Third Eye: Context-Aware Detection for Hidden Terminal Emulation Attacks in Cognitive Radio-Enabled IoT Networks

Moinul Hossain, *Member, IEEE*, and Jiang Xie, *Fellow, IEEE*

***Abstract*—Recently, the Internet of Things (IoT) technology has been drawing increasing attention because it has a great potential to positively impact human life in a broad range of applications. Nonetheless, the dense deployment of multiple co-located IoT networks that may follow different wireless protocols will essentially bring new network vulnerabilities. In this paper, we introduce a novel attack scenario in co-located cognitive radio (CR) enabled IoT networks, where a reactive attacker can emulate the radiation pattern of a hidden terminal (the attacker is from a different network) and can interfere with the transmissions from its hidden counterparts, namely the *hidden terminal emulation* (HTE) attack. As the dense deployment of IoT nodes—from different networks and technologies—will naturally create such hidden terminal scenarios among IoT devices of different networks, it provides the HTE attacker plausible deniability to reactively interfere with its hidden counterparts; hence, the state-of-the-art reactive attack detection techniques are infeasible in this scenario where benign hidden terminals could be flagged as reactive attackers. In this paper, we capture the behavior of a benign hidden terminal and an HTE attacker via parsimonious Markov models and propose a context-aware detection solution using the Markov chain hypothesis testing, namely the *Third Eye*. Though there has been extensive research on malicious interference detection, to the best of our knowledge, this work is the first that considers hidden terminals as benign interference sources, foresees this unique attack scenario, and leverages the existing carrier sensing technique as a natural and effective way to detect HTE attacks.**

***Index Terms*—IoT security, context-aware detection, Markov chain, hidden Markov model.**

I. Introduction

THE INTERNET of Things (IoT) [1] is a ubiquitous technology that can intricately integrate devices (or things) that surround us. These devices communicate within themselves by forming a closed connected network to intelligently solve real-life problems. Such a broad vision requires an enormous amount of IoT deployments at our homes, offices, transportation systems, health-care, and industries.

Manuscript received June 16, 2019; revised November 8, 2019; accepted January 8, 2020. Date of publication January 21, 2020; date of current version March 6, 2020. This work was supported in part by the US National Science Foundation (NSF) under Grant No. 1718666, 1731675, 1910667, and 1910891. The associate editor coordinating the review of this article and approving it for publication was L. Wang. *(Corresponding author: Jiang Xie.)*

The authors are with the Department of Electrical and Computer Engineering, University of North Carolina at Charlotte, Charlotte, NC 28223 USA (e-mail: mhossai4@uncc.edu; linda.xie@uncc.edu).

Digital Object Identifier 10.1109/TCCN.2020.2968324

However, the rapid and dense deployment of IoT engenders a new set of challenges; spectrum scarcity is one of the most important open research challenges among these. Currently, different wireless technologies that operate on the licensed spectrum are vying for the utilization of the unlicensed spectrum [2]–[7]. Therefore, the unlicensed spectrum is becoming less hospitable for resource sharing and more susceptible to interference. The dense deployment of IoT devices—using such wireless technologies as WiFi, ZigBee, and Bluetooth—in overpopulated unlicensed bands will aggravate these interference issues further; hence, FCC (Federal Communication Commission) proposes to reconsider the way we use spectrum resources and to devise strategies to allow resource sharing in the licensed spectrum in order to increase the overall spectrum utilization.

Cognitive radio (CR) offers an intelligent solution to offset this issue [8], [9], where a CR-enabled IoT device can opportunistically access a licensed channel and utilize it until a licensed user (or primary user, PU) reappears to avoid interference with other co-located IoT devices. *Spectrum sensing* helps CR-enabled IoT devices to be aware of and to be sensitive to the changes in its network environment [10]. Here, IoT devices utilize this real-time spectrum sensing information to help them in finding spectrum holes (i.e., underutilized licensed channels) and to avoid interference with PUs and other co-located IoT devices. Therefore, CR technology offers a feasible and compelling way to enable the dense deployment of IoT devices and to increase the spectrum utilization. Nonetheless, such an unprecedented deployment of numerous IoT devices in comparatively small physical spaces will likely bring unforeseen security implications.

Motivations: The dense deployment of IoT devices may bring a new vulnerability where attackers can exploit a natural interference scenario to corrupt transmissions or receptions of particular victim IoT devices, i.e., *interference from hidden terminal devices* of a different IoT network. Fig. 1 provides an illustration of this vulnerability, where nodes B2 and B4 are hidden terminals to nodes A1, A3, and A5, and vice versa. Note that these two sets of nodes are from two different networks (they may even follow different wireless technologies), and under the given scenario, each of these two sets has no idea about the transmissions of the other set (because there is no resolution technique to solve the hidden terminal issue among different networks and different technologies). Therefore, it is probable that, as these two sets of nodes are

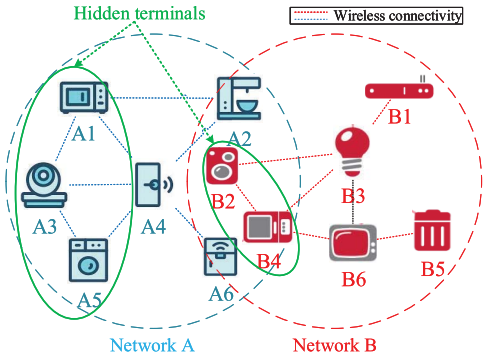


Fig. 1. Interference between coexisting IoT networks.

out of each other's radio range, nodes of these two sets may utilize the same radio channel and create interference at nodes that are exposed to both of these sets, i.e., A2 and A4.

The concurrent transmission from these hidden sets acts as an interference signal at the corresponding receiver or exposed node. Using state-of-the-art techniques, it is likely impossible to differentiate between a benign node (i.e., a hidden terminal) and a reactive attacker because hidden terminal interference bears the signature of reactive attack; hence, infeasible to deploy in the given scenario. Therefore, if an attacker can impersonate a hidden terminal to a particular IoT device, the attacker can hide behind the curtain of this natural interference scenario to corrupt the transmission intended for a particular receiver or the transmission generated from a particular transmitter. This creates an unsought challenge to differentiate between benign and malicious interference.

Challenges: In security research, a detection or defense strategy is as strong as the attack model. Therefore, the primary challenge to devise an effective detection technique is to devise a strong attack strategy. Unlike conventional jamming attackers, HTE attackers try to attack a particular network device; therefore, the straightforward approach of transmitting a constant noise signal in victim's operating channel is not ideal for the objective because it will also impact other network devices. A better approach is to attack only when a transmission to the victim is heard (i.e., receiver or exposed node is the victim), namely the reactive approach. Successful impersonation of a hidden terminal—by manipulating the antenna radiation pattern—helps the attacker to interfere with the reception of the victim reactively.

However, a naive reactive attacker may try to attack each time it hears a transmission to the victim device. Though it is the most damaging strategy against the victim and provides the highest attack efficiency, it increases the risk of being detected. Even if a detector can somehow manage to identify the malicious interference, a random strategy with uncertainty in the attacker's behavior would make conventional detection techniques futile against it. Therefore, the reactive attack must introduce randomness—as close as possible to the behavior of a benign hidden terminal—to trade-off between the attack objective (e.g., degrading victim's throughput) and the risk of exposure.

Prior works on detecting jamming attacks are mostly based on network performance measurements, such as the packet delivery rate (PDR), the received signal strength (RSS), the channel busy ratio, and the number of retransmission attempts. Although these detection methods are effective, they always considered the jammer as an outsider who creates only noise signal; hence, these are inapplicable in the illustrated scenario where the attacker is intelligently creating malicious interference using regular data packets. In addition, prior techniques may falsely categorize benign hidden terminals as reactive attackers. Therefore, we require a context-aware detection strategy that considers hidden terminals as benign interference sources and that can counteract the randomness in the attacker's behavior.

Contributions: In this paper, we study these challenges and propose solutions. The novel contributions of this paper are summarized in the following:

1. We propose a randomized reactive attack model by exploiting the hidden terminal scenario, namely the HTE attack. In the proposed model, the attacker poses as a hidden terminal by manipulating its antenna radiation pattern and interferes with the reception of the victim.
2. We propose a context-aware HTE attack detection method based on a five-state Markov model that detects an HTE attacker by its violation of the benign behavior of a hidden terminal, namely the *Third Eye*. We solve the detection problem by converting it into a hypothesis testing problem.

The rest of this paper is organized as follows. In Section II, prior jamming attacks and their detection techniques are reviewed briefly. Then in Section III, the system model that is considered in this paper is explained. We provide a brief overview of the proposed attack model in Section IV and followed by the mathematical formulation of the benign hidden terminal behavior in Section V. We further discuss the rationale behind the proposed attack strategy, as compared to other strategies, in Section VI and then formulate the detection problem in Section VII. Simulation results are shown and discussed in Section VIII, followed by the concluding remarks.

II. Related Work

Unlike traditional jamming attacks, the HTE attack does not rely on a strong noise signal to corrupt the wireless reception of the victim. Instead, it exploits the proximity to the victim and utilizes regular data transmissions to corrupt victim's reception. Though HTE is not a jamming attack, in this paper, we compare it to the jamming attack because of the close resemblance between these two attacks from the perspective of denial-of-service (DoS) attacks.

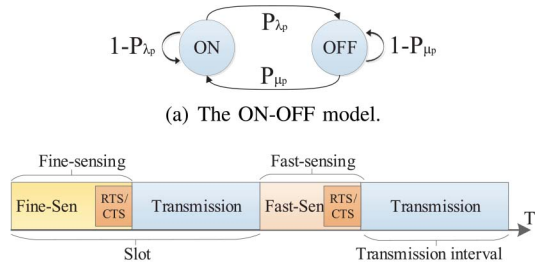
Discussion on Prior Work: In wireless networks, jamming is one of the well-researched attacks. The detection of traditional jamming attacks has been extensively studied in [11]–[22]. In [11], the influence of different jamming strategies on the PDR and the RSS of network links is analyzed and a thresholding algorithm is proposed. In addition to the PDR and the RSS, the channel busy ratio and the number of retransmission attempts are employed in [13], [14], and a machine learning based technique is proposed to detect jamming attacks. Jamming attacks in time-critical networks are studied in [15],

and numerical results on the impact of jamming on the network message invalidation ratio is presented. Moreover, in [23], an anomaly-based detection technique is proposed to detect anomalous behaviors of external neighboring nodes in dense IoT scenarios. An approach based on group testing to identify which node triggers the reactive attack is proposed in [16], in wireless sensor networks. In [24]–[27], the impact of jamming attacks on the theoretical performance of IEEE 802.11 networks is presented and analyzed for different types of jamming strategies; these theoretical analyses are based on Bianchi's Markov chain model of 802.11 distributed coordination function (DCF) [28]. In CR-enabled networks, DoS attacks are studied in [29]–[33], where the attacker attacks in the off-sensing interval and creates an illusion of PU reappearance to force the victim out of its current operating channel. In [18], a mathematical model of an optimal jamming strategy is proposed, where an attacker can regulate its jamming probability to trade-off between the reward of jamming and the penalty of exposure.

Differences From Prior Work: Although there is no direct comparable work to compare HTE with (except an earlier work [23]), differences between existing work on jamming and our proposed work can be noted as follows. Interestingly, [18] considers the slotted Aloha protocol, which does not incorporate the carrier sensing multiple access (CSMA)—an essential tool in modern wireless networks; in contrast, our work is based on the widely accepted CSMA approach. While the influence of *in network* hidden terminal interference is considered in [34], it did not explain how a reactive attacker can listen to the transmission of its hidden counterparts; in contrast, we capture the impact of hidden terminal interference from *external networks*, based on the carrier sensing, and we propose how an HTE attacker can listen to its hidden counterparts via antenna manipulation. Moreover, though an anomaly-based detection technique is proposed in [23], it fails to efficiently identify HTE attacks when there are multiple anomalies in the network. In summary, compared to all these prior works, we address the hidden terminal interference issue among different co-located networks/technologies, and we devise an attack model based on this. As prior work on attack detection mostly depends on the network performance and does not consider hidden terminals as benign interference sources (except [23], [34]), they may mis-categorize hidden terminals as reactive attackers. In this work, we consider hidden terminals as benign interference sources, address the way attackers can inappropriately use it for malice intentions, and propose a signature-based context aware detection model to uniquely identify HTE attacks.

III. System Model

We consider a benign IoT network with multiple CR-enabled IoT devices that are trying to communicate among themselves in an ad-hoc mode; we name it the *internal network*. These benign IoT devices are surrounded by other co-located CR-enabled IoT devices from a different network; we name the network as *external network*. To successfully perpetrate the attack, the external network must have at least two



(a) The ON-OFF model.

(b) The channel access schedule.

Fig. 2. System model.

IoT devices. We will explain the reason in Section IV. In the following, we explain our system model.

Channel Model: We consider the presence of M homogeneous channels, each with equal bandwidth, and M PUs using these channels. Here, time is divided into equal slots and transmissions are packet-based. A packet starts at the beginning of a slot and finishes at the end of a slot. Each PU randomly selects a channel to access and alternates between the ON and the OFF states, according to an ON-OFF model that follows the Poisson packet arrival process (with an average arrival rate λ_p) and the exponentially distributed packet length (with an average length μ_p). In Fig. 2(a), P_{λ_p} and P_{μ_p} denote the transition probabilities from the ON to OFF state and from the OFF to ON state, respectively.

IoT Node Model: We consider that the defending (or victim) IoT device has $k-1$ neighbors, and they use omni-directional antennas for communications. These k nodes (including the defender) have an available channel list (ACL) $m_i \in \{1, 2, \ldots, M\}$, where $i \in k$, based on the spectrum sensing result. Each internal IoT device is equipped with one radio for wide-band spectrum sensing [35] and one radio for control information exchange and data transmission. We consider that channel conditions are ideal and that a transmission failure results from interference among hidden terminals only. In the following, we use *interference* and *collision* interchangeably.

Channel Access: Each transmission attempt of an IoT device must be preceded by a sensing interval. As shown in Fig. 2(b), IoT devices employ their sensing antenna to sense the current channel before initiating a transmission, and they continue to sense the channel periodically during the transmission to minimize the collision between PUs and IoT devices. An IoT device is allowed to access a channel when it finds the sensing result is suitable to transmit (e.g., senses that no PU is present). After sensing that the channel is available, two IoT devices exchange request-to-send/clear-to-send (RTS/CTS) messages to reserve the channel. IoT devices initiate a new data packet transmission with the longer fine-sensing and employ the shorter fast-sensing for each successive frame.

During a sensing interval, if an IoT device senses that the current channel is busy, it pauses the communication attempt on the current channel, performs a spectrum handoff to a new channel (from the current ACL) in the next-slot, and resumes the communication attempt on the new channel.

Network Coordination Scheme: Here, we consider that a common control channel is unavailable and that two IoT

devices must find a common available channel between them to initiate communication. The rendezvous technique works as the process to find a common available channel [36]. However, the choice of a specific rendezvous scheme does not impact the performance of our work, as long as attackers have no prior knowledge of the victim's channel hopping sequence. Hence, we assume that IoT devices have already successfully performed rendezvous with each other using any existing rendezvous scheme, and they share a time-seeded pseudo-random channel hopping sequence for future communications.

Wireless Activity Monitoring: We considered a multi-channel spectrum band (similar to IEEE 802.11) for cognitive communications. Like IEEE 802.11, in the system model, wireless devices can monitor activities on other channels through spectrum sensing, i.e., the listen-before-talk mechanism. Moreover, an IoT node can learn the identity of neighboring out-of-network wireless nodes from the broadcast messages. For instance, every wireless node—such as Bluetooth, WLAN, ZigBee—broadcasts their identity for communication.

IV. Overview of the Proposed Hidden Terminal Emulation Attack

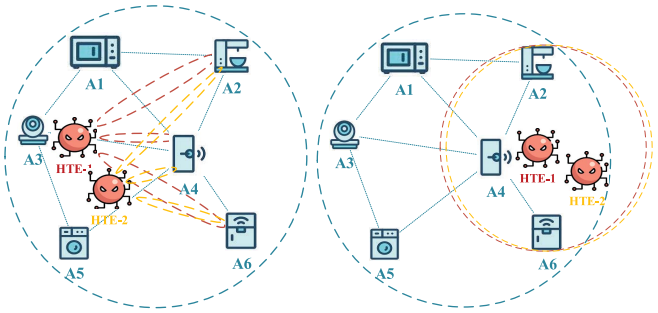
In this section, we briefly discuss how an attacker can exploit its antenna radiation pattern to impersonate a hidden terminal, which is essentially a form of location forging attack. In prior work, location forging is considered a localization problem, and anchor devices—specially equipped to locate any device—play an important role in detecting location forging attacks. However, in most IoT applications, IoT devices are highly unlikely to be equipped with sophisticated localization capabilities, and it is unrealistic to deploy anchor devices in dense IoT networks; hence, in dense IoT scenarios, off-the-shelf location spoofing detection methods are inapplicable. Therefore, we take a different approach in designing the HTE attack where we emphasize how an attacker must behave and reactively interfere after successfully emulating a hidden terminal. The attacker perpetrates the HTE attack in two sequential phases: the reconnaissance and emulation phase and the reactive interference phase.

A. HTE Attack Phases

In this subsection, we briefly enumerate different attack phases of the proposed HTE attack.

Reconnaissance and Emulation Phase: The primary task of an HTE attacker in this phase is to successfully emulate the radiation characteristics of a hidden terminal at the neighbors of the victim(s). In this paper, we consider the exposed node(s) as victim(s) (e.g., A2 and A4 in Fig. 3), and the attacker is motivated to reactively interfere with transmissions originating from the hidden nodes that are destined for the victim node(s).

To achieve its goal, the attacker first obtains the geometric locations of the IoT devices by wardriving [37] and other off-the-shelf techniques, such as the angle of arrival and distance to the transmitter [38], i.e., the reconnaissance phase. Now, depending on the objective of the attacker and its physical limitations, the attacker may try to pose as a hidden terminal to



(a) The real scenario. (b) The emulated scenario.

Fig. 3. The hidden terminal emulation attack.

all neighbors or selected neighbors of the victim. In Fig. 3(a), attackers try to pose themselves as hidden terminals to nodes A1, A3, and A5; they limit their transmissions only to nodes A2, A4, and A6. The intelligent utilization of antennas enables attackers to emulate a different physical scenario, which is represented in Fig. 3(b), i.e., the emulation phase.

However, with conventional omnidirectional radios, realizing HTE attack is not possible because the path loss vector is the same at each direction. An attacker, nonetheless, can use the smart antenna beamforming capability to solve this problem [39] and mimic the signal characteristics of the spoofed location. Please note that, as complex localization schemes are highly unlikely to be present in general IoT devices, an attacker does not mimic the exact RSS signature of the spoofed location; instead, it maintains an average signal strength equal to or above the receiver sensitivity threshold at the exposed node(s) and an average signal strength lower than the carrier sensing threshold at the hidden nodes.

Reactive Interference Phase: In this phase, the HTE attacker continues to sense the operating band through the wide-band sensing and sniffs the band for RTS and CTS messages addressed to or from the victim node, respectively. It tries to deliberately interfere with transmissions from nodes A1, A3, and A5 that are destined to the victim node (i.e., A4). However, the choice of the interference rate depends on the strategy of the attacker; it may interfere with each transmission, interfere randomly, or take an intermittent strategy between acting benignly or maliciously. In this paper, we discuss these different attack strategies and their ability to stay immune against a context-aware HTE detection approach. Such a detection technique will create a contextual model to differentiate between benign and malicious behavior. Therefore, an attacker will try to mimic the behavior of the benign model closely to stay undetected but to maintain its attack performance. We consider that the attacker (i.e., HTE-1) takes a subtle random approach where it poses as a legitimate node by continuing regular communications with its neighbors in its own network (i.e., HTE-2), and the attacker intelligently interferes with the victim's reception only when the attacker is idle (i.e., not in communication with HTE-2). Hence, it offers a different detection challenge in contrast to conventional reactive jamming attacks. A comprehensive analysis on different attack strategies is discussed in Section VI.

TABLE I
STATE DESCRIPTION OF THE PROPOSED CONTEXTUAL MODEL

$Z(t)$	$Y(t)$	$X(t)$	$E(t)$
0	0	0	0
1	0	0	1
2	0	1	0
3	0	1	1
4	1	X	X

B. Summary

The HTE attacker utilizes array antenna techniques that are widely available for communication purposes and weaponizes these to impersonate a legitimate hidden terminal. Different types of distinct reactive interference strategies can be studied given that the attacker successfully impersonates a hidden terminal. As traditional location spoofing detection techniques (i.e., pertaining to the emulation phase) are inapplicable in the given scenario, we argue that behavioral detection models make an appropriate design choice (i.e., pertaining to the reactive interference phase). In this paper, we propose an attack model to work better against the proposed context-aware detection technique. In the subsequent sections, we first formulate the contextual model of a benign hidden terminal and then discuss different attack strategies.

V. MATHEMATICAL MODELING OF HIDDEN TERMINALS

The reception behavior of the defending (or victim) IoT device is considered as an ON-OFF process: $(X(t); t \geq 0)$ with state space $\{0, 1\}$, where 0 and 1 correspond to the idle and the receiving state, respectively. Let A4 denote the IoT device that is evaluating abnormal interference, hereafter referred as the *node under test* (NUT), and the hidden terminal from the external network (i.e., HTE-1) is named as the *external node* (EX).

A. Proposed Markov Model

In this subsection, we formulate different components necessary to capture the benign behavior of a co-located hidden terminal of an external network, using a five-state Markov process that captures the key aspects of the interaction among PUs, NUT, and EX.

Markov States: We define $X(t)$, $E(t)$, and $Y(t)$ as the state of the NUT, the EX, and the PU in the current channel at time-slot t, respectively. Note that $E(t)$) and $Y(t)$ are ON-OFF processes with state space $\{0, 1\}$, where 0 and 1 correspond to the idle and the transmitting state, respectively. The interaction between $X(t)$, $E(t)$, and $Y(t)$- is captured in a five-state discrete-time Markov model, which is represented in Table I.

The Markov state $Z(t) \equiv \{Y(t), X(t), E(t)\}$ denotes the state of the proposed contextual model in NUT's current operating channel at the end of a time-slot. The brief descriptions of the states are:

0: The current channel is free (i.e., PU is idle), the NUT is idle (i.e., not receiving), and the EX is either idle or transmitting on another channel.

1: The current channel is free, the NUT is idle, and the EX is transmitting.

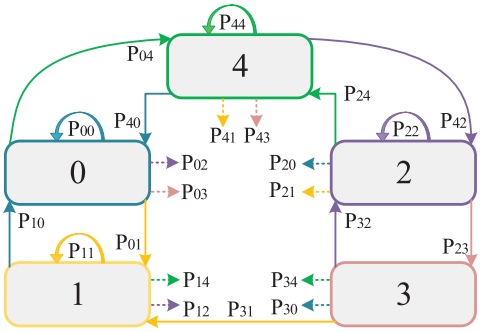


Fig. 4. The proposed Markov model.

TABLE II
NOTATIONS USED IN THE MARKOV MODEL

Symbol	Definition
P_{λ_p}	Pr{a PU packet arrival in a slot}
P_{μ_p}	Pr{a PU packet ending in a slot}
$P_{\lambda_{in}}$	Pr{an internal packet arrival in a slot for the NUT}
$P_{\mu_{in}}$	Pr{an internal packet ending in a slot}
$P_{\lambda_{ex}}$	Pr{an external packet arrival in a slot}
$P_{\mu_{ex}}$	Pr{an external packet ending in a slot}

2: The current channel is free, the NUT is receiving, and the EX is either idle or transmitting on another channel.

3: The current channel is free, the NUT is receiving, and the EX is transmitting. *This state represents the collision or interference*.

4: The current channel is busy (i.e., PU is active).

The state transition diagram of the proposed Markov model is shown in Fig. 4, which depicts the interaction between the PU, the NUT, and the EX. Transitions between non-neighboring states are presented by dashed arrows.

Transition Probabilities: We consider that each neighbor of the NUT has a packet arrival rate λ that is destined for the NUT and $\lambda_{in} = (k-1)\lambda$. We capture the effect of hidden terminals by the parameter $k_h \in \{0, \ldots, k-1\}$, which represents the number of internal nodes that are hidden terminals to the EX. In addition, we define the parameter $\alpha \equiv k_h/(k-1)$ as the fraction of internal IoT devices that are hidden to the EX. We assume that each IoT device broadcasts its identity periodically, and IoT devices sniff the wireless medium to discover the presence of other IoT devices—from external networks—within their radio range. In Fig. 3, though A1, A3, and A5 cannot listen to the transmission of the node HTE-1 (or EX), A2, A4, and A6 can listen to its transmission. Hence, each device maintains a list of external nodes that are hidden to them (by exchanging information within internal IoT devices), and it helps them to deduce the value of α. Table II summarizes the notations used in the proposed Markov model.

To derive steady-state probabilities, we first deduce the single-step transition probabilities. We use P_{ij} to denote $\Pr(Z(t+1) = j | Z(t) = i)$, i.e., the probability of transitioning to state j at the next slot from the current state i. We capture the feature of the random channel-hopping process in our model, where an IoT device can start a new transmission only when there is a channel available. In the following discussion,

we use the terms *states* in the proposed Markov model and the *status* of the NUT in a time-slot interchangeably.

The transition from state '**0**' depends on PU activities (P_{λ_p} and Π_b), internal traffic parameter ($P_{\lambda_{in}}$), external traffic parameter ($P_{\lambda_{ex}}$), and collision probability (P^b_{col}). Now, transitions from the idle state (i.e., $Z(t) = 0$):

$$P_{00} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)\Big(1 - P^b_{col}\Big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)\big(1 - P_{\lambda_{ex}}\big), \quad (1)$$

$$P_{01} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)P^b_{col} + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)P_{\lambda_{ex}}, \quad (2)$$

$$P_{02} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}}\Big(1 - P^b_{col}\Big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}}\big(1 - P_{\lambda_{ex}}\big), \quad (3)$$

$$P_{03} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}}P^b_{col} + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}}P_{\lambda_{ex}}, \quad (4)$$

$$P_{04} = \sum_{b=0}^{M-1} \Pi_b P_{\lambda_p}, \quad (5)$$

where Π_b = the steady-state probability that exactly b channels are busy by PUs, $P^b_{col} = (1-\rho_{ex})P_{\lambda_{ex}}P^b_{match}$, ρ_{ex} = the steady-state probability that the EX is active, and $P^b_{match} = 1/(M-b)$. Similarly, the transition from state '**1**' depends on PU activities (P_{λ_p} and Π_b), internal traffic parameter ($P_{\lambda_{in}}$), and external traffic parameter ($P_{\mu_{ex}}$). Now, transitions from the EX active state (i.e., $Z(t) = 1$):

$$P_{10} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)P_{\mu_{ex}}, \quad (6)$$

$$P_{11} = \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\mu_{ex}}\big), \quad (7)$$

$$P_{12} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}} + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}}P_{\mu_{ex}}, \quad (8)$$

$$P_{14} = \sum_{b=0}^{M-1} \Pi_b P_{\lambda_p}. \quad (9)$$

Now, the transition from state '**2**' depends on PU activities (P_{λ_p} and Π_b), internal traffic parameter ($P_{\mu_{in}}$), external traffic parameter ($P_{\lambda_{ex}}$), and collision probability (P^b_{col}). However, the collision probability (P^b_{col}) changes in this scenario because the NUT is already transmitting and a collision can only happen from hidden terminals. Therefore, the model must account the hidden terminal factor (α). Now, transitions from the NUT's receiving state (i.e., $Z(t) = 2$):

$$P_{20} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)P_{\mu_{in}}\Big(1 - P^b_{col}\Big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)P_{\mu_{in}}\big(1 - P_{\lambda_{ex}}\big), \quad (10)$$

$$P_{21} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)P_{\mu_{in}}(1-\rho_{ex})P_{\lambda_{ex}}P^b_{match} + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)P_{\mu_{in}}P_{\lambda_{ex}}, \quad (11)$$

$$P_{22} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\mu_{in}}\big)\Big(1 - P^b_{col}\Big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\mu_{in}}\big)\big(1 - \alpha P_{\lambda_{ex}}\big), \quad (12)$$

$$P_{23} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\mu_{in}}\big)P^b_{col} + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\mu_{in}}\big)\alpha P_{\lambda_{ex}}, \quad (13)$$

$$P_{24} = \sum_{b=0}^{M-1} \Pi_b P_{\lambda_p}, \quad (14)$$

where $P^b_{col} = (1-\rho_{ex})\alpha P_{\lambda_{ex}}P^b_{match}$ and $\alpha = k_h/(k-1)$.

Now, the NUT immediately tries to avoid a collision after detecting it, and the transition from state '**3**' depends on PU activities (P_{λ_p} and Π_b), internal traffic parameter ($P_{\lambda_{in}}$), and external traffic parameter ($P_{\mu_{ex}}$). Hence, transitions from the collision state (i.e., $Z(t) = 3$):

$$P_{30} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)P_{\mu_{ex}}, \quad (15)$$

$$P_{31} = \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\mu_{ex}}\big), \quad (16)$$

$$P_{32} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)P_{\lambda_{in}}, \quad (17)$$

$$P_{34} = \sum_{b=0}^{M-1} \Pi_b P_{\lambda_p}. \quad (18)$$

After experiencing the channel busy by a PU, the NUT hops to another available channel. The transition from state '**4**' depends on PU activities (P_{λ_p} and Π_b), internal traffic parameter ($P_{\lambda_{in}}$), external traffic parameter ($P_{\mu_{ex}}$), and collision probability (P^b_{col}). Now, transitions from the channel busy state (i.e., $Z(t) = 4$):

$$P_{40} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)\Big(1 - P^b_{col}\Big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)P_{free} + \Pi_M P_{\mu_p}, \quad (19)$$

$$P_{41} = \sum_{b=0}^{M-1} \Pi_b \Big(1 - P_{\lambda_p}\Big)\big(1 - P_{\lambda_{in}}\big)P^b_{col} + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big)\rho_{ex}\big(1 - P_{\mu_{ex}}\big), \quad (20)$$

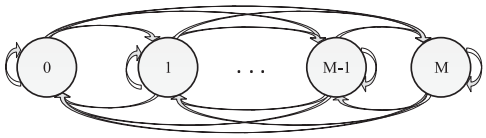


Fig. 5. The transition diagram of the number of busy channels in a time-slot.

$$P_{42} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big) P_{\lambda_{in}} \Big(1 - P_{col}^b\Big) + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big) P_{\lambda_{in}} P_{free}, \tag{21}$$

$$P_{43} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big) P_{\lambda_{in}} P_{col}^b + \Pi_{M-1}\Big(1 - P_{\lambda_p}\Big) P_{\lambda_{in}} (1-\rho_{ex}) P_{\lambda_{ex}}, \tag{22}$$

$$P_{44} = \sum_{b=0}^{M-1} \Pi_b P_{\lambda_p} + \Pi_M \big(1 - P_{\mu_p}\big), \tag{23}$$

where $P_{free} = \rho_{ex} P_{\mu_{ex}} + (1-\rho_{ex})(1-P_{\lambda_{ex}})$ and $P_{col}^b = (1-\rho_{ex}) P_{\lambda_{ex}} P_{match}^b$.

Note that all transition probabilities except the ones from the channel busy state (i.e., $Z(t) = 4$) are conditioned on the fact that at least one channel is available. Therefore, we must transform (1)-(18) and $P_{ij} \leftarrow P_{ij}/(1-\Pi_M)$, where $i \in \{0,1,2,3\}$ and $j \in \{0,1,2,3,4\}$.

Calculation of $\mathbf{\Pi_b}$*:* Π_b represents the probability that, at a given time, *b* PUs are active, where $b \in \{0,\ldots,M\}$. Here, we consider that PU traffic is homogeneous on each channel, the buffer in each PU can store at most one packet at a time, and a packet is kept in the buffer until it is transmitted successfully; hence, the PU traffic follows the $\mathbf{M/M/1/1}$ queuing model.

Let us consider that $\mathbb{A}(t) = b$ represents the number of active PUs at time-slot *t*. The process $\{\mathbb{A}(t), t = 0,1,\ldots\}$ forms a Markov chain whose state transition diagram is given in Fig. 5. To characterize the behavior of PU channels, we define $\mathbb{F}_f^\gamma$ as the event that *f* PUs will finish their transmission in the next slot, given that γ PUs are transmitting. In addition, we define $\mathbb{S}_s^\beta$ as the event that *s* PUs will start new transmissions in the next slot, given that β PUs are idle. Hence, the probabilities of events $\mathbb{F}_f^\gamma$ and $\mathbb{S}_s^\beta$ are:

$$\mathbb{F}_f^\gamma = \binom{\gamma}{f} P_{\mu_p}^f \big(1 - P_{\mu_p}\big)^{\gamma - f}, \tag{24}$$

$$\mathbb{S}_s^\beta = \binom{\beta}{s} P_{\lambda_p}^s \Big(1 - P_{\lambda_p}\Big)^{\beta - s}. \tag{25}$$

Therefore, the state transition probability from state $\{\mathbb{A}(t) = i\}$ to state $\{\mathbb{A}(t+1) = j\}$ can be written as:

$$P_{i,j} = \begin{cases} \sum_{f=0}^{i} \Pr\Big(\mathbb{F}_f^i\Big) \Pr(\mathbb{S}_{j-i+f}^{M-i+f}), & \text{for } j \geq i \\ \sum_{f=i-j}^{i} \Pr\Big(\mathbb{F}_f^i\Big) \Pr\Big(\mathbb{S}_{j-i+f}^{M-i+f}\Big), & \text{for } j < i. \end{cases} \tag{26}$$

Hence, we deduce the steady-state probability of the number of active PUs (or busy channels) in a time-slot, denoted as $\mathbf{\Pi} = [\Pi_0, \Pi_1, \ldots, \Pi_M]$, where Π_b denotes the steady-state probability that *b* channels are busy in a time-slot.

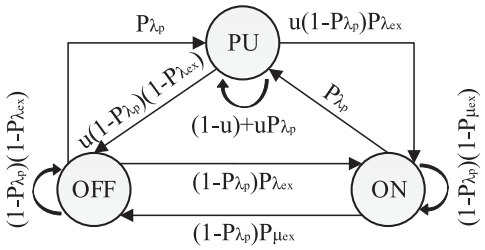


Fig. 6. The transition diagram of activities of the EX.

Calculation of ρ_{ex}*:* As mentioned, ρ_{ex} represents the steady-state probability of an external node in the active state. To calculate this, we design a separate Markov model without the influence of internal nodes. Hence, the model characterizes only the interaction between PUs and the EX. The state transition diagram is given in Fig. 6; the state **PU** represents the ON (i.e., 1) or OFF (i.e., 0) state of a PU on the current channel, and the **ON** and the **OFF** states represent the activity of EX on its current operating channel. The corresponding steady-state probabilities are given:

$$\Pi_{off} = \frac{\Big(1-P_{\lambda_p}\Big)\Big\{1-\Big(1-P_{\lambda_p}\Big)\big(1-P_{\mu_{ex}}\big)-uP_{\lambda_{ex}}P_{\lambda_p}\Big\}}{\Big(1-P_{\lambda_p}\Big)\big(P_{\lambda_{ex}}+P_{\mu_{ex}}\big)+P_{\lambda_p}}, \tag{27}$$

$$\Pi_{on} = \frac{\Big\{1-P_{\lambda_p}(1-u)\Big\}P_{\lambda_{ex}}\Pi_{off}}{1-\Big(1-P_{\lambda_p}\Big)\big(1-P_{\mu_{ex}}\big)-uP_{\lambda_{ex}}P_{\lambda_p}}, \tag{28}$$

$$\Pi_{pu} = \frac{P_{\lambda_p}\big(\Pi_{off}+\Pi_{on}\big)}{1-P_{\lambda_p}}, \tag{29}$$

where $\Pi_{off} + \Pi_{on} + \Pi_{pu} = 1$, $u = \sum_{b=0}^{M-1} \Pi_b$, and $\rho_{ex} = \Pi_{on}$.

B. Proposed Parameter Estimation

In the earlier subsection, we formulated the proposed contextual model using traffic characteristics of all entities in the network. Though the NUT knows its own traffic parameters, traffic parameters of other entities are unknown to it. In this subsection, we propose a Hidden Markov Model (HMM) based parameter estimation technique to extract the required parameters (i.e., $\lambda_{ex}, \mu_{ex}, \lambda_p, \text{and } \mu_p$) from the interaction (i.e., statistics from the wide-band sensing) with other entities. In the following, we first present the structure of the HMM, then we give a brief introduction of the forward-backward procedure in the Baum-Welch (BW) algorithm [40]. Finally, by analyzing the algorithm, we estimate the required parameters.

Hidden Markov Model: A hidden Markov process is a Markov process consisting of two different processes, where $\mathbb{X}$ is the hidden process that is never observable and $\mathbb{Z}$ is the observable process that is perceivable to the agent (i.e., the NUT). X_t and Z_t denote the hidden state and observation state at time *t*, respectively. Here, the hidden process follows a Markov process with a finite number of states and the observable process is a probabilistic function that generates *symbols* based on the hidden states. The set of symbols comes from a

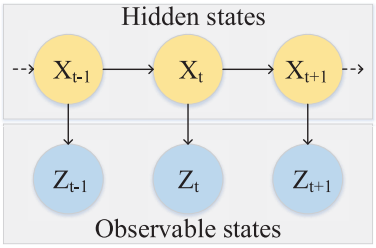


Fig. 7. The hidden Markov model.

defined *alphabet* $\mathbb{A}$. In our case, $\mathbb{A} = \{0, 1\}$ (i.e., 0 = OFF and 1 = ON).

The general concept of an HMM is illustrated in Fig. 7. A system of discrete time changes randomly from one state to another, within a finite state space $\mathbb{S}$. In our case, the finite space $\mathbb{S} = \{0, 1\}$. The evolution of the hidden sequence $X_1, X_2, \ldots, X_T$ is unknown, which represents PU or EX states. However, it can be expressed by a sequence of observed symbols from the alphabet $\mathbb{A}$ (i.e., $Z_t \in \mathbb{A}$), which represents the sensing decision on PU or EX activity. However, the sensing result is mixed with measurement errors and differs from the actual states of the PU or EX. To model the HMM, let us define the parameters first:

- Number of hidden states, $s = 2$.
- Number of symbols, $a = 2$.
- Initial state distribution, $\prod^{\mathbf{f}} = \{\pi_i^{\mathbf{f}}\}$, where $i = 0, \ldots, s-1$ and $\mathbf{f}$ ={PU, EX}.
- One-step state transition probabilities, $\mathbb{P}^{\mathbf{f}} = p_{ij}^{\mathbf{f}}$, where $i, j = 0, \ldots, s-1$.
- Symbol emission probability, $\mathbb{B}^{\mathbf{f}} = b_j^{\mathbf{f}}(k)$, where $j = 0, \ldots, s-1$ and $k = 0, \ldots, a-1$.

The one-step state transition probability is:

$$\begin{aligned}&\Pr\Big(X_t^{\mathbf{f}} = j | X_{t-1}^{\mathbf{f}} = i, X_{t-2} = i_{t-2}, \ldots, X_2^{\mathbf{f}} = i_2, X_1^{\mathbf{f}} = i_1\Big)\\ &= Pr^{\mathbf{f}}\Big(X_t^{\mathbf{f}} = j | X_{t-1}^{\mathbf{f}} = i\Big)\\ &= p_{ij}^{\mathbf{f}},\end{aligned} \tag{30}$$

where, $i_1, i_2, \ldots, i_{t-2}, i_{t-1}, i, j \in \{0, 1\}$ and $t > 1$. Therefore, the joint distribution of $X_1^{\mathbf{f}}, X_2^{\mathbf{f}}, \ldots, X_t^{\mathbf{f}}$ is expressed as:

$$\Pr\Big(X_1^{\mathbf{f}} = i_1, X_2^{\mathbf{f}} = i_2, \ldots, X_t^{\mathbf{f}} = i_t\Big) = \pi_{i_1}^{\mathbf{f}} P_{i_1 i_2}^{\mathbf{f}} \cdots P_{i_{t-1} i_t}^{\mathbf{f}}. \tag{31}$$

The emission probability, which represents the probability of observing $Z_t^{\mathbf{f}} = k$ when $X_t^{\mathbf{f}} = j$, i.e., $\mathbb{B}^{\mathbf{f}} = b_j^{\mathbf{f}}(k), j = 0, \ldots, s-1$ and $k = 0, \ldots, a-1$. Therefore,

$$b_j^{\mathbf{f}}(k) = \Pr\Big(Z_t^{\mathbf{f}} = k | X_t^{\mathbf{f}} = j\Big). \tag{32}$$

Now, as the sensing process is mixed with measurement errors, the sensing mechanism may experience misdetection and false-alarms. The probability of inferring a PU (or EX) idle while it is actually active is called the probability of misdetection. Similarly, the probability of inferring a PU (or EX) active while it is actually idle is called the probability of false-alarm. These are mathematically expressed as:

$$\begin{aligned}\Pr\Big(Z_t^{\mathbf{f}} = 1 | X_t^{\mathbf{f}} = 0\Big) &= b_0^{\mathbf{f}}(1),\\ \Pr\Big(Z_t^{\mathbf{f}} = 0 | X_t^{\mathbf{f}} = 1\Big) &= b_1^{\mathbf{f}}(0),\\ \Pr\Big(Z_t^{\mathbf{f}} = 1 | X_t^{\mathbf{f}} = 1\Big) &= b_1^{\mathbf{f}}(1).\end{aligned} \tag{33}$$

The BW algorithm proposes an iterative approach to estimate the HMM parameters $\eta^{\mathbf{f}} = [\prod^{\mathbf{f}}, \mathbb{P}^{\mathbf{f}}, \mathbb{B}^{\mathbf{f}}]$, such that the $\Pr(Z^{\mathbf{f}}|\eta^{\mathbf{f}})$ is maximized. For simplicity, we discard the notation $\mathbf{f}$ from the following calculations. Now, to estimate the parameters, we define the following:

- Forward probability, $\alpha_t(i) = \Pr(Z_1, Z_2, \ldots, Z_t, X_t = S_i|\eta)$, for $i \in \{0, 1\}$
- Backward probability, $\beta_t(i) = Pr(Z_{t+1}, Z_{t+2}, \ldots, Z_{T-1}, Z_T, X_t = S_i|\eta)$, for $i \in \{0, 1\}$
- State transition estimation, $\gamma_t(i, j) = Pr(X_t = i, X_{t+1} = j|\mathbb{Z}, \eta)$, for $i, j \in \{0, 1\}$. It represents the probability of being in state S_i at instant t and in state S_j at instant $t + 1$, given the observation sequence $\mathbb{Z}$ and the model parameters $\eta = [\pi, P, B]$
- Estimate of the state at each observation, $\delta_t(i) = Pr(X_t = i|\mathbb{Z}, \eta)$, for $i \in \{0, 1\}$. It represents the probability of being in state S_i at instant t, given the observation sequence $\mathbb{Z}$ and the model parameters η = $[\prod, \mathbb{P}, \mathbb{B}]$

The estimation variables for the HMM parameters are expressed in terms of $\gamma_t(i, j)$ and $\delta_t(i)$:

$$p_{ij} = \frac{\sum_{t=1}^{t=T-1} \gamma_t(i, j)}{\sum_{t=1}^{t=T-1} \delta_t(i)}, \tag{34}$$

$$b_j(k) = \frac{\sum_{t=1, Z_t=k}^{t=T} \delta_t(j)}{\sum_{t=1}^{t=T} \delta_t(j)}, \tag{35}$$

$$\pi_i = \delta_1(i). \tag{36}$$

In (34), the numerator represents the expected number of transitions from state i to state j over the interval $T - 1$, while the denominator represents the expected number of times a transition happens from state i. The numerator in (35) represents the expected number of transitions from state j at which symbol k is observed. In (34)-(36), $\gamma_t(i, j)$ and $\delta_t(i)$ are calculated as follows:

$$\gamma_t(i, j) = \frac{\alpha_t(i) p_{ij} b_j(Z_{t+1}) \beta_{t+1}(j)}{Pr(Z|\eta)}. \tag{37}$$

$$\delta_t(i) = \sum_{all\ S_j \in \{0,1\}} \gamma_t(i, j). \tag{38}$$

The forward and backward probabilities in the above equations are calculated recursively as follows:

Initialization:

$$\alpha_1(i) = \pi_i b_i(1), \quad 0 \le i \le s-1. \tag{39}$$

$$\beta_t(i) = 1, \quad 0 \le i \le s-1. \tag{40}$$

Recursion:

$$\alpha_{t+1}(j) = \left[\sum_{i=0}^{s-1} \alpha_t(i) p_{ij}\right] b_j(Z_{t+1}). \tag{41}$$

$$\beta_t(i) = \sum_{j=0}^{s-1} p_{ij} b_j(Z_{t+1}) \beta_{t+1}(j). \tag{42}$$

The recursion process terminates when $Pr(\mathbb{Z}|\eta)$ maximizes, which is the probability of observing the sequence $\mathbb{Z}$ given the parameter $\eta = [\prod, \mathbb{P}, \mathbb{B}]$:

$$Pr(\mathbb{Z}|\eta) = \sum_{i=0}^{s-1} \prod_{t=1}^{T} \alpha_t(i). \tag{43}$$

Extraction of Traffic Parameters: Here, we extract traffic parameters of the PU and EX from the estimated HMM parameters $\eta^{\mathbf{f}} = [\prod^{\mathbf{f}}, \mathbb{P}^{\mathbf{f}}, \mathbb{B}^{\mathbf{f}}]$, such that the $\Pr(Z^{\mathbf{f}}|\eta^{\mathbf{f}})$ is maximized. To do this, let us recall the parameters, $\theta_{\mathbf{f}} = [\lambda_{\mathbf{f}}, \mu_{\mathbf{f}}]$, where λ means the traffic arrival rate, μ means the packet service rate, and $\mathbf{f} = \{\text{PU, EX}\}$. From the network model, the length of the ON and OFF state are exponentially distributed. In [41], a useful method to compute the state transition rate matrix from the state transition probability matrix is provided. We denote the transition rate matrix as $Q_{\mathbf{f}}$ and

$$Q_{\mathbf{f}} = \begin{pmatrix} -\lambda_{\mathbf{f}} & \lambda_{\mathbf{f}} \\ \mu_{\mathbf{f}} & -\mu_{\mathbf{f}} \end{pmatrix}. \tag{44}$$

As described in η, $\mathbb{P}$ is the one-step state transition probability matrix. We know that $\mathbb{P} = \exp(Q\Delta)$ and $Q = \log(\mathbb{P})/\Delta$, where Δ is the sensing period. However, the computational procedure is cumbersome and $\log(\cdot)$ has a limitation when $\mathbb{P}$ has a non-positive eigenvalue. Therefore, we adopt the mapping approach introduced in [41], which provides an easier computational approach and provides a sufficient degree of accuracy. If the two-dimensional transition rate matrix is the form shown in (44), then the transition probability matrix is:

$$\mathbb{P} = \begin{pmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{pmatrix} = \begin{pmatrix} \exp^{-\lambda\Delta} & 1 - \exp^{-\lambda\Delta} \\ 1 - \exp^{-\mu\Delta} & \exp^{-\mu\Delta} \end{pmatrix}. \tag{45}$$

In (45), we can calculate Q from $\mathbb{P}$ inversely. In other words, the relation between $\mathbb{P}$ and Q unfolds the relationship between η and θ.

C. Summary

In this section, we explained the mathematical structure to formulate the building blocks of the proposed context-aware detection strategy. The calculations in this section helps to identify the accepted behavior of a benign hidden terminal of an external network. Though many parameters to deduce the context-aware model are unknown, we proposed an HMM-based estimation strategy to estimate the required parameters. Again, we utilized only the in-hand sensing statistics to compute the estimation without any hardware and networking overhead. The required probabilities can be expressed in terms of the estimated parameters (i.e., $\widehat{\lambda_{\mathbf{f}}}$ and $\widehat{\mu_{\mathbf{f}}}$) as follows:

$$P_{\lambda_{\mathbf{f}}} = 1 - \exp^{-\widehat{\lambda_{\mathbf{f}}} * \mathbf{t}}, \tag{46}$$

$$P_{\mu_{\mathbf{f}}} = 1 - \exp^{-\widehat{\mu_{\mathbf{f}}} * \mathbf{t}}. \tag{47}$$

Here, $\mathbf{t}$ represents the length of a time-slot. Next, we will discuss the strengths and weaknesses of different attack strategies against the proposed context-aware detection model.

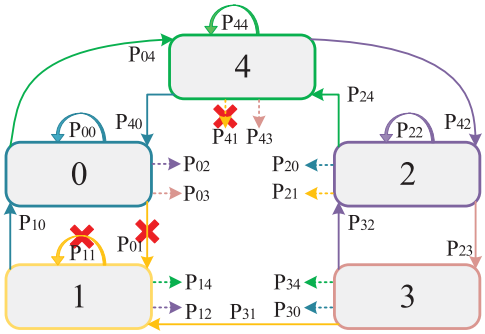


Fig. 8. Markov chain between a naive attacker and the NUT.

VI. The Reactive Interference Models

As discussed earlier in this paper, a strong detection strategy requires a strong attack model. In this section, we discuss different attack models and their efficacy against the proposed context-aware detection strategy.

A. Attack Models

Though an aggressive attack strategy that constantly interferes with the reception of the victim results in better attack performance, it deviates significantly from benign behaviors and to an reactive attacker. A context-aware detection strategy, which regularly monitors external nodes, can identify this malicious interference; hence, an attacker must haggle between the attack objective and the risk of exposure. In the following, we discuss three different attack strategies.

Naive Reactive Attacker: The interaction between the NUT and the EX is modeled as the Markov chain illustrated in Fig. 8, when the EX is a naive reactive attacker. The behavioral difference between a benign hidden terminal and a naive reactive attacker is that a benign hidden terminal transmits irrespective of the transmission from its hidden counterparts, whereas a naive reactive attacker transmits *only* when it senses transmissions from its hidden counterparts on the wireless channel (i.e., $\mathrm{P}_{23} = 1$). Thereby, the transition rates of the corresponding discrete time Markov chain (DTMC) from states 0, 1, and 4 to state 1 is zero. Now, if we observe Fig. 4 and Fig. 8, the state transition structures are distinct. It means that the Neyman-Pearson test of differentiating these two Markov chains is degenerate, i.e., it becomes a singular detection problem [42], meaning that the test results in an arbitrarily small error [43].

Naive Random Attacker: The only difference between a naive random attacker and a naive reactive attacker is that the naive random attacker does not interfere with each reception of the victim, i.e., $\mathrm{P}_{23} \neq 1$. Instead, it randomly chooses its attack window to interfere. Nonetheless, both of these attack models follow the similar state transition structures (i.e., $\mathrm{P}_{01} = \mathrm{P}_{11} = \mathrm{P}_{41} = 0$) and yield a singular detection problem. Therefore, though this attack strategy introduces randomness in its behavior, it still remains ineffective against the context-aware detection model.

Intelligent HTE Attacker: To avoid the singular detection problem, we propose a more advanced random reactive attacker, called the intelligent HTE attacker, that better

disguises its malicious behavior by mimicking characteristics of benign hidden terminals. In this attack model, the HTE attacker generates regular data packets and communicates with its neighbor (i.e., the passive attacker, HTE-2) regardless of the state of the PU and the victim, meaning that $\mathrm{P}_{01} = \mathrm{P}_{11} = \mathrm{P}_{41} \neq 0$. This attack model increses the detection difficulty since the incorporation of random behaviors makes the HTE attacker similar to a benign hidden terminal. Therefore, an attacker acts benignly by performing regular communications with its neighbor, and—if in its idle period (when the attacker is not transmitting to its neighbor) it finds the victim is receiving—it interferes with the reception of the victim (i.e., interference rate $= 1$). We can make the strategy more random by changing the interference rate; nonetheless, without loss of generality, in this work, we assume interference rate $= 1$. Hence, unlike the benign model, the transition probability from state 2 is:

$$P_{20} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big) P_{\mu_{in}} \rho_{ex}, \tag{48}$$

$$P_{21} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big) P_{\mu_{in}} (1 - \rho_{ex}) + \Pi_{M-1} \Big(1 - P_{\lambda_p}\Big) P_{\mu_{in}}, \tag{49}$$

$$P_{22} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big) \big(1 - P_{\mu_{in}}\big) \Big(1 - P_{col}^b\Big) + \Pi_{M-1} \Big(1 - P_{\lambda_p}\Big) \big(1 - P_{\mu_{in}}\big)(1 - \alpha), \tag{50}$$

$$\mathrm{P}_{23} = \sum_{b=0}^{M-2} \Pi_b \Big(1 - P_{\lambda_p}\Big) \big(1 - P_{\mu_{in}}\big) P_{col}^b + \Pi_{M-1} \Big(1 - P_{\lambda_p}\Big) \big(1 - P_{\mu_{in}}\big) \alpha, \tag{51}$$

$$P_{24} = \sum_{b=0}^{M-1} \Pi_b P_{\lambda_p}, \tag{52}$$

where $P_{col}^b = (1 - \rho_{ex})\alpha$ and $\alpha = k_h/(k-1)$.

B. Summary

Three different attack traits, including naive, naive-random, and intelligent, are discussed. Though a naive behavior yields a better attack performance, it increases the risk of exposure because of its distinct state transition structures. In contrast, the proposed intelligent HTE attack model that closely imitates a benign hidden terminal offers a different attack detection challenge. In Section VIII, we will illustrate the detection performance of our proposed context-aware detection strategy against these attack models. Next, we formulate the detection challenge as a binary hypothesis test to differentiate an observed behavior between benign and malicious.

VII. Detection of the Hidden Terminal Emulation Attack

The proposed detection approach is comprised of two steps: *i*) designing a contextual model to characterize the behavior of benign hidden terminals and *ii*) formulating the detection problem as a binary hypothesis testing problem to identify whether a sequence of observed behaviors is likely to be produced from the established benign model or attack model. In Section V, we comprehensively illustrated the first step, and now, we shed light on the second one.

A. Binary Hypothesis Test

The NUT monitors activities on all channels and collects transmission patterns of all wireless nodes in its surroundings over a time window of $\mathbf{d} = \mathbf{w/t}$ equal-length slots, where $\mathbf{w}$ is the observation time length and $\mathbf{t}$ is the length of a time-slot. To test whether or not the NUT is experiencing HTE attacks, we collect the sequence of observations of the NUT's status $\mathbf{z_d} \equiv \{Z(t)\}_{t=1}^{\mathbf{d}+1}$, called a *sample path* of the discrete time Markov chain that is generated by the influence of either a benign hidden terminal or by an HTE attacker. Now, let us denote transition probability matrices that characterizes a benign hidden terminal as $\mathbf{P^0}$, that characterizes an HTE attacker as $\mathbf{P}^A$, and that is generated from the observations as $\mathbf{P}$. Thus, a binary hypothesis testing problem can be formed:

$$\mathrm{H}_0 : \mathbf{P} = \mathbf{P^0} \;\; \mathrm{H}_A : \mathbf{P} = \mathbf{P}^{\mathrm{A}}. \tag{53}$$

Though most binary hypothesis testing problems require supervised learning, the proposed detection model does not require supervised training as we have formulated closed-form expressions to characterize benign and malicious behaviors. It is reasonable to assume that the initial-state probability distribution is similar to the steady-state probabilities of the states. However, as indicated in [15], the initial distribution has an effect on the detection threshold, which decreases to 0 in $\mathbf{d}$ as $1/\mathbf{d}$. Hence, it is insignificant when $\mathbf{d}$ is large.

Let us define the number of transitions from state *i* to state *j* of $\mathbf{z_d}$ as $N_{ij} = \sum_{t=1}^{\mathbf{d}} \mathbf{1}_{\{z_t = i, z_{t+1} = j\}}$, where z_t denotes the *t*-th element of the sequence $\mathbf{z_d}$ and $i, j \in \{0, 1, 2, 3, 4\}$. Now, the counts $N_i \equiv \sum_{j=0}^{4} N_{i,j} = \sum_{t=1}^{d} \mathbf{1}_{\{z_t = i\}}$. The log-likelihood of $\mathbf{z_d}$ under hypothesis $\mathrm{H_b}$ is (where $\mathrm{b} \in \{0, A\}$):

$$\log \Pr(\mathbf{z_d}|\mathrm{H_b}) = \log \Pi_{z_1}^{\mathrm{b}} \prod_{t=1}^{\mathbf{d}} \mathrm{P}_{z_t, z_{t+1}}^{\mathrm{b}} = \log \Pi_{z_1}^{\mathrm{b}} + \sum_{i=0}^{4} \sum_{j=0}^{4} N_{ij} \log \mathrm{P}_{i,j}^{\mathrm{b}}. \tag{54}$$

Therefore, the log-likelihood ratio between H_A and H_0 is:

$$\log \frac{\Pr(\mathbf{z_d}|\mathrm{H_A})}{\Pr(\mathbf{z_d}|\mathrm{H_0})} = \log \frac{\Pi_{z_1}^{\mathrm{A}}}{\Pi_{z_1}^{0}} + \sum_{i=0}^{4} \sum_{j=0}^{4} N_{ij} \log \frac{\mathrm{P}_{i,j}^{\mathrm{A}}}{\mathrm{P}_{i,j}^{0}}. \tag{55}$$

The log-likelihood ratio test with threshold τ:

$$\log \frac{\Pi_{z_1}^{\mathrm{A}}}{\Pi_{z_1}^{0}} + \sum_{i=0}^{4} \sum_{j=0}^{4} N_{ij} \log \frac{\mathrm{P}_{i,j}^{\mathrm{A}}}{\mathrm{P}_{i,j}^{0}} \underset{\mathrm{H_0}}{\overset{\mathrm{H}_A}{\gtrless}} \tau. \tag{56}$$

We can further fine-tune the threshold by dynamically adjusting it to compensate for the observation window size $\mathbf{d}$:

$$\sum_{i=0}^{4} \sum_{j=0}^{4} N_{ij} \log \frac{\mathrm{P}_{i,j}^{\mathrm{A}}}{\mathrm{P}_{i,j}^{0}} \underset{\mathrm{H_0}}{\overset{\mathrm{H}_A}{\gtrless}} \tau(\mathbf{d}) - \log \frac{\Pi_{z_1}^{\mathrm{A}}}{\Pi_{z_1}^{0}},$$

TABLE III
SIMULATION PARAMETERS

Parameter	Value
Simulation time	100 seconds
SU sensing range	50
The number of channels (or PUs)	10
PU traffic rate (in pkts/sec)	λ_p = 50; μ_p = 100
Bandwidth	2 Mbps
The size of (RTS+CTS)	160 + 112 bits (802.11b/g)
Fast and fine sensing duration	1 ms (802.22) and 2 ms
IoT traffic rate (in pkts/sec)	λ = 20, 30, 40, 50, 60; μ = 100
SU packet size	1024 bytes
Hidden terminal factor, α	5/7

$$\sum_{i=0}^{4}\sum_{j=0}^{4}\frac{N_{ij}}{\mathbf{d}}\log\frac{\mathrm{P}^{\mathrm{A}}_{i,j}}{\mathrm{P}^{0}_{i,j}}\underset{\mathrm{H}_0}{\overset{\mathrm{H}_A}{\gtrless}}\tau' \equiv \frac{\tau(\mathbf{d})-\log\frac{\Pi^{\mathrm{A}}_{z_1}}{\Pi^{0}_{z_1}}}{\mathbf{d}}. \quad (57)$$

Here, $\tau(\mathbf{d})$ varies with the observation window size $\mathbf{d}$ to balance the trade-off between the false alarm rate and misdetection rate. The educated approach is $\tau(\mathbf{d}) = \tau_0\mathbf{d}$ for which $\tau' \approx \tau_0$ as $\mathbf{d}$ increases. The test statistics of the log-likelihood ratio test is:

$$\mathbf{Z} \equiv \sum_{i=0}^{4}\sum_{j=0}^{4}\frac{N_{ij}}{\mathbf{d}}\log\frac{\mathrm{P}^{\mathrm{A}}_{i,j}}{\mathrm{P}^{0}_{i,j}}, \quad (58)$$

where $\mathbf{d}, \mathrm{P}^{0}_{i,j}$, and $\mathrm{P}^{\mathrm{A}}_{i,j}$ are constants, and to derive the distribution of $\mathbf{Z}$ under $\mathrm{H_b}$, we must know the distribution of N_{ij}. According to [44], N_{ij} are asymptotically Gaussian distributed; hence, as a linear combination of N_{ij}, the test statistic $\mathbf{Z}$ is also asymptotically Gaussian.

B. Summary

The detection model captures the interference pattern an IoT device experiences under the influence of a hidden terminal and flags the HTE attack when observations deviate towards the established attack model. The proposed Markov model accumulates all required information into five states, and the binary hypothesis test verifies how well the observed sequence fits with the established benign or malicious behavior model. Our proposed detection technique requires only the carrier sensing information, which is readily available for channel access purposes.

VIII. PERFORMANCE ANALYSIS

In this section, we present numerical and simulation results to evaluate the performance of our proposed work. Our work employs a five-state Markov model that is a tractable model, and it can capture the key characteristics of the network transmission patterns. Here, we consider that all CR-enabled IoT devices physically reside within the proximity of each other and share the same ACL at a given time. The simulation parameters are listed in Table III.

During the simulation, we assume that the NUT is able to capture the transmission pattern of all adjacent IoT devices, and it knows the number of IoT devices in its vicinity (via wireless sniffing). The objective of the NUT (which is receiving) is to determine if the observed interference maintains the pattern set by the mathematical model. During the HMM training phase, IoT devices may estimate the traffic parameters in a long enough training time, so that the estimated values are close to the true values. In contrast, the attacker tries to maintain a stable data packet rate to avoid suspicious behaviors and attacks in its inactive intervals.

A. Hidden Terminal Emulation Attack

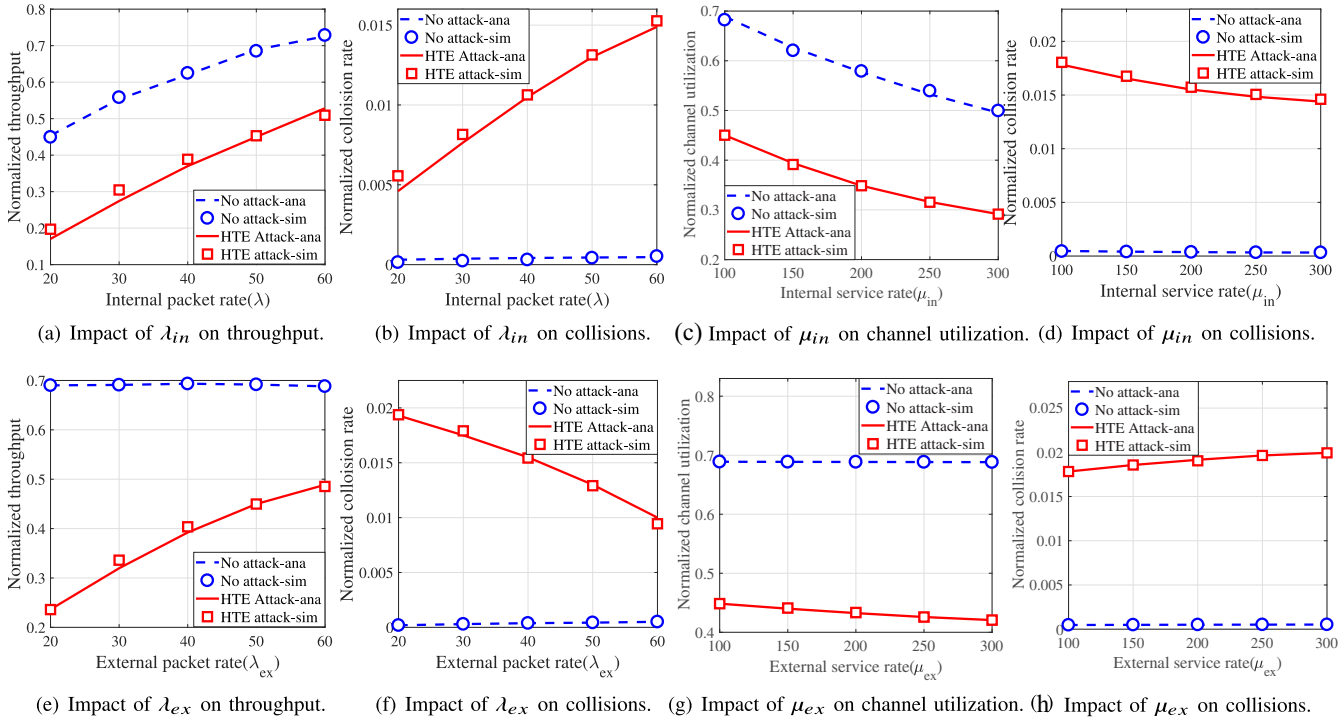
This subsection shows the impact of the proposed HTE attack on the network performance of the NUT.

Impact of λ_{in} on the HTE Attack: A higher rate of incoming traffic (i.e., $\lambda_{in} = (k-1)\lambda$) to the NUT increases the opportunity for the attacker to interfere with the NUT's reception. As the attacker tries to interfere each time it is inactive and the victim is receiving, in Fig. 9(a), we can observe that the effect of the attack increases with the increase of the incoming traffic rate. However, the effect is not clearly perceivable from this figure because the mean time (or the steady-state probability) in collision state (i.e., state '**3**' in Table I) is insignificant as compared to the normalized throughput.

Fig. 9(b) helps to grasp a better picture where the collision rate experienced by the NUT increases rapidly with the increase of the internal traffic rate. As we consider that the NUT can perceive collisions and discard packets instantly, it minimizes the total amount of time the NUT stays at the collision state. Nonetheless, these incidents engender in packet drops, stifle the throughput, and increase the collision rate.

Impact of μ_{in} on the HTE Attack: A higher service rate represents faster throughput and shorter packet length for a given data. Therefore, we use a different performance indicator than normalized throughput to illustrate the impact of μ_{in}, i.e., normalized channel utilization. Channel utilization represents the portion of time the NUT utilized the network successfully for communication purposes. Intuitively, we can understand that as we increase the service rate of each packet, the channel utilization decreases. Fig. 9(c) provides the corresponding impact of internal packet service rate on the channel utilization. Likewise, the collision rate decreases because attackers have less time to perpetrate the attack. Fig. 9(d) shows the change in collision rate with the increase of packet service rate.

Impact of λ_{ex} on the HTE Attack: Note that the attacker can only interfere if it is inactive during the transmission of its hidden counterparts; otherwise, it must continue and finish its own data packet transmission. As the traffic rate of the EX rises, the time it stays in the active state also increases (i.e., ρ_{ex}). Hence, the room for interference decreases. Therefore, to augment the impact of the attack, the attacker must decrease its packet arrival rate. In Fig. 9(e)-(f), we can observe that under no attack (i.e., when the EX is benign), the EX's traffic has an insignificant effect on the throughput and the collision of the NUT. However, under attack, it illustrates sensitivity to the change in λ_{ex}. Besides attack performance, λ_{ex} also influence the detection accuracy. Later, we will discuss the effect of λ_{ex} on the detection performance.



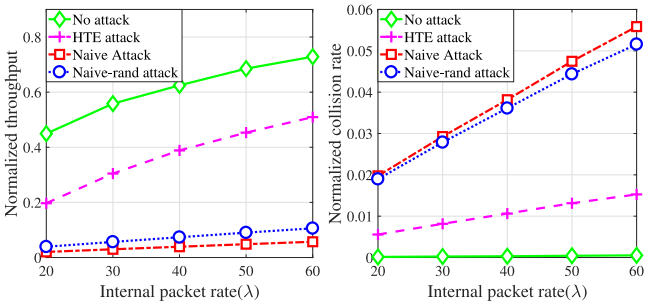
(a) Impact of λ_{in} on throughput. (b) Impact of λ_{in} on collisions. (c) Impact of μ_{in} on channel utilization. (d) Impact of μ_{in} on collisions.

(e) Impact of λ_{ex} on throughput. (f) Impact of λ_{ex} on collisions. (g) Impact of μ_{ex} on channel utilization. (h) Impact of μ_{ex} on collisions.

Fig. 9. The impact of different traffic parameters (λ_{in}, μ_{in}, λ_{ex}, and μ_{ex}) on NUT's throughput, channel utilization, and collision.

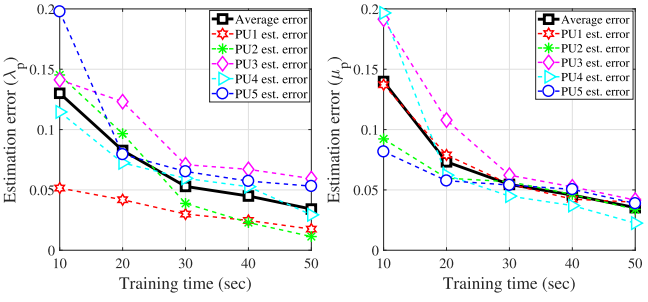
Impact of μ_{ex} on the HTE Attack: Similar to μ_{in}, we consider normalized channel utilization as a performance metric instead of normalized throughput. As we increase the service rate of the attacker (i.e., μ_{ex}), it shortens the amount of time the attacker remains busy with benign actions and provides the attacker with more opportunities to perpetrate the attack. As a result, the normalized channel utilization of the NUT decreases (Fig. 9(g)). Similarly, the normalized collision rate increases with the increase in μ_{ex} (Fig. 9(h)).

Different Attack Models: As discussed in Section VI, different attack models have their own advantages and disadvantages. In Fig. 10(a)-(b), the normalized throughput and collision rate of the NUT are shown for the naive, naive-random, and proposed HTE attack. It is evident that the naive and naive-random attack results in superior attack performance than the proposed HTE attack. Nonetheless, they suffer from singular detection problem and have a negligible immunity against the proposed context-aware detection technique, even with a small observation time.



(a) Impact on throughput. (b) Impact on collisions.

Fig. 10. Different attack performance.



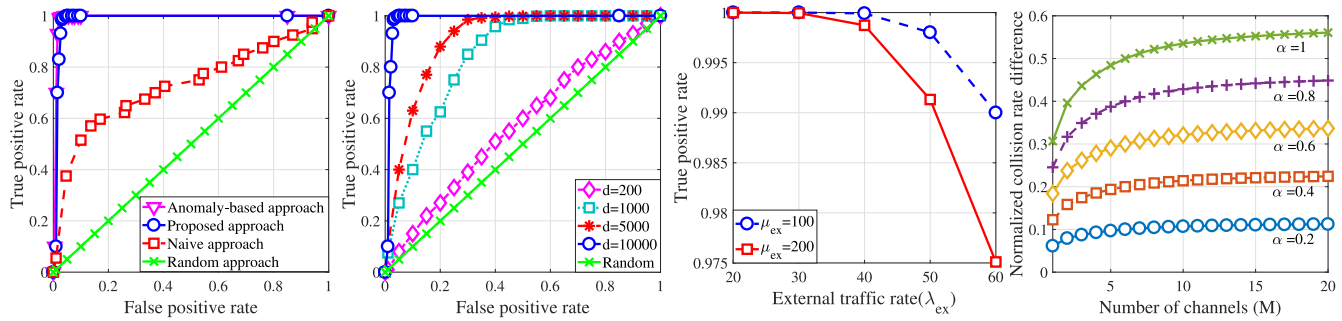
(a) Estimation error of λ_p. (b) Estimation error of μ_p.

Fig. 11. HMM estimation performance.

B. PU and EX Parameter Estimation

The performance of the proposed *Third Eye* depends on how accurately HMM-based estimators can estimate the required traffic parameters of PUs and EX in victim's sensing range. In addition, the length of a training sample is instrumental to the learning performance. In Fig. 11, we can observe the trend of estimation error for PU packet arrival rate (λ_p) and service rate (μ_p) (showed for 5 PUs). Estimation errors reduce to below 4% when the estimator is trained to 50 seconds.

In this work, we train the HMM estimator with 25 seconds of data and observe the impact of the attack detection for the next 75 seconds without changing the PU or EX activity rate. Nevertheless, in reality, the PU and EX activity rate is not going to be constant all the time and the HMM estimator must re-estimate to track changes.



(a) Performance comparison. (b) Impact of **d** on detection. (c) Impact of λ_{ex} and μ_{ex} on detection. (d) Impact of M and α.

Fig. 12. The HTE attack detection.

C. Attack Detection

The proposed mathematical model can effectively distinguish the activity of an attacker through carrier sensing and detect the interference created by HTE attackers. This subsection analyzes the performance of the detection model.

ROC Curve: To illustrate the effectiveness of our proposed detection strategy, we compare it with the jamming detection approach that considers the RSS and BER as the primary metrics of jamming detection [22]; here, we name it as the naive method. In this approach, the intuition is that when there is a bit error whereas the RSS value is high, this indicates jamming attack. In addition, we compare the performance to an earlier work [23], which detects anomalies in hidden nodes' behavior. We point out that, to the best of our knowledge, there is not yet a signature-based detection method for the proposed HTE attack to compare with. Our effort is to compare the ability of attack activity detection, with the naive method [22], the anomaly-based method [23], and the proposed *Third Eye*.

Fig. 12(a) illustrates the receiver operating characteristic (ROC) curve that represents the efficiency of detection by plotting the true positive rate (i.e., the probability of detection) versus the false positive rate (i.e., the probability of false alarm). Comparing these four ROC curves, we find that the proposed context-aware detection strategy results in a large area under the curve (AUC). Thus, it achieves significantly more reliable detection results. In the case of false negatives, the attacker conducts a very low level of interference, which the detector identifies as statistically insignificant to match with the behavior of an attacker.

Though the anomaly-based detection technique provides almost similar results—if not better—it fails to uniquely identify an HTE attacker because it does not consider exclusive characteristics of an HTE attacker in its detection approach; it only performs well when the goal is to detect anomalous behavior. Conversely, the naive method has a much smaller AUC and suffers extensively from poor false positive rate. As the naive approach does not consider that an interference source could be benign, it detects the interference from co-located benign neighboring nodes as malicious interference; hence, it exhibits poor performance.

Impact of Observation Window Size on the Detection: The observation window size plays an instrumental role in the effectiveness of HTE attack detection. Fig. 12(b) represents the ROC curves with respect to $\mathbf{d} = 200$, 1000, 5000, and 10000. We can observe that the detection performance declines as **d** decreases; with $\mathbf{d} = 200$, it performs very close to the random detection approach. A larger observation window size provides the NUT with better abilities to see through the randomness in an attacker's behavior and to differentiate an attacker from a benign one. Therefore, a larger observation window size is required to extract better performance from the detection strategy. As different window sizes offer different performance, a proper choice of **d** depends upon the cost and time-criticalness of the application.

Impact of λ_{ex} and μ_{ex} on the Detection: The traffic parameters of the attacker impact the performance of the proposed detection model. In Fig. 12(c), we represent the true positive rate vs. λ_{ex} (with a fixed false positive rate, 0.05) to illustrate the relationship between them. We can observe from the figure that the true positive rate decreases with the increase in λ_{ex}. Though a lower λ_{ex} facilitates heightened attack performance (Figs 9(c)-(d)), it also increases the probability of detection. Moreover, μ_{ex} also impacts the true positive rate. Hence, these findings create a practical design challenge for an attacker who wants to maximize the attack efficiency and remain undetected at the same time.

Impact of M and α on the Detection: The proposed signature-based detection model weighs in different network parameters to model a benign hidden terminal and a malicious one. Among them, the number of channels (M) and the hidden terminal factor (α) play pivotal roles. Intuitively, as the number of channels increases, the probability of collision decreases because co-existing IoT nodes have more channels to utilize. However, the number of channels does not make significant difference in collision rate after it passes a certain threshold, such as $M = 5$ in Fig. 12(d) where the normalized collision rate difference represents the difference between state transition probabilities P_{23} of benign and malicious hidden terminals. Here P_{23} represents the probability of experiencing interference from hidden terminals while the NUT is receiving.

However, as α increases, the difference increases significantly. Though higher values of α offers more performance increase for the attacker, it also exposes the attacker to higher risks of detection. Thereby an attacker remains constrained in its attack performance to avoid detection.

D. Qualitative Comparison With the Literature

The proposed signature-based detection strategy depends on learning the context of each transmission from its neighboring nodes; therefore, it requires different set of information than traditional strategies and, in some cases, may incur additional computational and memory resources. In this subsection, we shed light on these from a qualitative perspective.

Detection Parameters: Unlike general network performance indicators—such as packet delivery ratio, signal strength, bad packet ratio, throughput, delay—the proposed context-based detection strategy relies on the traffic characteristics of neighboring nodes from external networks (i.e., λ_{ex} and μ_{ex}) and the network topology (i.e., α).

Traditional detection strategies try to determine whether the NUT is under attack, and they do not consider the source of interference (or jamming). In contrast, our proposed strategy tries to determine whether the NUT is under attack based on the source of interference. Besides identifying the attack, this approach provides the ability to identify the attacker; this allows us to build a context-based detection model.

Computational and Memory Cost: The computation tasks are divided into two stages: i) offline phase: the NUT captures behaviors of a benign and a malicious node using the proposed Markov model and, afterward, the Markov model produces closed-form expressions to feed into the detector module. Note that, learning finishes in this phase and no further learning is required in the online phase and ii) online phase: the NUT keeps track of PUs' traffic parameters (λ_p and μ_p), EX's traffic parameters (λ_{ex} and μ_{ex}), and network topology (α), which are available from the sensing process. The computation steps are constant for each external node and increase linearly with the number of neighboring external nodes. Therefore, the computational cost, though higher than some traditional techniques, is tractable to support dense networks. However, unlike most traditional jamming detection strategies, this strategy incurs memory cost to maintain the tracking of the required parameters.

IX. Conclusion

In this paper, we proposed a vulnerability that the dense IoT deployment will likely bring, i.e., interference from hidden terminals of external IoT networks, and we illustrated how a reactive attacker can exploit this vulnerability to stifle the operation of the network. To the best of our knowledge, this is the first work that foresees this vulnerability of IoT deployment, studies it, and proposes a detection technique based on carrier sensing. We captured the effect of external hidden terminals through a Markov model and detected the aberrant behaviors of HTE attacks. The numerical and simulation results showed the superior performance of our proposed detection model as compared to the naive jamming detection approach.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] Y. Huang, Y. Chen, Y. T. Hou, W. Lou, and J. H. Reed, "Recent advances of LTE/WiFi coexistence in unlicensed spectrum," *IEEE Netw.*, vol. 32, no. 2, pp. 107–113, Mar./Apr. 2018.

[3] S. Parkvall, E. Dahlman, A. Furuskar, and M. Frenne, "NR: The new 5G radio access technology," *IEEE Commun. Stand. Mag.*, vol. 1, no. 4, pp. 24–30, Dec. 2017.

[4] Z. Xiong, Y. Zhang, D. Niyato, R. Deng, P. Wang, and L.-C. Wang, "Deep reinforcement learning for mobile 5G and beyond: Fundamentals, applications, and challenges," *IEEE Veh. Technol. Mag.*, vol. 14, no. 2, pp. 44–52, Jun. 2019.

[5] H.-C. Tsai, C.-H. Liu, and L.-C. Wang, "An analytical approach to coexisting evaluation in multi-RAT heterogeneous networks with opportunistic CSMA/CA," in *Proc. IEEE ICC*, 2016, pp. 1–6.

[6] C.-H. Liu and L.-C. Wang, "Modeling and analysis of coexisting multiple radio access technologies in heterogeneous wireless networks," in *Proc. ICCNC*, 2016, pp. 1–5.

[7] A.-H. Tsai, L.-C. Wang, J.-H. Huang, and T.-M. Lin, "Intelligent resource management for device-to-device (D2D) communications in heterogeneous networks," in *Proc. ISWPMC*, 2012, pp. 75–79.

[8] A. A. Khan, M. H. Rehmani, and A. Rachedi, "Cognitive-radio-based Internet of Things: Applications, architectures, spectrum related functionalities, and future research directions," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 17–25, Jun. 2017.

[9] C. X. Mavromoustakis, G. Mastorakis, and J. M. Batalla, *Internet of Things (IoT) in 5G Mobile Technologies*, vol. 8. Cham, Switzerland: Springer, 2016.

[10] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 1, no. 4, pp. 40–48, Apr. 2008.

[11] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM MobiHoc*, 2005, pp. 46–57.

[12] G. Thamilarasu, S. Mishra, and R. Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad hoc networks," in *Proc. IEEE MILCOM*, 2006, pp. 1–7.

[13] O. Puñal, I. Aktaş, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation," in *Proc. IEEE WoWMoM*, 2014, pp. 1–10.

[14] A. Marttinen, A. M. Wyglinski, and R. Jäntti, "Statistics-based jamming detection algorithm for jamming attacks against tactical MANETs," in *Proc. IEEE MILCOM*, 2014, pp. 501–506.

[15] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1746–1759, Aug. 2014.

[16] I. Shin, Y. Shen, Y. Xuan, M. T. Thai, and T. Znati, "Reactive jamming attacks in multi-radio wireless sensor networks: An efficient mitigating measure by identifying trigger nodes," in *Proc. 2nd ACM Int. Workshop Found. Wireless Ad Hoc Sensor Netw. Comput.*, 2009, pp. 87–96.

[17] A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," in *Proc. IEEE Int. Conf. Commun.*, 2009, pp. 1–6.

[18] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *Proc. IEEE INFOCOM*, 2007, pp. 1307–1315.

[19] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2nd Quart., 2011.

[20] M. Spuhler, D. Giustiniano, V. Lenders, M. Wilhelm, and J. B. Schmitt, "Detection of reactive jamming in DSSS-based wireless communications," *IEEE Trans. Wireless Commun.*, vol. 13, no. 3, pp. 1593–1603, Mar. 2014.

[21] D. Ciuonzo, A. Aubry, and V. Carotenuto, "Rician MIMO channel-and jamming-aware decision fusion," *IEEE Trans. Signal Process.*, vol. 65, no. 15, pp. 3866–3880, Aug. 2017.

[22] M. Strasser, B. Danev, and S. Čapkun, "Detection of reactive jamming in sensor networks," *ACM Trans. Sensor Netw.*, vol. 7, no. 2, p. 16, 2010.

[23] M. Hossain and J. Xie, "Detection of hidden terminal emulation attacks in cognitive radio-enabled IoT networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, 2019, pp. 1–6.

[24] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," in *Proc. IEEE MILCOM*, 2011, pp. 2129–2135.

[25] A. Benslimane, A. E. Yakoubi, and M. Bouhorma, "Analysis of jamming effects on IEEE 802.11 wireless networks," in *Proc. IEEE ICC*, 2011, pp. 1–5.

[26] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "Performance of IEEE 802.11 under jamming," *Mobile Netw. Appl.*, vol. 18, no. 5, pp. 678–696, 2013.

[27] J. McNair, T. Tugcu, W. Wang, and J. L. Xie, "A survey of cross-layer performance enhancements for mobile IP networks," *Comput. Netw.*, vol. 49, no. 2, pp. 119–146, 2005.
[28] 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.
[29] M. Hossain and J. Xie, "Impact of off-sensing attacks in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2017, pp. 1–6.
[30] M. Hossain and J. Xie, "Off-sensing and route manipulation attack: A cross-layer attack in cognitive radio based wireless mesh networks," in *Proc. IEEE INFOCOM*, 2018, pp. 1376–1384.
[31] M. Hossain and J. Xie, "Covert spectrum handoff: An attack in spectrum handoff processes in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2018, pp. 1–6.
[32] M. Hossain and J. Xie, "Hide and seek: A defense against off-sensing attack in cognitive radio networks," in *Proc. IEEE INFOCOM*, 2019, pp. 613–621.
[33] J. Xie, "User independent paging scheme for mobile IP," *Wireless Netw.*, vol. 12, no. 2, pp. 145–158, 2006.
[34] N. An and S. Weber, "Efficiency and detectability of random reactive jamming in wireless networks," in *Proc. IEEE SECON*, 2018, pp. 1–9.
[35] Z. Sun and J. N. Laneman, "Performance metrics, sampling schemes, and detection algorithms for wideband spectrum sensing," *IEEE Trans. Signal Process.*, vol. 62, no. 19, pp. 5107–5118, Oct. 2014.
[36] X. Liu and J. Xie, "A practical self-adaptive rendezvous protocol in cognitive radio ad hoc networks," in *Proc. IEEE INFOCOM*, 2014, pp. 2085–2093.
[37] D. Han, D. G. Andersen, M. Kaminsky, K. Papagiannaki, and S. Seshan, "Access point localization using local signal strength gradient," in *Proc. Int. Conf. Passive Active Netw. Meas.*, 2009, pp. 99–108.
[38] C. R. Karanam, B. Korany, and Y. Mostofi, "Magnitude-based angle-of-arrival estimation, localization, and target tracking," in *Proc. ACM/IEEE IPSN*, 2018, pp. 254–265.
[39] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *Proc. IEEE INFOCOM*, 2013, pp. 2778–2786.
[40] L. R. Rabiner, "A tutorial on hidden Markov models and selected applications in speech recognition," *Proc. IEEE*, vol. 77, no. 2, pp. 257–286, 1989.
[41] K. W. Choi and E. Hossain, "Opportunistic access to spectrum holes between packet bursts: A learning-based approach," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2497–2509, Aug. 2011.
[42] B. C. Levy, *Principles of Signal Detection and Parameter Estimation*. New York, NY, USA: Springer, 2008.
[43] S. Marano, V. Matta, and L. Tong, "Distributed inference in the presence of Byzantine sensors," in *Proc. IEEE Conf. Signals Syst. Comput.*, 2006, pp. 281–284.
[44] M. S. Bartlett, "The frequency goodness of fit test for probability chains," *Math. Proc. Cambridge Philosoph. Soc.*, vol. 47, no. 1, pp. 86–95, 1951.

Moinul Hossain (Member, IEEE) received the B.S. degree in electronics and communication engineering from the Khulna University of Engineering and Technology, Khulna, Bangladesh, in 2011. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, University of North Carolina at Charlotte, Charlotte, NC, USA. His research interests include wireless network security, wireless networking, Internet-of-Things, and spectrum coexistence.

Jiang Xie (Fellow, IEEE) received the B.E. degree in electrical and computer engineering from Tsinghua University, Beijing, China, in 1997, the M.Phil. degree in electrical and computer engineering from the Hong Kong University of Science and Technology in 1999, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology in 2002 and 2004, respectively. She joined the Department of Electrical and Computer Engineering, University of North Carolina at Charlotte (UNC-Charlotte) as an Assistant Professor in August 2004, where she is currently a Full Professor. Her current research interests include resource and mobility management in wireless networks, mobile computing, Internet of Things, and cloud/edge computing. She received the U.S. National Science Foundation Faculty Early Career Development (CAREER) Award in 2010, the Best Paper Award from IEEE Global Communications Conference in 2017, the Best Paper Award from IEEE/WIC/ACM International Conference on Intelligent Agent Technology in 2010, and the Graduate Teaching Excellence Award from the College of Engineering at UNC-Charlotte in 2007. She is on the editorial boards of the IEEE/ACM TRANSACTIONS ON NETWORKING and the *Journal of Network and Computer Applications* (Elsevier). She is a Senior Member of ACM.