A Network-Aware Internet-Wide Scan for Security Maximization of IPv6-Enabled WLAN IoT Devices

Shikhar Verma, *Student Member, IEEE*, Yuichi Kawamoto, *Member, IEEE*, and Nei Kato, *Fellow, IEEE*

***Abstract*—Despite unprecedented advancements, wireless local area network (WLAN) technologies for the Internet of Things (IoT), such as IEEE 802.11ah (i.e., WiFi-HaLow), are prone to serious security threats, owing to their constrained computational and memory resources, which limit the use of heavyweight intrusion protection and security protocols. To address this problem, security administrators (sec-admins) must perform regular and comprehensive vulnerability assessments of IoT devices. An Internet-wide port scan (IWPS) is the initial step. However, the medium access control mechanism of IEEE 802.11ah, designed specifically for heterogeneous IoT traffic and low-power operations, can degrade network performance in the case of traditional port-scan traffic. Moreover, Internet-security (IPSec) protocol support is mandatory for IPv6-enabled IoT devices to ensure data confidentiality, integrity, and availability. Although the objective of a port scan is to improve IoT security, the resultant network performance can adversely affect IPSec services. Therefore, in this study, we optimize the IWPS to maximize the IoT security over IEEE 802.11ah WLAN. To this end, we propose novel mathematical models to evaluate IoT security based on port-scan network performance and IPsec services, which derives an optimal scan rate for sec-admins. The effectiveness of the proposed framework is verified by comprehensive numerical analysis, which shows that our approach minimizes the risk to IoT devices while probing them at an optimal scan rate.**

***Index Terms*—IEEE 802.11ah networks, Internet of Things (IoT), IoT security, IoT vulnerability assessment, port scan.**

I. Introduction

THE Internet of Things (IoT) facilitates the interconnectivity of ultradense physical smart objects to enable innovative services. These devices include smart meters, healthcare devices, and industrial IoT, which have various heterogeneous requirements, such as data rates, traffic, and delays [1], [2]. For example, a smart manufacturing operation includes intelligent cameras, automated tools, and healthcare devices, where the smart cameras require a high data rate and delay tolerance, and the automated tools and healthcare devices require a low data rate and delay tolerance [3], [4]. Moreover, such heterogeneous IoT (Het-IoT) devices are expected to operate with low power consumption [5]. To support these features in a wireless local area network (WLAN), the IEEE 802.11ah (i.e., WiFi-HaLow) protocol has been fielded, providing an energy efficient and group-based channel-access restricted-access window (RAW) mechanism [6].

Apart from the advantages of IEEE 802.11ah, IoT communications are vulnerable to attacks, owing to their limited availability of computation and memory resources, which restricts the use of heavyweight security protocols, complex passwords, and intrusion protection systems [7], [8]. Moreover, attackers can exploit compromised IoT devices, such as those infected by Mirai and Persirai malware, to initiate Distributed-Denials-of-Service (DDoS) attacks on servers and network systems [9]. Therefore, in recent years, Internet-wide port scanning (IWPS) has attracted considerable attention as a means to troubleshoot vulnerable IoT ports and services [10]–[12]. Such comprehensive port scanning should be regularly performed for IoT devices, because, unlike traditional devices, these devices are publicly accessible, and network managers and users often neglect the regular updates required for these devices after deployment. Moreover, legacy port-scan traffic is transmitted through IoT-dedicated IEEE 802.11ah medium-access control (MAC) protocols via each WLAN. However, the latest protocol is intended to address Het-IoT traffic and low-energy consumption by giving IoT devices group-based channel access in a specific time slot and letting them sleep until the next transmission/reception. However, port-scan traffic cannot probe sleeping devices, which not only increases scan delays, but it also overloads the network at each slot. Thus, traditional port-scan approaches can degrade IoT network performance, further weakening security. Unfortunately, such challenges have not yet been addressed in [11]–[14]. Thus, to fill this gap, we investigate the network performance of port scans with respect to IoT security over IEEE 802.11ah networks.

All IoT devices will soon be IPv6 enabled, owing to the massive number of devices and the advantages of low-energy consumption [15], [16]. The Internet-security (IPsec) protocol is a promising technology for enabling end-to-end security of devices having low resources, owing to their integration into the Internet protocol (IP) [17], [18]. Additionally, IPsec support is mandatory for IPv6-enabled IoT devices. Thus, we assume that most such devices will use the IPSec protocol as a standard solution. In this study, we recognize that a high scan rate [i.e., number of scan packets (SPs) transmitted per unit time] can adversely affect IPsec services (e.g., confidentiality, integrity, and data availability) by restricting the available network resources for the implementation of stronger

Manuscript received September 29, 2020; revised November 27, 2020; accepted December 10, 2020. Date of publication December 18, 2020; date of current version May 7, 2021. This work was supported by the Ministry of Internal Affairs and Communications, Japan, through National Project "Research and Development of High-Efficiency Wide Area Network Scan for Efficient Use of Frequency in Wireless IoT," under Grant JPJ000254. *(Corresponding author: Shikhar Verma.)*

The authors are with the Graduate School of Information Sciences, Tohoku University, Sendai 9808579, Japan (e-mail: shikhar.verma@it.is.tohoku.ac.jp; youpsan@it.is.tohoku.ac.jp; kato@it.is.tohoku.ac.jp).

Digital Object Identifier 10.1109/JIOT.2020.3045733

encryption algorithms. Vulnerable services can easily compromise IoT devices, owing to weak algorithms. Furthermore, we identify the tradeoffs between the port-scan network performance at various scan rates and the patching delays (PDs) of vulnerabilities, which, in turn, can increase the likelihood of attack. Hence, a network-unaware port-scan approach can make an IoT device more vulnerable and increase risk. Therefore, we present novel mathematical models for the design of a network-aware IWPSs to maximize the security of IoT devices by setting an optimal scan rate. Moreover, we propose a new queueing model that includes scan and Het-IoT traffic over IEEE 802.11ah. Finally, the performance of the proposed framework is evaluated by mathematical analysis.

The remainder of this article is organized as follows. Section II delineates the background of IWPS, discusses the considered scenarios, and reviews the related studies. Section III extensively describes the research challenges encountered by port scanning. Section IV introduces the proposed network-aware model for port scanning. Section V presents the numerical analyses. Finally, Section VI concludes this article.

II. Considered Scenario and Related Work

In this section, we provide background for IoT IWPS technologies and present our considered scenario. We also discuss related studies to elucidate the background.

A. IWPS for IoT

IoT security has attracted considerable attention in academia and industry, owing to its importance in the face of challenges imposed by inherent IoT characteristics (e.g., computation, memory, and energy consumption). These restrictive characteristics limit the use of complex passwords and strong security protocols. Furthermore, IoT devices are designed to operate over long periods with unchanging connectivity and firmware implementations, which provide attackers with more opportunities to easily exploit vulnerabilities. Therefore, port scanners (e.g., ZMap, Masscan, and Shodan) have been recently applied with IWPS to probe IoT devices and identify vulnerabilities [12], [19]. In this study, we suppose that security admins (sec-admins) deploy such port scanners to survey IoT devices connected to the Internet to identify the operating system, open/closed ports, and vulnerabilities of the current version of services, as shown in Fig. 1. A port scanner generates SPs per unit time, giving us a scan rate. The scanner probes the entered blocks of IP addresses at the scan rate provided by the sec-admins. Although a higher scan rate can be beneficial from the scanner's perspective, it can overload the WLANs [11], [13]. Therefore, the scan rate is our key controllable input. However, there are various scanning techniques (e.g., open, half-open, and stealth) that can be applied. In this study, we consider a transmission control protocol (TCP) half-open scan, because it is stealthy and imposes a small burden on the network and devices, owing to its incomplete TCP handshake [10]. With the TCP half-open scan, the scanner generates synchronization (SYN) packets at a certain scan rate. With a TCP SYN request, an IoT device can respond with a reset (RST) in the case of closed ports or an acknowledgment (ACK) in the case of open ports, as shown in Fig. 1. The port scanner can RST the ports after receiving an ACK. Thereafter, the scanners analyze the responses to detect vulnerabilities. They then notify the telecommunication carriers to alert the device owners and support centers, which, in turn, suggest patching solutions. In this scenario, the IoT devices are equipped with the IEEE 802.11ah WLAN protocol for data transmission/reception, as shown in Fig. 1. Moreover, IPv6 will soon be implemented for all IoT devices, owing to the tremendous growth in the number of devices (more than available 4.2 billion IPv4 addresses) and the advantages of low-energy consumption [15], [16]. Additionally, IPv6-enabled devices are more secure, owing to their mandatory implementation of the IPsec protocol, which provides end-to-end encryption [17]. IPsec is also compatible with devices having low resources, such as IoT [18], because of its integration with the IP layer. Based on the advantages of IPv6 and IPsec for IoT, we assume that all IoT devices are addressed using IPv6 and are secured by the IPsec protocol over IEEE 802.11ah WLAN. The next section reviews the related studies on legacy IWPS to identify whether such scans are appropriate for IPv6 and IPSec-enabled IoT devices over IEEE 802.11ah.

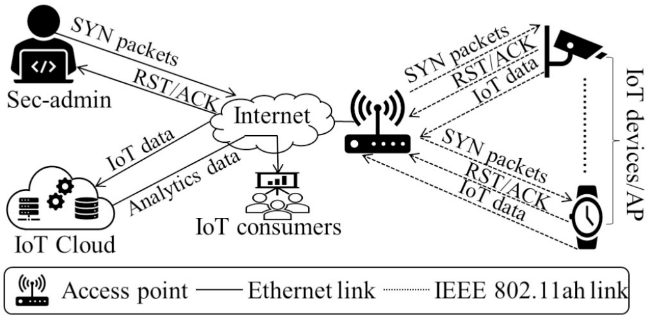

Fig. 1. Considered scenario: half-open port scan of IoT devices over IEEE 802.11ah WLAN.

B. Related Work

Vulnerability scanning was developed for local private network-scanning capabilities for less intrusive and IWPS for common public IPs. Most studies on the reconnaissance of connected device ports were related to the design of efficient frameworks/scanners using different approaches to generate and distribute SPs for IWPSs [12], [20]. Other studies focused on intrusion detection and prevention by analyzing the scan responses [21], [22]. However, most of these studies did not address the WLAN network limitations. For example, the ZMAP product claims that it is capable of scanning an entire IPV4 address in under 45 min for a given port [12] using 97% of the gigabit Ethernet capacity, which is not practical for IoT, owing to the unavailability of such throughput, plus the congestion caused by Het-IoT traffic. The Masscan product faces the same issue. However, both ZMap and Masscan have overcome the long scan delays issue of tools, such as network mappers, by generating SPs faster and distributing them randomly. However, the random distribution of SPs can overload

IoT networks at certain access points (APs) where fewer network resources are available for ultradense devices [13]. In [13], a model was proposed to set a high scan rate while maximizing the throughput for traditional IEEE 802.11 in order to deal with network constraints. However, this model considered only network improvements and ignored security, including the impact on IPsec services, which is a prime objective of the port scan. Moreover, the model was suited only to traditional IEEE 802.11; it was not applicable to the IEEE 802.11ah RAW mechanism. Hence, in this study, we address the high scan rate, which is not necessarily beneficial in terms of IoT security. Moreover, emerging energy-efficient WLAN MAC protocols, such as IEEE 802.11ah RAW, can restrict the scanning of sleeping IoT devices. Hence, disorganized and random probing of IoT device ports over IEEE802.11ah can degrade network and port-scan performance. Furthermore, most existing studies on IEEE 802.11ah have focused on grouping strategies and performance of the RAW protocol only, whereas the performance of traditional scan traffic under such IoT-centric protocols has not been investigated [6], [23]. Therefore, this study investigates a pioneering network-aware IWPS for IPV6-enabled IoT device security over the latest IEEE802.11ah networks. Moreover, we probe devices on specific APs together rather than randomly to avoid congestion at uncertain APs. In the next section, we discuss the research challenges faced by legacy port scanning over IEEE 802.11ah.

III. System Model and Research Challenges

In this section, we explain system model of our considered scenario. Thereafter, this article presents the research challenges that can degrade IoT security at various scan rate.

A. System Model

This article considers N_{AP} number of fully connected IEEE 802.11ah enabled APs over the Internet with an average of N number of IPsec and IPv6 enabled IoT devices per AP. In IEEE 802.11ah MAC protocol as shown in Fig. 2, a beacon interval (t_{b}) is divided into K RAW frames (RFrames), and length of each RFrame is $t_{\mathrm{R}} = t_{\mathrm{b}}/K$. These N devices access the wireless channel within a RFrame. However, a RFrame is slotted into RAW slots (Rslots) and length of each Rslot is t_{s}, as shown in Fig. 2. The RAW mechanism allows a group of devices to access the channel in an Rslot while allowing the other devices to sleep. Hence, there are M groups of devices with group size g. Each group accesses the channel using CSMA/CA process, as shown in Fig. 2. However, we consider the noncrossing case wherein an ongoing transmission is not allowed to cross the designated slot. To restrict transmission to another Rslot, IEEE 802.11ah introduces a holding time (t_{Ho}) at the end of the Rslot, which interrupts the ongoing transmission, as depicted in Fig. 2. Thus, the Rslot time available for transmission is $t'_{\mathrm{s}} = t_{\mathrm{s}} - t_{\mathrm{Ho}}$.
According to the considered scenario, we scan N_{p} number of ports per device within N_{AP} AP with scan rate of *TR*. Regarding the security technology in each device, CONFidentiality (CONF) and INTegrity (INT) of IoT packets are provided using IPSec by encrypting and authenticating IoT packets transmitted between devices. There are two primary types of IPSec protocols: 1) encapsulating security payload (ESP) and 2) authentication header (AH). However, ESP includes both encryption and authentication, which provides both CONF and INT services. AH checks only INT of packets. Hence, we consider ESP in this article. IPSec also provides the flexibility to choose an encryption algorithm between two IPsec devices by negotiation. In IPsec, first, sec-admins define a set of transform sets that is a collection of encryption algorithms for devices. During the negotiation process, IoT devices check their matching transform sets, and matched sets are communicated through the security association. Thus, each pair of devices choose the encryption algorithm for ESP protocols based on chosen transform set. Each transform set define encryption algorithm, and are sorted according to the priority of use of encryption algorithm in a IoT device. However, security admin can define an encryption algorithm for each transform set based on the observation of traffic and Quality-of-Service (QoS) [24]–[26] requirement. For example, in [26], a flexible game-theory approach was proposed to determine multilevel security based on the tradeoff between the encryption algorithms, the key length, and the network throughput as a QoS parameter. Here, we consider IoT throughput as a QoS metric to set the encryption algorithm. Moreover, in this article, we consider different encryption-algorithm choices, including hardware (HW) implementations of data encryption standards (DES-HW), Triple DES (3DES), AES-128 bit, etc. However, heavyweight protocols such as AES-256 bit, cannot be implemented in IoT owing to its computational complexity. Hence, in this study, we assume only those algorithms that are applicable to IoT. Security of IoT is evaluated using risk metric which considers both vulnerability attack and information security services such CONF, INT, and AVAilability (AVA). Risk is defined as a security metric which determines level of risks on any device that is estimated from impact of vulnerability, threat, and asset-importance on security of a device. The risk on a device is formulated as follows [27]:

$$Risk = V \times Th \times AI \tag{1}$$

where V is the common vulnerability scoring-system (CVSS) score of the a vulnerability in a device. *Th* and *AI* are the threat level and asset weight of device, respectively. The threat can be defined in terms of access level to any device by an attacker such as physical access, remote access, and so on.

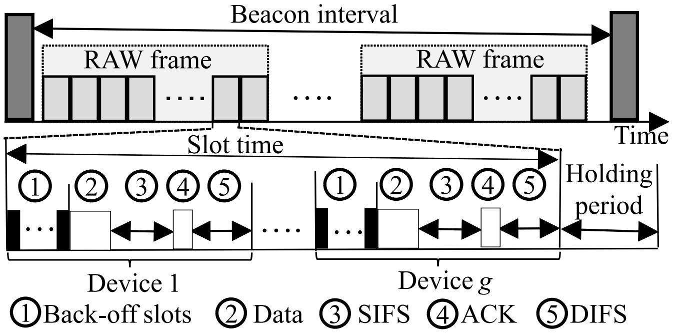

Fig. 2. RAW-based distributed coordination function process in IEEE 802.11ah.

The threat parameter is quantified as a weight value equals to the threat of actual access by an attacker compared to a high threat, i.e., physical access. Hence, the threat value lies from 0 to 1. A threat value zero means there is no threat while threat value of one denotes a high threat due to easy physical access. As we know IoT devices are publicly available and can have easy physical access and also have a weak password. Hence, threat value is set to 1 in this article and which is also considered in [28]. Moreover, asset is defined as the importance of a device, which can cause huge loss to users in case of security breaches or impacts of a compromised device. It is quantified as weight value of the importance of a device compared to a highly important device. Hence, the asset value of any device also varies from 0 to 1. IoT devices have high importance because any compromised IoT device can act as a bot agent and can initiate attacks on other network infrastructures, which can cause huge losses. Thus, asset value is set as 1 in this article, which is considered same in [28]. However, CVSS value varies from 0 to 10 [28], [29]. The CVSS metric defines severity levels for certain range of CVSS value. The qualitative severity scale of CVSS value are given as: CVSS = 0 signifies no risk, 0.1 to 3.9 defines low risk, 4.0 to 6.9 means medium risk, 7.0 to 8.0 considers high risk and 9.0 to 10.0 represents critical risk. Thus, risk values can be quantified from 0 to 10 according according to defined CVSS ranges, and constant value of threat, and asset. The risk value such as 1 represents lower risk and high security whereas higher risk value such as 10 represents highly insecure devices. However, the CVSS is a dynamic scoring standard for any vulnerability and covers three metrics: 1) base; 2) temporal; and 3) environmental scores [29]. The base score is the primary value of a vulnerability that is static with respect to time and the environment. Meanwhile, the temporal score reflects the variation in the base score over time owing to the attack likelihood (AL), available patching solution, and report confidence. Moreover, the environmental score represents the variation of the base and temporal scores, owing to the fluctuation in the device's security environment, such as the variations and requirements of CONF, INT, and AVA. Therefore, in the following sections, we show research challenges concerning the impact of inappropriate scan rate on temporal and environmental scores, owing to the poor network performance of IEEE 802.11ah that can increase the risk on IoT devices.

B. Research Challenges

This section presents the research challenges concerning the degradation of IoT security by impacting temporal and environmental score owing to network-oblivious IWPS.

1) Impact of Scan Rate on Temporal Score: The temporal score consists of remediation level, report confidence, and exploit code maturity (ECM) [29]. The remediation level of a vulnerability signifies whether an official patching solution is available. Because our focus is to study the network performance of IWPS, we assume that patching algorithms are available. Moreover, the report confidence signifies the confidence in the presence of vulnerabilities and the reliability of technical details. We also suppose that confirmed and technically sound reports on vulnerabilities exist owing to the contributions by reputed standards, such as common vulnerabilities and exposures [30]. However, ECM is evaluated on the basis of the AL of the vulnerability [29]. AL is a relative term that depends on the PD, defined as the time required to identify and fix a port vulnerability. For example, if secadmins can regularly identify and patch vulnerabilities before a compromise, then attackers will not have chance to attack any IoT device. Moreover, the PD is a function of both the scan delay for probing each port for vulnerabilities and the time taken for processing the patching algorithms. The execution time of patching algorithms is considered constant since it is independent of the scan rate. The PD can be affected significantly by an increase in the scan delay, leading to long PD and high AL. Therefore, the scan delay should be minimized to reduce AL and impact on the temporal score. Moreover, the scan rate influences the scan delay. Both low and high scan rates can increase the scan delay. For example, the probing of all ports (around 65 535) in each IoT device per AP with a low scan rate takes a longer time; whereas a high scan rate can increase the scan delay because of the numerous backoffs in obtaining channel resources or SPs drops, owing to the channel congestion in each Rslot. Hence, a low and high scan rate can increase AL by having long PD, which increases the temporal score and the risk to an IoT device. Therefore, an optimal scan rate is required to minimize this risk. Moreover, the scan rate can influence the environmental score of CVSS, which is discussed in the next section.

2) Impact of Scan Rate on Environmental Score: The environmental metric represents the impact on the security of devices, owing to modification of the devices' security environment, such as CONF, INT, AVA, and their requirements. The CVSS determines the CONF, INT, and AVA requirements based on the importance of the affected device to an organization (e.g., service availability). However, the requirements of these parameters for IoT are always high, owing to easy access to IoT devices. However, the security is low, owing to the constrained resources. The compromise of a single security services in IoT can lead to attacks on other IT assets of the organization (e.g., DDoS) [9]. Therefore, in this study, we consider providing high CONF, INT, and AVA. The full influence of the environment metric is estimated using the modified base score, which is altered because of the variation in the CONF and INT protocols. The value CONF and INT at any time depends on the strength of encryption algorithm. As discussed in the system model that security admin decides encryption algorithm based on available throughput for each IoT device. High available IoT throughput can allow to set strong encryption whereas low throughput allows weak encryption algorithm. A high scan rate leads to channel congestion at any WLAN and resource exhaustion for IoT packets. Hence, a high scan rate can cause low IoT throughput which in turn might impose the implementation of weak encryption algorithms. However, the size of SPs is small and frequency of incoming SPs are low. Though the scanning of an enormous number of ports for large number of devices per IEEE 802.11ah enabled AP can take several days or weeks owing to limited bandwidth availability in IEEE 802.11ah. During this scan duration, if security methods are not adjusted according to the scan rate then an IoT device can experience degraded services for several days or weeks, which can have serious impact on IoT services that require high throughput or low delay. Hence, security methods such as encryption algorithm should change at various scan rates. Based on these reasons, a high scan rate impacts the CONF and INT security services. Moreover, owing to high scan rate, network congestion may be responsible for packet loss if the packets are unable to obtain channel resources within their maximum number of permitted retransmissions. Hence, a high scan rate also reduces the AVA of IoT packets and services. Such a scenario is defined as a scan attack. Hence, AVA should be improved to avoid transformation of a positive scan into an attack and the consequent security degradation. Therefore, in the next section, we propose a novel security and network model to optimize the scan rate to minimize the risk to IoT.

IV. Network-Aware IWPS Model

In this section, we propose a novel mathematical model in support of network-aware IWPSs evaluating the risk of a device. We divide the proposed model into two submodels: IoT/scan throughput and network-aware risk evaluation. Finally, we formulate the optimization problem on the basis of these two models to estimate the optimal value of the scan rate needed to minimize the risk value.

A. IoT and Scan Throughput Model

First, we present a novel queue model for port scanning and Het-IoT traffic. Then, we propose a mathematical model to estimate scan and IoT throughput over IEEE 802.11ah.

1) Queue Model: There are two major types of traffic generated by IoT: 1) periodic update (PU) and 2) event-driven (ED) [31], which are uplink (UL) dominant. To model such traffic from each IoT device, a semi-Markov model that includes PU, ED, and a payload exchange (PE) was proposed in [31]. PE packets include the data generated following PUs or EDs that provide additional details after an event. However, PE packets can be merged with PUs and EDs, because their arrivals coincide. Hence, we revise the traffic model to provide a more precise and realistic Het-IoT scenario. In Het-IoT traffic, each IoT device can have different packet-arrival rates. Therefore, in this model, we consider that the PU of IoT device i has λ_i^{ULPU} packet arrivals for transmission per unit time, where i varies from 1 to N, and N is the total number of devices per AP. In this study, the packet-arrival rate is defined per unit time, which is equal to a beacon interval. The PU downlink (DL)-packet arrival rate for device i in an AP is λ_i^{DLPU}. We also assume that the arrival of the ED and the following DL control packets follow a Poisson process [31]. To estimate the total packet arrival for UL (including ED with PUs), we propose a Markov model, as shown in Fig. 3. Because IEEE-802.11ah-enabled IoT devices have a sleep mode, we consider the sleep state in our model. The Markov model in Fig. 3 represents the traffic model for device i. PU, ED, and Sleep are three states for device i, denoted as S_{A}^i, S_{B}^i, and S_{C}^i, respectively. Based on the Markov model, the average number of packet arrivals for UL (λ_i^{UL}) and DL (λ_i^{DL}) of device i per unit time is formulated as follows:

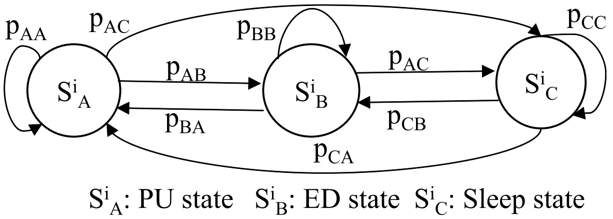

Fig. 3. Markov model used to estimate traffic for IoT device *i*.

$$\lambda_i^{\text{UL}} = \lambda_i^{\text{ULPU}} P_{\text{A}} + \lambda_i^{\text{ULB}} P_{\text{B}} \tag{2}$$

$$\lambda_i^{\text{DL}} = \lambda_i^{\text{DLPU}} P_{\text{A}} + \lambda_i^{\text{DLB}} P_{\text{B}} \tag{3}$$

where λ_i^{ULB} and λ_i^{DLB} are the respective packet-arrival rates for UL and DL (control packets) transmissions at S_{B}^i. However, there is zero packet generation during the sleep state. Hence, there is no arrival in the queue during sleep time. The DL IoT data packets are thus added to the AP queue. Let P_{A}, P_{B}, and P_{C} be the steady-state probabilities for states A, B, and C, respectively. These steady-state probabilities can be calculated by solving $\vec{\pi}T = \pi$, where $\vec{\pi}$ and T are the steady-state probability distribution vector and transition matrix, respectively, with constraint $P_{\text{A}} + P_{\text{B}} + P_{\text{C}} = 1$. In this model, we consider the M/M/1:∞/first-in-first-out queue, which supports the periodic and Poisson processes. Let Y_i and Y_{AP} be the packet-processing time of device i and the AP, respectively. This is defined as the time required to successfully transmit a packet. Hence, based on the Markov queue model, the probability of having at least a packet in device i (Q_i^{Dnemp}) and the AP (Q^{APnemp}) queue during Y_i and Y_{AP} is given by

$$Q_i^{\text{Dnemp}} = 1 - e^{-(\lambda_i^{\text{UL}}+\lambda_i^{\text{ACKscan}})Y_i} \tag{4}$$

$$Q^{\text{APnemp}} = 1 - e^{-(\sum_{i=1}^{N}(\lambda_i^{\text{DL}}+\lambda_i^{\text{scan}}))Y_{\text{AP}}}. \tag{5}$$

In the above-mentioned equations, λ_i^{scan} and $\lambda_i^{\text{ACKscan}}$ are the scan-packet arrival rate to an AP for device i and the ACK response of the SPs from device i per unit time. Using the above-mentioned queue model and carrier-sense multiple-access/collision avoidance (CSMA/CA) process, we formulate the IoT and scan throughput over the IEEE 802.11ah RAW mechanism in the next section.

2) IoT/Scan Throughput Estimation: Before modeling the CSMA/CA process at per Rslot by a group of devices in IEEE 802.11ah, we estimate the number of groups per AP (M) and number of devices (g) per group. M is estimated based on the length of the RFrame and the available the Rslot, formulated as $\lceil t_{\text{R}}/t'_{\text{s}} \rceil$. Without loss of generality, we consider a uniform distribution of devices among M groups in this study. The number of devices per group (g) is equal to N/M. In the case of N not being divisible by M, g in the $M-1$ group is $\lfloor N/M \rfloor$, and the last group has $N - (M \times \lfloor N/M \rfloor)$ devices. During the CSMA/CA process, a device invokes a backoff process after a packet arrives in the queue. After the backoff, a device j ($1 \leq j \leq g$), from any group, first senses the idle channel during the distributed interframe space (DIFS) equal to *DIFS* interval. If the channel is found idle after a DIFS, the device transmits the data followed by a short interframe space (SIFS). After the SIFS, an ACK is transmitted by the AP to indicate a successful transmission. The device again waits for a DIFS before initiating a backoff timer after data transmission. Each device initiates separate consecutive packet transmissions with a random backoff timer. In CSMA/CA, each device follows an exponential backoff that is selected in the range of (0, $W - 1$), where W is the contention window size equal to $2^m W_{\min}$, depending on the retransmission number (m). $W_{\min}$ is the contention window size of the first attempt. Consecutive mini-slots having lengths of ϕ are assigned for backoff counting within an Rslot, which are equal to the time required by a device to detect a packet transmitted by other devices.

In this study, we consider unsaturated traffic because of our queuing model, where there is a probability of having an empty queue. Moreover, we assume that the channel condition is ideal without any communication errors or capture effects. However, multiple transmission attempts in the same mini-slot can cause a collision and initiate a backoff. A device or an AP can transmit a packet in a mini-slot when the queue has at least a packet to transmit. Thus, the transmission probability by device j and AP is given as follows:

$$\tau_j = \tau_{\text{sat}} Q_j^{\text{Dnempslot}} = \tau_{\text{sat}}\left(1 - e^{-(\lambda_j^{\text{UL}} t_{\text{s}} + \lambda_j^{\text{ACKscanslot}}) Y_j}\right) \quad (6)$$

$$\tau_{\text{AP}} = \tau_{\text{sat}} Q^{\text{APnempslot}} = \tau_{\text{sat}}\left(1 - e^{-(\sum_{j=1}^{g} (\lambda_j^{\text{DL}} t_{\text{s}} + \lambda_j^{\text{scanslot}})) Y_{\text{AP}}}\right) \quad (7)$$

where τ_{sat} is the saturated transmission probability of a terminal when the terminal and the AP always have a packet to transmit in a mini-slot. In (6) and (7), $Q_j^{\text{Dnempslot}}$ and $Q^{\text{APnempslot}}$ are the probabilities of having at least a packet in the queue of device j and the AP during Y_i and Y_{AP}, respectively, derived based on (4) and (5). However, devices transmit in their Rslot. Hence, λ_j^{UL} and λ_j^{DL} are multiplied by t_{s} to estimate the average number of packets arriving per Rslot in (6) and (7). $\lambda_j^{\text{ACKscanslot}}$ and $\lambda_j^{\text{scanslot}}$ are the average numbers of scan and ACK response packets per Rslot that will be formulated later in the model. τ_{sat}, based on [32], is formulated as

$$\tau_{\text{sat}} = \frac{2(1 - C_{\text{sat}})}{(1 - 2C_{\text{sat}})(W_{\min} + 1) + C_{\text{sat}} W_{\min}(1 - (2C_{\text{sat}})^m)} \quad (8)$$

where C_{sat} is the conditional collision probability of a packet when at least one of the remaining $g - 1$ devices or the AP transmits data. Hence, C_{sat} should be expressed as

$$C_{\text{sat}} = 1 - (1 - \tau_{\text{sat}})^{g-1}(1 - \tau_{\text{sat}}) = 1 - (1 - \tau_{\text{sat}})^g. \quad (9)$$

Equations (8) and (9) can be solved using numerical techniques. However, to estimate the IoT/scan throughput, we must formulate the successful transmission of IoT and SPs. Hence, P_j^{succ} and $P_{\text{AP}}^{\text{succ}}$ are the probabilities for successful transmission by device j or the AP. A successful packet transmission occurs when exactly one device or one AP transmits on the channel when, at least one device/AP transmits during the considered mini-slot time. Based on this definition, P_j^{succ} and $P_{\text{AP}}^{\text{succ}}$ can be derived as

$$P_j^{\text{succ}} = \frac{(g+1)\tau_j(1 - \tau_{\text{AP}})(1 - \prod_{q=1, q\neq j}^{g}(1 - \tau_q))}{1 - \prod_{q=1}^{g}(1 - \tau_q)(1 - \tau_{\text{AP}})} \quad (10)$$

$$P_{\text{AP}}^{\text{succ}} = \frac{(g+1)\tau_{\text{AP}}(1 - \prod_{j=1}^{g}(1 - \tau_j))}{1 - \prod_{j=1}^{g}(1 - \tau_j)(1 - \tau_{\text{AP}})}. \quad (11)$$

q is a device-index term ranges from 1 to g. Before formulating the throughput, we must derive the equations for the service time in the queue of each device and the AP to substitute into (6) and (7). Here, the service time is defined in terms of the packet transmission time for each device or AP. The service time of a packet in the CSMA/CA process usually includes the waiting time during backoff and the transmission time. Moreover, a device cannot transmit packets during a sleep time. Thus, an unsuccessful packet in an Rslot must wait until the next Rslot for transmission (i.e., the sleep duration). Therefore, the service time for packets over IEEE 802.11ah should include the sleep time. The service time can thus be derived as

$$Y_j = T_j^{\text{bo}} N^{\text{bo}} + T_j^{\text{tr}} + (1 - P_j^{\text{succ}}) T_j^{\text{sleep}} \quad (12)$$

where T_j^{bo} and N^{bo} are the mean length of a backoff mini-slot and the average number of backoff mini-slots, respectively, and T_j^{tr} and $T_j^{\text{sleep}} = t_{\text{R}} - t_{\text{s}}$ are the successful transmission time and sleep duration, respectively. Furthermore, T_j^{bo} is calculated on the basis of the empty-slot time with no transmission by $g - 1$ devices or the AP, the successful transfer time by device j, and the idle time during the collision

$$T_j^{\text{bo}} = (1 - P^{\text{tr}})\phi + T^{\text{succ}} P^{\text{tr}} P_j^{\text{succ}} + T^{\text{col}}(1 - P_j^{\text{succ}}) P^{\text{tr}}. \quad (13)$$

In the above equation, P^{tr} is the probability that at least one transmission is performed by a device or an AP in the given mini-slots. Here, T^{succ} and T^{col} represent the average time spent during successful transmission plus the collision of a device or an AP using basic access, respectively. Furthermore, P^{tr}, T^{succ}, and T^{col} are formulated as

$$P^{\text{tr}} = 1 - \prod_{j=1}^{g}(1 - \tau_j)(1 - \tau_{\text{AP}}) \quad (14)$$

$$T^{\text{succ}} = T^{\text{data}} + SIFS + 2\delta + T_{\text{ACK}} + DIFS \quad (15)$$

$$T^{\text{col}} = T^{\text{data}} + DIFS + \delta \quad (16)$$

where $T^{\text{data}} = H/\text{datarate}$ is the transmission of a data frame. H is the IEEE 802.11ah frame size whose size is the sum of frame header (14 bytes), MAC payload, and frame control sequence (4 bytes) [33]. MAC payload size is the sum of IPv6 header size (P_{IPv6}), IPv6 extension header size (E_{IPv6}) and P, where P is the payload size of IoT data. IPv6 extension header is used to specify the ESP header. Furthermore, δ is the propagation delay, and $T_{\text{ACK}} = ACK/\text{datarate}$ is the transmission time of the ACK frame of size ACK. In addition, T_j^{tr} in (12) can be formulated as

$$T_j^{\text{tr}} = P_j^{\text{succ}} T^{\text{succ}} + (1 - P_j^{\text{succ}}) T^{\text{col}}. \quad (17)$$

For simplicity, the constant, N^{bo}, in (12) is considered to be $W/2$ in this study. However, the average number of backoffs based on an exponential distribution function can also be considered here as in other studies [32]. Similarly, we can formulate the service time for an AP as follows:

$$Y_{\mathrm{AP}} = T^{\mathrm{bo}}_{\mathrm{AP}} N^{\mathrm{bo}} + T^{\mathrm{tr}}_{\mathrm{AP}} \tag{18}$$

$$T^{\mathrm{bo}}_{\mathrm{AP}} = (1-P^{\mathrm{tr}})\phi + T^{\mathrm{succ}} P^{\mathrm{tr}} P^{\mathrm{succ}}_{\mathrm{AP}} + T^{\mathrm{col}}(1-P^{\mathrm{succ}}_{\mathrm{AP}})P^{\mathrm{tr}} \tag{19}$$

$$T^{\mathrm{tr}}_{\mathrm{AP}} = P^{\mathrm{succ}}_{\mathrm{AP}} T^{\mathrm{succ}} + (1-P^{\mathrm{succ}}_{\mathrm{AP}})T^{\mathrm{col}}. \tag{20}$$

For $Q^{\mathrm{Dnempslot}}_{j}$ and $Q^{\mathrm{APnempslot}}$ of (6) and (7), we must estimate $\lambda^{\mathrm{scanslot}}_{j}$ and $\lambda^{\mathrm{ACKscanslot}}_{j}$ per Rslot, respectively, before formulating the IoT/scan throughput. The number of SPs arriving at each AP (R) should be equal to TR/N_{AP}. The AP distributes these SPs according to the distribution of devices in groups. Because we considered the uniform distribution of devices, the AP uniformly distributes the SPs among the groups in each RFrame. Thus, $R' = R/(K \times M)$ is the number of SPs per Rslot. However, the distribution of SPs to each IoT device of a group in the Rslot is unknown, and it was not formulated in previous studies. Therefore, we propose a probability mass function (PMF) (P_{scan}) for the distribution of SPs per slot to a device in the group. Out of R', any number of packets can be assigned to a device. The derivation of PMF is presented in the Appendix and is expressed as follows:

$$P_{\mathrm{scan}}(X=x) = \frac{{}^{g-x+R'-2}\mathbf{C}_{R'-2}}{{}^{g+R'-1}\mathbf{C}_{R'-1}} \tag{21}$$

where ${}^{g+R'-1}\mathbf{C}_{R'-1}$ is the total number of ways SPs can be distributed among g devices, and ${}^{g-x+R'-2}\mathbf{C}_{R'-2}$ is number of ways x SPs can target a device. The average number of SPs aiming for device j in an Rslot can be formulated as

$$\lambda^{\mathrm{scanslot}}_{j}(g,R) = \sum_{x=1}^{R'} x \times P_{\mathrm{scan}}(X=x) \tag{22}$$

where R' is the function of R. The average number of ACK SPs ($\lambda^{\mathrm{ACKscanslot}}_{j}$) sent by device j per Rslot can be expressed as

$$\lambda^{\mathrm{ACKscanslot}}_{j}(g,R) = P^{\mathrm{succ}}_{\mathrm{sat}} \lambda^{\mathrm{scanslot}}_{j} \tag{23}$$

where $P^{\mathrm{succ}}_{\mathrm{sat}}$ is the success probability in the saturation case. The saturated probability is used to estimate the number of ACKs/RSTs, because these packets are received only if SPs are transmitted. Hence, $P^{\mathrm{succ}}_{\mathrm{sat}}$ should be used to estimate successful scan-packet transmission, and it can be derived from [6]

$$P^{\mathrm{succ}}_{\mathrm{sat}} = \frac{(g+1)(1-\tau_{\mathrm{sat}})^{g}}{1-(1-\tau_{\mathrm{sat}})^{(g+1)}}. \tag{24}$$

In (24), 1 is added for the AP in the expression (g+1). The IoT (Th_{IoT}) and scan (Th_{scan}) throughput can be derived using (4)–(24). The formulation of Th_{scan} is given by

$$Th_{\mathrm{scan}} = \sum_{j=1}^{g} (P^{\mathrm{succ}}_{\mathrm{AP}} \lambda^{\mathrm{scanslot}}_{j} + P^{\mathrm{succ}}_{\mathrm{j}} \lambda^{\mathrm{ACKscanslot}}_{j}) L_{\mathrm{scan}} MK \tag{25}$$

where L_{scan} is the packet size of the SPs. Similarly, the IoT throughput can be expressed as

$$Th_{\mathrm{IoT}} = \sum_{j=1}^{g} (\lambda^{\mathrm{UL}}_{j} P^{\mathrm{succ}}_{j} + \lambda^{\mathrm{DL}}_{j} P^{\mathrm{succ}}_{\mathrm{AP}}) L_{\mathrm{IoT}} \tag{26}$$

where L_{IoT} is the size of the UL and DL packets. Without a loss of generality, we consider the same packet size for both UL and DL data. Based on the IoT and scan throughputs, we present the security model to estimate the weights of CONF, INT, AVA, and AL. Finally, we formulate the risk as an objective function.

B. Risk Evaluation Model

In this section, we provide the complete mathematical formulation for risk, which is function of the CVSS value, as expressed in (1). Owing to changes in the temporal and environmental metrics, the overall CVSS score is given by [29]

$$V = \mathrm{round}(\mathrm{round}(\min(6.42 \times \mathrm{MISS} + \mathrm{Modexp}), 10) \times \mathrm{Temp}_{\mathrm{metric}}) \tag{27}$$

$$\mathrm{MISS} = \min(1 - ((1 - C_{\mathrm{req}} \times \boldsymbol{C}_{\mathbf{mod}})(1 - I_{\mathrm{req}} \times \boldsymbol{I}_{\mathbf{mod}}) (1 - A_{\mathrm{req}} \times \boldsymbol{A}_{\mathbf{mod}})), 0.915) \tag{28}$$

$$\mathrm{Temp}_{\mathrm{metric}} = \boldsymbol{AL} \times RL \times RC. \tag{29}$$

In (27), MISS is the modified impact score denoting the effects of attacks on any system causing changes in CONF, INT, and AVA, compared with their requirements, as defined in (28). In (28), C_{req} is the confidentiality requirement that is set according to the type of data (e.g., sensitive) communicated by an application or a system. I_{req} is the integrity requirement that depends on the importance of the accuracy of data communicated by an application, including healthcare data, which has steep requirements. Similarly, A_{req} is the availability requirement that is based on the importance of the accessibility of resources in the system. From (27) and (28), V is a function of the modified CONF (C_{mod}), modified INT (I_{mod}), and modified AVA (A_{mod}), modified because of changes in the environment, including available network resources. Moreover, V is also a function of the $\mathrm{Temp}_{\mathrm{metric}}$, which is function of AL, report confidence (RC), and remediation level (RL). AL varies because of changes in PD ($Pdelay$), which is formulated later in this section. The parameter RL and RC are independent of scan rate. Hence, we do not formulate them here. However, constant values are given as parameter settings in the next section. The details and importance of each parameter can be found in [29]. Furthermore, Modexp is the modified exploitability that reflects changes in attack approaches by attackers and characteristics of vulnerable components. Its expression is taken from [29]

$$\mathrm{Modexp} = 8.22 \times \mathrm{ModifiedAttackVector} \times \mathrm{ModifiedAttackComplexity} \times \mathrm{ModififedPrivilegesRequired} \times \mathrm{ModifiedUserInteraction}. \tag{30}$$

In (30), *ModifiedAttackVector* reflects a change in attack position of an attacker from any network, remotely, in an adjacent network, locally, etc. *ModifiedAttackComplexity* describes the modification in attacker capability or skill to exploit a vulnerability with information about the complexity of their approach. Moreover, *ModififedPrivilegesRequired* represents a change in an attacker's privilege before exploiting a vulnerability.

Similarly, *ModifiedUserInteraction* includes the need for any human access other than an attacker's to compromise the target network. The parameters in (30) are independent of the scan rate and depend on attackers' skills and approaches. Hence, we consider the value from [29], which is discussed in the Results section.

CONF and INT of IoT packets are provided by IPsec from the encryption and authentication of IoT packets transmitted between devices over untrusted networks. Moreover, we can say that C_{mod} and I_{mod} of (28) depend on the strength of the encryption algorithm. With IPsec, the sec-admin defines a set of encryption algorithms for devices based on the observation of traffic and QoS requirements, as discussed in Section III-A. Devices negotiate and choose an encryption algorithm that is transmitted during a security association. In this way, the ESP protocol gets the information about the encryption algorithm to be used. To generalize the model, we consider A to be the number of algorithms suitable for IoT. These algorithms can be identified as Algo_E, where E varies from 1 to A. In this study, we assign a weight value (E) to these algorithms according to their strengths (A). Thus, Algo_A has $E = A$ weight, which has a higher strength than the weight of Algo_{A-1} (i.e., $E = A - 1$), $A - 2, \ldots,$ and 1. As discussed, sec-admins define the encryption algorithm for IoT devices based on QoS requirements (e.g., throughput and delay) [24], [26]. Moreover, sec-admins can decide not to use any encryption algorithm or a weaker one in case of poor performance to meet the QoS requirements. Thus, we include no encryption for this article. With this model, we represent the assigned encryption algorithm using a weight value (WE) for each device on the basis of the throughput ratio (TH_{ratio}) [i.e., $Th_{\text{IoT}}/(Th_{\text{IoT}} + Th_{\text{scan}})$]. The weight based on the throughput ratio is defined as

$$WE = E, \text{ if } \frac{E-1}{A} < TH_{\text{ratio}} < \frac{E}{A}, E \in [1, A], \mathbb{N}. \quad (31)$$

For example, if $TH_{\text{ratio}} = 0.15$ and $A = 5$, then E can be calculated on the basis of the condition in (31), which is equal to two. From (31), WE is a function of IoT throughput, which is a function of scan rate. The weights of C_{mod} and I_{mod} are determined according to the ratio of the assigned WE to their maximum weight (A). However, C_{mod} and I_{mod} are defined as

$$C_{\text{mod}} = \frac{WE}{A} \quad (32)$$

$$I_{\text{mod}} = \frac{WE}{A}. \quad (33)$$

C_{mod} and I_{mod} have the same Formulas, owing to the ESP protocol with authentication, which provides both CONF and INT by encrypting payload and authentication data using the same encryption algorithm. Furthermore, we must estimate A_{mod}. Hence, A_{mod} represents the impact of the availability on the IoT, which can be expressed as the number of unsuccessful transmissions of IoT packets out of the total number of packets sent by a device in an Rslot. Hence, A_{mod} for a device, j, can be expressed as

$$A_{\text{mod}} = (1 - P_j^{\text{succ}})\left(\frac{\lambda_j^{\text{UL}} t_s}{\lambda_j^{\text{UL}} t_s + \lambda_j^{\text{ACKscanslot}}}\right). \quad (34)$$

After formulating the environmental submetrics, we derive the expression of our focused temporal submetric (AL), which depends on the PD of a device. AL is also function of mean time to compromise (MTTC) any device, denoted as TC. MTTC is estimated by an attacker's expertise and tools. However, there have been many studies that have estimated MTTC duration. An attacker usually takes a few days to attack any system based on abilities and tools. However, evaluating MTTC is beyond the scope of this study. We instead consider a constant value that can be substituted from [34]. Thus, AL can be defined as the ratio of PD to MTTC. However, if the MTTC is less than the PD, then there will be a 100% likelihood that the device will be attacked. Based on this definition, AL can be formulated as

$$AL = \begin{cases} \frac{P\text{delay}}{TC}, & \text{if } P\text{delay} < TC \\ 1, & \text{Otherwise.} \end{cases} \quad (35)$$

The PD is defined as the time required to fix the existing vulnerabilities in a device. There are two steps needed to patch the vulnerabilities: identifying vulnerabilities in any port of a device and implementing patching algorithms. Thus, the PD is equal to the time taken to identify vulnerabilities and the patching algorithm processing time. Hence, we scan all ports of a device to discover the vulnerabilities. The scan delay (t_{scan}) includes the identification time for all the vulnerabilities of a device. Moreover, we assume that patching algorithms are available. Hence, the processing time (t_{patch}) for patching is constant. The PD is formulated as

$$Pdelay = t_{\text{scan}} + t_{\text{patch}}. \quad (36)$$

In this study, we suppose that an SP is dedicated to probing a device port. Moreover, the port scanner performs a horizontal scan, thus scanning all the ports. However, as explained in Section III-B, the scan delay varies with the scan rate and network performance of the WLAN. Thus, the scan delay can be formulated based on

$$t_{\text{scan}} = \frac{N_{\text{P}} t_b}{N_{\text{Port}}^{\text{succ}}} \quad (37)$$

where N_{P} and $N_{\text{Port}}^{\text{succ}}$ are the total number of ports per device required to be probed and the number of successfully scanned ports per beacon interval, respectively. $N_{\text{Port}}^{\text{succ}}$ is calculated by the number of successful SYN packet transmissions and ACK packets per beacon interval, except for waiting packets in their queue, expressed as

$$N_{\text{Port}}^{\text{succ}} = (P_{\text{AP}}^{\text{succ}}(\lambda_j^{\text{scanslot}} - R_{\text{AP}}^{\text{Qscan}}) - R_j^{\text{QACKscan}})P_{\text{avg}}^{\text{succ}} MK. \quad (38)$$

$\lambda_j^{\text{scanslot}}$ is defined in (22). $P_{\text{avg}}^{\text{succ}}$ is the average probability of successfully transmitting a packet by any device within a group, formulated as

$$P_{\text{avg}}^{\text{succ}} = \frac{\sum_{j=1}^{g} P_j^{\text{succ}}}{g}. \quad (39)$$

In (38), $R_{\text{AP}}^{\text{Qscan}}$ and R_j^{QACKscan} are the average numbers of scan and ACK packets waiting in the queue of the AP and any

TABLE I
PARAMETER SETTINGS

Variables	*Values*
$\lambda_j^{\mathrm{ULPU}}$ (packets/second) $\lambda_j^{\mathrm{DLPU}}$,$\lambda_B^{\mathrm{UL}}$, λ_B^{DL}	j, $j \in [1, 10]$ 2, 5, 5
N_{RAW}, t_b, t_s	2, 1 s, 50 ms
$DIFS$, $SIFS$, ϕ [6]	252 μs, 160 μs, 52 μs, 0.132 ms
$W_{\min}$, m [6]	16, 7
$P = L_{\mathrm{scan/IoT}}$, ACK [6]	64 bytes, 250 bits
IPv6 parameters: P_{IPv6}, E_{IPv6}	40 bytes, 2 bytes
$datarate$, δ	4 Mbps, 1μs
Th, AI, RC, RL, TC [28] [34]	1, 1, 0.95, 1, 10 days

device per Rslot, respectively. In this study, we consider a stable and infinite buffer [i.e., $\lambda < (1/Y)$]. $R_{\mathrm{AP}}^{\mathrm{Qscan}}$ and R_j^{QACKscan} can be formulated using Little's theorem, expressed as

$$R_j^{\mathrm{QACKscan}} = \frac{(\lambda_j^{\mathrm{ACKscan}})^2}{\frac{1}{Y_j}\left(\frac{1}{Y_j} - \lambda_j^{\mathrm{ACKscan}}\right)} \tag{40}$$

$$R_{\mathrm{AP}}^{\mathrm{Qscan}} = \frac{(\lambda_j^{\mathrm{scan}})^2}{\frac{1}{Y_{\mathrm{AP}}}\left(\frac{1}{Y_{\mathrm{AP}}} - \lambda_j^{\mathrm{scan}}\right)}. \tag{41}$$

The CVSS score of any vulnerability can be derived using (31)–(41) in the CVSS equation, as presented in (27). The value of the calculated V of a device is then substituted in (1) to finally get the objective function to minimize the risk. The final optimization equation is given by

$$\begin{aligned} &\underset{TR}{\text{Minimize}} \quad Risk(TR) \\ &\text{Subject to:} \quad TR, t_{\mathrm{b}}, t_{\mathrm{R}}, t_{\mathrm{s}}, N > 0. \end{aligned} \tag{42}$$

From the overall mathematical model, we observe that the scan rate (R) influences the IoT throughput and scan delay, which, in turn, degrades encryption algorithms and increases the PD, respectively. Hence, we solve for the optimal R in the next section using numerical analysis and present our results, which show that the risk to any IoT device can be minimized.

V. Performance Evaluation

This section presents a numerical analysis of the mathematical model proposed in the previous section. According to the model, we initially analyze the IoT throughput at various scan rates per AP, which leads to changes in the weights of CONF, INT, and AVA. Furthermore, we show the effect of variations in the AL and PD on the scan rates per AP. In this analysis, our objective is to minimize the risk to an IoT device at an optimal scan rate. Thus, we finally analyze the objective function. Doing so, we can vary only N and R, because sec-admins are oblivious to other network settings. In this analysis, IEEE 802.11ah frame and IPv6 packet structure parameters are used as formulated in Section IV-A2, which are defined in Table I with other required parameters for the analysis.

A. IoT Throughput and Environmental Metrics Analysis

Fig. 4 shows the evaluation of the total IoT data throughput at various scan rates for $N = 100, 200$ Het-IoT devices per AP over the IEEE 802.11ah RAW mechanism. This analysis is performed on the basis of (26), where $P_{\mathrm{AP}}^{\mathrm{succ}}$ and $P_{\mathrm{j}}^{\mathrm{succ}}$ are derived from (11) and (10). From the result, we can observe that the IoT throughput decreases as the scan rate increases, ultimately reaching a saturation state (i.e., constant line). The reason for such behavior is the availability of channel resources at a low scan rate. Moreover, a low scan rate does not contribute significantly to network congestion via IoT packets. Furthermore, the rationale for saturated IoT throughput after a certain scan rate is the achievement of the maximum system load. We can also observe that $N = 200$ achieves a higher IoT throughput than does $N = 100$, owing to channel access by a greater number of devices per group for the former, which congests the limited network per slot. According to the IoT throughput, we determine the modified CONF and INT in Fig. 5. For this analysis, we consider five encryption algorithms that are suitable for IoT-type devices. Hence, A is equal to five in (31). The encryption algorithms include no encryption, DES-HW, DES, 3DES-HW, and AES-128, in increasing order of strength. We analyze C_{mod} and I_{mod} from (32) and (33), which are functions of TH_{ratio} according to WE. As discussed, the IoT throughput decreases as the scan rate increases, which forces security admins to set weaker algorithms or no encryption at a high scan rate. Consequently, the values of WE, C_{mod}, and I_{mod} decrease greatly. However, C_{mod} and I_{mod} are constant after a certain scan rate, owing to the saturated IoT throughput. For $N = 200$, the weights of C_{mod} and I_{mod} are lower than those for $N = 100$, owing to the lower IoT throughput of the former. Similarly, analysis of another parameter of environmental metrics (i.e., A_{mod}) is shown in Fig. 6, which is evaluated using (34). In Fig. 6, we can see that the availability of packets decreases as the scan rates increase, owing to an increase in the collision of IoT packets with a large number of SPs. The availability of packets is higher for $N = 100$ compared with $N = 200$, as in the former case, because there are few devices/groups. Thus, the congestion in every Rslot is reduced. This impact of SPs on regular data can also be considered to be a scan attack [10]. Hence, our approach to optimize the scan rate can avoid such types of attacks as well. From the discussion presented above, we can conclude that an appropriate scan rate should be set such that environmental submetrics can

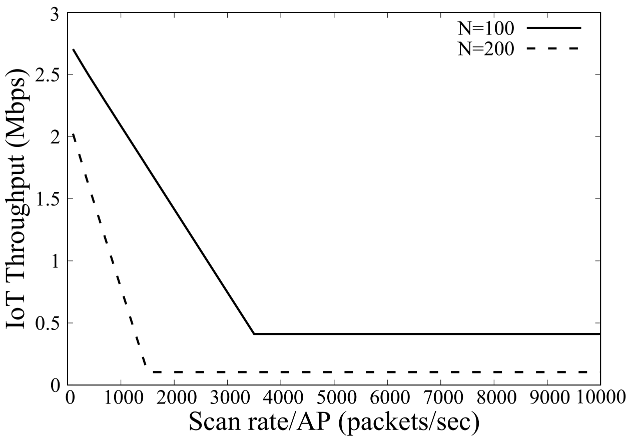

Fig. 4. IoT throughput at various scan rate.

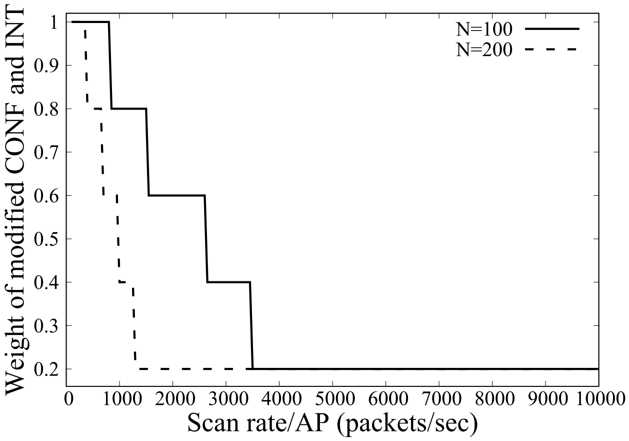

Fig. 5. Variation of C_{mod} and I_{mod} at various scan rates.

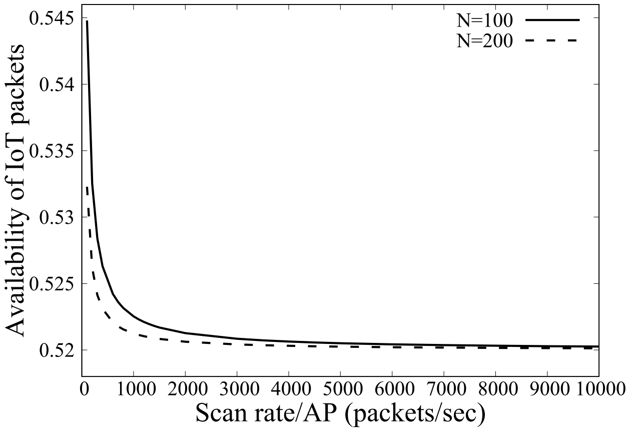

Fig. 6. Availability of IoT packets at different scan rates.

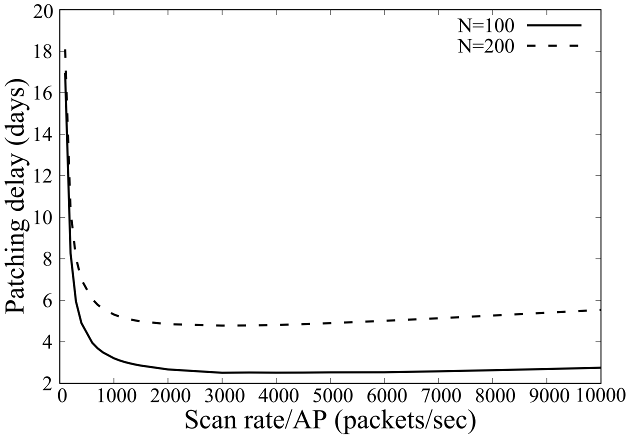

Fig. 7. Patching-delay analysis at various scan rates.

lead to high performance without significantly affecting the security.

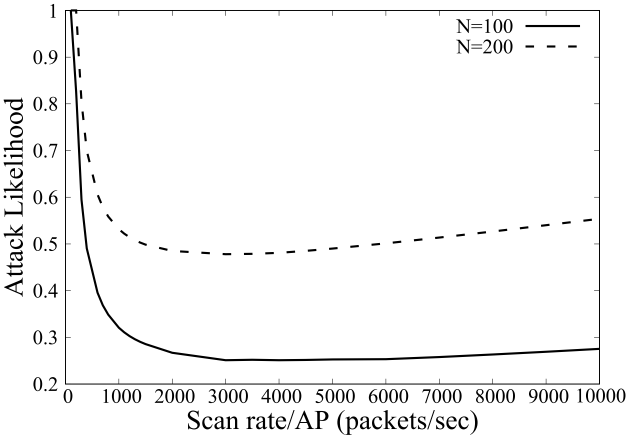

Fig. 8. AL for an IoT device.

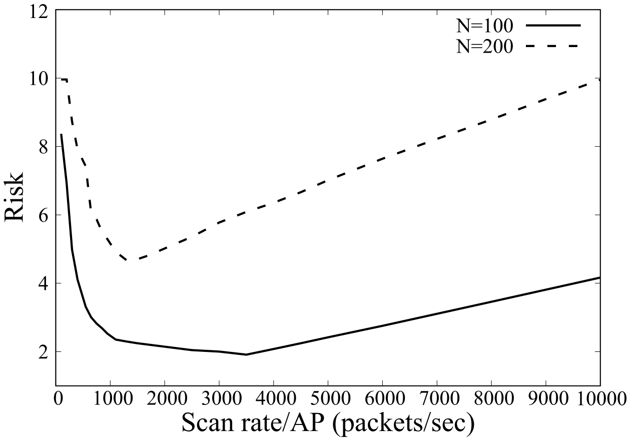

Fig. 9. Risk to each IoT device.

B. Temporal Metrics Analysis

The analysis of the temporal metrics is shown in Figs. 7 and 8. From Fig. 7, we observe that the PD is high at low scan rates, owing to the slow scan performance. It decreases to a certain scan rate. Thereafter, it increases because of network congestion and unsuccessful transmission of SPs. Unsuccessful transmission is responsible for the increase in the scan delay of the identification of vulnerabilities or services at all ports. AL is a function of the PD, as determined by (35). Hence, in Fig. 8, the AL has a higher value at low or high scan rates, and it is directly proportional to the PD. Therefore, it is imperative to set an appropriate scan rate such that the AL is minimized. Moreover, the PD and AL for $N = 100$ are lower than those for $N = 200$, owing to the small number of devices per group, which reduces the congestion at each Rslot. From this discussion, we can conclude that an appropriate scan rate for N IoT devices will reduce the impact on the temporal metrics of CVSS, which in turn will improve the security.

C. Risk Minimization

Our objective in this analysis is to minimize the risk caused by the impact of the scan rate on the security services of an IoT device. Finally, based on the previous analysis and risk formulae, we present the result of risk evaluation at various scan rates in Fig. 9. We can observe that the risk value is high at lower scan rates owing to the influence of a high PD and high AL. For instance, the risk value of 8.3 at a lower scan rate = 100 for $N = 100$. As quantitative values of risk provided in Section III-A, maximum value of risk can be 10, that denotes low security of an IoT device. The risk value of 8.3 is close to 10, which indicates that the risk on a IoT device is higher at a lower scan rate. Similarly, the risk value at a higher scan rate such as 9000 for $N = 200$ is 9.95, which is very close to 10. This implies that the IoT device can be highly unsecured. Therefore, the risk is minimized for an IoT device to 1.91 in the case of $N = 100$ at $R = 3500$. The risk value 1.91 is close to 0, which means it has low risk. Similarly, for $N = 200$, the risk is minimized at $R = 1300$ and obtained risk value is 4.6, which means risk is medium in this case. The optimal scan rate is high for $N = 100$ than $N = 200$ owing to low congestion at network due to less number of devices per group in $N = 100$. From Fig. 9 and quantitative analysis, we can see that our proposed model provides an optimal scan rate that minimizes risk and improves the security of IoT device.

VI. Conclusion

We proposed a novel network-aware IWPS used to set an optimal scan rate for sec-admins such that the security of IoT devices is maximized over emerging WLANs, such as IEEE 802.11ah. To include heterogeneous traffic of IoT and scan-packet arrival, we designed a novel queue model based on the Markov chain for each IoT device and AP. Then, we proposed a mathematical model to estimate the IoT and scan throughput based on the IEEE 802.11ah RAW mechanism, the CSMA/CA process, and the scan traffic for the proposed queue model. We also formulated a mathematical model used to evaluate the risk to each IoT device, which consists of new models used to assess CONF, INT, AVA, and AL at various scan rates. Using these models, we performed numerical analyses to ascertain the effect of the scan rate on the variations of CONF, INT, AVA, and AL caused by low network performance (e.g., IoT throughput, unsuccessful IoT packet transmissions, and scan delays) under scan-rate variations. We optimized this tradeoff by minimizing the risk to each device at an optimal scan rate in the final analysis. From our analyses, we observed that an optimal scan rate provides high security while ensuring QoS. However, this approach considers the perspective of a sec-admin, who cannot control the network parameters. Hence, the network cannot be utilized efficiently for security enhancements. Thus, in the future, we plan to design a security-aware adaptive IEEE-802.11ah-based model for network operators to optimize the RAW parameters according to the scan traffic.

Appendix

In this Appendix, we present the derivation of the PMF of the distribution of SPs (P_{scan}) to a device in an Rslot [i.e., as stated in (21)]. Let us assume that SPs arriving per Rslot are distributed randomly. Hence, we derive the distribution of incoming SPs per slot. Let X be a discrete random variable signifying the number of SPs assigned to a device, $x \in [1, R']$. There are g devices in a group. Hence, total number of ways SPs ($total_{\text{way}}$) can distribute among g devices can be given as formulation of distribution of identical objects into distinct bins (i.e., identical SPs to distinct devices), expressed as

$$\text{total}_{\text{way}} = {}^{g+R'-1}\mathbf{C}_{R'-1}. \tag{43}$$

However, the number of ways SPs [$total_{\text{xway}}(x)$] can be distributed, given a device receives x SPs that range from 1 to R', is formulated below:

$$\begin{aligned} \text{total}_{x\text{way}}(0) &= {}^{g+R'-2}\mathbf{C}_{R'-2} \\ \text{total}_{x\text{way}}(1) &= {}^{g-1+R'-2}\mathbf{C}_{R'-2} \\ &\vdots \\ \text{total}_{x\text{way}}(R') &= {}^{g-R'+R'-2}\mathbf{C}_{R'-2}. \end{aligned} \tag{44}$$

Based on (44), the expression for $total_{\text{xway}}(x)$ can be written as

$$\text{total}_{x\text{way}}(x) = {}^{g-x+R'-2}\mathbf{C}_{R'-2} \quad x \in [1, R']. \tag{45}$$

The PMF for receiving x packets by a device can be written as

$$P_{\text{scan}}(X = x) = \frac{{}^{g-x+R'-2}\mathbf{C}_{R'-2}}{{}^{g+R'-1}\mathbf{C}_{R'-1}}. \tag{46}$$

References

[1] J. Wu, M. Dong, K. Ota, J. Li, and W. Yang, "Application-aware consensus management for software-defined intelligent blockchain in IoT," *IEEE Netw.*, vol. 34, no. 1, pp. 69–75, Jan./Feb. 2020.

[2] H. Li, K. Ota, and M. Dong, "LS-SDV: Virtual network management in large-scale software-defined IoT," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 8, pp. 1783–1793, Aug. 2019.

[3] S. Verma, Y. Kawamoto, Z. M. Fadlullah, H. Nishiyama, and N. Kato, "A survey on network methodologies for real-time analytics of massive IoT data and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1457–1477, 3rd Quart., 2017.

[4] D. S. Roy, R. K. Behera, K. H. K. Reddy, and R. Buyya, "A context-aware fog enabled scheme for real-time cross-vertical IoT applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2400–2412, Apr. 2019.

[5] S. Verma, Y. Kawamoto, and N. Kato, "Energy-efficient group paging mechanism for QoS constrained mobile IoT devices over LTE-A pro networks under 5G," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9187–9199, Oct. 2019.

[6] L. Zheng, M. Ni, L. Cai, J. Pan, C. Ghosh, and K. Doppler, "Performance analysis of group-synchronized DCF for dense IEEE 802.11 networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6180–6192, Nov. 2014.

[7] B. Mao, Y. Kawamoto, J. Liu, and N. Kato, "Harvesting and threat aware security configuration strategy for IEEE 802.15.4 based IoT networks," *IEEE Commun. Lett.*, vol. 23, no. 11, pp. 2130–2134, Nov. 2019.

[8] D. L. Hoang, T. H. Tran, and Y. Nakashima, "Performance evaluation of 802.11ah physical layer phase encryption for IoT applications," in *Proc. IEEE Int. Conf. Adv. Technol. Commun. (ATC)*, Ho Chi Minh City, Vietnam, pp. 84–88, Oct. 2018.

[9] N. Vlajic and D. Zhou, "IoT as a land of opportunity for DDoS hackers," *IEEE Comput.*, vol. 51, no. 7, pp. 26–34, Jul. 2018.

[10] E. Bou-Harb, M. Debbabi, and C. Assi, "Cyber scanning: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1496–1519, 3rd Quart., 2013.

[11] L. Metongnon, E. C. Ezin, and R. Sadre, "Efficient probing of heterogeneous IoT networks," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, Lisbon, Portugal, May 2017, pp. 1052–1058.

[12] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-wide scanning and its security applications," in *Proc. 22nd USENIX Security Symp.*, Washington, DC, USA, Aug. 2013, pp. 605–620.

[13] H. Hashida, Y. Kawamoto, and N. Kato, "Efficient delay-based Internet-wide scanning method for IoT devices in wireless LAN," *IEEE Internet Things J.*, vol. 7, no. 2, pp. 1364–1374, Feb. 2020.

[14] F. Tang, Y. Kawamoto, N. Kato, K. Yano, and Y. Suzuki, "Probe delay based adaptive port scanning for IoT devices with private IP address behind NAT," *IEEE Netw.*, vol. 34, no. 2, pp. 195–201, Mar. 2020.

[15] C. Gomez, J. Paradells, C. Bormann, and J. Crowcroft, "From 6LoWPAN to 6Lo: Expanding the universe of IPv6-supported technologies for the Internet of Things," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 148–155, Dec. 2017.

[16] T. Savolainen, J. Soininen, and B. Silverajan, "IPv6 addressing strategies for IoT," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3511–3519, Oct. 2013.

[17] J. Guo, C. Gu, X. Chen, and F. Wei, “Model learning and model checking of IPSec implementations for Internet of Things,” *IEEE Access*, vol. 7, pp. 171322–171332, 2019.

[18] P. Varadarajan and G. Crosby, “Implementing IPsec in wireless sensor networks,” in *Proc. 6th IEEE Int. Conf. New Technol. Mobility Security (NTMS)*, Dubai, UAE, May 2014, pp. 1–5.

[19] L. Markowsky and G. Markowsky, “Scanning for vulnerable devices in the Internet of Things,” in *Proc. IEEE 8th Int. Conf. Intell. Data Acq. Adv. Comput. Syst. Technol. Appl. (IDAACS)*, Warsaw, Poland, Dec. 2015, pp. 463–467.

[20] R. Graham. *MASSCAN: Mass IP Port Scanner*. Accessed: Dec. 16, 2020. [Online]. Available: https://github.com/robertdavidgraham/masscan

[21] A. Sperotto, G. Schaffrath, R. Sadre, C. Morariu, A. Pras, and B. Stiller, “An overview of IP flow-based intrusion detection,” *IEEE Commun. Surveys Tuts.*, vol. 12, no. 3, pp. 343–356, 3rd Quart., 2010.

[22] F. J. Aparicio-Navarro, K. G. Kyriakopoulos, Y. Gong, D. J. Parish, and J. A. Chambers, “Using pattern-of-life as contextual information for anomaly-based intrusion detection systems,” *IEEE Access*, vol. 5, pp. 22177–22193, 2017.

[23] E. Khorov *et al.*, “Enabling the Internet of Things with Wi-Fi halow-performance evaluation of the restricted access window,” *IEEE Access*, vol. 7, pp. 127402–127415, 2019.

[24] W. He and K. Nahrstedt, “An integrated solution to delay and security support in wireless networks,” in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Las Vegas, NV, USA, Apr. 2006, pp. 2211–2215.

[25] B. Mao, Y. Kawamoto, and N. Kato, “AI-based joint optimization of QoS and security for 6G energy harvesting Internet of Things,” *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7032–7042, Aug. 2020.

[26] Z. M. Fadlullah, C. Wei, Z. Shi, and N. Kato, “GT-QoSec: A game-theoretic joint optimization of QoS and security for differentiated services in next generation heterogeneous networks,” *IEEE Trans. Wireless Commun.*, vol. 16, no. 2, pp. 1037–1050, Feb. 2017.

[27] S. Yazar, “A qualitative risk analysis and management tool—CRAMM,” SANS InfoSec, Rockville, MD, USA, White Paper, pp. 12–32, Apr. 2002.

[28] R. I. Bonilla, J. J. Crow, L. S. Basantes, and L. G. Cruz, “A metric for measuring IoT devices security levels,” in *Proc. IEEE 15th Int. Conf. Depend. Auton. Secure Comput.*, Orlando, FL, USA, Nov. 2017, pp. 704–709.

[29] Forum of Incident Response and Security Teams (FIRST). *Common Vulnerability Scoring System Version 3.1: Specification Document*. Accessed: Dec. 16, 2020. [Online]. Available: https://www.first.org/cvss/specification-document

[30] National Institute of Standards and Technology. *National Vulnerability Database (NVD)*. Accessed: Dec. 16, 2020. [Online]. Available: https://nvd.nist.gov/

[31] N. Nikaein *et al.*, “Simple traffic modeling framework for machine type communication,” in *Proc. IEEE 10th Int. Symp. Wireless Commun. Syst.*, Ilmenau, Germany, Aug. 2013, pp. 1–5.

[32] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” *IEEE J. Sel. Areas Commun.*, vol. 18, no. 3, pp. 535–547, Mar. 2000.

[33] *Draft-Delcarpio-6LO-Wlanah-01—IPv6 Over 802.11ah*. Accessed: Jan. 1, 2021. [Online]. Available: https://tools.ietf.org/html/draft-delcarpio-6lo-wlanah-01

[34] M. McQueen, W. Boyer, M. Flynn, and G. Beitel, “Time-to-compromise model for cyber risk reduction estimation,” in *Proc. Qual. Protect. Workshop*, Boston, MA, USA, Sep. 2005, pp. 49–64.

Shikhar Verma (Student Member, IEEE) received the bachelor’s degree in computer science and engineering from the National Institute of Science and Technology, Berhampur, India, in 2014, and the M.Sc. degree from the Graduate School of Information Sciences, Tohoku University, Sendai, Japan, in 2018, where he is currently pursuing the Ph.D. degree in applied information science.

Mr. Verma was a recipient of the prestigious MEXT Scholarship, the IEEE ComSoc Sendai Chapter Student Excellence Research Award in 2017, and the Best Paper Award at IEEE ICC 2018. He is currently a JSPS Fellow.

Yuichi Kawamoto (Member, IEEE) received the B.E. degree in information engineering from Tohoku University, Sendai, Japan, in 2013, and the M.S. and Ph.D. degrees from the Graduate School of Information Sciences (GSIS), Tohoku University, in 2016.

He has been an Associate Professor with GSIS, Tohoku University since 2019.

Dr. Kawamoto was a recipient of the prestigious Dean’s Award and President’s Award from Tohoku University in 2016. He also received best-paper awards at several conferences, namely, IWCMC’13, GLOBECOM’13, and WCNC’2014.

Nei Kato (Fellow, IEEE) Nei Kato received the M.D. and Ph.D. degrees in information engineering from Tohoku University, Sendai, Japan, in 1988 and 1991, respectively.

He is currently a Full Professor (Deputy Dean) with the Graduate School of Information Sciences and the Director of the Research Organization of Electrical Communication, Tohoku University, Sendai, Japan. He has been engaged in research on computer networking, wireless mobile communications, satellite communications, ad hoc, sensor, and mesh networks, smart grids, AI, IoT, big data, and pattern recognition. He has published more than 400 papers in prestigious peer-reviewed journals and conferences.

Prof. Kato awards include the Minoru Ishida Foundation Research Encouragement Prize in 2003, the Distinguished Contributions to Satellite Communications Award from the IEEE Communications Society, Satellite and Space Communications Technical Committee in 2005, the FUNAI Information Science Award in 2007, the TELCOM System Technology Award from the Foundation for Electrical Communications Diffusion in 2008, the IEICE Network System Research Award in 2009, the IEICE Satellite Communications Research Award in 2011, the KDDI Foundation Excellent Research Award in 2012, the IEICE Communications Society Distinguished Service Award in 2012, the IEICE Communications Society Best Paper Award in 2012, the Distinguished Contributions to Disaster-resilient Networks R&D Award from the Ministry of Internal Affairs and Communications, Japan, in 2014, the Outstanding Service and Leadership Recognition Award in 2016 from the IEEE Communications Society Ad Hoc & Sensor Networks Technical Committee, the Radio Achievements Award from the Ministry of Internal Affairs and Communications, Japan, in 2016, the IEEE Communications Society Asia–Pacific Outstanding Paper Award in 2017, the Prize for Science and Technology from the Minister of Education, Culture, Sports, Science and Technology, Japan, in 2018, the Award from Tohoku Bureau of Telecommunications, Ministry of Internal Affairs and Communications, Japan, 2018, and the best paper awards at IEEE ICC, GLOBECOM, WCNC, and VTC. He is the Vice President (Member & Global Activities) of the IEEE Communications Society from 2018 to 2021. He has been the Editor-in-Chief of IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY since 2017, and the Chair of IEEE Communications Society Sendai Chapter. He served as the Editor-in-Chief for the *IEEE Network Magazine* from 2015 to 2017, a Member-at-Large on the Board of Governors, IEEE Communications Society from 2014 to 2016, the Vice Chair of the Fellow Committee of IEEE Computer Society in 2016, and a member of the IEEE Communications Society Award Committee from 2015 to 2017. He has also served as the Chair of the Satellite and Space Communications Technical Committee from 2010 to 2012 and Ad Hoc & Sensor Networks Technical Committee from 2014 to 2015 of the IEEE Communications Society. He is a Distinguished Lecturer of the IEEE Communications Society and Vehicular Technology Society. He is also a Fellow of the Engineering Academy of Japan and IEICE.