Detection of Hidden Terminal Emulation Attacks in Cognitive Radio-enabled IoT Networks

Moinul Hossain and Jiang Xie
Department of Electrical and Computer Engineering
The University of North Carolina at Charlotte
Email: {mhossai4, Linda.Xie}@uncc.edu

***Abstract*—Recently, the Internet of Things (IoT) technology has been drawing increasing attention in that it has a great potential to positively impact human life in a broad range of applications. However, the dense deployment of multiple co-located IoT networks that may follow different wireless protocols would engender new vulnerabilities. In this paper, we introduce a novel attack scenario in co-located IoT networks, where a reactive jammer can emulate the transmission characteristics of a hidden terminal from another network and can interfere with its hidden counterparts, namely the *hidden terminal emulation* (HTE) attack. As the dense deployment of IoT nodes will naturally create such hidden terminal scenarios, it provides the HTE attacker plausible deniability to reactively interfere with its hidden counterparts; hence, the HTE attacker remains immune to conventional reactive jamming detection techniques. In this paper, we capture the behavior of a benign hidden terminal via a parsimonious Markov model and propose a detection solution using the goodness-of-fit hypothesis testing. Though there has been extensive research on jamming detection, our novelty lies in considering hidden terminals as benign interference sources and leveraging the existing carrier sensing technique as a natural and effective way to detect HTE attacks.**

I. Introduction

With the advent of the Internet of Things (IoT), a new path to infinite possibilities has emerged [1]. 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. The dense deployment of IoT nodes in overpopulated unlicensed bands will aggravate interference issues; hence, less throughput and higher delay may occur. Cognitive radio (CR) offers an intelligent solution to this issue, where a CR-enabled IoT device can opportunistically access licensed channels (i.e., when licensed users are idle) to avoid interference with other co-located IoT devices in the unlicensed spectrum. Here, IoT devices utilize the real-time channel sensing information to help them in finding spectrum holes (i.e., underutilized licensed channels) and to avoid interference with licensed users.

Researchers have envisioned the IoT as a ubiquitous technology, which will intricately integrate devices (or things) that surround us, and these devices will communicate within themselves by forming a closed connected network to intelligently solve real-life problems. Such a broad vision will require an enormous amount of IoT deployments at our homes, offices, transportation systems, health care, and industries. Intuitively, these IoT devices must form distinct independent networks to manage data within their own network and to provide security and privacy to the owners. Therefore, separate CR-enabled IoT networks must independently manage their own spectrum access and spectrum utilization strategies.

This work was supported in part by the US National Science Foundation (NSF) under Grant No. 1343355, 1718666, and 1731675.

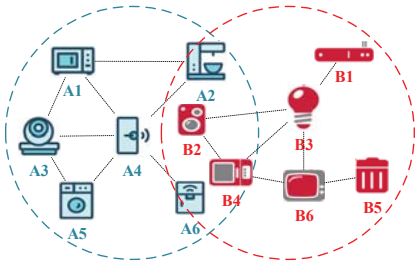


Fig. 1: Hidden terminal interference between coexisting IoT networks.

Motivations: The dense deployment of IoT devices may bring new vulnerabilities where attackers can exploit natural interference scenarios to corrupt transmissions of particular victim IoT devices, such as interference from hidden terminal devices in a different IoT network. Fig. 1 provides an illustration of this issue, 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, and under the given scenario, each of these two sets has no idea about the transmissions of the other set. Therefore, it is probable that nodes of these two sets may utilize the same radio channel (or spectrum hole) and create interference to each other.

The concurrent transmission from hidden nodes acts as a jamming signal at the corresponding receiver, and it is difficult to differentiate between a benign node (i.e., hidden terminal) and denial-of-service (DoS) attacker. Therefore, if an attacker can impersonate as a hidden terminal to a particular IoT node, it can capitalize on this scenario to corrupt the transmission intended for a particular receiver or the transmission generated from a particular transmitter.

Challenges: As attackers try to attack a particular node, the straightforward approach of constant jamming in a particular channel is not ideal for the objective. A better approach is to attack only when a transmission to the victim is heard, namely the reactive approach. A naive reactive jammer may try to attack each time it hears a transmission to the victim node. Though it is the most damaging strategy against the victim and provides the highest attack efficiency, it increases the risk of detection. Therefore, the reactive approach requires a random approach to trade-off between the attack objective

978-1-5386-8088-9/19/$31.00 ©2019 IEEE

(i.e., degrading victim's throughput) and the risk of exposure.

Nonetheless, the detection of such a random reactive attack requires a different approach. Prior works on detecting jamming attacks are mostly based on network performance measurements, such as the packet delivery rate (PDR) and the received signal strength (RSS). Although these detection methods are effective, they are inapplicable in the illustrated scenario where hidden terminals can be falsely categorized as attackers. Therefore, we require a more intelligent detection technique to counteract the randomness in attacks.

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. In the proposed model, the attacker poses as a hidden terminal by manipulating its antenna radiation pattern.
2. We propose an intelligent detection method based on a Markov model to detect the proposed attack despite the randomness in its behavior. We solve the detection problem by converting it into a goodness-of-fit test.

Related Work: In [2], the influence of different jamming strategies on the PDR and RSS of network links is analyzed and a thresholding algorithm is proposed. In [3], [4], different network metrics, such as the channel busy ratio and the number of retransmission attempts are employed. Jamming attacks in time-critical networks are studied in [5] and numerical results on the impact of jamming on the network message invalidation ratio are presented. In [6]–[9], the impact of jamming attacks on the performance of IEEE 802.11 networks is analyzed. In CR-enabled networks, DoS attacks are studied in [10]–[14], where the attacker attacks in the off-sensing interval. In [15], 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 getting detected. One limitation of the model is that it considers the slotted Aloha protocol, which does not incorporate the carrier sensing multiple access — an essential tool in modern wireless networks.

Nonetheless, none of these works considered the presence of hidden terminals from different networks. As previous works mostly depend on the network performance, they may mis-categorize hidden terminals as jammers. Although the influence of hidden terminal interference is considered in [16], it did not explain how a reactive jammer 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 a reactive jammer can listen to its hidden counterparts.

II. System Model

We consider a benign IoT network with multiple IoT nodes that are trying to communicate among themselves in an ad-hoc mode; we name it the *internal network*. These benign IoT nodes are surrounded by other co-located IoT nodes from a different network; we name the network as *external network*.

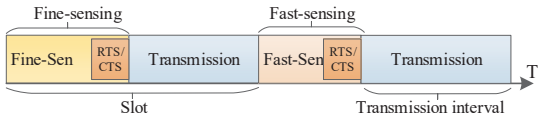


Fig. 2: The channel access schedule.

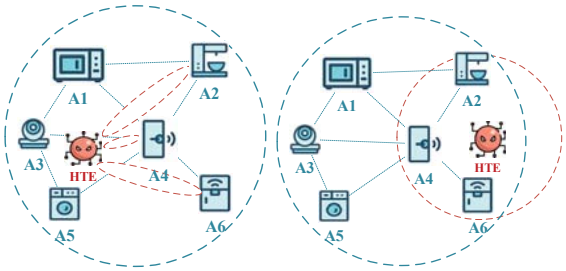
Channel Model: We consider the presence of M homogeneous channels each with equal bandwidth, and M licensed or primary users (PUs) using these channels. Here, time is divided into equal slots and transmissions are packet-based. A packet starts at the beginning of a slot and ends at the end of a slot. 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 and the exponential packet length process. Let 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 IoT node has $k-1$ neighbors (excluding itself), and they use omni-directional antennas for communications. These k nodes have an available channel list (ACL) $m_i \in \{1, 2, \cdots, M\}$, where $i \in k$. Each IoT node (both internal and external) is equipped with one radio for wide-band spectrum sensing [17] and one radio for control information exchange and data transmission. We consider that channel conditions are ideal and that a transmission failure is only resulted from one reason: interference from a hidden terminal. In the following, we use *interference* and *collision* interchangeably.

Channel Access: Each transmission attempt of an IoT node must be preceded by a sensing interval. As shown in Fig. 2, IoT nodes employ their wide-band sensing antenna to sense the current channel before initiating a transmission, and they continue to sense the channel during the transmission to negate the collision between PUs and IoT nodes. An IoT node 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 the channel available, two IoT nodes exchange request-to-send/clear-to-send (RTS/CTS) messages to reserve the channel. IoT nodes initiate a new packet transmission with the longer fine-sensing and employ the shorter fast-sensing for each successive frame.

During a sensing interval, if an IoT node 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 nodes must find a common available channel between them to initiate a data transmission. Rendezvous technique works as the process to find a common available channel [18]. However, the choice of a specific rendezvous scheme does not impact the performance of our proposed work, as long as attackers have no prior knowledge of the victim's channel hopping sequence for rendezvous. Hence, we assume that IoT nodes have already successfully performed rendezvous with each other using any



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

Fig. 3: The hidden terminal emulation attack.

existing scheme, and they share a time-seeded pseudo-random channel hopping sequence for future communications.

III. Hidden Terminal Emulation Attack

A jamming strategy generally regulates how to transmit a noise signal to create undesired interference at the victim to thwart normal communications. However, in this case, instead of noise signals, an attacker transmits its normal signals to create interference at the victim. The attacker perpetrates the hidden terminal emulation (HTE) attack in two phases:

Reconnaissance and Emulation Phase: The primary task of an HTE attacker is to successfully emulate itself as a hidden terminal to the neighbors of the victim. We consider that the attacker is capable of directional transmissions, and it can deduce the geometric location of benign IoT nodes by using off-the-shelf techniques, such as angle of arrival and distance to the transmitter [19]. Depending on the objective of the attacker and its physical limitations, the attacker may try to pose as a hidden terminal to all neighbors or selected neighbors of the victim. In Fig. 3(a), the attacker tries to pose itself as a hidden terminal to nodes $A1$, $A3$, and $A5$; it limits its transmissions only to nodes $A2$, $A4$, and $A6$ through directional antennas. The intelligent utilization of directional transmissions enables the attacker to create a different physical scenario than the real one, which is represented in Fig. 3(b).

Attack 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. Afterwards, it deliberately interferes transmissions from nodes $A1$, $A3$, and $A5$, that are destined to the victim node (i.e., $A4$). However, the choice of jamming rate depends on the strategy of the attacker; it may jam each transmission or randomly choose to jam. In this paper, we consider that the attacker takes a subtle random approach where it poses as a legitimate node by continuing regular communications with its neighbors in its own network, and it intelligently interferes with the victim's reception only when it is idle. Hence, it offers a different detection challenge in contrast to conventional reactive jamming attacks.

Summary: The HTE attacker utilizes directional transmission techniques that are widely available for communication purposes and weaponizes these to perpetrate the attack. A wide range of distinct attack strategies can be studied from the proposed generalized attack strategy. In this paper, we focus on proposing a generalized model to detect such anomalous behavior from a hidden terminal. In contrast to traditional reactive jamming detection techniques, we require an approach that can consider a hidden node as an interference source, does not mis-categorize benign hidden terminals as attackers, and can detect anomalous behaviors of hidden terminals.

IV. Detection of the Hidden Terminal Emulation Attack

The proposed detection approach is comprised of two steps: i) designing a mathematical model to characterize the behavior of benign hidden terminals; ii) formulating the detection problem as a goodness-of-fit hypothesis testing problem, to identify whether a sequence of observed behaviors is likely to be produced from the established mathematical model.

A. Mathematical Model

The reception behavior of the defending IoT node is considered as an ON-OFF process: $(X(t); t \geq 0)$ with state space $\{0, 1\}$, where 0 and 1 correspond to the ideal and the receiving state, respectively. Let $A4$ denote the IoT node that is evaluating abnormal interference, hereafter referred to as the *node under test* (NUT), and the hidden terminal from the external network is named as the *external node* (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 $(E(t); t \geq 0)$ and $(Y(t); t \geq 0)$ are ON-OFF processes with state space $\{0, 1\}$, where 0 and 1 correspond to the ideal and the transmitting state, respectively. The interaction between $X(t)$, $E(t)$, and $Y(t)$ is captured as a five-state discrete-time Markov model $Z(t)$.

The Markov state $Z(t) \equiv \{Y(t), X(t), E(t)\}$ denotes the state of the NUT in its current operating channel at the end of a time-slot. The brief descriptions of the states are:

0$\{0, 0, 0\}$: 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$\{0, 0, 1\}$: The current channel is free, the NUT is idle, and the EX is transmitting.

2$\{0, 1, 0\}$: The current channel is free, the NUT is receiving, and the EX is either idle or transmitting on another channel.

3$\{0, 1, 1\}$: The current channel is free, the NUT is receiving, and the EX is transmitting. *This represents the collision.*

4$\{1, X, X\}$: 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 $k_h \in \{0, \cdots, k-1\}$, 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 nodes that are hidden to the EX. We assume that each IoT node broadcasts

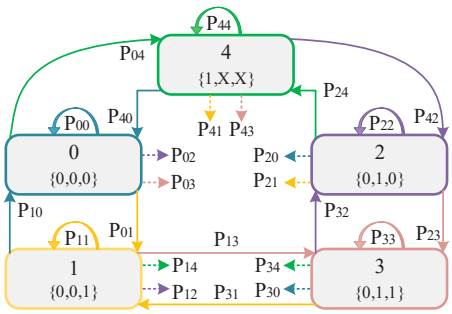


Fig. 4: The proposed Markov model.

its identity periodically, and IoT nodes sniff the wireless medium to discover the presence of IoT nodes within their surroundings. In Fig. 3, though $A1$, $A3$, and $A5$ cannot listen to the transmission of the node HTE (or EX), $A2$, $A4$, and $A6$ can listen to its transmission. Hence, each node maintains a list of external nodes that are hidden to them (by exchanging information within internal IoT nodes), and it helps them to deduce the value of α. Table I summarizes the notations used in the proposed Markov model.

TABLE I: 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}

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 node 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.

Transitions from the idle state (i.e., $Z(t)=0$):

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

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

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

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

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

where Π_b = the steady-state probability that exactly b channels are busy by PUs, $P_{col}^b = (1-\rho_{ex})P_{\lambda_{ex}}P_{match}^b$, ρ_{ex} = the steady-state probability that the EX is active, and $P_{match}^b = 1/(M-b)$.

Transitions from the EX active state (i.e., $Z(t)=1$):

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

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

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

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

Transitions from the NUT's receiving state (i.e., $Z(t)=2$):

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

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

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

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

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

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

Transitions from the collision state (i.e., $Z(t)=3$):

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

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

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

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

Transitions from the channel busy state (i.e., $Z(t)=4$):

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

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

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

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

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

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 $j \in \{0, 1, 2, 3, 4\}$.

B. Goodness-of-Fit Test

The NUT monitors activities on all channels and collects transmission patterns of all wireless nodes in its surroundings over a time window of $\mathbf{d} = \mathbf{w}/\mathbf{t}$ 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 either generated by a benign hidden terminal or by an HTE attacker. Now, let us denote transition probability matrices that characterize a benign hidden terminal as $\mathbf{P}^0$ and that is generated from the observations as $\mathbf{P}$. Thus, a goodness-of-fit hypothesis testing problem can be formed:

$$\mathbf{H_0} : \mathbf{P} = \mathbf{P^0}, \;\; \mathbf{H_1} : \mathbf{P} \neq \mathbf{P^0}. \quad (24)$$

We use the chi-square test to verify the observed sequence. Let us define the number of transitions from state i to state j of $\mathbf{z_d}$ as $N_{ij} = \sum_{t=1}^{d} \mathbf{1}_{\{z_t = i, z_{t+1} = j\}}$, 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 $N_i \equiv \sum_{j=0}^{4} N_{i,j} = \sum_{t=1}^{d} \mathbf{1}_{\{z_t = i\}}$, and according to [20], N_{ij} are asymptotically Gaussian distributed. Now, the chi-square test statistic:

$$\chi^2 = \sum_{i=0}^{4} \sum_{j=0}^{4} \frac{(N_{i,j} - \mathbf{P}_{ij}^0 N_i)^2}{\mathbf{P}_{ij}^0 N_i}. \quad (25)$$

It is reasonable to assume the initial-state probability distribution is similar to the steady-state probabilities of the states. However, as [5] indicated, 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.

Summary: The detection model captures the interference pattern an IoT node experiences under the influence of benign hidden terminals and flags the HTE attack when observations deviate from the established model. The proposed Markov model accumulates all required information into five states, and the chi-square test verifies how well the observed sequence fits the established benign behavior model. Our proposed detection technique requires only the carrier sensing information that is readily available for channel access purposes.

V. Performance Analysis

In this section, we present numerical and simulation results to evaluate the performance of our proposed work. Here, we consider that all IoT nodes physically reside within close proximity of each other and share the same ACL at a given time. The simulation parameters are listed in Table II.

TABLE II: 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)	$\lambda_p = 50$; $\mu_p = 100$
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)	$\lambda = 20, 30, 40, 50, 60$; $\mu = 100$
SU packet size	1024 bytes
Hidden terminal factor, α	$5/7$

The objective of the NUT, that is receiving, is to determine if the observed interference maintains the pattern set by the mathematical model. In contrast, the attacker tries to maintain a stable packet rate to avoid suspicious behaviors and attacks in its inactive periods by reactively initiating a new transmission.

A. Hidden Terminal Emulation Attack

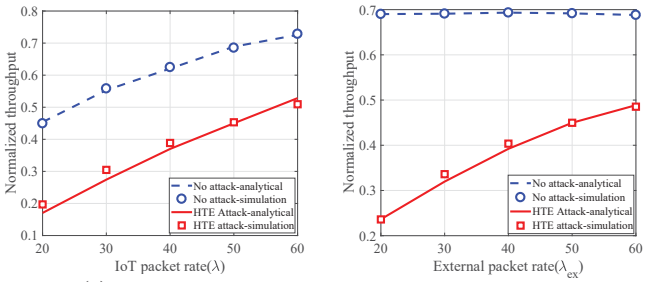
This subsection shows the impact of the proposed HTE attack on the network performance of the NUT.

Impact of λ_{in} on the HTE Attack: A higher rate of incoming traffic (i.e., λ_{in}) 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. 5(a), we can observe that the effect of the attack increases with the increase in incoming traffic 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 packet transmission. As the traffic rate of the EX increases, the time it stays in active state increases (i.e., ρ_{ex}). Hence, the room for interference decreases. Therefore, to increase the impact of the attack, the attacker must decrease its packet arrival rate. In Fig. 5(b), we can observe that under no attack (i.e., when EX is benign), the EX's traffic has an insignificant effect on the throughput of the NUT. However, under attack, it illustrates sensitivity to the change.

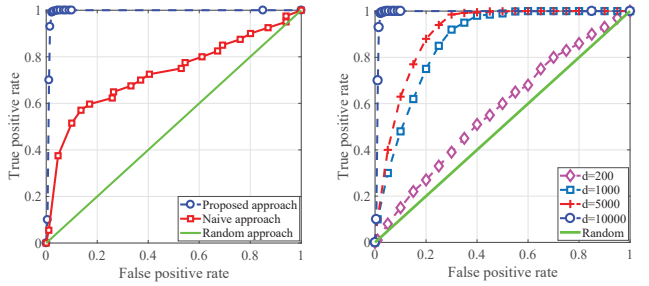
B. Attack Detection

The proposed 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 proposed detection model.



(a) Impact of λ_{in}. (b) Impact of λ_{ex}.

Fig. 5: The impact of different parameters on NUT's throughput.



(a) Performance comparison. (b) Impact of $\mathbf{d}$ on detection.

Fig. 6: The HTE attack detection.

ROC Curve: To illustrate the effectiveness of our proposed model, we compare it with the naive jamming detection approach. As other literature has proposed, we consider the PDR and BER as the primary metrics of jamming detection in the naive approach. In addition, we point out that, to the best of our knowledge, there is not yet a detection method for the proposed attack to compare with. Our effort is to compare the ability of attack activity detection, that is, jamming detection, with the naive method and the random method.

Fig. 6(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 three ROC curves, we find that the proposed detection strategy results in a larger area under the curve (AUC). Thus, it achieves significantly more reliable detection results. Conversely, the naive method has a much smaller AUC. Hence, it is inferior to the proposed method.

Impact of Observation Window Size on the Detection: The observation window size plays an instrumental role on the effectiveness of HTE attack detection. Fig. 6(b) represents the ROC curves with respect to $\mathbf{d} = 200, 1000, 5000, 10000$. We can observe that the detection performance decreases as $\mathbf{d}$ decreases; with $\mathbf{d} = 200$, it performs very close to the random detection approach. As different window sizes offer different performance, a proper choice of $\mathbf{d}$ depends upon the cost and time-criticalness of the application.

VI. 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 jammer 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 reactive jamming 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," *Elsevier Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

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

[3] 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*, pp. 1–10, 2014.

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

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

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

[7] A. Benslimane, M. Bouhorma, *et al.*, "Analysis of jamming effects on IEEE 802.11 wireless networks," in *Proc. IEEE ICC*, pp. 1–5, 2011.

[8] E. Bayraktaroglu *et al.*, "Performance of IEEE 802.11 under jamming," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 678–696, 2013.

[9] J. McNair, T. Tugcu, W. Wang, and J. L. Xie, "A survey of cross-layer performance enhancements for Mobile IP networks," *Computer Networks*, vol. 49, no. 2, pp. 119–146, 2005.

[10] M. Hossain and J. Xie, "Impact of off-sensing attacks in cognitive radio networks," in *Proc. IEEE GLOBECOM*, pp. 1–6, 2017.

[11] 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*, pp. 1376–1384, 2018.

[12] M. Hossain and J. Xie, "Covert spectrum handoff: An attack in spectrum handoff processes in cognitive radio networks," in *Proc. IEEE GLOBECOM*, pp. 1–6, 2018.

[13] M. Hossain and J. Xie, "Hide and seek: A defense against off-sensing attack in cognitive radio networks," in *Proc. IEEE INFOCOM*, 2019.

[14] J. Xie, "User independent paging scheme for Mobile IP," *Wireless Networks*, vol. 12, no. 2, pp. 145–158, 2006.

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

[16] N. An and S. Weber, "Efficiency and detectability of random reactive jamming in wireless networks," in *Proc. IEEE SECON*, pp. 1–9, 2018.

[17] Z. Sun and J. N. Laneman, "Performance metrics, sampling schemes, and detection algorithms for wideband spectrum sensing," *IEEE Transactions on Signal Processing*, vol. 62, no. 19, pp. 5107–5118, 2014.

[18] X. Liu and J. Xie, "A practical self-adaptive rendezvous protocol in cognitive radio ad hoc networks," in *Proc. IEEE INFOCOM*, pp. 2085–2093, 2014.

[19] C. R. Karanam, B. Korany, and Y. Mostofi, "Magnitude-based angle-of-arrival estimation, localization, and target tracking," in *Proc. ACM/IEEE IPSN*, pp. 254–265, 2018.

[20] M. S. Bartlett, "The frequency goodness of fit test for probability chains," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 47, pp. 86–95, 1951.