Sentinel Based Malicious Relay Detection in Wireless IoT Networks

Anshoo Tandon, Teng Joon Lim, and Utku Tefek

Abstract: **Increased device connectivity and information sharing in wireless IoT networks increases the risk of cyber attack by malicious nodes. In this paper, we present an effective and practical scheme for detecting data integrity and selective forwarding attacks launched by malicious relays in wireless IoT networks. The proposed scheme exploits the broadcast nature of wireless transmission and provides a sentinel based approach to intrusion detection. Our detection scheme assumes a general noise model for the network where different wireless links may have different packet error probability (PEP). Further, our detection scheme is effective even in scenarios where different wireless links in the network employ distinct modulation and coding schemes at the physical layer. This detection scheme has application in practical wireless IoT networks, such as those based on the recently introduced IEEE 802.11ah standard.**

Index Terms: **Malicious relay detection, packet error probability, sentinel, wireless relay network.**

I. INTRODUCTION

The number of IoT devices being deployed in average households and industries is increasing at a fast pace [1], and IoT based applications have transformed many critical infrastructure, such as health-care and smart cities [2]. However, most IoT devices are built with cost and efficiency as the driving factor, but suffer from poor security configurations and open designs [3]–[5], thereby presenting a challenge in detecting security breaches.

In this paper, we present a scheme for detecting malicious nodes in a wireless IoT network where low power IoT devices connect to the access point (AP) (or base station) via relay nodes. Such a relay-based model for wireless information exchange conserves power in the transmitting IoT device, and is adopted by the recently introduced IoT networking standard IEEE 802.11ah (also called Wi-Fi HaLow) [6]. The Wi-Fi HaLow standard has emerged as a promising solution for connecting IoT devices due to its large coverage area, extended power-saving mode, and device-grouping option for reducing contention [7], [8].

In practice, a wireless relay node responsible for forwarding data packets to/from IoT devices may become compromised, and used by an adversary to hinder information transfer. A relay node may get compromised via (i) malicious access to the local network (for instance, in Stuxnet attack [9]), (ii) malicious remote access through the Internet, (iii) malicious physical access to IoT networks in public areas, such as shopping malls, hotels, and health-care centers [10]. For instance, ARP poisoning [11] could be employed by the attacker to associate its MAC address with the IP address of a relay, that results in the traffic meant for the relay to be diverted to the attacker, which may then modify the incoming packets before forwarding. We remark that we have implemented the data integrity attack using ARP poisoning in a WiFi-based network.

We present an effective scheme for detecting two attacks by a malicious relay: (i) Data integrity attack (where a relay corrupts the packet) and (ii) selective forwarding attack (where a relay selectively drops packets). The data integrity attack is especially serious as wrong decisions, based on maliciously modified data, could disrupt the operation of the IoT system. For instance in healthcare applications, fatal erroneous treatment decisions could be made when packets containing personal health information are modified by a malicious relay. Similarly, maliciously altering the commands sent from/to security cameras and door locks can have critical consequences [10].

The proposed scheme employs special trusted passive nodes, called 'sentinel' nodes, which monitor information exchange at relay nodes by exploiting the broadcast nature of wireless transmission. The distinctive features of our proposed scheme are as follows:

(a) In contrast to most existing detection schemes, our sentinel based scheme does not require any change in existing PHY/MAC protocols.
(b) The probability of false alarm in our detection scheme is negligible. This is unlike standard detection schemes which trade probability of missed detection with the probability of false alarm.
(c) The proposed scheme is effective even in scenarios where different wireless links in the network may employ distinct modulation and coding schemes at the physical layer.

A. Related Work

Wireless IoT networks, consisting of resource-constrained nodes with relatively low computing and communication capability, are vulnerable to attack by an adversary which aims to disrupt and alter the communication of vital information in the network. The application of physical layer techniques for detecting false data injection by a relay was examined in [12], [13]. While the detection scheme in [12] is at the modulated symbol level, a Bayesian test approach at the packet level is adopted in [13]. However, the detection performance in [12] is unsat-

Manuscript received January 30, 2019.

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd.

A. Tandon and T. J. Lim are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (email: anshoo.tandon@gmail.com, eleltj@nus.edu.sg).

U. Tefek was with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583 (email: utku@u.nus.edu).

Digital Object Identifier: 10.1109/JCN.2019.000049

1229-2370/19/$10.00 © 2019 KICS

isfactory when the channel gain between the source-destination link is small, while the approach in [13] is unreliable when the relay corrupts only a small fraction of bits. A channel-aware detection of selective forwarding attack is proposed in [14], but suffers from high missed-detection probability when the malicious node drops only a small fraction of packets. In contrast, our *sentinel* based scheme is robust even when only a small number of packets are dropped.

An efficient cross-layer scheme for malicious relay detection in two-hop wireless sensor networks was proposed in [15]. However, the detection scheme in [15] relied on the assumption that some devices forward the same information through two different relays. Detection of selective forwarding attack via received signal strength indicator readings at certain monitor nodes was proposed in [16]. This approach however requires implementation of a sophisticated localization algorithm to estimate distances among nodes. In [17], a selective forwarding attack detection approach involving a random selection of a checkpoint node along the forwarding path was proposed. This scheme involves the use of one-way hash functions and exchange of acknowledgement (ACK) packets with timing information, requiring major changes to existing wireless sensor network protocols.

In [18], an overhearing-based misbehavior detection scheme was proposed, where *each* node reports the packet forwarding ratio for itself and its neighbors. However, this incurs heavy computational load on the network, as every resource-constrained device continuously monitors the traffic at neighboring nodes. A related approach was proposed in [19], where nodes were assumed to have knowledge of their two-hop neighbors via the use of special 'Hello' packets.

In [20], a watchdog technique was proposed where each node monitors the next hop transmission to detect any data integrity attack. This watchdog scheme [20] requires that the IoT devices are always awake and active in order to listen to the packets being transmitted and received by neighboring nodes. Therefore, this scheme suffers from heavy computational load at *each* IoT node due to traffic monitoring across all neighboring nodes.

We remark that an important distinction between our sentinel based malicious detection, and previous works based on the watchdog approach [18]–[20], is that the sentinel based detection scheme *does not require any changes to standard wireless/IoT protocols*: The task of monitoring and reporting malicious behavior is entrusted *only* to special sentinel nodes which are positioned appropriately by the network designer, and protected with adequate security protocols. Moreover, our paper is distinct from previous works based on the watchdog approach in that it presents a detailed analysis of the impact of channel noise and packet error probability on the detection performance.

B. Our Contribution

In this paper, we present a sentinel based malicious relay detection scheme for wireless IoT networks. We provide a detailed analysis for the detection of the data integrity attack and the selective forwarding attack. The analysis assumes a general noisy channel model for the IoT network, where each wireless link may potentially have distinct packet error probability (PEP) due to different channel noise conditions. We quantify the probability of early detection of malicious relay behavior as a function of PEP on different wireless links across the network. We also present a framework to quantify the number of sentinels required to monitor a certain geographical area populated with relays and associated devices, such that the desired early detection probability is achieved.

The salient features which make the sentinel based detection scheme effective for practical use are as follows: (i) It does not require any change in existing PHY/MAC protocols, such as IEEE 802.11ah. (ii) The false alarm rate is negligible as it occurs only in the unlikely scenario where the packet CRC fails to *detect* errors, even though the decoded packet is in error. (iii) The detection scheme operates at the MAC layer and therefore remains effective even in scenarios where different wireless links may employ distinct modulation and coding schemes at the physical layer. (iv) The scheme is robust in detecting selective forwarding attacks even when a small fraction of packets are dropped by a malicious relay.

This paper extends our workshop paper [21] in two directions. First, we present a unified framework for analyzing detection performance as a function of number of sentinels placed in the network. Second, this paper provides extensive simulation results highlighting the detection performance as a function of varying PEP on different wireless links, and depicting the probability of early detection of malicious relays as a function of the number of sentinel nodes.

The rest of the paper is structured as follows. The system model is presented in Section II. The data integrity attack and the selective forwarding attack are discussed in Section III. The probability of early detection of these attacks is derived in Section IV. In Section V, we jointly analyze the packet stream from different devices connected to a malicious relay, and also provide a framework to quantify the number of sentinels required to achieve a desired early detection probability. In Section VI, we present numerical results highlighting the impact of PEP on different wireless links on the performance, and demonstrate how the choice of number of sentinels influences early attack detection probability.

II. SYSTEM MODEL

Consider a wireless IoT network where IoT devices connect to the access point AP via a relay node (see Fig. 1). We assume that each relay node uses a decode-and-forward mechanism. Thus, a relay node first demodulates and decodes the received physical layer payload, before re-encoding and forwarding the medium access (MAC) payload to the destination. It is assumed that there is a unique sequence number counter associated with packets transmitted from each IoT device, as in IEEE802.11 networks. The MAC layer adds appropriate packet sequence number and cyclic redundancy check (CRC) bits to the packet before passing it to the physical layer for error correction encoding and modulation. The CRC bits help to detect residual bit errors due to channel impairments, after the forward error correction decoder at a receiver has attempted to remove errors from the received signal. Similar to the IEEE 802.11ah protocol, the multiple access scheme is assumed to be carrier-sense multiple access with collision avoidance (CSMA/CA). The system model considers a practical scenario where different wire-

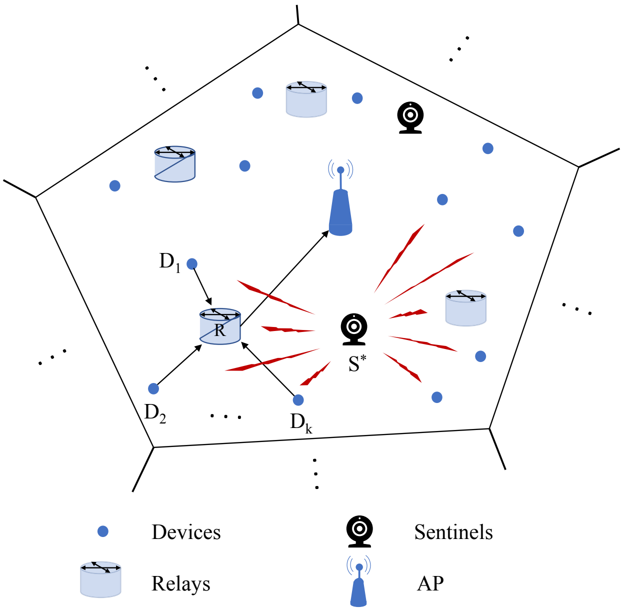

Fig. 1. Model of a wireless IoT network with relay and sentinel nodes.

less links may have different packet error probabilities due to different channel conditions.

The proposed intrusion detection scheme employs special nodes, called sentinel nodes, which constantly monitor the received and forwarded data packets at relay nodes. These sentinel nodes could be especially designed to be extra secure, protected with adequate security protocols, and placed at appropriate locations for traffic monitoring. Further, sentinel nodes installed exclusively for network monitoring could listen to ambient traffic in a passive manner, making them resistant to security threats from a malicious entity.

Fig. 1 depicts a typical network setting with sentinel nodes deployed for monitoring data traffic. Since the multiple access scheme is CSMA/CA, neighboring clusters of nodes (each served by one relay) transmit in orthogonal time/frequency channels with high probability. Thus, a sentinel node can monitor traffic from multiple relay clusters in its vicinity. For example, in Fig. 1, the sentinel S^* is shown to overhear transmissions from two neighboring relay clusters. We remark that although we focus on uplink transmissions from IoT devices to the AP in this paper, the same approach is applicable for downlink transmissions from the AP to IoT devices.

Our aim is to effectively detect the presence of a malicious relay node in the network. Without loss of generality, we focus on a particular relay node R, with k IoT devices $D_1, \cdots, D_k$ associated with this relay, and a sentinel node S^* responsible for the security of this relay cluster, as labeled in Fig. 1. We consider a practical scenario where, for each wireless link, there is a certain PEP due to factors such as noise, fading, and packet collision. We use the notation $p_{A\to B}$ to denote the PEP on the wireless link from node A to node B. Therefore, for instance, $p_{D_j\to S^*}$ will denote the PEP for the wireless link between device D_j and sentinel S^*.

Note that for a given packet transmission from device D_j to relay R, if the CRC fails at R due to noise, then R does not send back an ACK packet to D_j, and the packet is retransmitted by D_j. It is assumed that a packet is retransmitted by D_j until it receives the ACK packet from R. Further, we assume that ACK packets are small and encoded with a robust error correction scheme, so that ACK packets are received without error. We adopt the convention where the first transmission of a packet is referred to as its 0-th *retransmission*.

In this paper, we consider the following two potential attacks launched by a malicious relay node.

1. *Data integrity attack*: Here, the relay corrupts the received MAC payload (also called the MAC service data unit (MSDU) [6]) before forwarding it.
2. *Selective forwarding attack*: Here, the relay selectively drops some data packets which it was expected to forward to AP. This attack might result in loss of sensitive information or a significant increase in end-to-end delay, thereby disrupting normal operations.

We remark that our proposed scheme can also be applied for detecting malicious nodes in multi-hop networks. Our proposed scheme complements cryptography based approaches, in the sense that cryptography can defend against eavesdropping, but not against selective forwarding attacks. In addition, cryptography based detection of data integrity attack cannot pinpoint the malicious relay node in multi-hop networks [22].

III. SENTINEL BASED ATTACK DETECTION

We consider the scenario where an attack is directed on a given packet which originates from IoT device D_j and is to be transferred to the AP via R. The wireless transmission by D_j is heard by relay R, and with a certain probability by sentinel S^*. Note that the link from D_j to R is effectively error-free due to the use of ARQ on the $D_j \to R$ link, where R requests packet retransmissions from D_j until R receives an error free copy of the packet. The following lemma quantifies the probability that a packet is successfully transferred from D_j to R, but is *not* successfully received by S^*.

Lemma 1: Let $q_{D_j\to R}$ denote the probability that a given packet is successfully transferred from device D_j to relay R, but is *not* successfully received by sentinel S^*. Then we have

$$q_{D_j\to R} = \frac{\left(1 - p_{D_j\to R}\right) p_{D_j\to S^*}}{1 - p_{D_j\to R} \cdot p_{D_j\to S^*}}. \tag{1}$$

Proof: For a given packet to be transferred from D_j to R, the probability that it is correctly received at R in its i-th retransmission is given by $\left(1 - p_{D_j\to R}\right) p^i_{D_j\to R}$, while the probability that this packet is not correctly received by S^* during the course of its i retransmissions is equal to $p^{i+1}_{D_j\to S^*}$. Thus, we have

$$\begin{aligned} q_{D_j\to R} &= \sum_{i=0}^{\infty} (1 - p_{D_j\to R}) p^i_{D_j\to R} \cdot p^{i+1}_{D_j\to S^*} \qquad (2) \\ &= \frac{\left(1 - p_{D_j\to R}\right) p_{D_j\to S^*}}{1 - p_{D_j\to R}\, p_{D_j\to S^*}}. \end{aligned}$$

□

Remark: The above lemma can be generalized to the scenario where the maximum number of packet retransmissions allowed are finite (denoted by M). In this case, the expression in (2) is replaced by

$$q_{D_j \to R} = \sum_{i=0}^{M} (1 - p_{D_j \to R}) p_{D_j \to R}^{i} \cdot p_{D_j \to S^*}^{i+1}.$$

Note that (1) is equivalently expressed as

$$q_{D_j \to R} = \frac{p_{D_j \to S^*}}{1 + p_{D_j \to R} \cdot \left(1 - p_{D_j \to S^*}\right) / \left(1 - p_{D_j \to R}\right)}, \quad (3)$$

which shows that $0 \leq q_{D_j \to R} \leq p_{D_j \to S^*}$. Further, we have $q_{D_j \to R} \to p_{D_j \to S^*}$ as $p_{D_j \to R} \to 0$, while $q_{D_j \to R} \to 0$ as $p_{D_j \to R} \to 1$.

We now consider the case where the sentinel listens to the transmission from relay R to AP. Let $q_{R \to AP}$ denote the probability that a given packet is successfully transferred from R to AP, but is not successfully received at S^*. Then, similar to (1), we observe that $q_{R \to AP}$ is given by

$$\begin{aligned} q_{R \to AP} &= \frac{\left(1 - p_{R \to AP}\right) p_{R \to S^*}}{1 - p_{R \to AP}\, p_{R \to S^*}} && (4) \\ &= \frac{p_{R \to S^*}}{1 + p_{R \to AP} \left(1 - p_{R \to S^*}\right) / \left(1 - p_{R \to AP}\right)}. && (5) \end{aligned}$$

This shows that $0 \leq q_{R \to AP} \leq p_{R \to S^*}$, and we observe that $q_{R \to AP} \to p_{R \to S^*}$ as $p_{R \to AP} \to 0$ while $q_{R \to AP} \to 0$ as $p_{R \to AP} \to 1$.

A. Detecting Data Integrity Attack

Consider a tampering attack by relay R on a packet received by R from device D_j, where R corrupts some bits of the MAC payload before encoding, modulating, and forwarding the packet to AP. Note that when R forwards this corrupted packet to AP, its MAC header contains fields indicating the source of the packet (device D_j) and the packet sequence number (say, i). The transmission from R to AP is potentially decodable by the sentinel S^*.

When all the links are noiseless, the sentinel always receives an exact copy of the packet forwarded by R to AP. The sentinel then compares the MAC payload of this packet to the corresponding payload of the stored copy of the packet received from D_j with sequence number i. Hence, in this scenario when R corrupts the payload, the attack is easily detected by S^* when it observes that the MAC payload forwarded by R is different from the payload transmitted by device D_j.

When the links are noisy, there is a non-zero probability that the sentinel S^* is not able to successfully receive the packet transmitted by D_j to R, with this probability given by $q_{D_j \to R}$ in (1). Similarly, there is a non-zero probability that S^* is not able to successfully receive the packet transmitted by R to AP, with this probability given by $q_{R \to AP}$ in (4). The sentinel S^* cannot detect the data integrity attack on this packet originating from D_j in the event that it does not successfully receive either the transmission from D_j or the corresponding corrupted packet forwarded by R. The following theorem quantifies this probability.

Theorem 1: Let q_{D_j} denote the probability that sentinel S^* is unable to detect a data integrity attack by relay R on a given packet originating from device D_j. Then we have

$$q_{D_j} = 1 - (1 - q_{D_j \to R})(1 - q_{R \to AP}), \quad (6)$$

and $q_{D_j \to R}$ and $q_{R \to AP}$ are given by (1) and (4), respectively.

Proof: The sentinel S^* can successfully detect the tampering attack on a given packet from D_j if and only if S^* successfully receives this packet when it is transferred from $D_j \to R$ and also successfully receives the tampered version which is forwarded from $R \to AP$. Thus, S^* successfully detects the tampering with probability $(1 - q_{D_j \to R})(1 - q_{R \to AP})$, and the probability that S^* is unsuccessful in detecting this tampering is given by (6). □

The quantity q_{D_j} can be upper bounded as follows

$$\begin{aligned} q_{D_j} &\leq q_{D_j \to R} + q_{R \to AP} \\ &\leq p_{D_j \to S^*} + p_{R \to S^*}. && (7) \end{aligned}$$

We remark that q_{D_j} is independent of the sequence number of the packet transmitted by D_j because the network statistics are assumed to be invariant over the observation window. We also remark that a false alarm occurs only in the unlikely scenario where the packet CRC fails to *detect* errors in the decoded packet (after error correction), even though the decoded packet is in error. In this scenario, the sentinel may mistake an erroneous packet to be a corrupted packet, thereby raising a false alarm.

B. Detecting Selective Forwarding Attack

Consider a selective forwarding attack where relay R drops packets i to $i+l-1$ from IoT device D_j. The packet originating from device D_j with sequence number $i + l$ is forwarded by R to the AP. Note that the link from R to AP is effectively error-free due to the use of ARQ on the $R \to AP$ link. Hence, in case relay R forwards the packet with sequence number $i + l$ originating from D_j to the AP without modifying the sequence number, then this selective forwarding attack is readily detected at the AP due to the missing sequence numbers. However, if R changes the sequence number from $i+l$ to i, then the AP cannot detect this attack involving selective forwarding of packets.

Therefore, we assume that relay R *not only drops certain packets, but also modifies the sequence numbers* of the subsequent packets so that the AP does not observe any discontinuity in the packet sequence number. We assume that the MAC payloads of packets originating from device D_j corresponding to different sequence numbers have different content. This is justified, for instance, when the MAC payload includes a *time-stamp* to represent the time when IoT device D_j senses a certain attribute.

Therefore our scenario is that R drops packets from D_j with sequence numbers $i, i+1, \cdots, i+l-1$, and then forwards the subsequent packet to AP after modifying its sequence number from $i + l$ to i. Further, consider the following case where

(i) S^* successfully receives the packet with sequence number i transmitted from D_j to R, and

(ii) S^* also successfully receives the packet forwarded by R to AP for which R modified the sequence number from $i + l$ to i.

In the above scenario, the selective forwarding attack is successfully detected at S^* by comparing the MAC payload of the packet with sequence number i transmitted by D_j to R, with the MAC payload of the forwarded packet by R to AP with sequence number i.

However, when the communication links are noisy, there is a non-zero probability that S^* is not able to successfully receive the packet(s) transmitted by both D_j and R. The next theorem quantifies this probability.

Theorem 2: Let $\tilde{q}_{D_j,i}$ denote the probability that sentinel S^* is unable to detect the packet dropped by relay R on a packet originating from device D_j, with packet sequence number i. Then we have

$$\tilde{q}_{D_j,i} = 1 - (1 - q_{D_j \to R})(1 - q_{R \to AP}) \triangleq \tilde{q}_{D_j}, \tag{8}$$

where $q_{D_j \to R}$, and $q_{R \to AP}$ are given by (1), and (4), respectively.

Proof: The sentinel S^* can successfully detect this packet drop at the relay if and only if S^* successfully receives the packet with sequence number i when it is transferred from $D_j \to R$ and also successfully receives the packet with tampered sequence number (from $i + l$ to i) which is forwarded from $R \to AP$. Thus, S^* successfully detects the tampering with probability $(1 - q_{D_j \to R})(1 - q_{R \to AP})$, and therefore (8) represents the probability that S^* is not successful in detecting this attack. Note that the expression for $\tilde{q}_{D_j,i}$ given by (8) is independent of the sequence number i, and we can therefore simplify it to $\tilde{q}_{D_j}$. □

Similar to data integrity attack detection, a false alarm occurs while detecting selective forwarding attack only in the unlikely scenario where CRC fails to *detect* errors in the decoded packet, and the sentinel uses an erroneous packet for comparing corresponding packet transmissions by a device and its associated relay.

C. Impact of Path Loss on PEP

In this subsection, we analyze the impact of path loss on the PEP for a given wireless link. Let P_{d_0} denote the mean received power at a receiver which is located d_0 meters away from a transmitter. Then, a general path loss expression for P_d, the mean received power at distance d from the transmitter, is given by

$$P_d = P_{d_0}\left(\frac{d_0}{d}\right)^{\epsilon}, \tag{9}$$

where ϵ denotes the path loss exponent. The mean received energy per bit at distance d, denoted $E_b(d)$, is related to P_d as follows

$$E_b(d) = \frac{P_d}{r}, \tag{10}$$

where r denotes the transmission rate in bits per second. The noise power spectral density, N_0, on the other hand is approximately given by -174 dBm/Hz $\approx 4 \times 10^{-18}$ mW/Hz at room temperature. Therefore, when P_{d_0} is expressed in mW, then we have

$$\frac{E_b(d)}{N_0} = \frac{P_{d_0} \times 10^{18}}{4r}\left(\frac{d_0}{d}\right)^{\epsilon}. \tag{11}$$

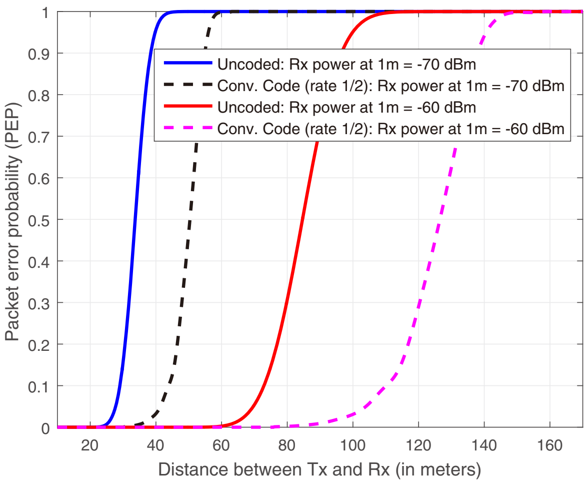

Fig. 2. Plot depicting the impact of distance on PEP, when path loss exponent is 2.5, transmission rate is 1 Mbps, and the packet is composed of 240 information bits.

C.1 Uncoded Packet

We will provide an exact analytical expression for PEP as a function of d, the distance between a transmitter and a receiver, for an uncoded packet composed of n information bits. When the transmitter uses binary phase shift keying (BPSK), bit error rate (BER) is related to $E_b(d)/N_0$ as

$$BER = Q\left(\sqrt{\frac{2E_b(d)}{N_0}}\right), \tag{12}$$

where $Q(\cdot)$ is the tail probability of the standard normal distribution, and is expressed as follows

$$Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-u^2/2}du. \tag{13}$$

The PEP for an uncoded packet with n bits is

$$PEP = 1 - (1 - BER)^n. \tag{14}$$

Combining (11), (12), and (14), the PEP at distance d is

$$PEP = 1 - \left[1 - Q\left(10^9\sqrt{\frac{P_{d_0}}{2r}}\left(\frac{d_0}{d}\right)^{\epsilon/2}\right)\right]^n. \tag{15}$$

C.2 Packet protected by Convolutional Coding

We know that PEP on a given wireless link can be reduced by appropriate error correction coding [23]. From (1), (4), and (6), we see that a reduction in $p_{D_j \to S^*}$ or $p_{R \to S^*}$ leads to a reduction in q_{D_j} which, in turn, helps to reduce $\bar{N}_{D_j}$ (see (18)). Therefore, a reduction in PEP via error correction helps in lowering the expected number of packets required to detect a malicious relay.

Fig. 2 compares PEP for uncoded and coded packets as a function of distance d with $d_0 = 1$ (meters), $P_{d_0} \in \{-70, -60\}$ dBm (or equivalently $P_{d_0} \in \{10^{-7}, 10^{-6}\}$ mW), and the power spectral density of thermal noise is -174 dBm/Hz. We have considered a transmission rate of $r = 1$ Mbps, while the path loss exponent, ϵ, is 2.5. The error correction coding scheme is a rate 1/2 convolutional code supported by WiFi HaLow [6], and has a constraint length of 7. The curve for the uncoded case is obtained using (15), while the curve for convolutional coding is obtained using Monte-Carlo simulation where a Viterbi decoder [24] is employed for 8-bit quantized soft-decision decoding. It is seen from the figure that for a fixed target PEP, convolutional coding provides significant increase in coverage distance over the uncoded case.

The path loss model discussed in this subsection will be applied later in Section V.B to quantify the number of sentinels required to monitor a given network in order to achieve the required detection performance.

IV. EARLY DETECTION PROBABILITY

In this section, we quantify the probability of early detection of malicious relay behavior. Towards this, we define and discuss the early detection probability for the data integrity attack and selective forwarding attack.

(a) *Early detection of data integrity attack*: For data packets originating from a given device D_j, we define the *m-early detection probability of data integrity attack* to be the probability that sentinel S^* detects the data integrity attack when not more than m packets originating from device D_j have been tampered with by relay R. Let N_{D_j} denote the index of the tampered packet originating from device D_j, with which the sentinel S^* successfully detects the tampering attack. Then the m-early detection probability of data integrity attack for packets originating from D_j is equal to the probability $Pr(N_{D_j} \leq m)$.

(b) *Early detection of selective forwarding attack*: As mentioned earlier, there is a unique sequence number counter associated with transmitted packets from each IoT device. For packets originating from a given device D_j, the implication of the selective forwarding attack is the following: *Even if one packet originating from D_j is dropped*, the sequence number of all future packets originating from D_j which are forwarded by R to AP need to be modified by R in order to maintain sequence number continuity. Now, *following the first instance of a dropped packet originating from D_j*, let M_{D_j} denote the count for the number of subsequent packets (which originate from D_j and are forwarded by R to AP) that are required for the sentinel to detect the attack. For a given device D_j, we define the *m-early detection probability of selective forwarding attack* to be the probability $Pr(M_{D_j} \leq m)$.

Remark: The above discussion shows that the sentinel based detection of selective forwarding attack is robust even when the relay drops just a single data packet from a given device.

The following theorem quantifies the m-early detection probability of data integrity attack and the m-early detection probability of selective forwarding attack.

Theorem 3: We have

$$Pr(N_{D_j} \leq m) = \sum_{n=1}^{m} (1 - q_{D_j}) \left(q_{D_j}\right)^{n-1} \qquad (16)$$
$$= Pr(M_{D_j} \leq m). \qquad (17)$$

Proof: We have $Pr(N_{D_j} \leq m) = \sum_{n=1}^{m} Pr(N_{D_j} = n)$, so it suffices to show that $Pr(N_{D_j} = n) = (1 - q_{D_j}) \left(q_{D_j}\right)^{n-1}$ in order to prove the first equality in (16). As q_{D_j} denotes the probability that sentinel S^* is unable to detect a data integrity attack on a given packet originating from D_j, it follows that $Pr(N_{D_j} = 1) = 1 - q_{D_j}$. Now, if S^* detects the data integrity attack only after $n > 1$ packets originating from D_j have been corrupted, it implies that S^* was unsuccessful in detecting the data integrity attack on the previous $n - 1$ packets, and hence $Pr(N_{D_j} = n) = (1 - q_{D_j}) \left(q_{D_j}\right)^{n-1}$.

We now prove the equality in (17). Comparing (6) and (8), we observe that $\tilde{q}_{D_j} = q_{D_j}$, and hence it suffices to show that $Pr(M_{D_j} = n) = (1 - \tilde{q}_{D_j}) \left(\tilde{q}_{D_j}\right)^{n-1}$ in order to prove the second equality in (16). Let i denote the sequence number of the first packet originating from D_j which gets dropped at the relay. Then $\tilde{q}_{D_j,i}$ denotes the probability that sentinel S^* is unable to detect this packet dropped by relay R. Note that the expression for $\tilde{q}_{D_j,i}$ given by (8) is independent of i and is referred as $\tilde{q}_{D_j}$. Following the first dropping of a packet at R corresponding to packet source D_j, in order to maintain the continuity of sequence numbers at the AP, the relay has to tamper the sequence number of every successive packet (with packet source D_j) which R forwards to AP. For every such packet forwarded by R to AP with tampered sequence number, the probability of successful detection at sentinel S^* is given by $1 - \tilde{q}_{D_j}$. Now, following the first packet drop by the relay, if S^* detects the selective forwarding attack only after n packets (with modified sequence numbers) have been forwarded by R to AP, then we have $Pr(M_{D_j} = n) = (1 - \tilde{q}_{D_j}) \left(\tilde{q}_{D_j}\right)^{n-1}$. □

Remark: Note that N_{D_j} is a geometrically distributed random variable with $Pr(N_{D_j} = n) = (1 - q_{D_j}) \left(q_{D_j}\right)^{n-1}$. The expected value of N_{D_j}, denoted $\bar{N}_{D_j}$, is therefore

$$\bar{N}_{D_j} = \frac{1}{1 - q_{D_j}}. \qquad (18)$$

As N_{D_j} and M_{D_j} have the same probability distribution (see (16)), it follows from the above remark that the expected value of M_{D_j} is also equal to $1/(1 - q_{D_j})$.

V. DISCUSSIONN

A. Packets from Different Devices: A Unified View

So far, we have analyzed the packet stream originating from a given device, say D_j, and have quantified the distribution of the number of packets tampered with by the relay before the sentinel detects the data integrity attack (see Theorem 3). In this subsection, we take a unified view where we jointly analyze the received packet stream from all the devices connected to the relay. In particular, we analyze the data integrity attack, and focus on the set of all packets tampered with by the relay, rather than partitioning them into subsets based on the packet source.

For $n = 1, 2, \cdots$, let j_n denote the index of that device which transmitted the nth packet modified by relay R, i.e., device D_{j_n} is the originator of the nth packet tampered with by the relay. Let N_D denote the index of that tampered packet for which the sentinel S^* successfully detects the tampering attack. The m-early detection probability of data integrity attack in this scenario is equal to the probability $Pr(N_D \leq m)$. The following theorem quantifies this probability.

Theorem 4: We have

$$Pr(N_D \leq m) = \sum_{n=1}^{m} Pr(N_D = n), \tag{19}$$

$$Pr(N_D = n) = \begin{cases} 1 - q_{D_{j_1}}, & n = 1 \\ \left(1 - q_{D_{j_n}}\right)\left(\prod_{t=1}^{n-1} q_{D_{j_t}}\right), & n > 1, \end{cases} \tag{20}$$

where the probability q_{D_j} for device D_j is given by (6).

Proof: Note that q_{D_j} denotes the probability that sentinel S^* is unable to detect the tampering attack on a given packet transmitted by device D_j. Since j_1 denotes the index of that device which transmitted the first packet modified by R, the probability that this attack is immediately detected by S^* is equal to $Pr(N_D = 1) = 1 - q_{D_{j_1}}$. Now, if S^* detects the attack only after $n > 1$ packets have been tampered with, it implies that S^* was unsuccessful in detecting the attack on the previous $n - 1$ packets, and hence $Pr(N_D = n) = \left(1 - q_{D_{j_n}}\right)\left(\prod_{t=1}^{n-1} q_{D_{j_t}}\right)$. □

B. How Many Sentinels are Needed?

In this subsection, we provide a framework that helps us to trade cost (in terms of number of sentinels) with performance (in terms of early detection probability of a malicious relay). In particular, for a given positive integer m and desired early detection probability $Pr(N_D \leq m)$, the framework can be applied to numerically quantify the number of sentinels required to monitor a network populated with relays and associated devices, such that the desired performance is achieved.

We consider a general wireless sensor network consisting of one AP, multiple relays, and different devices associated to each relay. Since the multiple access scheme is CSMA/CA, neighboring clusters of nodes transmit in orthogonal channels with high probability, and therefore a sentinel node can monitor traffic from multiple relay clusters in its vicinity. Let $\mathcal{R}$ denote the number of relays connected to the AP, let $\mathcal{D}$ denote the number of devices connected to each relay, and let $\mathcal{S}$ denote the number of sentinel deployed to monitor network traffic. Let the number of malicious relays (among the $\mathcal{R}$ relays connected to the AP) be denoted by ρ.

We aim to quantify the number of sentinels $\mathcal{S}$ which ensure that all the malicious relays are detected by sentinels with a sufficiently high probability before each malicious relay corrupts not more than m packets. Towards this, we use a relay-clustering framework and a general path loss model (refer Section III.C) to quantify the PEP on a given wireless link. This approach is outlined in the following algorithm.

Step 1) Let $\mathcal{R}$, $\mathcal{D}$, and m be given. Initialize $\mathcal{S} = 1$.

Step 2) Let P_{tar} denote the target probability with which a malicious relay is detected before it corrupts not more than m packets.

Step 3) Let AP be placed at the origin. Use Monte-Carlo simulation to generate $\mathcal{R}$ relays uniformly distributed within a radius d_1 from the AP. Generate $\mathcal{D}$ devices around each relay, where the devices are uniformly distributed within a radius d_2 from associated relays. For each realization of $\mathcal{R}$ relays and $\mathcal{D}$ devices around each relay, use a clustering algorithm (such as *k-means clustering* [25]) to cluster the relays into $\mathcal{S}$ groups and place a sentinel at the centroid of each cluster. Therefore, each sentinel monitors traffic flowing through relays associated with the same cluster.

Step 4) Apply the path loss model in Section III.C to quantify the PEP on a given wireless link as a function of the transmit power and the distance between transmitting and receiving nodes.

Step 5) Let the malicious relay corrupts packets originating from different devices connected to it with equal probability. Compute the probability of early detection of malicious relay using Theorem 4, and average this probability over the $\mathcal{R}$ relays. For a given relay R, its corresponding sentinel S^*, and device D_j associated with R, the value of q_{D_j} is computed using (1), (4), and (6).

Step 6) If the early detection probability computed in the previous step is less than P_{tar}, then let $\mathcal{S} = \mathcal{S}+1$ and re-compute the early detection probability by repeating the process from Step 3 onwards; else stop.

The above framework help us quantify the number of sentinels required to detect a malicious relay ($\rho = 1$) with probability *at least* P_{tar} when the malicious relay has not corrupted more than m packets before it is detected.

We remark that the outcome of the above framework can be directly applied to compute early detection probability of *multiple* malicious relays ($\rho > 1$). Since the detection of a malicious relay depends only on packet error probabilities on the associated wireless links, the detection process for different malicious relays is mutually independent. Therefore, if there are $\rho > 1$ malicious relays present in the network, the probability that all malicious relays are detected before each malicious relay corrupts not more than m packets, is lower bounded by $(P_{tar})^\rho$.

VI. NUMERICAL RESULTS

In this section we present several numerical results highlighting the performance of the sentinel based detection scheme. In Section VI.A, we consider the case where a given malicious relay R is monitored by a fixed sentinel S^*, while in Section VI.B we consider a unified framework where a network consisting of several relays and IoT devices is monitored by a given number of sentinel nodes.

A. Detecting a Given Malicious Relay

In this subsection, we consider the scenario where a given malicious relay R is monitored by a fixed sentinel S^*. We demonstrate the impact of PEP over different wireless links, on the performance of the proposed sentinel based detection scheme. The corresponding Monte-Carlo simulation results, obtained by considering 10^4 end-to-end packet transmissions, are marked with '+' symbol in the following figures.

We first present results for $q_{D_j \rightarrow R}$, which denotes the probability that a given packet transmitted by IoT device D_j is successfully transferred to relay R, but is *not* successfully received

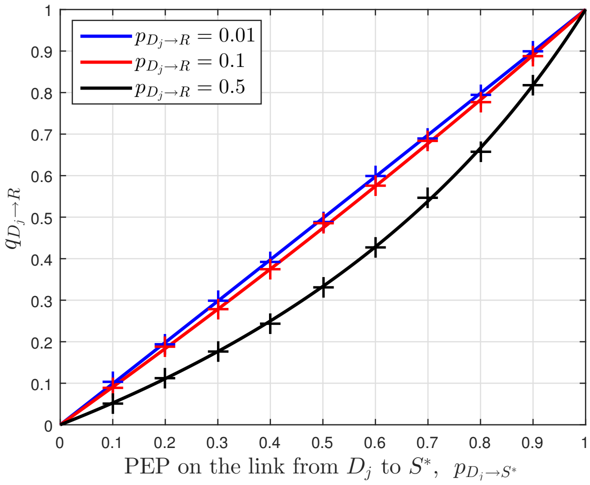

Fig. 3. Plot depicting $q_{D_j\to R}$, the probability that a given packet transmitted by IoT device D_j is successfully transferred to relay R, but is *not* successfully received by sentinel S^*.

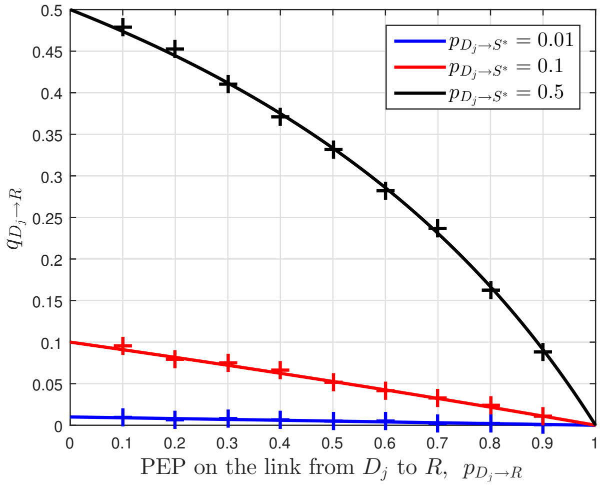

Fig. 4. Plot depicting $q_{D_j\to R}$ as a function of $p_{D_j\to R}$.

by sentinel S^*. Fig. 3 plots $q_{D_j\to R}$ as a function of $p_{D_j\to S^*}$, where $p_{D_j\to S^*}$ denotes the PEP due to channel noise on the wireless link from D_j to S^*. The dependence of $q_{D_j\to R}$ on $p_{D_j\to S^*}$ and $p_{D_j\to R}$ is given by Lemma 1. As mentioned in the remark after Lemma 1, we observe from Fig. 3 that $q_{D_j\to R} \le p_{D_j\to S^*}$ and that $q_{D_j\to R}$ tends to $p_{D_j\to S^*}$ as $p_{D_j\to R}$ tends to zero. Further, using (1) we observe that for a given value of $p_{D_j\to R}$, the partial derivative

$$\frac{\partial q_{D_j\to R}}{\partial p_{D_j\to S^*}} = \frac{1-p_{D_j\to R}}{\left(1-p_{D_j\to R}\cdot p_{D_j\to S^*}\right)^2} > 0,$$

and thus $q_{D_j\to R}$ is an increasing function of $p_{D_j\to S^*}$, as depicted in Fig. 3.

Fig. 4 plots $q_{D_j\to R}$ as a function of $p_{D_j\to R}$. The curves are plotted for four different values of $p_{D_j\to S^*}$. As mentioned in the remark after Lemma 1, it is observed from the figure that $q_{D_j\to R} \le p_{D_j\to S^*}$. For a given value of $p_{D_j\to S^*}$, it is seen that $q_{D_j\to R} = p_{D_j\to S^*}$ when $p_{D_j\to R} = 0$. Moreover, $q_{D_j\to R}$ is a strictly decreasing function of $p_{D_j\to R}$ as

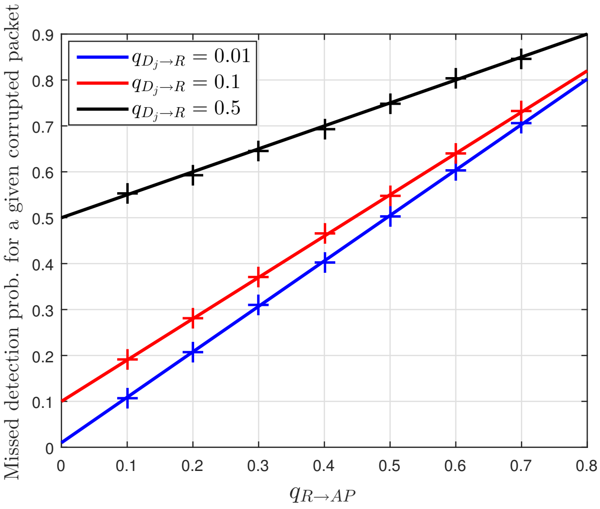

Fig. 5. Plot depicting the missed detection probability for a data integrity attack by R on a given packet transmitted by D_j (denoted by q_{D_j}), as a function of $q_{R\to AP}$, the probability that a packet transmitted by R is successfully transferred to AP but is not successfully received by S^*.

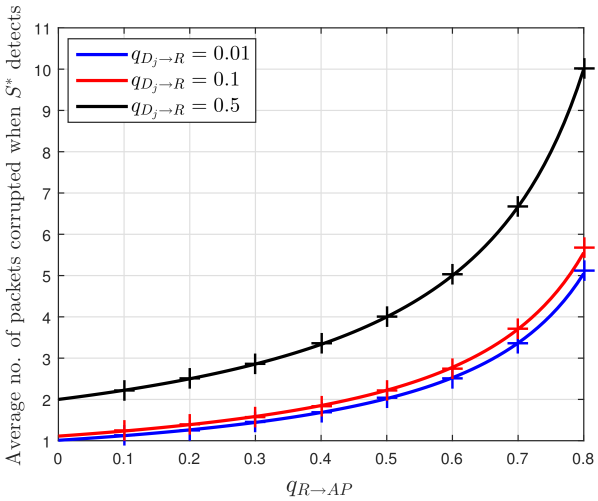

Fig. 6. Plot depicting average number of packets corrupted by relay before S^* detects data integrity attack (denoted by $\bar{N}_{D_j}$), as a function of $q_{R\to AP}$.

$$\frac{\partial q_{D_j\to R}}{\partial p_{D_j\to R}} = \frac{-p_{D_j\to S^*}(1-p_{D_j\to S^*})}{\left(1-p_{D_j\to R}\cdot p_{D_j\to S^*}\right)^2} < 0.$$

Fig. 5 plots the missed detection probability for a data integrity attack by R on a given packet transmitted by D_j (denoted by q_{D_j}), as a function of $q_{R\to AP}$. Using (6), we have $q_{D_j} = q_{D_j\to R} + q_{R\to AP}(1-q_{D_j\to R})$ and thus q_{D_j} varies linearly with $q_{R\to AP}$, when $q_{D_j\to R}$ is fixed. Further, we observe from (6) that q_{D_j} is symmetric in $q_{R\to AP}$ and $q_{D_j\to R}$, and hence q_{D_j} will remain unchanged when values of $q_{R\to AP}$ and $q_{D_j\to R}$ are interchanged.

Fig. 6 plots the average number of packets corrupted by a relay before sentinel S^* detects the data integrity attack (denoted by $\bar{N}_{D_j}$), as a function of $q_{R\to AP}$. Note that combining (18) and (6), we observe that $\bar{N}_{D_j}$ increases with $q_{R\to AP}$, as depicted in

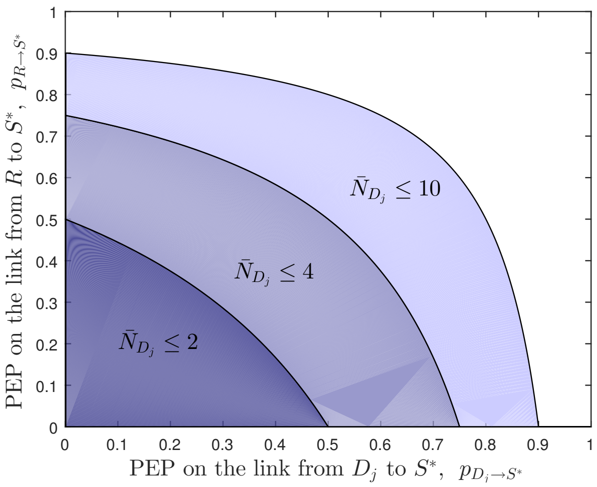

Fig. 7. Shaded area for which $\bar{N}_{D_j}$ (the average number of packets corrupted by relay before S^* detects data integrity attack) is less than certain thresholds.

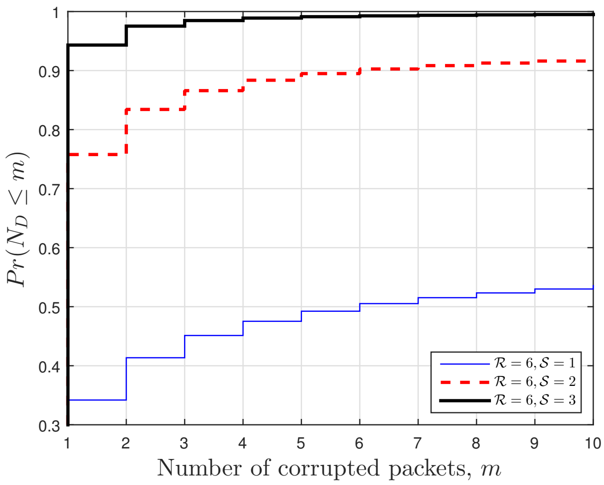

Fig. 8. Early malicious relay detection probability, $Pr(N_D \leq m)$, as a function of m when $\mathcal{R} = 6$ and number of sentinels $\mathcal{S} \in \{1, 2, 3\}$.

the Fig. 6. Further, $\bar{N}_{D_j}$ is symmetric in $q_{R\to AP}$ and $q_{D_j\to R}$, and hence $\bar{N}_{D_j}$ will remain unchanged when values of $q_{R\to AP}$ and $q_{D_j\to R}$ are interchanged.

Using (1), it is observed that

$$\frac{\partial q_{D_j\to R}}{\partial p_{D_j\to R}} = \frac{-p_{D_j\to S^*}(1 - p_{D_j\to S^*})}{\left(1 - p_{D_j\to R} \cdot p_{D_j\to S^*}\right)^2} < 0,$$

and therefore $q_{D_j\to R}$ decreases with $p_{D_j\to R}$. Similarly, using (4), it can be shown that $q_{R\to AP}$ decreases with $p_{R\to AP}$. Fig. 7 shows the shaded area for which $\bar{N}_{D_j}$ is less than certain thresholds, for the *worst-case* performance scenario where $p_{D_j\to R} = 0$ and $p_{R\to AP} = 0$. As $q_{D_j\to R}$ (resp. $q_{R\to AP}$) is a decreasing function of $p_{D_j\to R}$ (resp. $p_{R\to AP}$), it follows from (6) and (18) that an increase in $p_{D_j\to R}$ or $p_{R\to AP}$ will only reduce $\bar{N}_{D_j}$, and therefore *improve* detection performance.

Fig. 7 highlights the robustness of the sentinel based intrusion detection scheme by showing that the average number of corrupted packets required for detection are reasonably small even when the packet error probabilities on the $D_j \to S^*$ link and the $R \to S^*$ links are sufficiently high.

As shown in Theorem 3, the early detection probability of selective forwarding attack is similar to that of the data integrity attack, and therefore the corresponding numerical results have been omitted.

B. Early Detection Probability: A Unified View

This subsection presents numerical results for a unified framework with the following properties:

- Given $\mathcal{R}$ relays, each relay serving $\mathcal{D}$ devices, and a total of $\mathcal{S}$ sentinels for network monitoring, the *relays are clustered into $\mathcal{S}$ different groups*. A sentinel is placed at the centroid of each cluster.
- The $\mathcal{R}$ relays are uniformly distributed spatially over a radius of d_1 meters from the AP. The $\mathcal{D}$ devices connected to a given relay are uniformly distributed over a radius of d_2 meters from the relay.
- A malicious relay corrupts packets from different devices associated with the relay with equal probability.
- Every transmitted packet is protected by a rate 1/2 convolutional code with constraint length 7, and the PEP follows the path loss model in Section III.C.

In the following plots, we assume that the received signal strength at a distance of 1m from a transmitting relay (resp. transmitting device) is -60 dBm (resp. -70 dBm). The path loss exponent is 2.5, the transmission rate is 1 Mbps, and the encoded packet size is 480 bits. The values of $\mathcal{D}$, d_1, and d_2, are 5, 100, and 20, respectively. The $\mathcal{R}$ relays are clustered into $\mathcal{S}$ different groups using the *k-means* clustering algorithm [25]. The following plots present $Pr(N_D \leq m)$, representing the probability that a malicious relay is detected before it corrupts not more than m data packets, under different scenarios. The results are obtained via Monte-Carlo simulations by averaging the performance over 10^6 iterations, with each iteration comprising a random placement of relays and devices in the network.

Fig. 8 plots the early detection probability, $Pr(N_D \leq m)$, as a function of m when $\mathcal{R} = 6$. For a given m, it is seen that $Pr(N_D \leq m)$ increases with number of sentinels, and $Pr(N_D \leq 10)$ exceeds 99.95% for $\mathcal{S} = 3$.

Fig. 9 depicts $Pr(N_D \leq m)$ as a function of m for different values of $\mathcal{R}$ when $\mathcal{S}/\mathcal{R} = 1/3$. As the number of sentinels scale linearly with $\mathcal{R}$, it is seen that for a given m, the early detection probability, $Pr(N_D \leq m)$, increases with $\mathcal{R}$. Note that the network becomes denser with increasing $\mathcal{R}$, and hence the radius of a relay cluster decreases, in general. A decrease in relay cluster radius lowers the average PEP on device-to-sentinel and relay-to-sentinel links due to shorter distances, which results in improved performance.

Fig. 10 shows the detection performance when the ratio $\mathcal{S}/\mathcal{R}$ is equal to $1/2$. In contrast to Fig. 9, the early detection probability is higher in Fig. 10 due to higher value of the ratio $\mathcal{S}/\mathcal{R}$ which results in lower average radius of a relay cluster.

Fig. 11 presents the detection performance for different values of $\mathcal{R}$, where the number of sentinel $\mathcal{S}$ are fixed to 5. It is seen that $Pr(N_D \leq 10) > 99\%$ for $\mathcal{R} \in \{15, 20, 25, 30\}$, and that $Pr(N_D \leq 10)$ does not vary significantly with changing values of R. As the performance is only expected to improve

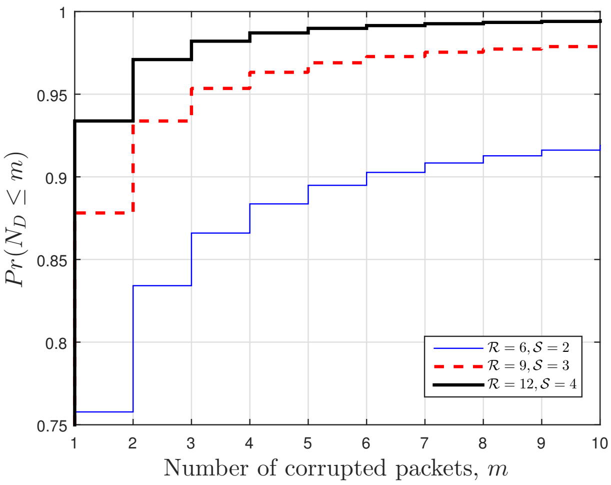

Fig. 9. Early malicious relay detection probability, $Pr(N_D \leq m)$, as a function of m when the ratio $\mathcal{S}/\mathcal{R}$ is fixed to $1/3$.

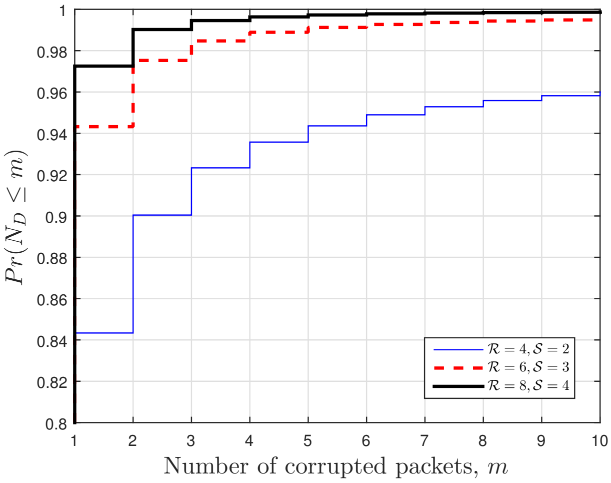

Fig. 10. Early malicious relay detection probability, $Pr(N_D \leq m)$, as a function of m when the ratio $\mathcal{S}/\mathcal{R}$ is fixed to $1/2$.

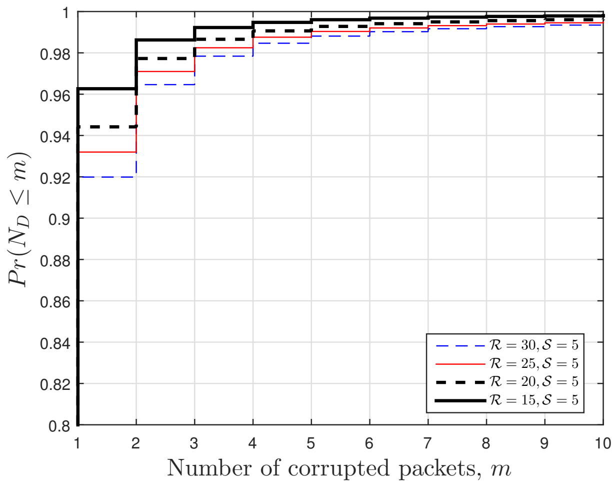

Fig. 11. Early malicious relay detection probability, $Pr(N_D \leq m)$, as a function of m for $\mathcal{S} = 5$.

upon reducing R, we observe that the detection performance is fairly robust for $\mathcal{S} = 5$. The intuition behind this phenomenon, where a fixed number of sentinels achieve robust performance, independent of the number of relays, is as follows. Consider a scenario where all devices transmit at a fixed power, and let $\tilde{d_2}$ be the maximum distance (in meters) from a device where the PEP is less than 10^{-1}. The sentinel fails to detect data integrity attack on a given packet if it fails to successfully receive either the packet transmitted from a device or the corrupted packet forwarded by the relay. In general, we can assume that relays transmit at a higher power compared to devices, so a misdetection typically occurs when a packet transmitted by a device is not successfully received at a sentinel. When relays are uniformly distributed within a radius d_1 meters from the AP, then roughly $(d_1/\tilde{d_2})^2$ sentinels are required to effectively cover the network area to ensure that a transmission from a device is successfully received by a sentinel with probability at least 0.9. For the parameters chosen for Fig. 11, we have $d_1 = 100$ and $\tilde{d_2} \approx 45$, and so $(100/45)^2 \approx 5$ sentinels are sufficient to effectively monitor the network, independent of number of relays in the network. In essence, the fact that the network can be effectively monitored by a fixed number of sentinels, independent of the number of relays, helps us to bound sentinel cost for achieving a desired detection performance.

VII. CONCLUSION

We presented an effective and practical sentinel based scheme for malicious relay detection in noisy wireless networks. This scheme has the advantage that it does not require any change in existing PHY/MAC protocols (such as IEEE 802.11ah Wi-Fi HaLow), as it employs passive sentinel nodes for traffic monitoring. The detection scheme exploited the broadcast nature of wireless transmission to overhear information being forwarded by relay nodes. The false alarm occurred only in the unlikely scenario where the packet CRC fails to *detect* errors, even though the decoded packet is in error. This implies that the false alarm probability in our detection scheme can be made negligible by using a sufficiently long CRC.

The detection scheme operated at the MAC layer by comparing packets transmitted by IoT devices and the corresponding relay. This has the advantage over other physical layer approaches that our scheme remains effective even in scenarios where different wireless links in the network may employ distinct modulation and coding schemes at the physical layer.

We provided a detailed analysis for the detection of the data integrity attack and the selective forwarding attack. The analysis assumed a general noisy channel model for the IoT network, where each wireless link may potentially have distinct PEP due to different noise conditions. We quantified the probability of early detection of malicious relay behavior as a function of PEP on different wireless links across the network. Moreover, our scheme is robust in detecting selective forwarding attacks when a small fraction of packets are dropped by a malicious relay.

We presented several numerical results to highlight the impact of PEP on the probability of detection of data integrity attack on a given data packet. The results showed that the proposed detection scheme is robust even in the scenario where the PEP on the wireless link from an IoT device to sentinel (resp. relay to sentinel) is high. We also provided results for a unified framework where a network with several relays and devices is monitored by a given number of sentinels. The results showed that a given network area can be effectively monitored by a fixed number of sentinels, independent of the number of relays, thereby bounding the cost for achieving a desired detection performance.

REFERENCES

[1] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial internet of things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78 238–78 259, Dec. 2018.

[2] Y. Mehmood et al., "Internet-of-things-based smart cities: Recent advances and challenges," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 16–24, Sept. 2017.

[3] B. Malik, "Why IoT security should be top of your list," May 2019. [Online]. Available: https://www.techradar.com/news/why-iot-security-should-be-top-of-your-list

[4] K. Roby, "Why IoT devices pose a bigger cybersecurity risk than most realize," Feb. 2019. [Online]. Available: https://www.zdnet.com/article/iot-devices-pose-bigger-security-risks-than-most-realize/

[5] B. Krebs, "P2P weakness exposes millions of IoT devices," Apr. 2019. [Online]. Available: https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/

[6] "IEEE standard for information technology–telecommunications and information exchange between systems - local and metropolitan area networks–specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 2: Sub 1 GHz License Exempt Operation," *IEEE Std 802.11ah-2016 (Amendment to IEEE Std 802.11-2016, as amended by IEEE Std 802.11ai-2016)*, pp. 1–594, May 2017.

[7] L. F. D. Carpio, et al., "Comparison of 802.11ah and BLE for a home automation use case," in *Proc. PIMRC*, Sept. 2016, pp. 1–6.

[8] N. Ahmed, H. Rahman, and M. I. Hussain, "A comparison of 802.11ah and 802.15.4 for IoT," *ICT Express*, vol. 2, no. 3, pp. 100–102, 2016.

[9] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, May 2011.

[10] X. Liu, M. Abdelhakim, P. Krishnamurthy, and D. Tipper, "Identifying malicious nodes in multihop IoT networks using diversity and unsupervised learning," in *Proc. ICC*, May 2018, pp. 1–6.

[11] S. Y. Nam, D. Kim, and J. Kim, "Enhanced ARP: Preventing ARP poisoning-based man-in-the-middle attacks," *IEEE Commun. Lett.*, vol. 14, no. 2, pp. 187–189, Feb. 2010.

[12] S. W. Kim, "Physical integrity check in cooperative relay communications," *IEEE Trans. Wireless Commun.*, vol. 14, no. 11, pp. 6401–6413, Nov. 2015.

[13] X. Liu, Y. Guan, and S. W. Kim, "Bayesian test for detecting false data injection in wireless relay networks," *IEEE Commun. Lett.*, vol. 22, no. 2, pp. 380–383, Feb. 2018.

[14] J. Ren, Y. Zhang, K. Zhang, and X. Shen, "Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 5, pp. 3718–3731, May 2016.

[15] C. Jia and T. J. Lim, "Detecting cluster head attacks in heterogeneous wireless sensor networks," in *Proc. VTC*, June 2017, pp. 1–6.

[16] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," in *Proc. ICICS*, Dec. 2009, pp. 1–5.

[17] C. Pu and S. Lim, "A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: Design, analysis, and evaluation," *IEEE Syst. J.*, vol. 12, no. 1, pp. 834–842, Mar. 2018.

[18] D. Agarwal, R. R. Rout, and S. Ravichandra, "Detection of node-misbehavior using overhearing and autonomous agents in wireless ad-hoc networks," in *Proc. AIMoC*, Feb. 2015, pp. 152–157.

[19] T. H. Hai and E. N. Huh, "Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge," in *Proc. IEEE NCA*, July 2008, pp. 325–331.

[20] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. ACM MobiCom*, Aug. 2000, pp. 255–265.

[21] A. Tandon, T. J. Lim, and U. Tefek, "Sentinel based malicious relay detection scheme for wireless IoT networks," in *Proc. IEEE GLOBECOM Workshops*, Dec. 2018.

[22] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 2, pp. 198–212, June 2007.

[23] W. Wesley Peterson and E. J Weldon, Jr., *Error-Correcting Codes (2nd ed.).* The M.I.T. Press, 1972.

[24] R. G. Gallager, *Principles of Digital Communication.* Cambridge University Press, 2008.

[25] J. A. Hartigan and M. A. Wong, "Algorithm AS 136: A K-Means clustering algorithm," *Applied Statistics*, vol. 28, no. 1, pp. 100–108, 1979.

Anshoo Tandon received the B.E. degree in Computer Science and Engineering from Kumaun University, Nainital, India, in 1998, the M.E. degree in Signal Processing from the Indian Institute of Science, Bangalore, India, in 2000, and the Ph.D. degree from the National University of Singapore (NUS), Singapore, in 2016. Between 2000 and 2011, he worked in different capacities in the industry towards developing efficient cellular and wireless connectivity solutions. He is currently a Research Fellow in the department of Electrical and Computer Engineering at NUS, Singapore. His research interests include information and coding theory.

Teng Joon Lim obtained the B.Eng. degree in Electrical Engineering from the National University of Singapore (NUS) in 1992, and the Ph.D. degree from the University of Cambridge in 1996. From September 1995 to November 2000, he was at the Centre for Wireless Communications in Singapore, one of the predecessors of the Institute for Infocomm Research (I2R). From December 2000 to May 2011, he was Assistant Professor, Associate Professor, then Professor at the University of Toronto's Edward S. Rogers Sr. Department of Electrical and Computer Engineering. Since June 2011, he has been a Professor at the ECE Department of NUS, where he served as a Deputy Head from July 2014 to August 2015. Since September 2015, he has served as Vice-Dean (Graduate Programs) in the NUS Faculty of Engineering. Professor Lim was an Area Editor of the IEEE Transactions on Wireless Communications from September 2013 to September 2018, and previously served as on the Editorial Boards of several other international journals. He chaired the Singapore chapter of the IEEE Communications Society in 2017 and 2018, and is a Distinguished Lecturer of the IEEE Vehicular Technology Society for 2019-20.

Utku Tefek received the B.Sc. degree with high honors in Electrical and Electronics Engineering from Bilkent University, Turkey in 2013 and the Ph.D degree from the National University of Singapore in 2017. From October 2017 to October 2018, he was a postdoctoral fellow at the National University of Singapore. Since October 2018, he has been a Researcher at Advanced Digital Sciences Center, a Singapore-based research center established by the University of Illinois at Urbana-Champaign. His research interests include the application of stochastic models to wireless networks, machine-to-machine communications, cyber-physical systems security with a recent focus on urban transportation systems.