); *Session Hijacking* [52] (tampering with the network in such a way that the attacker's host seems to be the intended destination); *Masquerading* [53], [54] (pretending to be an authorized user to gain access to a system); *MITM* [55], [56].
- **Availability Attacks** disrupt the supply of services to legal users by disabling WLAN resources or by refusing users access to those resources. This attack makes wireless network services unavailable to legitimate users. Attackers can perform availability attacks in various ways: *Disassociation Attacks* [57], [58] (severing the connection between an access point and a client to make the target inaccessible to other devices); *Beacon Flood* [59] (producing hundreds of bogus 802.11 beacons to make it more difficult for clients to locate a legal access point); *Denial-of-Service* [60], [61]; *De-authenticate Flood* [62], [63] (to disconnect users from an access point by flooding clients with fake de-authenticates or disassociates); *Routing Attacks* (distributing routing information within the network).
- **Authentication Attacks** compromise Wi-Fi customers' identities, confidential information, and account credentials to gain illegal access to the network. Some different types of confidentiality attacks are *PSK Cracking* [64], [65] (using a dictionary attack to recover a WPA PSK from captured key handshake frames); Key Reinstallation Attack [66]–[68] (exploiting the four-way handshake of the WPA2 protocol).

It can be seen that Wi-Fi networks always face many threats despite continuous improvements in authentication and encryption methods. Additionally, malware attacks have arisen as a danger to Wi-Fi networks. The next subsection will briefly analyze malware attacks in Wi-Fi networks.

C. MALWARE THREAT IN WI-FI NETWORKS

As discussed above, attackers can take control of a Wi-Fi router by exploiting vulnerabilities in the configuration and protocols used in the router device. After gaining control of the Wi-Fi device, attackers can completely deploy man-in-the-middle attacks, redirecting to a malicious website to infect users, conduct denial of service, and steal personal information, causing much damage.

Today, one of the most common hijacking attacks is malware attacks [5]. The special feature of malware is that it can propagate in network environments quickly and silently.

There are many reasons for malware attacks in Wi-Fi networks becoming increasingly common:

- Most Access Points (or we usually call Routers) are always on and connected to the Internet. It is a very good chance for hackers to exploit vulnerabilities and perform attacks at any time.
- Unlike PCs, Wi-Fi routers rarely have tools to prevent malware.
- A single router may handle several devices, including a phone, a laptop, a smart home system, and even an electricity meter. It provides hackers with a variety of attack options.
- Users' interest and understanding are limited, leading to using old encryptions or setting weak passwords, even using default passwords or not using passwords for their Wi-Fi networks.
- Current malware can use many different methods to gain access to the system (for example, the ability to perform brute-force) and spread widely.
- The mesh Wi-Fi networks model [69], [70], in which routers connect and exchange data, unintentionally creates a favorable environment for malware to propagate more quickly between different Wi-Fi networks.

There has been quite a lot of malware created to attack routers. A typical example is the VPNFilter malware [71], [72]. VPNFilter is a well-known piece of router malware. Since 2016, it has infected over half a million routers and network-attached storage devices in more than 54 countries [71]. VPNFilter is extremely persistent since it may continue to harm your network even after a router is reset, and removing malware from a router requires much effort. This malware can intercept users' internet traffic and manipulate the pages the user visits. It has a destructive capacity that makes infected devices inoperable, and it may be activated on specific victim PCs.

Additionally, it can disable internet access for over a thousand victims linked to the network on a global scale. Once launched on the router, VPNFilter can disable it, gather data from systems connected to the network, and restrict network traffic. Many routers from different vendors are affected by this malware attack, such as Asus, ZTE, Netgear, D-link, MikroTik, TP-link, Huawei, Ubiquiti.

Another type of malware with greater danger than VPNFilter is the Emotet trojan. For example, the new malware, Emotet [73], is fully capable of brute-forcing authentication and rapidly propagating between routers, resulting in catastrophic effects. Emotet initiates the infection process by infecting a host. The malware then downloads and runs the Wi-Fi spreader module. After that, this module enumerates all enabled Wi-Fi devices. It then generates a list of reachable wireless networks. Afterward, the module conducts brute-force operations against each identified Wi-Fi network. If this effort is successful, a second brute-force attempt is launched to guess the login credentials for devices connected to the hacked Wi-Fi network [74].

A few years ago, a research team from the University of Liverpool identified a malware called Chameleon [75]. It spreads "*as efficiently as the common cold between humans*" over Wi-Fi in densely populated places. Chameleon is designed to attack APs that utilize default passwords, do not need passwords, or have insufficient encryption measures. Once an access point has been compromised, an attacker may simply discover the login details of the connected devices then use them to continue their attack. Chameleon spreads mostly unnoticed because it affects wireless networks rather than PCs or phones, where security tools might identify strange behavior. Chameleon signals the dawn of a new era of technological viruses, for which we should prepare.

In addition, many other types of malware can attack and spread in Wi-Fi networks, such as Agent Tesla [76], Switcher [77], Worm [78], Botnet [79], [80], Backdoor [81], Trojan [82].

As seen in the above investigation, preventing malware from propagating over the network is critical. Numerous factors affect this process. To mitigate malware's impact and prevent it from propagation over the network, a malware spreading model adapted to the characteristics of each network type is necessary. There are different models of spreading, which will be described in further depth in the next section. However, most current spreading models use only three epidemiological states: Susceptible-Infectious-Recovered (SIR) for the routers.

Additionally, recent malware has plenty of capabilities and may result in different states of Wi-Fi routers rather than just three states above. Which states must we consider? How does the state transition in the network occur? What is the impact of the encryption and authentication characteristics in Wi-Fi on the state transition? To address these concerns, we propose a malware spreading model based on the features of the employed authentication and encryption techniques of Wi-Fi and malware behaviors. Our primary contributions are as follows:

- Analyze and reviewing the security issues and threats, especially malware attacks on Wi-Fi networks.
- Propose a mathematical model describing the spread of malware in a Wi-Fi network based on several possible states caused by malware and based on encryption methods and the complexity level of passwords in the encryption methods.
- Provide the method for calculating the fundamental reproduction number $\boldsymbol{R}_0$ and analyzing the stability of malware-free and endemic equilibrium. $\boldsymbol{R}_0$ showed whether the malware spreading process will be diminished or remain robust over time.
- Indicate the spreading conditions and control conditions for the spread of malware in Wi-Fi. The main solution for limiting the spread of malware is to use new encryptions methods such as WPA2/WPA3 and increase the complexity of passwords.

The rest of the paper is organized as follows: In section 2, we briefly review related studies. Section 3 presents the fundamental of the SIR model. In section 4, we detail the proposed mathematical model and analyze that model. Section 5 evaluates the proposed model using numerical simulation. Section 6 includes the conclusions and the proposed model's shortcomings.

II. RELATED WORKS

Malware spreading models have been of interest for quite some time. Various models have been proposed for many types of networks, such as models for wireless sensor networks [83]–[86], peer-to-peer network [87], IoT networks [88], [89], Vehicular Ad-hoc Network (VANET) [90], [91], mobile network [92], heterogeneous networks [93], [94], scale-free networks [95]–[98] etc. Most of these models are mathematical models based on epidemiological models, in which the population (by whom the infectious disease is spread) is classified according to the disease's features, for example, susceptible, infectious, recovered.

There have been few studies considering the spread of malware in the Wi-Fi network until now. The first study referring to malware epidemiology in Wi-Fi networks is done by Hao Hu et al. in [99]. In that paper, they built an epidemiological model that considers the routers' common security weaknesses. They simulated the malware spreading on real-world data collected from Wireless Geographic Logging Engine (WiGLE) website for georeferenced wireless routers. This pure SIR model considers the strong and weak forms of authentication and encryption methods: WEP, WPA, and no password. They developed the spreading model using an approach similar to that used in epidemic modeling. Each individual (i.e., each router) is classified according to the phase of the infection. There basic levels (classes) of encryption and authentication were considered: routers without encryption are grouped to the first category of susceptible class S; routers using the WEP encryption method are grouped to the second category of the susceptible class denoted S_{WEP}; and routers using the WPA encryption method correspond to the removed class R. This paper highlighted a real concern about the malware propagation in Wi-Fi.

In the paper [100], Shan Bowei built an epidemiology model to describe the spread of malware on Wi-Fi networks. This study also used the SIR model and built a transition diagram based on three classes: routers with no encryption and no strong password, routers with no encryption but with a strong password, routers with WEP encryption. The author considered attack rates according to different sizes of Wi-Fi networks. However, there were no details about the model, its appearance, and how to compute important parameters of that model. The results were also not validated by any real data or simulation result.

Hamdi Kavak et al. in [101] had revisited the research [99] with real data from WiGLE at that time (December 18, 2016). This study has some findings: model predictions are dependent on the amount of Wi-Fi routers and their density; they noted that the model in [99] could not forecast current malware spread because it was only evaluated using data acquired at the time of their research; they suggested that spreading model needs to account for weaknesses in WPA encryption and the flaw in the WPS mechanism.

In [18], Amirali Sanatinia et al. employed an epidemiological methodology in conjunction with experimental war-driving measures to examine the rate of spreading infection in four different cities. This study used statistical information of encryption methods collected from large-scale Wi-Fi networks to analyze the spreading. They noted that all examined situations display significant similarities in infection and spread, despite their disparate population demographics.

In [102], Yi-Hong Du and Shi-Hua Liu constructed an epidemic spread model with three states as in the SIR model, but instead of the Recovered state, they used the Immune state. Furthermore, the authors assumed that the WPA/WPA2 encryption could be cracked with a specified probability of a successful infection. The authors also assumed that a worm could use the Kernel Density Estimation (KDE) algorithm to assist the worm in infecting the network efficiently. The performance test was carried out with raw data collected in a region in Beijing City.

From that research context, it can be seen that the Wi-Fi malware spreading models are still quite sketchy and do not consider many of the characteristics of modern malware. Some of the described models are unclear or use the collected raw data to analyze the spread of malware. These results are difficult to help us understand the propagation process and predict the impact and prevent malware effectively. Similar to epidemiology, for ''epidemics'' with such a rapid and widespread form, it is usually necessary to have a model to predict the extent of spread. We can suggest solutions to cluster, isolate, or recover infectious cases from the predicted result.

That fact motivated us to carry out this study with several specific tasks:

- It is necessary to select mathematical tools appropriate to the characteristics and scope of the Wi-Fi networks and the characteristics of the malware.
- It is necessary to build a model of malware spreading in Wi-Fi networks considering the corresponding factors as in epidemiology: infection, suspicion, isolation, recovery, re-infection, etc. This model helps predict the spreading state and suggests appropriate solutions to deal with malware.

III. SIR MODEL

In this section, we briefly present the fundamental model of epidemics, based on which we propose our malware spreading model. Kermack and McKendrick introduce this model in [103]. The model is known as the SIR model.

According to disease states, this model categorizes the people into three categories: i) (**Susceptible**) - people who are

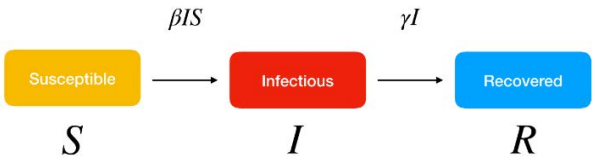

FIGURE 1. SIR spreading model.

susceptible to disease; ii) (**Infected**) - people who are infected and can distribute the disease to others; and iii) (**Removed** or **Recovered**) - people who are no longer susceptible to disease. A person cannot be infected again, and the state may only change from S –> I or I –> R (Figure 1).

The amount of individuals in each category at every moment is given by **S(t)**, **I(t)**, and **R(t)**. The entire population is assumed to be constant in the simple SIR model, which means that S(t) + I(t) + R(t) = N does not vary on t. The most concerned state is I(t): the degree of its rise or decline indicates the epidemic's proclivity.

When N is "big enough," the following set of differential equations can be used to estimate the change in the SIR model:

$$\begin{cases} \dfrac{dS}{dt} = -\beta SI \\ \dfrac{dI}{dt} = \beta SI - \gamma I \\ \dfrac{dR}{dt} = \gamma I \end{cases} \tag{1}$$

The equations reflect the rate of change of the S, I, and R according to t as a function of the system's state. The infection rate (transition from S –> I) is denoted by β. The recovery rate is denoted by γ. Therefore, the average disease period (i.e., in I state) is $1/\gamma$.

The SIR model has an essential quantity - the basic reproduction number or coefficient $\boldsymbol{R}_0$. In the simple SIR model, $\boldsymbol{R}_0 = \beta N/\gamma$. If $\boldsymbol{R}_0 > 1$, the disease will spread widely. Conversely, if $\boldsymbol{R}_0 < 1$, the disease will gradually decrease.

IV. MALWARE SPREADING SEIQ-VS MODEL IN WI-FI NETWORKS

A. NOTATION

The symbols and descriptions used in this study are summarized in Table 1.

B. PROPOSED MALWARE SPREADING MODEL FOR ROUTERS IN WI-FI NETWORKS

1) RESEARCH GAP AND MOTIVATION

As the related works section analyzed, the existing models have almost used the simple SIR model to build a spreading model for Wi-Fi networks. However, the limitation of the SIR model is that the number of states is not enough to describe the behavior of malware in the network. Modern malware has a lot of special capabilities and is constantly changing its behavior on infected systems. In [104], the author discussed common malware behavior patterns and spreading models, which include Susceptible (S), Exposed (E), Infectious (I), Recovered (R), Quarantined (Q), Vaccinated (V), and Immunized (I). As is obvious, those states match epidemiological states. We may create a variety of alternative variations of these states due to the circumstances, for example, SEIR, SIRS, SIRQ, SEIQV, and SEIQRS. The combination of those states encouraged us to develop a novel model of malware spreading across a Wi-Fi network.

While the terms **Susceptible** and **Infectious** are synonymous with those used in the epidemic model, the term **Exposed** requires additional definition. If a router in the Wi-Fi network has been infected but has not infected other devices, it belongs to this state. We suggest employing this state because several varieties of malware take advantage of Windows API calls such as *Sleepex*, *NtdelayExecution*, *GetSystemTimeSfiletime*, and *Sleep* [105] to freeze their actions on the target machine temporarily.

In this paper, we also use the **Quarantined** state to describe a possible state of a Wi-Fi router when attacked by malware. We consider that when a router device is attacked, there may be some cases such as the network speed is significantly reduced, the network connection is constantly unstable. Or, for some reason, the owner detects the hacked device and performs a router shutdown, reconfigures the router, or even installs new firmware to remove the malware. In this case, that router will not be able to spread the malware to the whole network anymore. That is why we use the Quarantined state in the proposed model.

In addition, since there are already some Wi-Fi routers equipped with antivirus firmware or software, we assume that malware will not be able to infect these routers. Therefore, we additionally use the **Vaccinated** state to describe the state of these routers. However, it should be noted that this state may change if malware has new updates that can bypass the antivirus on these routers.

Besides, because previous studies have not considered the risk of WPS attack as a factor leading to state changes of the malware spreading model and WPS has its characteristics compared to other encryption methods, we will separate the WPS enabled routers into a separate group in the **Susceptible** state.

In our model, we also consider the addition of new routers and the removal of out-of-use routers. It means the total number of routers in the network is a quantity that changes over time.

According to that analysis, we propose a malware spreading model that describes the state transitions of routers based on the malware behaviors and the characteristics of the Wi-Fi network. The model is named **SEIQ-VS**.

2) SEIQ-VS MODEL

a: FORMULATION OF MATHEMATICAL SEIQ-VS MODEL

This subsection discusses the proposed model SEIQ-VS in detail. This model works with five different states of Wi-Fi

TABLE 1. Notation.

Symbol	Description
WPAm	Routers using encryption methods *WPA2* and *WPA3*
$S_{WPS}, S_{WEP}, S_{WPA}, S_{WPAm}$	Number of routers using corresponding encryption methods *WPS, WEP, WPA, WPAm*
S_{WEAK}, S_{STRONG}	Number of routers using low-complexity and high-complexity passwords
$\beta_{WPS}, \beta_{WEP}, \beta_{WPA}, \beta_{WPAm}$	The average attack rate of malware on $S_{WPS}, S_{WEP}, S_{WPA}, S_{WPAm}$ states
$\beta_{WEAK}, \beta_{STRONG}$	The average attack rate of malware on S_{WEAK}, S_{STRONG}
N or $N(t)$	Total number of routers in the network at t
S or $S(t)$	Number of susceptible routers at t
E or $E(t)$	Number of exposed routers at t
I or $I(t)$	Number of infectious routers at t
Q or $Q(t)$	Number of quarantined routers at t
V or $V(t)$	Number of vaccinated routers at t
S_{pass}	Number of routers that are under password attack at a given time
A	The average number of new routers joining the network
a_1, a_2, a_3, a_4	The probabilities that a new router using one of the following encryption methods *WPS, WEP, WPA, WPAm*
s	The probability that a node in S_{WPS} is successfully attacked by malware
q	The probability that a node in S_{WEP} is successfully attacked by malware
r	The probability that a node in S_{WPA} is successfully attacked by malware
p	The probability that a node in S_{WPAm} is successfully attacked by malware
b	The probability of a router using a weak password
v	The probability that a node belonging to S_{WEAK} is successfully attacked by malware
u	The probability that a node belonging to S_{STRONG} is successfully attacked by malware
α	The transition rate S –> V of a router
β	The transition rate S –> E of a router
θ	The transition rate E –> I of a router
γ	The transition rate I –> Q of a router
ω	The transition rate E –> Q of a router
μ	The transition rate Q –> S of a router
η	The transition rate V –> S of a router
λ	The rate that a router is removed from the network but not due to malware
ε	The rate that a router is removed from the network due to malware
P^0	Malware-free equilibrium
P^*	Endemic equilibrium
$\boldsymbol{G}$	Next-generation matrix
$\boldsymbol{R}_0$	Basic reproduction number

routers: (i) **S** - routers are susceptible to malware infection; (ii) **E** - infected routers have not spread malware to other routers yet; (iii) **I** - infected routers are spreading the infection to other routers; (iv) **Q** - infected routers are detected and are being disconnected from surrounding routers; (v) **V** - routers are considered immune to malware or have a very high level of security.

This model is based on the following state transitions and conventions:

- Wi-Fi network is considered a large network with a significant number of routers in the network
- There are always many new routers set up in the network after a certain period
- We assume that all the routers in the network are using one of the encryption methods listed above (WEP, WPA, WPA2, WPA3, WPS). No router works with open access
- Routers using encryption methods WPA2 and WPA3 with a high level of protection are grouped in a group called ***WPAm***
- The network's overall number of routers (nodes) varies over time as new routers are deployed, and some are removed from the network
- For the routers belonging to the S state, if they use strong encryption with high complex passwords, then the speed and the probability of state transition S –> V increased
- If a router is infected by malware, it will move from state S –> E
- If a router is infected and in the E state, it will change to the I state (E –> I) at a specified rate. However, if it is discovered, it changes to quarantined (E –> Q)
- We assume that malware always takes a certain amount of time to penetrate and exploit a router, so the router will always be in an E state before it can switch to state I (E –> I), and there is no direct transition from other states to I state
- Routers become infected solely by interaction with other routers in the I state
- For routers in the I state: if malware is not detected and handled, these routers will remain in the I state. If malware is detected, those routers will enter Q state (I –> Q)
- Routers in Q state after being processed (e.g., updating firmware, using antivirus, resetting default configuration, rebooting) will return to S state (Q –> S). We suggest this transition since various types of malware can exist on Wi-Fi. Other malware is capable of infecting the router once again
- Routers in the V state can still switch to the S state (V –> S) with a specific rate because the malware can be improved and overcome the Wi-Fi-antivirus

- A router may be disconnected from the network in any of these states, although this is not due to malware. For instance, the router may be broken, and the connection fails. This rate is assumed to be constant for all states S, E, I, Q, and V. Additionally, we expect that malware may occasionally result in a loss of connectivity, even damage the router and make the router out of the network with a specific rate

Figure 2 presents the SEIQ-VS model with Wi-Fi encryption methods and different states generated by malware in the network.

In the SEIQ-VS malware spreading model, state S is divided into subclasses corresponding to the encryption methods: S_{WPS}, S_{WEP}, S_{WPA} and S_{WPAm}. In addition, each node in each of these subclasses can belong to one of two other subclasses with specific probabilities: S_{WEAK} (nodes use low-complexity passwords (can be attacked by dictionary attacks $\sim$ 65000 words)) and S_{STRONG} (nodes use high-complexity passwords (must attack with dictionaries up to millions of words)).

In the model, we use the following symbols:

- In certain other research, the quantity of routers in a particular state at a given time is sometimes symbolized as $N(t)$, $S(t)$, $I(t)$, $E(t)$, $Q(t)$, $V(t)$. In this paper, for simplicity's sake, we only use the symbols **N**, **S**, **I**, **E**, **Q**, **V**.
- A: The average number of new routers added to the network.
- a_1, a_2, a_3, a_4: the probabilities that a new router joins the network using encryption methods *WPS*, *WEP*, *WPA*, *WPAm*, respectively. Where $a_1 + a_2 + a_3 + a_4 = 1$.
- b: the probability of a node using a weak password. Thus, (*1-b*) is the probability that a node uses a strong password.
- β_{WPS}, β_{WEP}, β_{WPA}, β_{WPAm}: the average attack rate of malware on S_{WPS}, S_{WEP}, S_{WPA}, S_{WPAm} states. There are two cases: transition to E or V states from S state. It depends on the strength of the password and the attacking ability of the malware.
- s, q, r, p: the probability that a node in S_{WPS}, S_{WEP}, S_{WPA}, S_{WPAm} is successfully attacked by malware, respectively.
- v, u: the probability that a node belonging to S_{WEAK}, S_{STRONG} is successfully attacked by malware, respectively. Then there is the transition from S –> E state. Thus, (*1-v*), (*1-u*) are the probabilities that the malware will fail to attack a node belonging to S_{WEAK}, S_{STRONG}, respectively. Then there is the transition from S –> V state.
- β_{WEAK}, β_{STRONG}: the average attack rate of malware on S_{WEAK}, S_{STRONG}.
- θ: The transition rate E –> I.
- ω: The transition rate E –> Q.
- γ: The transition rate I –> Q.
- μ: The transition rate Q –> S.
- η: The transition rate V –> S.
- λ: The rate that a router is removed from the network but not due to malware.
- ε: The rate that a router is removed from the network due to malware.

It should be noted that, at any given time, only a certain number of routers in the S state are subjected to password attacks. We call the number of such routers: S_{pass}. Then we have: $S_{pass} = S - S[a_1(1-s)+a_2(1-q)+a_3(1-r)+a_4(1-p)]$.

Let $k = a_1(1-s) + a_2(1-q) + a_3(1-r) + a_4(1-p)$, we have $S_{\text{pass}} = S(1-k)$.

Based on the SIR model, the number of nodes transitioning from state S to state E in a unit of time can be found as: $(v\beta_{WEAK}S_{WEAK} + u\beta_{STRONG}S_{STRONG})\frac{I}{N} = [vb(1-k)\beta_{WEAK} + u(1-b)(1-k)\beta_{STRONG}]\frac{SI}{N}$.

Let $\beta = vb(1-k)\beta_{WEAK} + u(1-b)(1-k)\beta_{STRONG}$. Then β is the transition rate from S –> E, and the number of nodes transitioning from S –> E state is $\frac{\beta SI}{N}$.

The number of nodes transitioning from S –> V state in a unit of time is: $(1-s)\beta_{WPS}S_{WPS} + (1-q)\beta_{WEP}S_{WEP} + (1-r)\beta_{WPA}S_{WPA} + (1-p)\beta_{WPAm}S_{WPAm} + (1-v)\beta_{WEAK}S_{WEAK} + (1-u)\beta_{STRONG}S_{STRONG}$.

Let $\alpha = a_1(1-s)\beta_{WPS} + a_2(1-q)\beta_{WEP} + a_3(1-r)\beta_{WPA} + a_4(1-p)\beta_{WPAm} + b(1-v)(1-k)\beta_{WEAK} + (1-b)(1-u)(1-k)\beta_{STRONG}$. Then α is the transition rate from S –> V, and the number of nodes transitioning from S –> V is αS.

The process of changing the state of the nodes in the network is shortened, as shown in Figure 3:

From the analysis above, we can develop a system of differential equations that adequately reflects the state transitions in the SEIQ-VS model:

$$\begin{cases} S' = A - \dfrac{\beta SI}{N} - (\alpha + \lambda)S + \mu Q + \eta V \\ E' = \dfrac{\beta SI}{N} - (\omega + \theta + \lambda)E \\ I' = \theta E - (\gamma + \lambda + \varepsilon)I \\ Q' = \omega E + \gamma I - (\mu + \lambda)Q \\ V' = \alpha S - (\eta + \lambda)V \end{cases} \tag{2}$$

where derivative notation S', E', I', Q', V' are the rates of change of S, E, I, Q, V versus time:

$$\begin{cases} S' = \dfrac{dS}{dt} \\ E' = \dfrac{dE}{dt} \\ I' = \dfrac{dI}{dt} \\ Q' = \dfrac{dQ}{dt} \\ V' = \dfrac{dV}{dt} \end{cases} \tag{3}$$

N denotes the network's overall number of routers at time t:

$$N = S + E + I + Q + V \tag{4}$$

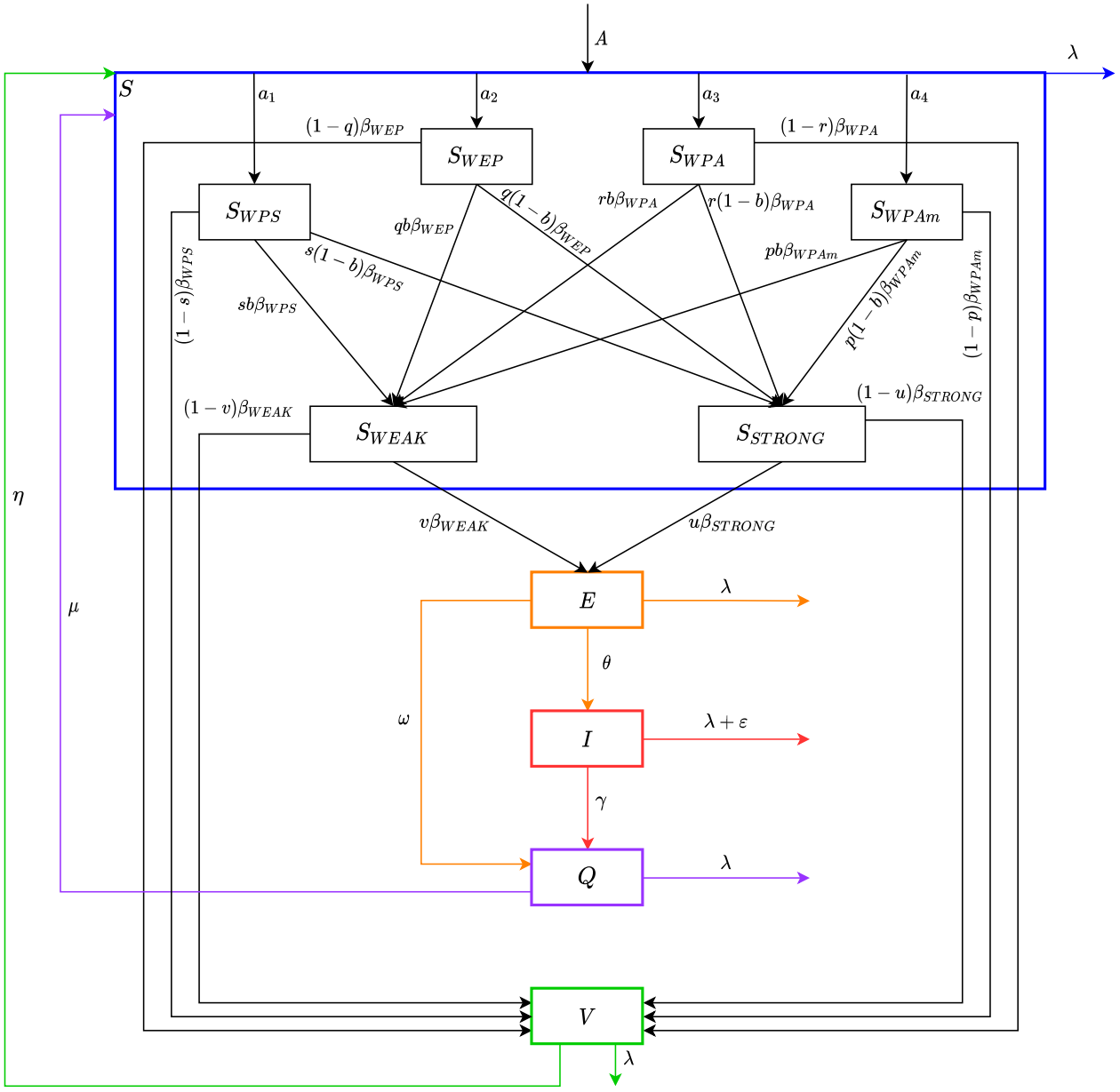

FIGURE 2. SEIQ-VS malware spreading model with different encryption methods.

By combining the equations in (2), we obtain: $(S+E+I+Q+V)' \leq A - \lambda N - \varepsilon I$. Because $0 \leq \varepsilon \leq 1$, we can obtain:

$$\frac{dN}{dt} \leq A - \lambda N \tag{5}$$

Applying the well-known Gronwall's inequality in its differential form [106] to (5), we obtain:

$$N \leq \frac{A}{\lambda} + \left(N^0 - \frac{A}{\lambda}\right) e^{-\lambda t} \tag{6}$$

where, $N^0 = S^0 + E^0 + I^0 + Q^0 + V^0$. It is an initial value $(S^0, E^0, I^0, Q^0, V^0) \in \mathcal{R}^5_+$. If $N^0 \leq \frac{A}{\lambda}$, then $N \leq \frac{A}{\lambda}$. So the region $\mathbf{\Omega} = \{(S, E, I, Q, V) : S > 0, E \geq 0, I \geq 0, Q \geq 0, V \geq 0, S + E + I + Q + V \leq \frac{A}{\lambda}\}$ is a positively invariant set for model (2). If $N^0 > \frac{A}{\lambda}$ then it turns out that $\lim_{t\to\infty} N(t) = \frac{A}{\lambda}$. Thereby, the set Ω is the globally attractive set for model (2).

From now on, we always assume that $(S^0, E^0, I^0, Q^0, V^0) \in \mathbf{\Omega}$.

b: MALWARE-FREE EQUILIBRIUM

To investigate the stability of model (2), we must first determine the malware-free equilibrium point at steady states of the SEIQ-VS model.

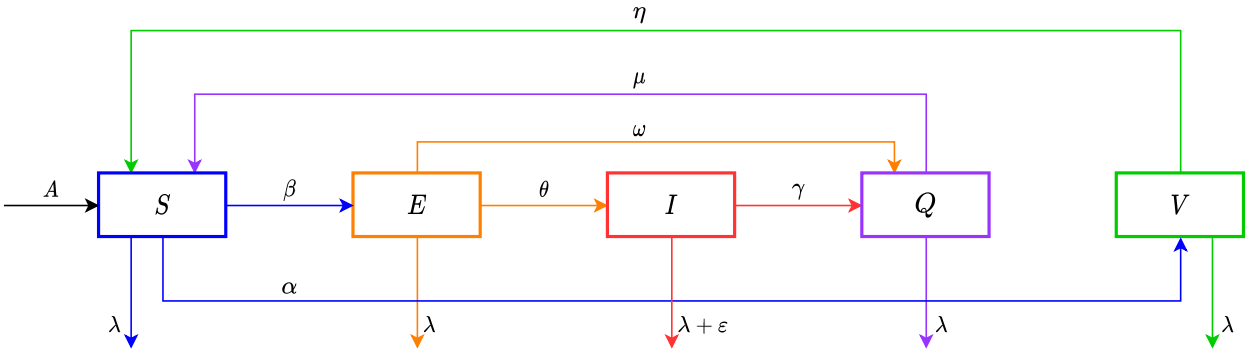

FIGURE 3. The transitions of states in the SEIQ-VS model.

Let $P^0 = (S^0, E^0, I^0, Q^0, V^0)$, with $N^0 = S^0 + E^0 + I^0 + Q^0 + V^0$, is the point at which model (2) has a malware-free equilibrium. At this state, we have $E^0 = 0, I^0 = 0, Q^0 = 0$. Then (2) becomes:

$$\begin{cases} 0 = A - \dfrac{\beta S^0 I^0}{N^0} - (\alpha + \lambda)S^0 + \mu Q^0 + \eta V^0 \\ 0 = \dfrac{\beta S^0 I^0}{N^0} - (\omega + \theta + \lambda)E^0 \\ 0 = \theta E^0 - (\gamma + \lambda + \varepsilon)I^0 \\ 0 = \omega E^0 + \gamma I^0 - (\mu + \lambda)Q^0 \\ 0 = \alpha S^0 - (\eta + \lambda)V^0 \end{cases} \tag{7}$$

Replace $E^0 = 0, I^0 = 0, Q^0 = 0$ to (7) we obtain the malware-free equilibrium point $P^0 = (S^0, E^0, I^0, Q^0, V^0) = (\frac{A(\eta+\lambda)}{\lambda(\alpha+\eta+\lambda)}, 0, 0, 0, \frac{A\alpha}{\lambda(\alpha+\eta+\lambda)})$.

Let $x = (S^*, E^*, I^*, Q^*, V^*)$. x is the malware-epidemic state of the model (2). At this state, the malware infection spreads throughout the network. Model (2) may be stated as follows:

$$\frac{dx}{dt} = \mathcal{F}(x) - \mathcal{V}(x) \tag{8}$$

where

$$\mathcal{F}(\chi) = \begin{pmatrix} 0 \\ \frac{\beta SI}{N} \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

and

$$\mathcal{V}(x) = \begin{pmatrix} -A + \frac{\beta SI}{N} + (\alpha + \lambda)S - \mu Q - \eta V \\ (\omega + \theta + \lambda)E \\ -\theta E + (\gamma + \lambda + \varepsilon)I \\ -\omega E - \gamma I + (\mu + \lambda)Q \\ -\alpha S + (\eta + \lambda)V \end{pmatrix}$$

$\mathcal{F}(x)$ is the matrix representing the rate at which new infections occur in the infection states. $\mathcal{V}(x)$ is the matrix illustrating the transition between states without regard for new infections.

Differentiating these matrices for S, E, I, Q, V and analyzing at the malware-free equilibrium $P^0 = (\frac{A(\eta+\lambda)}{\lambda(\alpha+\eta+\lambda)}, 0, 0, 0, \frac{A\alpha}{\lambda(\alpha+\eta+\lambda)})$, we will have Jacobian matrices:

$$D\mathcal{F}\left(P^0\right) = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{\beta S}{N} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$D\mathcal{V}\left(P^0\right) = \begin{pmatrix} \alpha + \lambda & 0 & \frac{\beta S}{N} & -\mu & -\eta \\ 0 & \omega + \theta + \lambda & 0 & 0 & 0 \\ 0 & -\theta & \gamma + \lambda + \varepsilon & 0 & 0 \\ 0 & -\omega & -\gamma & \mu + \lambda & 0 \\ -\alpha & 0 & 0 & 0 & \eta + \lambda \end{pmatrix}$$

c: BASIC REPRODUCTION NUMBER R_0

Now we can discover the basic reproduction number $\boldsymbol{R}_0$. The number $\boldsymbol{R}_0$ is the estimated number of secondary cases generated by a typical infective router in an entirely susceptible network. Diekmann *et al.* [107] defined $\boldsymbol{R}_0$ as the spectral radius of the next generation matrix. The next-generation matrix is defined as the square matrix $\boldsymbol{G}$ in which the ijth element of $\boldsymbol{G}$, g_{ij}, is the expected number of secondary infections of type i caused by a single infected individual of type j, again assuming that the population of type i is entirely susceptible. Each element of the matrix $\boldsymbol{G}$ is a reproduction number, but one where who infects whom is accounted for [108]. Additionally, the spectral radius of the next generation matrix is also referred to as the dominant eigenvalue of $\boldsymbol{G}$. It is worth noting that the matrix $\boldsymbol{G}$ is a non-negative matrix, which means that there will be a unique and real eigenvalue. This eigenvalue is greater than others, and it is also called $\boldsymbol{R}_0$.

Following [107], let $G = \mathcal{F}\mathcal{V}^{-1}$ is the next-generation matrix for our model, we have:

$$\boldsymbol{R_0} = \rho\left(\mathcal{F}\mathcal{V}^{-1}\right) \tag{9}$$

where $\rho(M)$ defines the spectral radius of a matrix M. From that we have:

$$\boldsymbol{R_0} = \frac{\beta S^0 \theta}{N^0(\omega+\theta+\lambda)(\gamma+\lambda+\varepsilon)} \tag{10}$$

Replace S^0 and N^0, which are calculated from (7) to (10) we have:

$$\boldsymbol{R_0} = \frac{\beta\theta(\eta+\lambda)}{(\alpha+\eta+\lambda)(\omega+\theta+\lambda)(\gamma+\lambda+\varepsilon)} \tag{11}$$

d: THE STABILITY ANALYSIS FOR EQUILIBRIUMS

The following equations describe the equilibriums of the model (2):

$$\begin{cases} A - \dfrac{\beta SI}{N} - (\alpha+\lambda)S + \mu Q + \eta V = 0 \\ \dfrac{\beta SI}{N} - (\omega+\theta+\lambda)E = 0 \\ \theta E - (\gamma+\lambda+\varepsilon)I = 0 \\ \omega E + \gamma I - (\mu+\lambda)Q = 0 \\ \alpha S - (\eta+\lambda)V = 0 \end{cases} \tag{12}$$

As is evident, for the case $E^* = 0, I^* = 0, Q^* = 0$, we obtain the malware-free equilibrium $P^0 = (S^0, E^0, I^0, Q^0, V^0) = (\frac{A(\eta+\lambda)}{\lambda(\alpha+\eta+\lambda)}, 0, 0, 0, \frac{A\alpha}{\lambda(\alpha+\eta+\lambda)})$.

Let

$$\begin{cases} \varphi_1 = \alpha+\eta+\lambda \\ \varphi_2 = \omega+\theta+\lambda \\ \varphi_3 = \gamma+\lambda+\varepsilon \end{cases} \tag{13}$$

We can obtain:

$$\begin{cases} S^* = \dfrac{\varphi_2\varphi_3}{\beta\theta} \\ E^* = \dfrac{\varphi_3 I^*}{\theta} \\ I^* = \dfrac{\lambda\left(\frac{A}{\lambda} - \frac{1}{R_0}\right)}{\frac{(\varphi_2+\mu)\varphi_3}{\theta(\mu+\lambda)} + \frac{\mu(\lambda+\varepsilon)}{\lambda(\mu+\lambda)}} \\ Q^* = \dfrac{\omega\varphi_3 + \theta\gamma}{\theta(\mu+\lambda)} I^* \\ V^* = \dfrac{\alpha\varphi_2\varphi_3}{\beta\theta(\eta+\lambda)} \end{cases} \tag{14}$$

e: STABILITY ANALYSIS OF MALWARE-FREE EQUILIBRIUM

It is trivial to demonstrate that model (2) has a malware-free equilibrium defined by $P^0 = (\frac{A(\eta+\lambda)}{\lambda(\alpha+\eta+\lambda)}, 0, 0, 0, \frac{A\alpha}{\lambda(\alpha+\eta+\lambda)})$.

Lemma 1: If $\boldsymbol{R}_0 < 1$, P^0 is locally asymptotically stable with respect to $\boldsymbol{\Omega}$. Otherwise, P^0 is unstable.

Proof of Lemma 1: With $P^0 = (\frac{A(\eta+\lambda)}{\lambda(\alpha+\eta+\lambda)}, 0, 0, 0, \frac{A\alpha}{\lambda(\alpha+\eta+\lambda)})$, the Jacobian matrix at the malware-free equilibrium P^0 in (15), as shown at the bottom of the next page.

The corresponding eigenvalues of $J\left(P^0\right)$ are real roots δ of the equation:

$$\det\left(J - \delta \boldsymbol{I}_5\right) = 0 \tag{16}$$

The left part of (16) is called characteristic polynomial, and $\boldsymbol{I}_5$ denotes the identity matrix of size 5.

After solving (16), we obtain the following eigenvalues:

$$\begin{cases} \delta_1 = -\lambda \\ \delta_2 = -(\mu+\lambda) \\ \delta_3 = -\varphi_1 \\ \delta_4 = -\left(\dfrac{\varphi_2+\varphi_3+\sqrt{(\varphi_2-\varphi_3)^2+4\theta\varphi_4}}{2}\right) \\ \delta_5 = \dfrac{\sqrt{(\varphi_2-\varphi_3)^2+4\theta\varphi_4}}{2} - \dfrac{\varphi_2+\varphi_3}{2} \end{cases} \tag{17}$$

where $\varphi_4 = \frac{\beta(\eta+\lambda)}{\alpha+\eta+\lambda}$.

According to stability theory [109], the fundamental requirement for the five-dimensional model to be asymptotically stable is that $\delta_i < 0$, for $i = 1, 2, 3, 4, 5$. It is rather obvious $\delta_1 < 0, \delta_2 < 0, \delta_3 < 0, \delta_4 < 0$. To have $\delta_5 < 0$ we must have:

$$\begin{aligned} &\frac{\sqrt{(\varphi_2-\varphi_3)^2+4\theta\varphi_4}}{2} - \frac{\varphi_2+\varphi_3}{2} < 0 \\ &\Leftrightarrow \theta\varphi_4 < \varphi_2\varphi_3 \\ &\Leftrightarrow \theta\varphi_4 < \varphi_2\varphi_3 \\ &\Leftrightarrow \frac{\beta\theta(\eta+\lambda)}{\alpha+\eta+\lambda} < (\omega+\theta+\lambda)(\gamma+\lambda+\varepsilon) \\ &\Leftrightarrow \boldsymbol{R_0} < 1 \end{aligned} \tag{18}$$

Hence, we can conclude that if (18) is satisfied or $\boldsymbol{R}_0 < 1$, P^0 is locally asymptotically stable. Otherwise, P^0 is unstable.

If $\boldsymbol{R}_0 < 1$, an infected router generates on average less than one new infected router throughout its infectious period, and the malware cannot spread. On the other hand, if $\boldsymbol{R_0} > 1$, each infected router creates more than one new infection on average, and the malware can spread across the network.

Lemma 2: When $\boldsymbol{R_0} \leq 1$, the malware-free equilibrium P^0 is globally asymptotically stable in $\boldsymbol{\Omega}$. When $\boldsymbol{R_0} > 1$, otherwise, P^0 is unstable.

Proof of Lemma 2: Let $L(S, E, I, Q, V) = I > 0$ as a Lyapunov function; then $L\left(P^0\right) = 0$. Its derivative along the solutions to the model (2) is:

$$\begin{aligned} \frac{dL}{dt}(S,E,I,Q,V) &= \theta E - (\gamma+\lambda+\varepsilon)I \\ &= \frac{\beta\theta SI}{N\varphi_2} - \varphi_3 I \\ &= \varphi_3 I\left(\frac{\beta\theta(\eta+\lambda)}{(\alpha+\eta+\lambda)(\omega+\theta+\lambda)(\gamma+\lambda+\varepsilon)} - 1\right) \\ &\times \frac{dL}{dt}(S,E,I,Q,V) = \varphi_3 I\left(\boldsymbol{R_0} - 1\right) \end{aligned} \tag{19}$$

It is obvious that, $L' = 0$ if and only if $I = 0$ or $\boldsymbol{R_0} = 1$. Thus, the largest compact invariant set in $\{(S, E, I, Q, V) \mid L' = 0\}$ is the singleton $\{P^0\}$. When $\boldsymbol{R_0} \leq 1$, the global stability of P^0 follows from LaSalle's invariance principle [110]. It implies that P^0 is globally asymptotically stable in $\boldsymbol{\Omega}$. When $\boldsymbol{R_0} > 1$, we have $L' > 0$ if $I > 0$. As a result, the lemma is proven.

f: ENDEMIC EQUILIBRIUM AND ITS STABILITY ANALYSIS

Lemma 3: If $\boldsymbol{R_0} > \frac{\lambda}{A}$, P^* is locally asymptotically stable with respect to $\boldsymbol{\Omega}$. Otherwise, P^* is unstable.

Proof of Lemma 3: We examine the local stability of the endemic equilibrium $P^* = (S^*, E^*, I^*, Q^*, V^*)$. Model (2) has the following Jacobian matrix at the endemic equilibrium P^* in (20), as shown at the bottom of the next page.

Therefore, the characteristic equation corresponding to this matrix can be expressed as:

$$\delta^5 + C_1\delta^4 + C_2\delta^3 + C_3\delta^2 + C_4\delta + C_5 = 0 \tag{21}$$

From (20) we can write the (21) as follows:

$$\begin{aligned}(\delta^2 + (\frac{\beta I^*}{N^*} + (\alpha + \lambda) + \varphi_2)\delta \\ + \varphi_2(\frac{\beta I^*}{N^*} + (\alpha + \lambda)))(\delta^2 + ((\mu + \lambda) + \varphi_3)\delta \\ + \varphi_3(\mu + \lambda))(\delta + (\eta + \lambda)) = 0\end{aligned} \tag{22}$$

The real roots δ of the equation (22) are the corresponding eigenvalues of J (P^*).

The equation (22) has five roots δ, which are: $\delta_1, \delta_2, \delta_3, \delta_4$ and δ_5. Where:

$$\begin{cases} \delta_1 + \delta_2 = -\left(\dfrac{\beta I^*}{N^*} + (\alpha + \lambda) + \varphi_2\right) < 0 \\ \delta_1\delta_2 = \varphi_2\left(\dfrac{\beta I^*}{N^*} + (\alpha + \lambda)\right) > 0 \\ \delta_3 + \delta_4 = -((\mu + \lambda) + \varphi_3) < 0 \\ \delta_3\delta_4 = \varphi_3(\mu + \lambda) > 0 \\ \delta_5 = -(\eta + \lambda) < 0 \end{cases} \tag{23}$$

From (23), we can find that $\delta_3 < 0, \delta_4 < 0$ and $\delta_5 < 0$. To have $\delta_1 < 0, \delta_2 < 0$, the following condition must be satisfied:

$\frac{\beta I^*}{N^*} + (\alpha + \lambda) > 0 \quad \Leftrightarrow \frac{\beta I^*}{N^*} > 0$

In combination with (14), we have:

$$\frac{\lambda\beta\left(\frac{A-1}{\lambda R_0}\right)}{\frac{(\varphi_2+\mu)\varphi_3}{\theta(\mu+\lambda)} + \frac{\mu(\lambda+\varepsilon)}{\lambda(\mu+\lambda)}} > 0$$

$$\Leftrightarrow R_0 > \frac{\lambda}{A} \tag{24}$$

Hence we can conclude that if $\boldsymbol{R_0} > \frac{\lambda}{A}$ then $\delta_1 < 0$ and $\delta_2 < 0$. It means P^* is locally asymptotically stable. Otherwise, P^* is unstable.

Lemma 4: If $\boldsymbol{R_0} \leq \frac{\eta+\lambda}{\varphi_1}$, P^* is globally asymptotically stable with respect to Ω. Otherwise, P^* is unstable.

Proof of Lemma 4: By employing the same proving technique as in **Lemma 2** with $P^* = (S^*, E^*, I^*, Q^*, V^*)$, we have:

$$\begin{aligned}\frac{dL}{dt}(S, E, I, Q, V) &= \frac{\varphi_1\varphi_3}{(\eta + \lambda)} I\left(\frac{\beta\theta(\eta + \lambda)S}{\varphi_1\varphi_2\varphi_3 N} - \frac{\eta + \lambda}{\varphi_1}\right) \\ &= \frac{\varphi_1\varphi_3}{(\eta + \lambda)} I\left(\boldsymbol{R}_0\frac{S}{N} - \frac{\eta + \lambda}{\varphi_1}\right)\end{aligned}$$

Model (2) is globally asymptotically stable if $\frac{dL}{dt}(S, E, I, R) \leq 0$ at $P^* = (S^*, E^*, I^*, Q^*, V^*)$. It means that we need:

$$\begin{aligned}&\frac{\varphi_1\varphi_3}{(\eta + \lambda)} I\left(\boldsymbol{R}_0\frac{S}{N} - \frac{\eta + \lambda}{\varphi_1}\right) \leq 0 \\ &\Leftrightarrow \boldsymbol{R}_0\frac{S}{N} - \frac{\eta + \lambda}{\varphi_1} \leq \boldsymbol{R}_0 - \frac{\eta + \lambda}{\varphi_1} \leq 0 \\ &\Leftrightarrow \boldsymbol{R}_0 \leq \frac{\eta + \lambda}{\varphi_1}\end{aligned} \tag{25}$$

We may summarize the above discussion as follows: if $R_0 \leq \frac{\eta+\lambda}{\varphi_1}$, the unique positive equilibrium P^* of the model (2) is globally asymptotically stable in Ω.

g: MALWARE EPIDEMIC CONTROL

Lemma 2 implies that collective efforts (as described in the formulation of $\boldsymbol{R}_0$) are capable of eradicating malware prevalence over the network. We analyze how to maintain a malware-free equilibrium in the Wi-Fi network using the SEIQ-VS propagation model.

It is easy to see that, to control and limit the spread of malware in Wi-Fi networks, we need to improve the security level, the complexity of passwords, and encryption methods. It is equivalent to the fact that we need to increase the transition rate from S –> V state. The parameter α plays a major role in this process.

From (11) and (18), we have:

$$\alpha > (\eta + \lambda)\left(\frac{\beta\theta}{(\omega + \theta + \lambda)(\gamma + \lambda + \varepsilon)} - 1\right) \tag{26}$$

where,

$$\alpha = a_1(1 - s)\beta_{WPS} + a_2(1 - q)\beta_{WEP} + a_3(1 - r)\beta_{WPA}$$

$$\mathrm{J(P^0)} = \begin{pmatrix} -(\alpha + \lambda) & 0 & -\frac{\beta S^0}{N^0} & \mu & \eta \\ 0 & -(\omega + \theta + \lambda) & \frac{\beta S^0}{N^0} & 0 & 0 \\ 0 & \theta & -(\gamma + \lambda + \varepsilon) & 0 & 0 \\ 0 & \omega & \gamma & -(\mu + \lambda) & 0 \\ \alpha & 0 & 0 & 0 & -(\eta + \lambda) \end{pmatrix} \tag{15}$$

$$+ a_4(1-p)\beta_{WPAm} + b(1-v)(1-k)\beta_{WEAK}$$
$$+ (1-b)(1-u)(1-k)\beta_{STRONG}$$

From this condition, we realize that to control the epidemic in the network, one of the solutions is to increase α. We cannot change the characteristics of malware or the capability of cracking the password of malware. Therefore, to increase, it is necessary to reduce the number of devices using weak passwords and increase the number of devices using complex passwords and high-level security encryption methods such as *WPA* and *WPAm*. It means that when we decrease *s,q,r,p* parameters, the number of routers in the V state will be increased. It is an effective way to prevent the possibility of malware from spreading in the Wi-Fi network. Because devices that use weak passwords in the S_{WEAK} are often more vulnerable than devices in the S_{STRONG}.

In addition, to prevent and limit malware from spreading more effectively, the isolation measures for nodes used in E, I states need to be considered. If inequality (26) cannot be satisfied, malware will disseminate broadly over networks.

V. NUMERICAL ANALYSIS

In this section, we use numerical simulation to analyze and illustrate different scenarios of model SEIQ-VS. We will show the change of states respectively in each scenario $\boldsymbol{R}_0 < 1$ and $\boldsymbol{R}_0 > 1$. To observe a clear difference between the two scenarios mentioned above, we use two different sets of parameters, as shown in Table 2. In addition, there are some notes in the selection of parameters as follows:

- Since the time to crack the weak password will be faster than when cracking the strong password, we have $\beta_{WEAK} > \beta_{STRONG}$ and the parameters u, v are chosen so that $u < v$.
- Because the security level of *WPS*<*WEP*<*WPA*< *WPAm*, we will have $\beta_{WPS} > \beta_{WEP} > \beta_{WPA} > \beta_{WPAm}$ and the parameters *s, q, r, p* are chosen so that $p<r<q<s$.

The difference between the two sets of parameters is mainly related to the strength of the password and the ability of malware to crack the password. In the scenario of $\boldsymbol{R}_0 > 1$, the parameter set *s, q, r, p* will increase because, at this time, the number of cracked routers will increase, leading to a decrease in the number of routers transitioning from S –> V. Besides, the time it takes for malware to attack a router is also reduced when $\boldsymbol{R}_0 > 1$ compared to the scenario $\boldsymbol{R}_0 < 1$, so β_{WEAK}, β_{STRONG} also increases in scenario 2 compared to scenario 1. The values of *b, u, v* also change according to the same logic.

TABLE 2. Different sets of parameters for the numerical analysis.

Parameters	Scenario 1: $\boldsymbol{R}_0 < 1$	Scenario 2: $\boldsymbol{R}_0 > 1$
β_{WPS}	0.15	0.15
β_{WEP}	0.1	0.1
β_{WPA}	0.05	0.05
β_{WPAm}	0.02	0.02
β_{WEAK}	0.5	0.7
β_{STRONG}	0.2	0.35
a_1	0.25	0.25
a_2	0.25	0.25
a_3	0.25	0.25
a_4	0.25	0.25
s	0.6	0.95
q	0.45	0.9
r	0.3	0.75
p	0.1	0.7
b	0.6	0.95
v	0.425	0.931
u	0.376	0.9
$\boldsymbol{N}_0$	1000	1000
A/N	0.35	0.35
θ	0.5	0.95
γ	0.174	0.174
ω	0.017	0.017
μ	0.594	0.594
η	0.1	0.1
λ	0.02	0.02
ϵ	0.03	0.03

Scenario 1 ($\boldsymbol{R}_0 < 1$): In this scenario, we set the parameters to the appropriate values to ensure that many routers use high-level security encryption methods with highly complex passwords. It ensures that the basic reproduction number is always low and the malware cannot propagate aggressively in the Wi-Fi network.

In this scenario, $\boldsymbol{R}_0 = 0.13$, the ability of malware to propagate in the network is reduced according to Lemma 1 and Lemma 2 (Figure 4). As a result, the I state tends to decline; meanwhile S state and V state increase over time. In the early stage, because the parameters *s, q, r, p* are small, the number of routers switching from S –> V state increases, while the transition rates from V –> S and Q –> S are maintained at a small level. Hence, the number of routers in the V state tends to increase initially. Then, because some routers are removed from the network (parameter λ) and due to the impact of malware, the number of routers in state V will decrease. Under the impact of malware (parameters β, θ), the number of routers switching from S –> E and E –> I began to rise. Despite this, the number of routers that are not infected with malware is still maintained at a high level because the impact of malware in this scenario is not significant.

$$\mathrm{J(P^*)} = \begin{pmatrix} -\frac{\beta I^*}{N^*} - (\alpha+\lambda) & 0 & -\frac{\beta S^*}{N^*} & \mu & \eta \\ \frac{\beta I^*}{N^*} & -(\omega+\theta+\lambda) & \frac{\beta S^*}{N^*} & 0 & 0 \\ 0 & \theta & -(\gamma+\lambda+\varepsilon) & 0 & 0 \\ 0 & \omega & \gamma & -(\mu+\lambda) & 0 \\ \alpha & 0 & 0 & 0 & -(\eta+\lambda) \end{pmatrix} \tag{20}$$

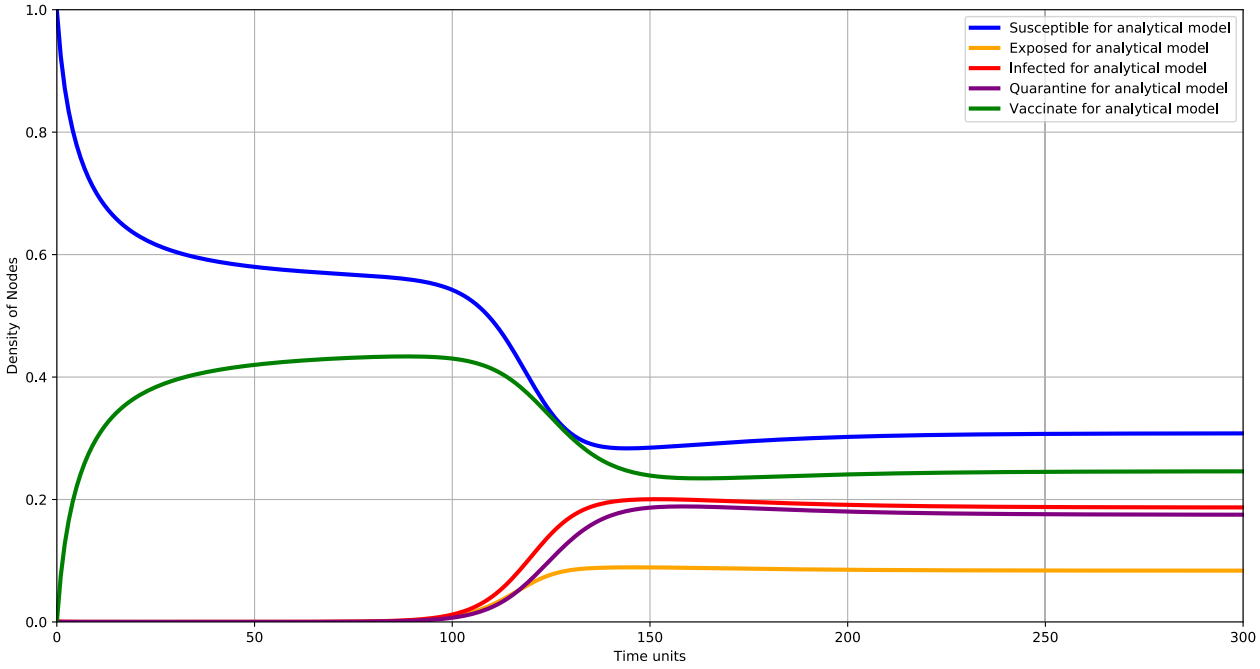

FIGURE 4. Fraction of routers in five states when $R_0 < 1$.

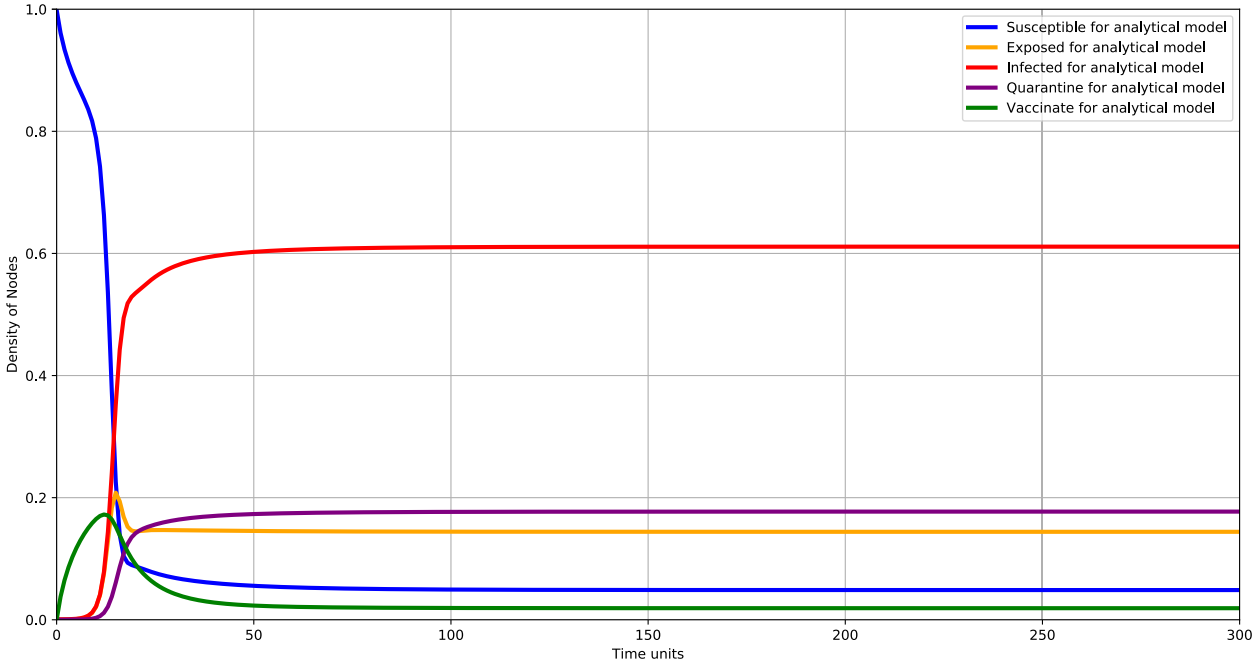

FIGURE 5. Fraction of routers in five states when $R_0 > 1$.

Scenario 2 ($\boldsymbol{R}_0 > 1$): In this scenario, we have the basic reproduction number $\boldsymbol{R}_0 = 1.62$. With $\boldsymbol{R}_0 > 1$, the ability of malware to propagate in the network increases (Figure 5). The I state tends to increase; meanwhile S state and V state decrease over time. With the set of parameters in this scenario, the malware can crack passwords faster. The number of devices using low-level security encryption methods with weak passwords increases significantly, decreasing the number of routers in the V state. At the same time, we also increased the transition rate from E –> I to ensure malware propagation in the network is stronger and faster. Under the impact of malware (the parameters β, θ increase), the number

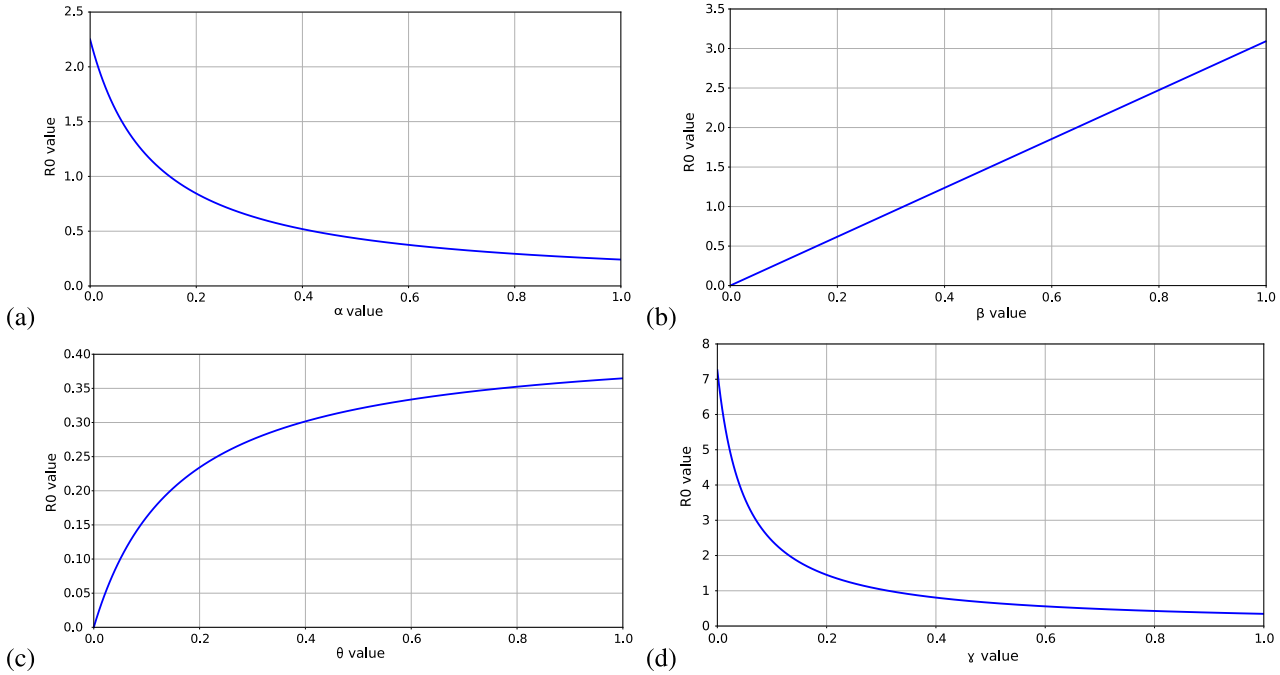

FIGURE 6. (a) Impact of transition rate from S –> V on R_0 (b) Impact of transition rate from S –> E on R_0 (c) Impact of transition rate from E –> I on R_0 (d) Impact of transition rate from I –> Q on R_0.

of routers switching from S –> E and E –> I increased significantly. The number of infected routers will remain high because the impact of the malware in this scenario is large enough. It is perfectly consistent with the above stability analysis of endemic equilibrium.

From (11), it can be seen that there are many factors affecting the change of $\boldsymbol{R}_0$. To evaluate the impact of these factors on $\boldsymbol{R}_0$ we use the same set of parameters in scenario 2 and change the necessary parameters.

Figure 6a depicts the effect of α on $\boldsymbol{R}_0$. This influence shows how to control the malware epidemic in the network. Increasing the transition rate from the S –> V state increases the ability to limit the spread of malware.

Figure 6b depicts the linear influence of parameter β on $\boldsymbol{R}_0$. The transition rate from S –> E is an important factor leading to the spread of malware in the network because it increases the number of routers that have successfully been cracked passwords.

Figure 6c depicts the change of $\boldsymbol{R}_0$ under the impact of the transition rate from E –> I state. As θ increases, $\boldsymbol{R}_0$ will also increase. However, $\boldsymbol{R}_0$ does not increase rapidly, and the impact of θ will not be as great as the impact of β because when in the E state, routers have not yet caused malware propagation; only when routers switch to the I state the process of spreading will take place.

Figure 6d demonstrates the dependence of $\boldsymbol{R}_0$ on the transition rate from I –> Q. $\boldsymbol{R}_0$ decreases rapidly as γ increases, while γ is small, $\boldsymbol{R}_0$ is greatly affected. It is completely understandable because if routers infected with malware (i.e., potentially causing the spread of malware in the network) switch to the quarantined state, they will reduce the malware threat and limit the spread of malware. From that, it can be seen that the method of isolating routers used in E, I states needs to be considered.

VI. CONCLUSION

Wi-Fi networks have become very popular. However, security issues in Wi-Fi networks have always been a big challenge. Like other types of networks, Wi-Fi networks have fallen victim to malware attacks in recent years. To analyze the impact of malware within a wide-ranging Wi-Fi network and come up with solutions to limit the impact of malware, we need to build a malware spreading model for this network. This model needs to consider the characteristics of encryption methods and the complexity of passwords used by routers in the network. Besides, it is also necessary to consider the specific characteristics of the malware in each stage of the attack. Therefore, in this paper, we proposed a mathematical SEIQ-VS model with five states: Susceptible (S), Exposed (E), Infectious (I), Quarantined (Q), and Vaccinated (V) to describe the malware spreading behavior in Wi-Fi network.

We calculated the basic reproduction number $\boldsymbol{R}_0$ to show whether the spreading of malware would be weakened ($\boldsymbol{R}_0 < 1$) or remained high over time ($\boldsymbol{R}_0 > 1$). We also provided an analysis of malware-free and endemic equilibrium stability. The analysis pointed out how to control the malware in the Wi-Fi network. We should use more routers with high-level security encryption methods and complex passwords.

However, there are still some limitations:

- The model only considered the spread between routers but did not consider the spread of malware from the client to the Wi-Fi router.

- The model is built on some assumptions, and, in some cases, it may not be suitable for real cases. This model works well in the scenario of a mesh network.
- The mathematical model was not verified by a real test case because this model requires a huge number of routers, and there is no chance of having a real test case for it.
- We ignore the case of routers that do not use any security (i.e., OPEN Wi-Fi), although there are still many such routers, especially in public places.

In future works, we will consider the spread of malware from clients to routers and consider the scenario when malware uses roaming as a way to spread in Wi-Fi networks. In addition, we will implement some ways to verify the mathematical model, for example, using an agent-based simulation environment.

ACKNOWLEDGEMENT

This work was partly supported by The University of Danang, University of Science and Technology, under Project T2021-02-06. The authors also express their gratitude to Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R323), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

REFERENCES

[1] K. Pahlavan and P. Krishnamurthy, "Evolution and impact of Wi-Fi technology and applications: A historical perspective," *Int. J. Wireless Inf. Netw.*, vol. 28, no. 1, pp. 3–19, Nov. 2020, doi: 10.1007/s10776-020-00501-8.

[2] E. Khorov, I. Levitsky, and I. F. Akyildiz, "Current status and directions of IEEE 802.11be, the future Wi-Fi 7," *IEEE Access*, vol. 8, pp. 88664–88688, 2020, doi: 10.1109/ACCESS.2020.2993448.

[3] C. Deng, X. Fang, X. Han, X. Wang, L. Yan, R. He, Y. Long, and Y. Guo, "IEEE 802.11be Wi-Fi 7: New challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2136–2166, 4th Quart., 2020, doi: 10.1109/COMST.2020.3012715.

[4] A. Garcia-Rodriguez, D. Lopez-Perez, L. Galati-Giordano, and G. Geraci, "IEEE 802.11be: Wi-Fi 7 strikes back," *IEEE Commun. Mag.*, vol. 59, no. 4, pp. 102–108, Apr. 2021, doi: 10.1109/MCOM.001.2000711.

[5] Cisco. (Mar. 2020). *Cisco Annual Internet Report (2018–2023) White Paper*. Accessed: Apr. 6, 2022. [Online]. Available: https://bit.ly/Cisco_Annual_Report_2018_2023

[6] Cisco. (Feb. 2019). *Cisco Visual Networking Index: Forecast and Trends, 2017–2022*. Accessed: Apr. 6, 2022. [Online]. Available: https://bit.ly/cisco_trends_2017_2022

[7] D. Schepers, A. Ranganathan, and M. Vanhoef, "Let numbers tell the tale," in *Proc. 14th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2021, pp. 100–105, doi: 10.1145/3448300.3468286.

[8] H. S. Choi, D. Carpenter, and M. S. Ko, "Risk taking behaviors using public Wi-Fi," *Inf. Syst. Frontiers*, pp. 1–18, Feb. 2021, doi: 10.1007/s10796-021-10119-7.

[9] C.-Y. Chiang and X. Tang, "Use public Wi-Fi? Fear arouse and avoidance behavior," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 73–81, Feb. 2020, doi: 10.1080/08874417.2019.1707133.

[10] F. Inusah, I. M. Gunu, and G. Abdul-Salaam, "Security threat and data consumption as mojor nuisance of social media on Wi-Fi network," *Int. J. Commun., Netw. Syst. Sci.*, vol. 14, no. 2, pp. 15–29, 2021, doi: 10.4236/ijcns.2021.142002.

[11] J. K. Adams, "WiFiCue: Public wireless access security assessment tool," 2019, *arXiv:1910.04325*.

[12] S. Ma, H. Li, W. Yang, J. Li, S. Nepal, and E. Bertino, "Certified copy? Understanding security risks of Wi-Fi hotspot based Android data clone services," in *Proc. Annu. Comput. Secur. Appl. Conf.*, Dec. 2020, pp. 320–331, doi: 10.1145/3427228.3427263.

[13] A. Abedi and O. Abari, "WiFi says 'Hi!' back to strangers!" in *Proc. 19th ACM Workshop Hot Topics Netw.*, Nov. 2020, pp. 132–138, doi: 10.1145/3422604.3425951.

[14] D. Schepers, M. Singh, and A. Ranganathan, "Here, there, and everywhere: Security analysis of wi-fi fine timing measurement," in *Proc. 14th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2021, pp. 78–89, doi: 10.1145/3448300.3467828.

[15] S. Viehböck, "Wi-Fi protected setup pin brute force vulnerability," CERT Vulnerability Note VU, CERT Coordination Center, Software Eng. Inst., Carnegie Mellon Univ., Pittsburgh, PA, USA, Tech. Rep. 723755, 2011.

[16] D. Costantin, K. Sansurooah, and P. A. H. Williams, "Vulnerabilities associated with Wi-Fi protected setup in a medical environment," in *Proc. Australas. Comput. Sci. Week Multiconference*, Jan. 2017, pp. 1–12, doi: 10.1145/3014812.3014872.

[17] N. Pimple, T. Salunke, U. Pawar, and J. Sangoi, "Wireless security—An approach towards secured Wi-Fi connectivity," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 872–876, doi: 10.1109/ICACCS48705.2020.9074350.

[18] A. Sanatinia, S. Narain, and G. Noubir, "Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2013, pp. 430–437, doi: 10.1109/CNS.2013.6682757.

[19] S. Alblwi and K. Shujaee, "A survey on wireless security protocol WPA2," in *Proc. Int. Conf. Secur. Manage. (SAM)*, 2017, pp. 12–17.

[20] ESET. (Feb. 2020). *Krook—CVE–2019–15126 Serious Vulnerability Deep Inside Your Wi-Fi Encryption*. Accessed: Apr. 6, 2022. [Online]. Available: https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf

[21] E. Baray and N. K. Ojha, "'WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique,"' in *Proc. 5th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, Apr. 2021, pp. 23–30, doi: 10.1109/iccmc51019.2021.9418230.

[22] H.-J. Lu and Y. Yu, "Research on WiFi penetration testing with kali Linux," *Complexity*, vol. 2021, pp. 1–8, Feb. 2021, doi: 10.1155/2021/5570001.

[23] S. Atluri and R. Rallabandi, "Deciphering WEP, WPA, and WPA2 pre-shared keys using fluxion," in *Smart Computing Techniques and Applications*. Singapore: Springer, 2021, pp. 377–385, doi: 10.1007/978-981-16-0878-0_37.

[24] D. Schepers, A. Ranganathan, and M. Vanhoef, "Practical side-channel attacks against WPA-TKIP," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Jul. 2019, pp. 415–426, doi: 10.1145/3321705.3329832.

[25] S. Domien, R. Aanjhan, and V. Mathy, "Breaking WPA-TKIP using side-channel attacks," Black Hat Eur. Briefings, London, U.K., 2019.

[26] M. Vanhoef and F. Piessens, "Practical verification of WPA-TKIP vulnerabilities," in *Proc. 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur. (ASIA CCS)*, 2013, pp. 427–436, doi: 10.1145/2484313.2484368.

[27] P. K. Singh, P. Vij, A. Vyas, S. K. Nandi, and S. Nandi, "Elliptic curve cryptography based mechanism for secure Wi-Fi connectivity," in *Distributed Computing and Internet Technology*. Bhubaneswar, India: Springer, Dec. 2018, pp. 422–439, doi: 10.1007/978-3-030-05366-6_35.

[28] C.-L. Chen and S. Punya, "Enhanced WPA2/PSK for preventing authentication cracking," in *Proc. Int. Conf. Mobile Wireless Middleware, Operating Syst., Appl.* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). Hohhot, China: Springer, 2020, pp. 156–164, doi: 10.1007/978-3-030-62205-3_15.

[29] C. C. T. Teyou and P. Zhang, "Solving downgrade and DoS attack due to the four ways handshake vulnerabilities (WiFi)," *Int. J. Eng. Manage. Res.*, vol. 8, no. 4, pp. 1–10, Aug. 2018, doi: 10.31033/ijemr.8.4.1.

[30] D. E. Goncharov, S. V. Zareshin, R. V. Bulychev, and D. S. Silnov, "Vulnerability analysis of the WiFi spots using WPS by modified scanner vistumbler," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Jan. 2018, pp. 48–51, doi: 10.1109/EIConRus.2018.8317027.

[31] M. Patel, P. Amritha, and R. S. jasper, "Active dictionary attack on WPA3-SAE," in *Advances in Computing and Network Communications* (Lecture Notes in Electrical Engineering). Singapore: Springer, 2021, pp. 633–641, doi: 10.1007/978-981-33-6977-1_46.

[32] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2020, pp. 517–533, doi: 10.1109/SP40000.2020.00031.

[33] M. A. Abo-Soliman and M. A. Azer, "A study in WPA2 enterprise recent attacks," in *Proc. 13th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2017, pp. 323–330, doi: 10.1109/ICENCO.2017.8289808.

[34] F. Schwarz, K. Schwarz, D. Fuchs, R. Creutzburg, and D. Akopian, "Firmware vulnerability analysis of widely used low-budget TP-link routers," *Electron. Imag.*, vol. 33, no. 3, p. 135, Jun. 2021, doi: 10.2352/issn.2470-1173.2021.3.mobmu-135.

[35] E. Eldaw, A. M. Zeki, and S. Senan, "Analysis of wardriving activity and WiFi access points," in *Wireless Sensor Networks for Developing Countries* (Communications in Computer and Information Science). Berlin, Germany: Springer, 2013, pp. 51–59, doi: 10.1007/978-3-642-41054-3_5.

[36] M. Kim, S. Kwon, D. Elmazi, J.-H. Lee, L. Barolli, and K. Yim, "A technical survey on methods for detecting rogue access points," in *Innovative Mobile and Internet Services in Ubiquitous Computing*. Sydney, NSW, Australia: Springer, Jun. 2019, pp. 215–226, doi: 10.1007/978-3-030-22263-5_21.

[37] B. Alotaibi and K. Elleithy, "Rogue access point detection: Taxonomy, challenges, and future directions," *Wireless Pers. Commun.*, vol. 90, no. 3, pp. 1261–1290, 2016, doi: 10.1007/s11277-016-3390-x.

[38] J. Hu, Y. Li, Y. Cui, and L. Bu, "A technical survey on approaches for detecting rogue access points," in *Advances in Wireless Communications and Applications*. Singapore: Springer, Sep. 2020, pp. 169–174, doi: 10.1007/978-981-15-5697-5_20.

[39] C. Benzaïd, A. Boulgheraif, F. Z. Dahmane, A. Al-Nemrat, and K. Zeraoulia, "Intelligent detection of MAC spoofing attack in 802.11 network," in *Proc. 17th Int. Conf. Distrib. Comput. Netw.*, Jan. 2016, pp. 1–5, doi: 10.1145/2833312.2850446.

[40] J. Choi, "Detection of misconfigured BYOD devices in Wi-Fi networks," *Appl. Sci.*, vol. 10, no. 20, p. 7203, Oct. 2020, doi: 10.3390/app10207203.

[41] M. Miettinen and N. Asokan, "Ad-hoc key agreement: A brief history and the challenges ahead," *Comput. Commun.*, vol. 131, pp. 32–34, Oct. 2018, doi: 10.1016/j.comcom.2018.07.030.

[42] O. Michael and A. Poguda, "Studying IEEE-802.11 encryption protocol," in *Proc. XVI Int. School-Conf. Students, Postgraduates Young Scientists Innovatika*, 2020, pp. 1–5.

[43] C. Gherghina and G. Petrica, "Wireless LAN security issues (I)-types of attacks," *Int. J. Inf. Sec. Cybercrime*, vol. 2, p. 61, Feb. 2013.

[44] T. M. Refaat, T. K. Abdelhamid, and A.-F. M. Mohamed, "Wireless local area network security enhancement through penetration testing," *Int. J. Comput. Netw. Commun. Secur.*, vol. 4, no. 4, p. 114, 2016.

[45] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, "On success probability of eavesdropping attack in 802.11ad mmWave WLAN," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6, doi: 10.1109/ICC.2018.8422192.

[46] S. Balakrishnan, P. Wang, A. Bhuyan, and Z. Sun, "Modeling and analysis of eavesdropping attack in 802.11ad mmWave wireless networks," *IEEE Access*, vol. 7, pp. 70355–70370, 2019, doi: 10.1109/ACCESS.2019.2919674.

[47] A. Kumar, B. Raj, and P. Paul, "Detection and prevention against evil twin attack in WLAN," *Int. J. Comput. Eng. Appl., Special Ed.*, pp. 1–6, Aug. 2016.

[48] Q. Lu, H. Qu, Y. Zhuang, X.-J. Lin, and Y. Ouyang, "Client-side evil twin attacks detection using statistical characteristics of 802.11 data frames," *IEICE Trans. Inf. Syst.*, vol. 101, no. 10, pp. 2465–2473, Oct. 2018, doi: 10.1587/transinf.2018edp7030.

[49] A. Burns, L. Wu, X. Du, and L. Zhu, "A novel traceroute-based detection scheme for Wi-Fi evil twin attacks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8253957.

[50] R. Chandrashekar, "Threats monitoring in Wi-Fi networks using honeypot," M.S. thesis, Univ. Mining, Tech. Univ. Ostrava, Ostrava, Czech Republic, 2020. Accessed: Apr. 6, 2022. [Online]. Available: https://dspace.vsb.cz/handle/10084/92853

[51] C. Nila, M. Preda, I. Apostol, and V.-V. Patriciu, "Reactive WiFi honeypot," in *Proc. 13th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jul. 2021, pp. 1–6, doi: 10.1109/ECAI52376.2021.9515048.

[52] E. Letsoalo and S. Ojo, "A model to mitigate session hijacking attacks in wireless networks," in *Proc. IST-Afr. Week Conf. (IST-Africa)*, May 2018, p. 1.

[53] O. Nakhila, "Masquerading techniques in IEEE 802.11 wireless local area networks," M.S. thesis, Univ. Central Florida, Orlando, FL, USA, 2018. Accessed: Apr. 4, 2022. https://stars.library.ucf.edu/etd/5815/

[54] S. Suroto, "WLAN security: Threats and countermeasures," *JOIV: Int. J. Inform. Vis.*, vol. 2, no. 4, p. 232, Jun. 2018, doi: 10.30630/joiv.2.4.133.

[55] D. Steinmetzer, Y. Yuan, and M. Hollick, "Beam-stealing: Intercepting the sector sweep to launch man-in-the-middle attacks on wireless IEEE 802.11ad networks," in *Proc. 11th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, Jun. 2018, pp. 12–22, doi: 10.1145/3212480.3212499.

[56] M. Vondráček, J. Pluskal, and O. Ryšavý, "Automation of MitM attack on Wi-Fi networks," in *Digital Forensics and Cyber Crime* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering). Prague, Czech Republic: Springer, 2018, pp. 207–220, doi: 10.1007/1275 978-3-319-73697-6_16.

[57] H. A. Noman, S. M. Abdullah, and H. I. Mohammed, "An automated approach to detect deauthentication and disassociation dos attacks on wireless 802.11 networks," *Int. J. Comput. Sci. Issues*, vol. 12, no. 4, p. 107, 2015.

[58] Y. Kristiyanto and E. E, "Analysis of deauthentication attack on IEEE 802.11 connectivity based on IoT technology using external penetration test," *CommIT (Commun. Inf. Technol.) J.*, vol. 14, no. 1, p. 45, May 2020, doi: 10.21512/commit.v14i1.6337.

[59] H. Lee and S. Bahk, "Beacon flooding problem in high-density WLANs," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2017, pp. 595–597, doi: 10.1109/ICTC.2017.8191048.

[60] E. Chatzoglou, G. Kambourakis, and C. Kolias, "How is your Wi-Fi connection today? DoS attacks on WPA3-SAE," *J. Inf. Secur. Appl.*, vol. 64, Feb. 2022, Art. no. 103058, doi: 10.1016/j.jisa.2021.103058.

[61] B. Tushir, Y. Dalal, B. Dezfouli, and Y. Liu, "A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6282–6292, Apr. 2021, doi: 10.1109/JIOT.2020.3026023.

[62] D. Joshi, V. V. Dwivedi, and K. Pattani, "De-Authentication attack on wireless network 802.11 I using Kali Linux," *Int. Res. J. Eng. Technol.*, vol. 4, pp. 1666–1669, Jan. 2017.

[63] P. Satam and S. Hariri, "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," *IEEE Trans. Netw. Service Manage.*, vol. 18, no. 1, pp. 1077–1091, Mar. 2021, doi: 10.1109/TNSM.2020.3036138.

[64] A. Abdelrahman, H. Khaled, E. Shaaban, and W. S. Elkilani, "Detailed study of WLAN PSK cracking implementation," in *Proc. 15th Int. Conf. Comput. Eng. Syst. (ICCES)*, Dec. 2020, pp. 1–6, doi: 10.1109/ICCES51560.2020.9334660.

[65] A. Abdelrahman, H. Khaled, E. Shaaban, and W. S. Elkilani, "WPA-WPA2 PSK cracking implementation on parallel platforms," in *Proc. 13th Int. Conf. Comput. Eng. Syst. (ICCES)*, Dec. 2018, pp. 448–453, doi: 10.1109/ICCES.2018.8639328.

[66] L. Zhang and M. Ma, "Secure and efficient scheme for fast initial link setup against key reinstallation attacks in IEEE 802.11ah networks," *Int. J. Commun. Syst.*, vol. 33, no. 2, p. e4192, Sep. 2019, doi: 10.1002/dac.4192.

[67] G. Abare and E. Garba, "A proposed model for enhanced security against key reinstallation attack on wireless networks," *Int. J. Sci. Res. Netw. Secur. Commun.*, vol. 7, no. 3, pp. 21–27, 2019.

[68] M. Vanhoef and F. Piessens, "Key reinstallation attacks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1313–1328, doi: 10.1145/3133956.3134027.

[69] R. Parvin, "An overview of wireless mesh networks," in *wireless Mesh Networks-Security, Architectures and Protocols*. London, U.K.: IntechOpen, 2020.

[70] A. Belogaev, E. Khorov, A. Krasilov, and A. Lyakhov, "Study of the enhanced algorithm for control information dissemination in Wi-Fi mesh networks," in *Proc. IEEE 27th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Sep. 2016, pp. 1–6, doi: 10.1109/PIMRC.2016.7794916.

[71] J. C. S. Sicato, P. K. Sharma, V. Loia, and J. H. Park, "VPNFilter malware analysis on cyber threat in smart home Network," *Appl. Sci.*, vol. 9, no. 13, p. 2763, 2019, doi: 10.3390/app9132763.

[72] M. Hahad. (Jun. 2018). *VPNfilter: A Global Threat Beyond Routers*. Accessed: Apr. 6, 2022. [Online]. Available: https://blogs.juniper.net/en-us/threat-research/vpnfilter-a-global-threat-beyond-routers

[73] S. Research Team, "Emotet exposed: Looking inside highly destructive malware," *Netw. Secur.*, vol. 2019, no. 6, pp. 6–11, Jun. 2019, doi: 10.1016/s1353-4858(19)30071-6.

[74] C. Cimpanu. (Feb. 2020). *Emotet Trojan Evolves to Spread Via WiFi Connections*. Accessed: Apr. 6, 2022. [Online]. Available: https://www.zdnet.com/article/emotet-trojan-evolves-to-spread-via-a-wifi-connection/
[75] McAfee. (Mar. 2014). *Chameleon: The Wi-Fi Virus That Hides in Plain Sight & Spreads Like a Cold*. Accessed: Apr. 6, 2022. [Online]. Available: https://bit.ly/Chameleon_Wifi_virus
[76] H. Jazi. (Apr. 2020). *New Agenttesla Variant Steals WiFi Credentials*. Accessed: Apr. 6, 2022. [Online]. Available: https://bit.ly/AgentTesla_Wifi
[77] A. Drozhzhin. (Apr. 2020). *Switcher Hacks Wi-Fi Routers, Switches DNS*. Accessed: Apr. 6, 2022. [Online]. Available: https://www.kaspersky.com/blog/switcher-trojan-attacks-routers/13771/
[78] T. Wang, C. Xia, X. Li, and Y. Xiang, "Epidemic heterogeneity and hierarchy: A study of wireless hybrid worm propagation," *IEEE Trans. Mobile Comput.*, vol. 21, no. 5, pp. 1639–1656, May 2022, doi: 10.1109/TMC.2020.3026342.
[79] C. Grace. (Nov. 2021). *WiFi Botnet Malware Can Spam, Hack Your Router: How to Check if You're Infected, Fix With Updates*. Accessed: Apr. 6, 2022. [Online]. Available: https://www.itechpost.com/articles/106653/20210811/wifi-botnet-malware-spam-hack-router-check-youre-infected-fix.htm
[80] S. M. Sajjad, M. Yousaf, H. Afzal, and M. R. Mufti, "EMUD: Enhanced manufacturer usage description for IoT botnets prevention on home WiFi routers," *IEEE Access*, vol. 8, pp. 164200–164213, 2020, doi: 10.1109/ACCESS.2020.3022272.
[81] A. Adithyan, K. Nagendran, R. Chethana, G. Pandy D., and G. Prashanth K., "Reverse engineering and backdooring router firmwares," in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Mar. 2020, pp. 189–193, doi: 10.1109/ICACCS48705.2020.9074317.
[82] K. S. Subraman, A. Antonopoulos, A. A. Abotabl, A. Nosratinia, and Y. Makris, "Demonstrating and mitigating the risk of an FEC-based hardware trojan in wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 10, pp. 2720–2734, Oct. 2019, doi: 10.1109/TIFS.2019.2900906.
[83] S. Shen, H. Zhou, S. Feng, J. Liu, and Q. Cao, "SNIRD: Disclosing rules of malware spread in heterogeneous wireless sensor networks," *IEEE Access*, vol. 7, pp. 92881–92892, 2019, doi: 10.1109/ACCESS.2019.2927220.
[84] A. Queiruga-Dios, A. H. Encinas, J. Martín-Vaquero, and L. H. Encinas, "Malware propagation models in wireless sensor networks: A review," in *Proc. Int. Joint Conf. (SOCO'16-CISIS'16-ICEUTE'16)*. San Sebastian, Spain: Springer, Oct. 2016, pp. 648–657, doi: 10.1007/978-3-319-47364-2_63.
[85] Á. Martín Del Rey, F. K. Batista, and A. Queiruga Dios, "Malware propagation in wireless sensor networks: Global models vs individual-based models," *ADCAIJ: Adv. Distrib. Comput. Artif. Intell. J.*, vol. 6, no. 3, pp. 5–15, Sep. 2017, doi: 10.14201/adcaij201763515.
[86] F. K. Batista, A. Martín del Rey, and A. Queiruga-Dios, "A new individual-based model to simulate malware propagation in wireless sensor networks," *Mathematics*, vol. 8, no. 3, p. 410, Mar. 2020, doi: 10.3390/math8030410.
[87] A. Musa, H. Almohannadi, and J. Alhamar, "Malware propagation modelling in peer-to-peer networks: A review," in *Proc. 6th Int. Conf. Future Internet Things Cloud Workshops (FiCloudW)*, Aug. 2018, pp. 198–202, doi: 10.1109/W-FiCloud.2018.00038.
[88] S. M. P. Dinakarrao, X. Guo, H. Sayadi, C. Nowzari, A. Sasan, S. Rafatirad, L. Zhao, and H. Homayoun, "Cognitive and scalable technique for securing IoT networks against malware epidemics," *IEEE Access*, vol. 8, pp. 138508–138528, 2020, doi: 10.1109/ACCESS.2020.3011919.
[89] L. Li, J. Cui, R. Zhang, H. Xia, and X. Cheng, "Dynamics of complex networks: Malware propagation modeling and analysis in industrial Internet of Things," *IEEE Access*, vol. 8, pp. 64184–64192, 2020, doi: 10.1109/ACCESS.2020.2984668.
[90] D. T. Le, K. Q. Dang, Q. L. T. Nguyen, S. Alhelaly, and A. Muthanna, "A behavior-based malware spreading model for vehicle-to-vehicle communications in VANET networks," *Electronics*, vol. 10, no. 19, p. 2403, Oct. 2021, doi: 10.3390/electronics10192403.
[91] M. Chitra and S. S. Sathya, "SEIR epidemic spreading model to suppress broadcast storm in vehicular ad hoc networks," *Int. J. Vehicle Saf.*, vol. 9, no. 3, p. 228, 2017, doi: 10.1504/ijvs.2017.085204.
[92] A. Mahboubi, S. Camtepe, and K. Ansari, "Stochastic modeling of IoT botnet spread: A short survey on mobile malware spread modeling," *IEEE Access*, vol. 8, pp. 228818–228830, 2020, doi: 10.1109/ACCESS.2020.3044277.
[93] S. Hosseini and M. A. Azgomi, "The dynamics of an SEIRS-QV malware propagation model in heterogeneous networks," *Phys. A, Stat. Mech. Appl.*, vol. 512, pp. 803–817, Dec. 2018, doi: 10.1016/j.physa.2018.08.081.
[94] S. König, S. Schauer, and S. Rass, "A stochastic framework for prediction of malware spreading in heterogeneous networks," in *Secure IT Systems*. Oulu, Finland: Springer, 2016, pp. 67–81, doi: 10.1007/978-3-319-47560-8_5.
[95] W. Liu and S. Zhong, "A novel dynamic model for web malware spreading over scale-free networks," *Phys. A, Stat. Mech. Appl.*, vol. 505, pp. 848–863, Sep. 2018, doi: 10.1016/j.physa.2018.04.015.
[96] S. Hosseini and M. A. Azgomi, "A model for malware propagation in scale-free networks based on rumor spreading process," *Comput. Netw.*, vol. 108, pp. 97–107, Oct. 2016, doi: 10.1016/j.comnet.2016.08.010.
[97] S. Hosseini, M. Abdollahi Azgomi, and A. Rahmani Torkaman, "Agent-based simulation of the dynamics of malware propagation in scale-free networks," *SIMULATION*, vol. 92, no. 7, pp. 709–722, Jun. 2016, doi: 10.1177/0037549716656060.
[98] T. Li, X. Liu, J. Wu, C. Wan, Z.-H. Guan, and Y. Wang, "An epidemic spreading model on adaptive scale-free networks with feedback mechanism," *Phys. A, Stat. Mech. Appl.*, vol. 450, pp. 649–656, May 2016, doi: 10.1016/j.physa.2016.01.045.
[99] H. Hu, S. Myers, V. Colizza, and A. Vespignani, "WiFi networks and malware epidemiology," *Proc. Nat. Acad. Sci. USA*, vol. 106, no. 5, pp. 1318–1323, Feb. 2009, doi: 10.1073/pnas.0811973106.
[100] B. Shan, "The spread of malware on the WiFi network: Epidemiology model and behaviour evaluation," in *Proc. 1st Int. Conf. Inf. Sci. Eng.*, Dec. 2009, pp. 1916–1918, doi: 10.1109/ICISE.2009.1285.
[101] H. Kavak, D. Vernon-Bido, J. J. Padilla, S. Y. Diallo, and R. J. Gore, "The spread of Wi-Fi router malware revisited," in *Proc. 20th Commun. Netw. Symp.*, 2017, pp. 1–10.
[102] Y.-H. Du and S.-H. Liu, "Epidemic model of algorithm-enhanced dedicated virus through networks," *Secur. Commun. Netw.*, vol. 2018, pp. 1–7, Jun. 2018, doi: 10.1155/2018/4691203.
[103] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. Roy. Soc. London. Ser. A*, vol. 115, pp. 700–721, Aug. 1927, doi: 10.1098/rspa.1927.0118.
[104] A. M. del Rey, "Mathematical modeling of the propagation of malware: A review," *Secur. Commun. Netw.*, vol. 8, no. 15, pp. 2561–2579, Oct. 2015, doi: 10.1002/sec.1186.
[105] Y. Oyama, "Investigation of the diverse sleep behavior of malware," *J. Inf. Process.*, vol. 26, pp. 461–476, 2018, doi: 10.2197/ipsjjip.26.461.
[106] J. Duan, *An Introduction to Stochastic Dynamics*, vol. 51. Cambridge, U.K.: Cambridge Univ. Press, 2015.
[107] O. Diekmann, J. Heesterbeek, and J. Metz, "On the definition and the computation of the basic reproduction ratio R_0 in models for infectious diseases in heterogeneous populations," *J. Math. Biol.*, vol. 28, no. 4, pp. 365–382, Jun. 1990, doi: 10.1007/bf00178324.
[108] J. H. Jones, "Notes on R_0," *Califonia: Dept. Anthropological Sci.*, vol. 323, pp. 1–19, 2007.
[109] R. C. Robinson, *An Introduction to Dynamical Systems: Continuous and Discrete*, vol. 19. Providence, RI, USA: American Mathematical Society, 2012.
[110] J. LaSalle, "The stability of dynamical systems," in *Proc. Conf. Appl. Math.*, vol. 25. Philadelphia, PA, USA: SIAM, 1976, pp. 418–420.

DUC TRAN LE graduated from the St. Petersburg State University of Telecommunications, in 2014, under the supervision of Prof. M. A. Bonch-Broevich in the specialty of multichannel telecommunication systems, and the Ph.D. degree from the Admiral Makarov State University of Maritime and Inland Shipping, Russia, in 2018. He currently works at the Information Technology Faculty, The University of Danang–University of Science and Technology, Da Nang, Vietnam. He is the Head of the NetSec-ITDUT Laboratory. His research interests include wireless networks, network security, and malware analysis.

THONG TRUNG TRAN graduated from the University of Science and Technology–The University of Danang, in 2021. He is currently working as a Research Assistant at the NetSec-ITDUT Laboratory. His research interests include malware analysis and blockchain technology.

KHANH QUOC DANG graduated from the University of Science and Technology–The University of Danang, in 2022. He is currently a member of the NetSec-ITDUT Laboratory. His research interests include VANET, malware analysis, and blockchain technology.

REEM ALKANHEL (Member, IEEE) received the B.S. degree in computer sciences from King Saud University, Riyadh, Saudi Arabia, in 1996, the M.S. degree in information technology (computer networks and information security) from the Queensland University of Technology, Brisbane, Australia, in 2007, and the Ph.D. degree in information technology (networks and communication systems) from the University of Plymouth, Plymouth, U.K., in 2019. She has been with Princess Nourah Bint Abdulrahman University, Riyadh, since 1997. She is currently an Assistant Professor at the College of Computer and Information Sciences. Her current research interests include communication systems, networking, the Internet of Things, software-defined networking, and information security.

AMMAR MUTHANNA (Member, IEEE) received the B.Sc., M.Sc., and Ph.D. degrees from the Saint-Petersburg State University of Telecommunications, in 2009, 2011, and 2016, respectively.

From 2017 to 2019, he has worked as a Postdoctoral Researcher at RUDN University. In 2012 and 2013, he took part in the Erasmus student Program with the Faculty of Electrical Engineering, University of Ljubljana, and in 2014, he was a Visitor Researcher at Tampere University, Finland. He is currently an Associate Professor at the Department of Telecommunication Networks, the Deputy Head of science, and the Head of SDN Laboratory. He has been an Expert at the Judges Panel and Challenge Management Board at AI-5G-Challenge, ITU, and a Russian host organizer. His research interests include wireless communications, 5G/6G cellular systems, the IoT applications, edge computing, and software-defined networking. He has been an active member of the technical program committee on many international conferences and journals.