Jump and Wobble: A Defense Against Hidden Terminal Emulation Attack in Dense IoT Networks

Moinul Hossain* and Jiang Xie**
*Towson University, Towson, MD, USA
**The University of North Carolina at Charlotte, Charlotte, NC, USA
Email: mhossain@towson.edu, Linda.Xie@uncc.edu

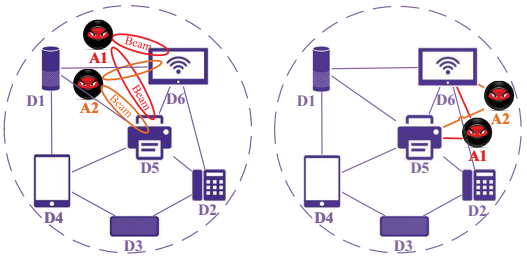
ICC 2021 - IEEE International Conference on Communications | 978-1-7281-7122-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICC42927.2021.9500963

***Abstract*—The unprecedented growth in Internet of Things (IoT) deployment is making it difficult to safeguard IoT infrastructures against novel security threats. Recently, a new attack, hidden terminal emulation (HTE), has shed light on a vulnerability in the co-located and dense IoT networks, where the attacker emulates a hidden node from an external co-located network. HTE attack exploits the *heterogeneity* among different IoT networks, the *shared* nature of spectrum access, and the *proximity* to the victim IoT device in a dense IoT scenario to interrupt the victim's communication. Prior work on HTE attack, however, considers an omniscient attack model, which has strong assumptions. In contrast, we propose a constrained attack model, which considers the sensing constraints of an attacker. Afterward, we propose a *novel safeguard approach* based on the Markov decision process to counteract the proposed attack model, namely Jump and Wobble. This work is among the very few to highlight the lower-layer vulnerabilities of spectrum coexistence in dense co-located IoT networks and, to the best of our knowledge, it is the *first* to propose a defense mechanism against HTE attacks.**

I. Introduction

In recent years, a significant amount of progress has been made on computing and communication technologies, which paved the way for device miniaturization and control of smart appliances. Internet-of-Things (IoT) consists of these smart devices that intricately integrate our surrounding physical systems to deal with complex real-life problems. As a result, the number of connected IoT devices is growing exponentially. Such growth brings a unique scenario where there will be *numerous IoT devices in a small physical space, and they may utilize the same spectrum (e.g., unlicensed band) and follow different wireless technologies (e.g., Cellular and WiFi)*; hence, radio interference issue will aggravate. Though several options have been proposed [1], [2], mutual spectrum sharing provides the most promising solution toward interference aware coexistence among different technologies [3], [4].

Motivations. This new spectrum coexistence scenario creates novel lower-layer vulnerabilities that existing defensive approaches are inadequate to address because *they do not consider sharing the spectrum with external wireless networks that follow different wireless technologies*. Previous works on IoT security mostly addressed upper-layer vulnerabilities [5]–[7], whereas lower-layer ones remain under-studied. Though [8]–[20] discussed different variants of denial-of-service (DoS) attacks in the lower layers of relevant technologies, they do not consider spectrum coexistence. The physical proximity and shared spectrum operation in dense scenarios significantly impact the lower layers' dynamics. Recently, [21]–[23] have proposed a coordinated multi-layer attack, namely hidden terminal emulation (HTE), in PHY and MAC layers to execute DoS attacks. Here, the attacker is a wireless device from a co-located external network, impersonating a hidden terminal to a victim IoT device and interferes with the transmission of that device as a hidden terminal. Unlike traditional jamming attacks, *the emulation of hidden terminals justifies this malicious interference; hence, it is challenging to detect*. Thereby, conventional defensive measures are futile since the source of interference is a legitimate external device.



(a) Real scenario. (b) Emulated scenario.
Fig. 1. Illustration of hidden terminal emulation attack.

Though handshaking mechanisms can help avoid the benign hidden terminal interference issue within a network, there is no solution to manage this among heterogeneous technologies, and *HTE-attack takes advantage of this limitation*. Fig. 1(a) illustrates this attack where attackers (i.e., A1 and A2) try to pose as hidden terminals to D1 and interfere with D1's packets to D5 and D6; they broadcast their identity only to nodes D5 and D6 by manipulating antenna radiation characteristics. This ingenious way of exploiting antenna properties enables attackers to emulate a different physical location than the actual one, illustrated in Fig. 1(b). As an example, network D and A could represent WiFi and LTE-U enabled IoT devices—sharing the 5GHz band—that physically reside in two neighboring rooms, apartments, or houses. The exponential growth of IoT devices will aggravate this vulnerability, and it can become life-threatening if an attacker can compromise a critical IoT device (e.g., oxygen pump or pacemaker). Though [22] proposes a detection technique, it does not discuss how to evade such attacks and, to the best of our knowledge, it remains unstudied.

Therefore, given the colossal impact and time criticality of this vulnerability, we must investigate the attack rigorously and propose adequate defensive strategies.

Challenges. In [22], it considers an omniscient attack model

This work was supported in part by the US National Science Foundation (NSF) under Grant No. 1718666, 1731675, 1910667, 1910891, and 2025284.

where the attacker can instantly sense all the channels. However, in reality, an attacker may have *constrained* sensing ability. Therefore, we require an attack model that considers the practical sensing constraints of the attacker.

Finally, a proactive defense approach—regardless of an attacker's strategy—must take into account the versatility (e.g., channel and route diversity) offered by multi-channel dense IoT networks and employ these unique attributes to fortify against (or avoid) unwanted malicious interference, even if it results from benign interference sources.

Contributions. The unique contributions of this paper are: (1) we modify the HTE attack model of [21] and propose a channel hopping-based attack model where the attacker randomly hops through different channels to detect the operating channel of the victim, and (2) we propose a Markov decision process (MDP) based novel safeguard strategy to thwart the HTE attack, where a defender exploits the diversity in a multi-channel network by randomly hopping through different channels and exploits the proximity in dense IoT networks by diverting traffic through intermediate devices.

Related Work. The research community has discovered numerous security vulnerabilities and proposed their defenses in IoT [24]–[28]. In [5], a distributed DoS attack is studied where Mirai botnet was used to compromise 0.6 million IoT devices. Honeywell home controllers are shown vulnerability in their authentication system [29]. In a recent work [30], it is demonstrated that home assistant devices can be compromised by an attacker using inaudible voice commands. A large-scale coordinated attack on the power grid is shown in [31] where attackers can compromise high wattage devices to manipulate the load demand and create blackouts. Yet, these works only focus on upper-layer vulnerabilities. In contrast, *we focus on the vulnerabilities caused by the changes in lower-layers in dense IoT networks under shared spectrum operation*. In addition, unlike [21]–[23], *we propose a constrained attack model and design a safeguard strategy against the HTE attack*. Moreover, though multi-channel defenses against smart jamming attacks are discussed in [11], [12], [16], [17], [19], they do not consider the aspect of routing diversity in dense IoT scenarios. In contrast, in addition to channel diversity, *we propose to utilize packet rerouting to avoid HTE attacks.*

II. System Model

We consider a network that consists of benign IoT devices (i.e., network D in Fig. 1). These benign IoT devices are surrounded by other co-located IoT devices (i.e., A1 and A2) on the same spectrum, who follow different wireless technologies. We consider these out-of-network devices as potential attackers. Here, the victim or defender is D1, and it has channel hopping capability.

Transmission and Channel Models. We consider that time is slotted and transmissions are packet-based. D1 transmits a packet at each time-slot (i.e., saturated scenario) with a fixed power. A1 randomly sends packets to A2 to act as a benign hidden terminal and reactively creates malicious interference to reduce the received signal-to-interference-plus-noise ratio (SINR) of D1's packets at D5 and D6. Attackers have multi-radio configurations, where transmission (Tx) and reception (Rx) antennas are used for beamforming and channel sniffing, respectively. Unlike Tx antenna, Rx employs isotropic radiation to sniff all neighboring devices. The geometric locations of the surrounding IoT devices are considered a priori.

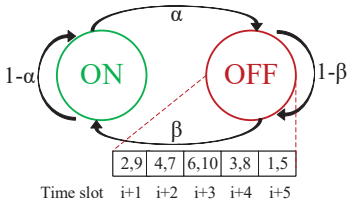


Fig. 2. Activity of HTE attacker.

We consider N non-overlapping channels where each channel experiences additive white Gaussian noise (AWGN). The two-state Gilber-Elliot channel model is adopted to characterize the channel fading process [32]. At each time slot, the channel can be in a fading state with a probability $\mathrm{P_{fad}}$. In the absence of channel fading, a transmission failure can only occur due to interference from the neighbors.

Network Coordination and Channel Access. We consider the Listen-Before-Talk (LBT) scheme for coordination in network D and adopt a channel access model where each transmission attempt is preceded by a sensing interval and a handshake process. After sensing the channel available, the source and destination IoT devices handshake to reserve the channel for future communications. The destination sends back an ACK or a NACK message to the source at the end of each packet—along with the perceived SINR and received signal strength (RSS) of the current packet—to inform the reception status.

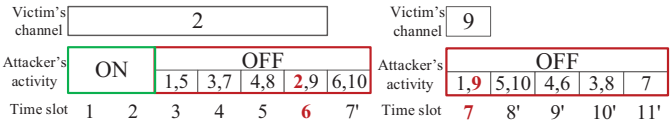
III. Random-HTE Attack: The Interference Phase

The proposed HTE attack model consists of two phases: 1) the emulation phase [21], which encompasses the strategy to manipulate antenna configurations, and 2) the interference phase, which demonstrates the strategy to create malicious interference. This paper considers that the attacker has achieved successful emulation and focuses on the interference phase.

An omniscient HTE attacker can instantly find the victim's operating channel and degrade the SINR well enough to make it infeasible for communication. However, in reality, an attacker has realistic constraints and restricted knowledge of the victim. This section discusses a random strategy for an HTE attacker, where the attacker randomly fluctuates between acting benignly (by communicating among devices in its own network) and maliciously. The interference phase pans out in two parts: (1) *plausible deniability* and (2) *detect and interfere*.

A. Plausible Deniability

Unlike a traditional DoS attacker, an HTE attacker acts as a legitimate network device that performs regular communications with devices in its network (e.g., A2 in Fig. 1); this, along with the emulation of a hidden terminal, provides the attacker *an alibi* to reactively interfere with its hidden counterparts. This behavior helps the attacker avoid traditional reactive jamming detection systems; an attacker randomly generates (i.e., OFF to ON state) and terminates packets (i.e., ON to OFF



(a) Before an HTE attack. (b) After an HTE attack.

Fig. 3. Randomization after each successful attack.

state) at each time-slot with probabilities β and α, respectively. These are attack parameters, and their influence on the defense policy will be discussed in Section V.

B. Detect and Interfere

In its OFF period, the attacker randomly sweeps through the channels to detect the operating channel of the victim. Assuming A1 (Fig. 1) has finished its communication with A2 at i^{th} time-slot (Fig. 2), it will start the channel sweeping process from $(i+1)^{th}$ time-slot. As the attacker plans to execute a DoS attack, it tries to cause successive transmission failures and forces the victim to drop the current packet by reaching the maximum transmission failures.

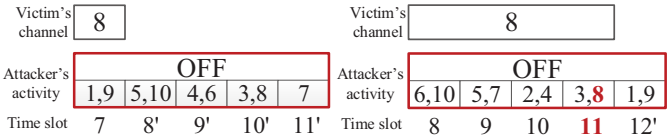
Attacker's Constraints. We assume that the attacker can only sense n channels ($n < N$) at each slot, and it sniffs for handshaking messages in its OFF period; it detects the transmission of a particular device from these messages. After the detection, the attacker interferes with the reception of the victim. However, the attacker has limited interference power to use in each channel. If it fails to corrupt the packet (with a probability $1-\nu$) at the first attempt, it will divert all its interference power to the target channel at the next time-slot—the attacker will be successful at the second attempt.

Channel Hopping. Here, the attacker randomly generates a channel hopping sequence and visits the sequence periodically until it detects the intended victim's operating channel. This strategy fosters the attacker to restrict the victim's ability to continuously utilize a channel (i.e., the channel residence time) when the attacker is in the OFF state. Given N channels, if the victim resides on the same channel, the attacker will detect it within $\lceil N/n \rceil$ slots. Therefore, the maximum residence time (in OFF state) in a channel is $K = \lceil N/n \rceil - 1$.

Fig. 3(a) provides an example of the attack sequence with $N = 10$ and $n = 2$, where the attacker initiates malicious actions from slot-3. Here, the victim operates in channel-2; at slot-6, the attacker detects it and perpetrates the attack. After a packet drop, the defender hops to channel-9, and, at the same time, the attacker randomizes its attack sequence discarding the earlier attack channel (i.e., channel-2). This strategy helps the attacker detect the victim faster (due to the omission of earlier attack channels) after every attack. In Fig. 3(b), the attacker attacks again at the subsequent slot (i.e., slot-7).

If the attacker cannot detect the victim in the subsequent slot, it will re-randomize its sequence, without altering the channels it visited in the current slot, to avoid a deterministic behavior, i.e., omission of earlier attacked channels. Fig. 4(a) shows a different situation if the victim had chosen channel-8 in Fig. 3(b), and Fig. 4(b) shows the re-randomized sequence.

Summary. The attack model unfolds in four steps: 1) alternate between ON and OFF states, 2) hop through the attack sequence until the victim is detected, 3) randomize the sequence after each attack, and 4) re-randomize when a successful attack attempt is followed by an unsuccessful one.



(a) Randomization after an attack. (b) Re-randomization.

Fig. 4. An unsuccessful attack preceded by a successful one.

IV. Proposed Defense Approach: Jump and Wobble

This section proposes a safeguard approach to counteract the random-HTE attack by modeling the defense problem as an MDP with three available actions: $stay$, $handoff$, and $route$. Besides $stay$ and $handoff$ strategy, we utilize the routing diversity in dense IoT networks to increase defense heterogeneity. In $route$, instead of transmitting the packet directly to the intended device, an IoT device utilizes intermediate devices to forward the packet to that receiver. The $route$ action is based on the constraint that it is highly challenging for an HTE attacker to remain hidden to the victim and impersonate an exposed terminal to all neighboring nodes of the victim at the same time [21]. In the following, we model a single agent MDP-based defense method to evade the random-HTE attack.

A. Formation of the MDP

As discussed, the attacker has a limited sensing capability and does not know the channel hopping sequence of the defender. Therefore, the attacker iteratively sweeps through different channels in search of the victim's operating channel. Meanwhile, the defender continues to take actions at the end of each time-slot depending on the current state. The defender achieves an immediate reward $U(t)$ in the t_{th} time-slot,

$$\begin{aligned} U(t) = {} & R_1.\mathbb{1}(Direct\ successful\ transmission) \\ & + R_2.\mathbb{1}(Indirect\ successful\ transmission) \\ & - F.\mathbb{1}(Transmission\ failure) - C.\mathbb{1}(Handoff) \\ & - P.\mathbb{1}(Policy\ violation) - Q.\mathbb{1}(Packet\ drop), \end{aligned} \tag{1}$$

where $\mathbb{1}(\cdot)$ is an indicator function of the event in brackets. The expected discounted reward with infinite horizon is,

$$\overline{U} = \sum_{t=1}^{\infty} \delta^{t-1} U(t), \tag{2}$$

where δ represents the discount factor ($0 < \delta \leq 1$) and signifies the importance of the future reward values.

B. Markov Model

This subsection enumerates the proposed MDP and defines state space, action space, state transition probabilities, and rewards. As discussed, the attacker randomly jumps between ON and OFF states and performs sweeping through the channels only when it is in the OFF state. In addition, the probability of detecting the operating channel of the victim (in the OFF period) dictates by the channels that have been visited earlier in the sequence. Together they conform to Markovian property, i.e., the future state depends only on the current state.

Markov States. The state represents the status of the defender at the end of a time-slot, which is deduced from the embedded SINR and RSS information of ACK and NACK messages. We define a state based on the following state variables:

ACK_t: denotes whether an ACK message ($\text{ACK}_\text{t} = \text{S}$) or a

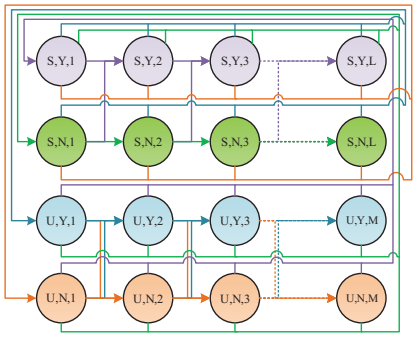


Fig. 5. The proposed Markov model.

NACK is received ($\mathrm{ACK_t} = \mathrm{U}$) in time-slot t.

$\mathrm{IF_t}$: denotes whether the transmitted packet experienced interference ($\mathrm{IF_t} = \mathrm{Y}$) or not ($\mathrm{IF_t} = \mathrm{N}$) in time-slot t.

$\mathrm{CS_t}$: denotes the consecutive successful or failed transmissions, where $\mathrm{CS_t} \in \{\mathbb{Z} > 0\}$.

The states represent combinations of these state variables. Here, the proposed MDP (Fig. 5) has four kinds of states:

S, Y, i : i consecutive successful transmissions, despite experiencing co-channel interference at the current slot.

S, N, i : i consecutive successful transmissions without any interference at the current slot.

U, Y, j : The defender experienced j consecutive transmission failures, the current one due to co-channel interference.

U, N, j : The defender experienced j consecutive transmission failures, the current one due to channel fading.

As a design consideration, we assume $1 \leq i \leq L < N$, where after L consecutive transmissions, the defender will $handoff$, and $1 \leq j \leq M < N$, where M denotes the maximum transmission attempts after which the packet will drop.

Actions. The proposed MDP has three available actions,

$stay$ (s): The defender remains on the current channel at the next time-slot and initiates a transmission.

$handoff$ (h): The defender randomly hands-off to a new channel at the next time-slot and initiates a transmission.

$route$ (r): The defender randomly hands-off to a new channel and forwards the packet to an intermediate node.

Transition Probabilities. As the attacker sweeps through its attack sequence, at state SN_i, only $\max(N - i \times n, 0)$ channels are remained to be visited, and another n channels will be visited at the next slot. Therefore, the probability of detecting the victim (with $stay$) without experiencing channel fading is,

$$\Pr_{i,i+1}^{det|s} = \begin{cases} \dfrac{n}{N - i \times n}, & \text{if } i < K \\ 1, & \text{otherwise,} \end{cases} \tag{3}$$

where we consider that the attacker is in its OFF period and actively sweeping through the channels. However, the attacker may also reside in the ON period, and the victim may not experience malicious interference in the current cycle (i.e., successful transmissions for L slots). The transition probabilities from state SN_i with action $stay$ is,

$$\begin{aligned} &\Pr(SN_{i+1}|SN_i, s) = (1 - \mathrm{P_{fad}})(1 - \Pr_{i,i+1}^{att|s|SN}), \\ &\Pr(SY_{i+1}|SN_i, s) = (1 - \mathrm{P_{fad}})\Pr_{i,i+1}^{att|s|SN}(1 - \nu), \\ &\Pr(UN_1|SN_i, s) = \mathrm{P_{fad}}, \\ &\Pr(UY_1|SN_i, s) = (1 - \mathrm{P_{fad}})\Pr_{i,i+1}^{att|s|SN}\nu, \end{aligned} \tag{4}$$

where the probability of experiencing malicious interference from the attacker in the $(i+1)^{th}$ slot is represented by $\Pr_{i,i+1}^{att|s|SN}$, and $1 \leq i \leq L-1$. It depends on two factors: 1) the current traffic state of the attacker (i.e., $\rho_{ex} = \beta/(\alpha + \beta)$: attacker's ON state probability), and 2) the number of channels it has swept through in the OFF state (i.e., $\Pr_{i,i+1}^{det|s}$).

If the first attempt of the attacker is not successful and the defender stays in the current channel, the attacker employs maximum interference power in the next slot. Therefore, $\Pr(UY_1|SY_i, s) = 1 - \mathrm{P_{fad}}$ and $\Pr(UN_1|SY_i, s) = \mathrm{P_{fad}}$.

Now, the state transition probabilities from channel fading states (i.e., UN_j) with action $stay$ is,

$$\begin{aligned} &\Pr(SN_1|UN_j, s) = (1 - \mathrm{P_{fad}})(1 - \Pr_{UN,1}^{att|s|UN}), \\ &\Pr(SY_1|UN_j, s) = (1 - \mathrm{P_{fad}})\Pr_{UN,1}^{att|s|SN}(1 - \nu), \\ &\Pr(UN_{j+1}|UN_j, s) = \mathrm{P_{fad}}, \\ &\Pr(UY_{j+1}|UN_j, s) = (1 - \mathrm{P_{fad}})\Pr_{UN,1}^{att|s|SN}\nu, \end{aligned} \tag{5}$$

where $1 \leq j \leq M-1$ and $\Pr_{UN,1}^{att|s|UN} = (1 - \rho_{ex})\dfrac{n}{N}$.

The probabilities from state UY_j with action $stay$ is, $\Pr(UY_{j+1}|UY_j, s) = 1 - \mathrm{P_{fad}}$ and $\Pr(UN_{j+1}|UY_j, s) = \mathrm{P_{fad}}$.

When a defender takes action $handoff$ from states SN_i, it randomly selects a channel from the remaining $N-1$ channels. Hence, if the attacker is in the OFF state, the probability of detection from state SN_i with action $handoff$ is,

$$\Pr_{i,1}^{det|h|SN} = \frac{N - i \times n - 1}{N - 1} \Pr_{i,i+1}^{det|s}. \tag{6}$$

Now, after we incorporate the current traffic state of the attacker, the probability of experiencing malicious interference from state SN_i with action $handoff$ $\Pr_{i,1}^{att|h|SN}$ is,

$$\begin{cases} (1-\rho_{ex})(1-\beta)^i \Pr_{i,1}^{det|h|SN} + \rho_{ex}\alpha(1-\alpha)^{i-1}\dfrac{n}{N} \\ +\rho_{ex}\alpha\sum_{j=2}^{i}(1-\beta)^{j-1}(1-\alpha)^{i-j}\Pr_{j-1,1}^{det|h|SN}, & \text{if } i < K \\ (1-\rho_{ex})(1-\beta)^K \Pr_{i,1}^{det|h|SN} + \rho_{ex}\alpha(1-\alpha)^{K-1}\dfrac{n}{N} \\ +\rho_{ex}\alpha\sum_{j=2}^{K}(1-\beta)^{j-1}(1-\alpha)^{i-j}\Pr_{j-1,1}^{det|h|SN}, & \text{otherwise.} \end{cases} \tag{7}$$

The transition probabilities from state SN_i with $handoff$ is,

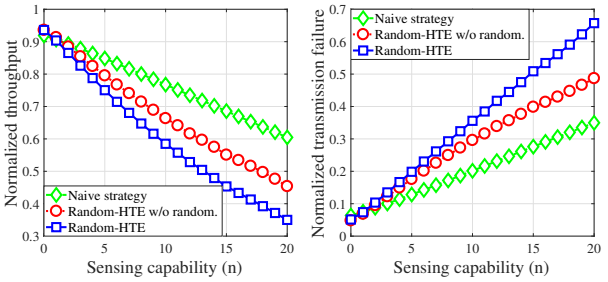
$$\begin{aligned} &\Pr(SN_1|SN_i, h) = (1 - \mathrm{P_{fad}})(1 - \Pr_{i,1}^{att|h|SN}), \\ &\Pr(SY_1|SN_i, h) = (1 - \mathrm{P_{fad}})\Pr_{i,1}^{att|h|SN}(1 - \nu), \\ &\Pr(UN_1|SN_i, h) = \mathrm{P_{fad}}, \\ &\Pr(UY_1|SN_i, h) = (1 - \mathrm{P_{fad}})\Pr_{i,1}^{att|h|SN}\nu, \end{aligned} \tag{8}$$

The transition probabilities from state SY_i with $handoff$ is,

$$\begin{aligned} &\Pr(SN_1|SY_i, h) = (1 - \mathrm{P_{fad}})(1 - \Pr_{i,1}^{att|h|SY}), \\ &\Pr(SY_1|SY_i, h) = (1 - \mathrm{P_{fad}})\Pr_{i,1}^{att|h|SY}(1 - \beta_1), \\ &\Pr(UN_1|SY_i, h) = \mathrm{P_{fad}}, \\ &\Pr(UY_1|SY_i, h) = (1 - \mathrm{P_{fad}})\Pr_{i,1}^{att|h|SY}\beta_1, \end{aligned} \tag{9}$$

$\Pr_{i,1}^{att|h|SY}$ represents the probability of experiencing malicious interference from state SY_i with action hop,

$$\begin{cases} (1-\beta)\Pr_{i,1}^{det|h|SY}, & \text{if } i = 1 \\ (1-\rho_{ex})(1-\beta)^i \Pr_{i,1}^{det|h|SY} + \rho_{ex}\alpha \\ \sum_{j=1}^{i}(1-\beta)^j(1-\alpha)^{i-j-1}\Pr_{j,1}^{det|h|SY}, & 1 < i \leq K \\ (1-\rho_{ex})(1-\beta)^{K+1}\dfrac{n}{N} + \\ \rho_{ex}\alpha\sum_{j=1}^{K}(1-\beta)^j(1-\alpha)^{K-j}\Pr_{j,1}^{det|h|SY}, & \text{otherwise,} \end{cases} \tag{10}$$



(a) Victim's throughput. (b) Victim's transmission failure.

Fig. 6. Performance of random-HTE attack.

When the defender takes action $handoff$ from state UN_j and selects a random channel, the probability of experiencing malicious interference can be represented as $\Pr^{att|h|UN} \approx n/N$ (assuming $N >> n$). Now, the transition probabilities from state UN_j with action $handoff$ is,

$$\begin{aligned}
&\Pr(SN_1|UN_j,h) = (1-\mathrm{P_{fad}})(1-\Pr^{att|h|UN}),\\
&\Pr(SY_1|UN_j,h) = (1-\mathrm{P_{fad}})\Pr^{att|h|UN}(1-\nu),\\
&\Pr(UN_{j+1}|UN_j,h) = \mathrm{P_{fad}},\\
&\Pr(UY_{j+1}|UN_j,h) = (1-\mathrm{P_{fad}})\Pr^{att|h|UN}\nu.
\end{aligned} \tag{11}$$

While performing $handoff$ in state UY_j, the defender selects a random channel from $N-j$ channels. Since the attacker also discards these channels from its attack sequence, the probability of detection increases with j. The transition probabilities from state UY_j with action $handoff$ is,

$$\begin{aligned}
&\Pr(SN_1|UY_j,h) = (1-\mathrm{P_{fad}})(1-\Pr_j^{att|h|UY}),\\
&\Pr(SY_1|UY_j,h) = (1-\mathrm{P_{fad}})\Pr_j^{att|h|UY}(1-\nu),\\
&\Pr(UN_{j+1}|UY_j,h) = \mathrm{P_{fad}},\\
&\Pr(UY_{j+1}|UY_j,h) = (1-\mathrm{P_{fad}})\Pr_j^{att|h|UY}\nu,
\end{aligned} \tag{12}$$

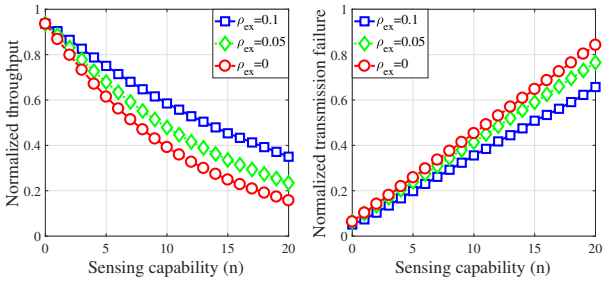
where $\Pr_j^{att|h|UY} = \dfrac{n}{N-j}$.

Similar to action $handoff$, action $route$ hands-off to another channel, but routes the packet through a forwarding node. Therefore, in the case of action $route$, $\Pr^{att|r|X} = \Pr^{att|h|X} \cdot \mathrm{P}^{\mathrm{det}}_{\mathrm{route}}$, where $\mathrm{P}^{\mathrm{det}}_{\mathrm{route}}$ depends on the topology of the network and the attacker's configuration. Hence, we replace $\Pr^{att|r|X}$ in (8), (9), (11), and (12) to deduce the transition probabilities from corresponding states with action $route$.

Now, we model the defense problem as an MDP and find the optimal policy by solving it. The optimal policy can be represented by two critical states $l^* \in \{1,2,\cdots,L\}$ and $m^* \in \{1,2,\cdots,M\}$,

$$\begin{aligned}
&\pi^*(SN_i) = \begin{cases} s, & \text{if } i < l^* \\ h, & \text{otherwise,} \end{cases} \qquad \pi^*(SY_i) = h, \forall i,\\
&\pi^*(UY_j) = \begin{cases} h, & \text{if } j < m^* \\ r, & \text{otherwise,} \end{cases} \qquad \pi^*(UN_j) = s, \forall j.
\end{aligned} \tag{13}$$

Summary. The defender's behavior to utilize a channel *as long as feasible* and the attacker's *random and iterative strategy* facilitate the design of the defense problem as an MDP. The defender keeps using a channel for l^* time-slots, then hands-off to a new channel and after m^* consecutive transmission failures, the defender chooses the action $route$ to exploit the proximity in dense IoT networks.



(a) Victim's throughput. (b) Victim's transmission failure.

Fig. 7. Performance of random-HTE attack with variable ρ_{ex}.

V. Performance Evaluation

The simulation parameters are: communication gain $R_1 = 5$, cost of transmission failure $F = 5$, handoff cost $C = 1$, penalty for policy violation $P = 50$, maximum residence time $L = 30$, maximum transmission attempts $M = 30$, cost of packet drop $Q = M \cdot F$, communication gain (routing) $R_2 = 4$, discount factor $\delta = 0.95$, and channel parameters are $\alpha = 0.09$, $\beta = 0.01$, and $N = 60$.

A. Random-HTE Attack

Random-HTE Attack. The performance of the random-HTE strategy in comparison to the naive-random approach is presented in Fig. 6, where the attacker randomly (memoryless) selects n channels at each slot (i.e., n/N). In addition, we compare it to the random-HTE without the re-randomization approach, where the attacker does not re-randomize after each unsuccessful attempt followed by a successful one. In Fig. 6(a), the victim experiences the least throughput in random-HTE attack due to the iterative process and re-randomization of random-HTE. Similarly, in Fig. 6(b), the victim of random-HTE attack endures most transmission failures.

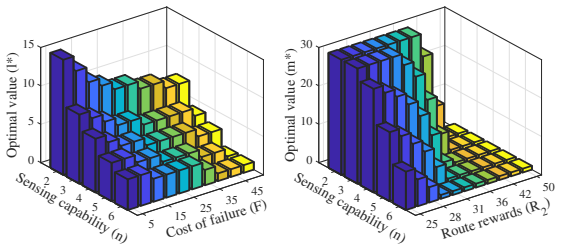
Effect of ρ_{ex}. The attacker randomly fluctuates between benign and malicious behaviors to reduce the risk of detection. Therefore, it loses opportunities to attack when it is behaving benignly. The benign behavior is represented by ρ_{ex}, which denotes the amount of time the attacker acts benignly. From Fig. 7, we can observe that the attacker's performance degrades with the increase in its benign behavior, i.e., ρ_{ex}.

B. Jump and Wobble

We demonstrate the critical states l^* and m^* (Fig. 8) derived from the value iteration of the MDP, with the change in the attacker's sensing capability (n), the cost of transmission failure (F), and the communication gain with routing (R_2).

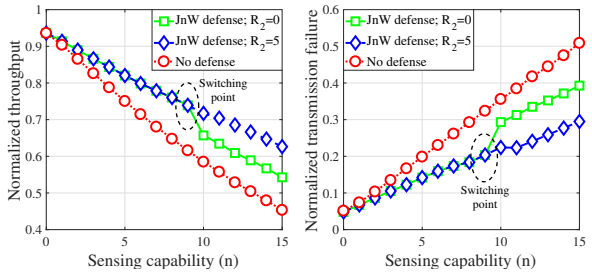
Critical States. In Fig. 8(a), l^* decreases with the increase in n. As n increases, K starts to decrease, and IoT nodes have fewer channels to handoff; hence, IoT devices must handoff more frequently to avoid the attack. Moreover, as the cost of transmission failure F increases, IoT nodes handoff more to avoid transmission failures (i.e., l^* decreases). Likewise, in Fig. 8(b), m^* maintains a downward trend with the increase in n. However, R_2 largely dictates the action $handoff$, and as the routing reward increases, IoT nodes become more motivated to route the packets through intermediate nodes.

Routing Gain R_2. Fig. 9 compares the performance of this proposed strategy in three scenarios: no defense, jump and wobble with $R_2 = 0$ (i.e., [17], [19]), and jump and wobble



(a) Optimal value l^*; n vs. F.(b) Optimal value m^*; n vs. R_2.

Fig. 8. The sensitivity of optimal values to the changes in n, F, and R_2.



(a) Victim's throughput. (b) Victim's transmission failure.

Fig. 9. Performance of Jump and Wobble.

with $R_2 = 5$. It illustrates that both $R_2 = 0$ and $R_2 = 5$ follow the same trend until the attacker's sensing capability surpasses $n = 9$, yet the throughput ($R_2 = 0$ line) stays above the no defense line. We denote this moment as the *switching point* after which the defender prefers to route data packets (using the action $route$). As R_2 decreases, the victim becomes less motivated to route data packets, and the switching point moves further to the left. Likewise, in Fig. 9(b), the transmission failure increases after the switching point. Therefore, R_2 serves as a tuning parameter between actions $handoff$ and $route$.

VI. Conclusion

First, we proposed random-HTE strategy to perpetrate HTE attacks *without any predetermined knowledge of the victim's operating channel*. Afterward, we proposed an MDP-based safeguard approach, jump and wobble, to avoid the proposed attack. We showed that by randomly changing the operating channel, a defender can avoid the attack, and when it becomes necessary, it can route packets through intermediate devices.

Numerical investigations and simulation results showed that the random-HTE outperforms the naive approach. The jump and wobble improves the performance compared to state-of-the-art that only utilizes channel diversity. To the best of our knowledge, this is the first work that introduced a constrained attack model of HTE and designed a defensive measure.

References

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[2] Y. Saito *et al.*, "Non-orthogonal multiple access (NOMA) for cellular future radio access," in *Proc. IEEE VTC Spring*, pp. 1–5, 2013.

[3] G. Ding *et al.*, "On the limits of predictability in real-world radio spectrum state dynamics: From entropy theory to 5G spectrum sharing," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 178–183, 2015.

[4] V. Sathya *et al.*, "Wi-Fi/LTE-U coexistence: Real-time issues and solutions," *IEEE Access*, vol. 8, pp. 9221–9234, 2020.

[5] M. Antonakakis *et al.*, "Understanding the mirai botnet," in *Proc. USENIX Security Symposium*, pp. 1093–1110, 2017.

[6] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. IEEE Symposium on Security and Privacy (SP)*, pp. 636–654, 2016.

[7] M. Naveed, X.-y. Zhou, S. Demetriou, X. Wang, and C. A. Gunter, "Inside job: Understanding and mitigating the threat of external device mis-binding on Android," in *Proc. NDSS*, pp. 1–14, 2014.

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

[9] 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.

[10] 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.

[11] M. Hossain and J. Xie, "Hide and seek: A defense against off-sensing attack in cognitive radio networks," in *Proc. IEEE INFOCOM*, pp. 613–621, 2019.

[12] M. Hossain and J. Xie, "Hide and seek: A markov-based defense strategy against off-sensing attack in cognitive radio networks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 3028–3041, 2020.

[13] L. Xin, D. Starobinski, and G. Noubir, "Cascading denial of service attacks on Wi-Fi networks," in *Proc. IEEE CNS*, pp. 91–99, 2016.

[14] T. D. Vo-Huu, T. D. Vo-Huu, and G. Noubir, "Interleaving jamming in Wi-Fi networks," in *Proc. ACM WiSec*, pp. 31–42, 2016.

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

[16] M. K. Hanawal *et al.*, "Joint adaptation of frequency hopping and transmission rate for anti-jamming wireless systems," *IEEE Transactions on Mobile Computing*, vol. 15, no. 9, pp. 2247–2259, 2015.

[17] K. Zhang *et al.*, "Efficient anti-jamming strategies in multi-channel wireless networks," in *Proc. IEEE ICCP*, pp. 109–112, 2013.

[18] A. M. Srivatsa and J. Xie, "A performance study of mobile handoff delay in IEEE 802.11-based wireless mesh networks," in *Proc. IEEE ICC*, pp. 2485–2489, 2008.

[19] J. P. Vilela and J. Barros, "Collision-free jamming for enhanced wireless secrecy," in *Proc. IEEE WoWMoM*, pp. 1–6, 2013.

[20] Y. Song and J. Xie, "Finding out the liars: Fighting against false channel information exchange attacks in cognitive radio ad hoc networks," in *IEEE GLOBECOM*, pp. 2095–2100, 2012.

[21] M. Hossain and J. Xie, "Hidden terminal emulation: An attack in dense IoT networks in the shared spectrum operation," in *Proc. IEEE GLOBECOM*, pp. 1–6, 2019.

[22] M. Hossain and J. Xie, "Third eye: Context-aware detection for hidden terminal emulation attacks in cognitive radio-enabled IoT networks," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 1, pp. 214–228, 2020.

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

[24] T. Denning *et al.*, "Computer security and the modern home," *Communications of the ACM*, vol. 56, no. 1, pp. 94–103, 2013.

[25] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[26] V. Sachidananda *et al.*, "Poster: Towards exposing Internet of Things: A roadmap," in *Proc. ACM CCS*, pp. 1820–1822, 2016.

[27] A. K. Simpson *et al.*, "Securing vulnerable home IoT devices with an in-hub security manager," in *Proc. IEEE PerCom*, pp. 551–556, 2017.

[28] T. Yu *et al.*, "Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things," in *Proc. ACM Workshop on Hot Topics in Networks*, pp. 1–7, 2015.

[29] Pair of Bugs Open Honeywell Home Controllers up to Easy Hacks, "https://threatpost.com/pair-of-bugs-open-honeywell-home-controllers-up-to-easy-hacks/113965/," Accessed July 2019.

[30] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice commands," in *Proc. ACM SIGSAC Conference on Computer and Communications Security*, pp. 103–117, 2017.

[31] S. Soltan, P. Mittal, and H. V. Poor, "BlackIoT: IoT botnet of high wattage devices can disrupt the power grid," in *Proc. USENIX Security Symposium*, pp. 15–32, 2018.

[32] E. O. Elliott, "Estimates of error rates for codes on burst-noise channels," *The Bell System Technical Journal*, vol. 42, no. 5, pp. 1977–1997, 1963.