A GLRT Based Mechanism for Detecting Relay Misbehavior in Clustered IoT Networks

Nalam Venkata Abhishek, Anshoo Tandon, *Member, IEEE*, Teng Joon Lim, *Fellow, IEEE* and Biplab Sikdar, *Senior Member, IEEE*
National University of Singapore
Email: abhishek_nalam@u.nus.edu, anshoo.tandon@gmail.com, eleltj@nus.edu.sg, bsikdar@nus.edu.sg

***Abstract*—Clustering Internet of Things (IoT) Networks, to alleviate the network scalability problem, provides an opportunity for an adversary to compromise a set of nodes by simply compromising the relay they are associated with. In such scenarios, an adversary who has compromised the relay can affect the network's performance by deliberately dropping the packets transmitted by the IoT devices and/or by corrupting the packets to be forwarded by the relay. In this way, the adversary can successfully mimic a bad radio channel between the IoT devices and the relay, thereby requiring the IoT devices to retransmit more frequently. Such a strategy increases the processing load on the IoT devices and will drain their batteries at a faster rate. To detect such an attack, we present hybrid intrusion detection systems that rely on the monitoring of uplink and downlink packets transmitted between IoT devices and the relay. Specifically, we compare the observed packet drop probabilities against their long-term expected values. The detection rules proposed originate from the generalized likelihood ratio test, where the adversary parameters are estimated using maximum likelihood estimation. A semi-analytical approach to obtain the expressions for the false alarm probability is presented in order to determine the decision thresholds. Results presented show the effectiveness of the proposed detection systems, demonstrate the impact of the choice of adversary parameters on them and validate the expressions obtained for the false alarm probability.**

I. Introduction

With the growing interest in using Internet of Things (IoT) technologies, the demand for connecting resource-constrained devices to the Internet has been increasing quickly. In order to realize this potential growth, many issues like security, network scalability, etc. [1]–[4] need to be addressed. It is estimated that more than fifty billion devices would be connected to the Internet by 2050 [5]. Such an increase in the number of wireless networked devices can lead to radio access network congestion. Hence, the need to resolve the network scalability issue is apparent. One of the solutions is the clustering approach [6]. In such an approach, a set of IoT devices are grouped (or clustered) and are assigned a relay (or cluster head) which would assist in forwarding the traffic to and from the Base Station (assuming a cellular architecture). The clustering strategy could be based on Quality of Service requirements, geographical location, etc. Relays would often be user-installed equipment, which are not professionally maintained and updated, making them vulnerable to security breaches. Therefore, implementing such a strategy also causes security issues i.e. an adversary can compromise a set of IoT devices merely by comprising the relay they are associated with.

An IoT network is vulnerable to many attacks other than eavesdropping, which can be effectively defended against through cryptography [7]. For instance, to degrade the performance of an IoT network, an attacker may attempt to deplete the battery of IoT devices at a faster than normal rate. One possible way for an adversary to drain the batteries at a faster pace, is to increase the rate of retransmissions, on the uplink and/or downlink, by mimicking a bad radio link between IoT device and the relay. **Such scenarios where both uplink and downlink channel are active are common in IoT networks (e.g. Health care [8], [9], Intelligent Transportation Systems [10]).** This attack can be implemented if the attacker can obtain root access to a relay, which is often not a problem because many user-installed devices do not have updated firmware and use default login credentials, and the relay has vulnerabilities in its operating system that allows manipulation of its protocol stack. Such an attack can successfully drain the batteries of the IoT devices as well as severely compromise network throughput and therefore result in economic loss. These attacks are hard to distinguish from naturally occurring instances of weak wireless channels, making them difficult to detect. Hence, developing Intrusion Detection systems (IDS) to detect such attacks is an important task, which we address in this paper. IDS's can be categorized according to where most of the detection intelligence resides – centralized, distributed, or hybrid [11]. In this paper, we propose a hybrid IDS system which relies on the IoT devices being able to count the rate of packet retransmissions on the uplink, and the rate of unsuccessful packet deliveries on the downlink, and report these measurements back to a trusted server which will then decide whether a relay has been compromised.

A. Related Work

Examples of attacks which cryptography cannot defend against are Selective Forwarding, Black Hole and Channel degradation. Researchers in the past have proposed to overcome such attacks using various methods. Machine learning algorithms (such as the ones in [12]), when designed using

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.

sufficient and appropriate training data samples, can provide the desired performance. However, in reality, it is problematic to inject malicious packets into the networks to build the training data. Authors in [13] propose a detection technique called SVELTE to detect the presence of a selective forwarding attack. The proposed system detects the adversary when it filters all the packets or sends only the mapping request packets. In [14], the authors have presented an approach based on the channel conditions to detect selective forwarding attacks. A similar approach was proposed in [15] to detect forwarding misbehavior of nodes. However, a sensor monitoring the data packets of the forwarding nodes can be expensive in terms of the energy consumed. Detecting selective forwarding attacks using the traffic eavesdropped by monitor nodes was proposed in [16]. It is however not practical if the system requires a large number of monitor nodes. In [17], the authors have proposed to detect selective forwarding attacks by random selection of a single checkpoint node. To implement it, however, we need to make major changes to the existing protocols. A sequential probability ratio based detection system was presented in [18] for detecting selective forwarding attacks. Their decision is based on the expected transmission count of the nodes. A light-weight heart-beat protocol is proposed in [19]. In this approach, an echo is sent to every node in the network. A selective forwarding attack is detected when there is no reply received from the affected nodes. However, an intelligent attacker might simply refrain from dropping the echo packets and thus stay undetected.

In [20], a trust based anaomaly detection technique was used to identify a malicious node. The trust is based on the number of malicious packets injected into the network. It is however not clear as to how a packet is classified as legal or malicious. Therefore, the detection algorithm cannot be extended to identifying the attacker presented in this paper. The mechanisms presented in [21], [22] require data for training the IDSs. In contrary, our detection system does not required any training data is based on theoretical foundations. Also, insufficient training data could limit the performance of the detection systems. The detection scheme in [23], where the detection is based on the observed bit patterns, cannot be used to identify the attacker described in this paper since a packet drop event cannot be correlated with the bit patterns.

B. Comparison to our Previous Work

In our previous work in [24] we considered an adversarial relay which corrupts packets (unicast) to be forwarded to IoT devices (i.e. the relay attacks the downlink channel of the IoT devices). The probability of attack was assumed to be constant over all the devices. In [25] we considered an adversarial relay which attacks the uplink channel (unicast) of the IoT devices. The probability of attack is assumed to be different for different devices, for greatest generality. In both cases, we assume that each user is transmitting or receiving a different packet from other users, and that all channels are independent. Hence, packets are dropped independently of each other.

In addition to the unicast scenarios above, in this paper, we consider the case of broadcast packets on the downlink

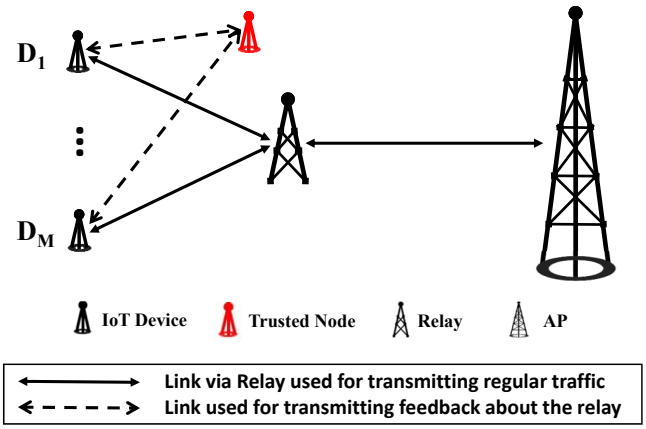

Fig. 1: Network Model Illustration.

where, in the presence of an attack, a corrupted packet is received at all devices and thus the packet drop event at all devices become dependent. The detection of an adversary implementing such an attack is presented and is based on the Generalized Likelihood Ratio Test. The observations required are shared with a trusted node. We numerically obtain the expressions for the false alarm probability for all the detection systems proposed, by modeling the distribution of the detection algorithm (in the absence of attack) using a Gamma distribution. More extensive simulations than those in [16, 17], elaborated upon in Section IV-C, are also presented.

II. System Model

A. Network Model

We consider an IoT network with one access point, AP, one relay, R, and a set of M IoT devices, $\mathcal{D} = \{D_j, j = 1, 2, \cdots, M\}$, associated with the relay. The IoT devices exchange information with the secured access point AP via the relay. Such a model can be widely implemented in both IEEE 802.11 local area networks and cellular wide area networks with "decode and forward" relays.

We assume the existence of a side channel from the IoT devices to a trusted node, as depicted in Figure 1, that will be used by the proposed detection system. The same will be elaborated upon in Section III. In this paper, we present two possibilities for deploying such trusted nodes:

1) **The access point can be used as the trusted node. It can be assumed that every IoT device has the ability to directly communicate with the access point wirelessly, but at a bit rate much lower than it can communicate with its relay. To extend the coverage of the network in order to enable the IoT devices to communicate with the AP and vice-versa, techniques like frequency hopping, power boosting, etc. can be used [26].**
2) **The other possibility is to deploy special trusted nodes, called sentinel nodes [27]. It can be assumed that at least one sentinel node is in the range of every IoT device. The placement of these nodes is out of the scope of this paper and therefore not discussed in detail.**

Before the IoT device associates itself with the trusted node, it will disassociate itself from its relay R. The network model is illustrated in Fig. 1. The dashed lines represent links between IoT devices and the trusted node and the solid lines represent the link via R. The wireless channel between any two devices in the network is assumed to be memoryless. For any network in normal operation, there is a non-zero probability of decoding the bits in a packet in error due to various naturally occurring channel and network non-idealities, and/or protocol level behavior. In such a case, the following possibilities exist:

- When a packet (transmitted by an IoT device) is dropped by the relay, a retransmission request is sent by the relay to the IoT device, hence making the IoT device transmit it again. In this paper, the packet drop probability (PDP) of the $D_j \rightarrow R$ link is assumed to be known and denoted by α_{uj} (i.e. uplink PDP).
- When a packet (transmitted by the relay) is dropped by the IoT device, the IoT device sends a retransmission request to the relay. In this paper, the average PDP on the $R \rightarrow D_j$ link is assumed to be known and denoted by α_{dj} (i.e. downlink PDP).

One of the possible ways to estimate the natural or normal PDP is by measurements when the network is operating normally, and therefore the above assumptions are not impractical.

B. Adversary Model

We now describe the strategy employed by an adversary who has compromised the relay R. **A compromised relay can be used to steal data and credentials of the IoT devices. However, such attacks require the attackers to possess extra knowledge of the network parameters. For instance, when encryption is employed by higher layers, the eavesdropper requires access to the private key of the server in order to steal confidential information. In this paper, we describe a lower level attack that is easy to implement and has considerable impact on the performance of the network.** It is assumed that the adversary disrupts the communication between the access point and IoT devices connected to R by implementing the following strategies:

- On the uplink, the adversary can deliberately ask an IoT device to retransmit a successfully received packet. The attacked relay can choose to forward the packet to the AP in order to avoid having the application layer report a session failure, in order to evade detection.
- On the downlink, the adversary can deliberately corrupt a packet which needs to be forwarded to the IoT device. This can be achieved by corrupting the channel pilots which are used for equalization and/or flipping some of the bits of the physical layer payload. When the packet received by the IoT device is corrupted, it will be dropped and the IoT device requests for a re-transmission.

The attacker, by deliberately implementing the above strategies, can create an adverse impact on the battery lifetime of the IoT devices and at the same time considerably slow down the network. Note that, in the presence of such an attack, a packet can be dropped either due to the network non-idealities or the action of the relay. Such attacks are therefore difficult to detect. All of the following packets may be subjected to such attacks:

- Unicast uplink packets: This refers to the packets transmitted by an IoT device to the relay. In this case we assume that the probability that the relay requests the device D_j to re-transmit a successfully received packet is $\delta_{uj}(> 0)$.
- Unicast downlink packets: This refers to the packets transmitted by the relay to an IoT device. In this case, we assume that the probability that the relay corrupts a packet to be forwarded to the device D_j is $\delta_{dj}(> 0)$.
- Broadcast packets: This refers to the packets transmitted by the relay to all the IoT devices. In this case, we assume that the probability that the relay corrupts a packet to be forwarded to the devices is $\delta_b(> 0)$.

Symbol	Description
α_{uj}	Uplink PDP of D_j under H_0
α_{dj}	Downlink PDP of D_j under H_0
δ_{uj}	Uplink unicast attack probability for D_j
δ_{dj}	Downlink unicast attack probability for D_j
δ_b	Broadcast attack probability
β_{uj}	Uplink PDP of D_j under H_1
β_{dj}	Downlink PDP of D_j under H_1
K_u	Uplink unicast packet window size
K_d	Downlink unicast packet window size
K_b	Broadcast packet window size
$\hat{\delta}_{uj}$	Estimated value of δ_{uj}
$\hat{\delta}_{dj}$	Estimated value of δ_{dj}
$\hat{\delta}_b$	Estimated value of δ_d
N_{uj}	Packet retransmitted by device D_j
N_{dj}	Packet dropped by device D_j
B_{ij}	Feedback reported by device D_j about broadcast packet i
μ_{uj}	Mean of $\hat{\delta}_{uj}$
μ_{dj}	Mean of $\hat{\delta}_{dj}$
μ_b	Mean of $\hat{\delta}_b$
σ_{uj}	Standard deviation of $\hat{\delta}_{uj}$
σ_{dj}	Standard deviation of $\hat{\delta}_{dj}$
σ_b	Standard deviation of $\hat{\delta}_b$
S_u	Simplified Likelihood ratio of the unicast uplink scenario
S_d	Simplified Likelihood ratio of the unicast downlink scenario
S_b	Simplified Likelihood ratio of the broadcast scenario
Γ_u	Threshold for the unicast uplink scenario
Γ_d	Threshold for the unicast downlink scenario
Γ_b	Threshold for the broadcast scenario
α_Γ^u	Shape parameter of the distribution of S_u under H_0
α_Γ^d	Shape parameter of the distribution of S_d under H_0
α_Γ^b	Shape parameter of the distribution of S_b under H_0
N_{ua}	Average number of uplink packets retransmitted by the IoT devices
Γ_a	Threshold for the naive scheme used for comparison

TABLE I: List of symbols used in the paper

III. Intrusion Detection System

In this section, we present the details of our hybrid intrusion detection system (IDS) that is deployed at the trusted node. It can be seen from Section II-B that the packet drop probability of all the types of packets increases in the presence of the described attacks. Hence, we use the measured PDP to classify the relay as malicious or not. The proposed

IDS performs a binary hypothesis test with the following hypotheses:

- Hypothesis H_1: Relay is compromised and is affecting the packets.
- Hypothesis H_0: Relay is not compromised and is in normal operation.

We now proceed to derive the detection rules required to detect an adversary targeting the various types of packets.

A. Intrusion Detection System - Unicast Uplink Packets

To detect attacks on unicast uplink packets, the IDS requires the following features to be enabled in the network:

- Each IoT device D_j has to track the number of packets (N_{uj}), out of the past K_u packets transmitted (including retransmitted packets), for which a NACK is received from the gateway either explicitly or implicitly.
- **All the IoT devices will regularly update the trusted node about N_{uj}.**

1) Conditional Probability Distributions of Decision Statistics: In the absence of attack, we can assume that the packet drops of different devices are independent. When there is no attack, packets are dropped with probability α_{uj} (i.e. uplink PDP in the absence of attack), and hence the probability distribution of the variables $N_{uj}, j \in \{1, \cdots, M\}$ under H_0 are given as follows:

$$P(N_{uj} = k|H_0) = \binom{K_u}{k}(\alpha_{uj})^k(1-\alpha_{uj})^{K_u-k} \quad (1)$$

for $k \in \{1, \cdots, K_u\}$. When the relay is compromised, the uplink PDPs increase to $\beta_{uj}, j \in \{1, \cdots, M\}$ which are given by:

$$\beta_{uj} = \delta_{uj} + (1-\delta_{uj})\alpha_{uj} \quad (2)$$

where $\delta_{uj}, j \in \{1, \cdots, M\}$ are unknown random variables. Using this, the probability distribution of the variables $N_{uj}, j \in \{1, \cdots, M\}$ under H_1 are given as follows:

$$P(N_{uj} = k|H_1) = \binom{K_u}{k}(\beta_{uj})^k(1-\beta_{uj})^{K_u-k} \quad (3)$$

for $k \in \{1, \cdots, K_u\}$. We can assume that the wireless channels used by the IoT devices in the network are independent since they will likely be placed more than a few wavelengths apart from each other. Using this assumption, variables $N_{uj}, j \in \{1, \cdots, M\}$ are independent. The joint probability distribution under H_0 is now defined below, where $N_u = [N_{u1}, \cdots, N_{uM}]$ and $n_u = [n_{u1}, \cdots, n_{uM}]$.

$$P(N_u = n_u|H_0) = \prod_{j=1}^{M} P(N_{uj} = n_{uj}|H_0). \quad (4)$$

Similarly, the joint probability distribution under H_1 is

$$P(N_u = n_u|H_1) = \prod_{j=1}^{M} P(N_{uj} = n_{uj}|H_1). \quad (5)$$

2) Detection Algorithm: The likelihood ratio test (LRT) [28], which is known to maximize the probability of detection for any given probability of false alarm, is the optimum detection rule. The LRT decides in favor of H_1 if and only if the following holds:

$$\frac{P(N_u = n_u|H_1)}{P(N_u = n_u|H_0)} > \gamma_u. \quad (6)$$

Since (6) involves parameters $\delta_{uj}, j \in \{1, \cdots, M\}$ which are assumed unknown at the detector, we use the Generalized LRT (GLRT) [28] where the unknown parameters are replaced with their maximum likelihood estimates (MLE) [29]. This will be further elaborated on in Section III-A3. Assuming that $\hat{\delta}_{uj}, j \in \{1, \cdots, M\}$ are the MLEs of $\delta_{uj}, j \in \{1, \cdots, M\}$, we now proceed to derive the detection algorithm as follows where β_{uj} is replaced by $\hat{\beta}_{uj} \triangleq \hat{\delta}_{uj} + (1-\hat{\delta}_{uj})\alpha_{uj}$. The detection algorithm decides in favor of H_1 when

$$\prod_{j=1}^{M} \frac{(\hat{\beta}_{uj})^{n_{uj}}(1-\hat{\beta}_{uj})^{K_u-n_{uj}}}{(\alpha_{uj})^{n_{uj}}(1-\alpha_{uj})^{K_u-n_{uj}}} > \gamma_u \quad (7)$$

$$\Rightarrow \prod_{j=1}^{M} a_{uj}^{n_{uj}}(1-\hat{\delta}_{uj})^{K_u} > \gamma_u \quad (8)$$

$$\Rightarrow S_u = \sum_{j=1}^{M} S_{uj} > \log(\gamma_u) = \Gamma_u \quad (9)$$

where $S_{uj} = n_{uj}\log(a_{uj}) + P_u\log(1-\hat{\delta}_{uj})$ and $a_{uj} = \frac{\hat{\beta}_{uj}}{\alpha_{uj}(1-\hat{\delta}_{uj})}$.

3) Probability Estimation: In this section, we derive the MLEs of the probabilities $\delta_{uj}, j \in \{1, \cdots, M\}$. This is obtained by maximizing (5) over $\delta_{uj}, j = \{1, \ldots, M\}$. It can be observed that the values of the probabilities which maximize (5) are the same values which maximize their individual probability distributions. Hence, the MLE of δ_{uj} is obtained by setting the derivative of $P(N_{uj} = n_{uj}|H_1)$ with respect to δ_{uj} to zero, under the constraint that $\delta_{uj} \geq 0$, i.e.,

$$\hat{\delta}_{uj} = \max\left(0, \frac{\frac{n_{uj}}{P_u} - \alpha_{uj}}{1-\alpha_{uj}}\right). \quad (10)$$

We now provide an upper bound on the variance of the estimate $\hat{\delta}_{uj}$. Since estimating the mean ($\hat{\mu}_{uj}$) and the variance ($\hat{\sigma^2}_{uj}$) of the estimate of δ_j ($\neq 0$) is difficult, we calculate bounds on both the mean and variance. Say, $\hat{\delta'}_{uj} = \frac{\frac{n_{uj}}{P_u} - \alpha_{uj}}{1-\alpha_{uj}}$ which implies that $\hat{\delta}_{uj} = \max(0, \hat{\delta'}_{uj})$. It can be seen that $\hat{\delta'}_{uj} \leq \hat{\delta}_{uj}$ which implies that $E[\hat{\delta'}_{uj}] \leq E[\hat{\delta}_{uj}]$. Also, $\hat{\delta'}^2_{uj} \geq \hat{\delta}^2_{uj}$ which implies that $E[\hat{\delta'}^2_{uj}] \geq E[\hat{\delta}^2_{uj}]$. Using these observations, the following can be inferred:

$$E[\hat{\delta}^2_{uj}] - (E[\hat{\delta}_{uj}])^2 \leq E[\hat{\delta'}^2_{uj}] - (E[\hat{\delta'}_{uj}])^2. \quad (11)$$

Hence, the bounds on the mean and the variance of $\hat{\delta}_j$ are as follows:

$$\hat{\mu}_{uj} \geq \mu'_{uj} \quad (12)$$

$$\hat{\sigma^2}_{uj} \leq \sigma'^2_{uj} \quad (13)$$

where $\mu'_{uj} \triangleq \delta_{uj}$ is the mean of $\hat{\delta'}_{uj}$ and $\sigma'^2_{uj} \triangleq \frac{\beta_{uj}(1-\delta_{uj})}{K_u(1-\alpha_{uj})}$ is the variance of $\hat{\delta}_{uj}$. Using (13) we get

$$\hat{\sigma^2}_{uj} \leq \frac{\beta_{uj}(1-\delta_{uj})}{K_u(1-\alpha_{uj})}. \tag{14}$$

It can be seen from (14) that the variance decreases as we increase K_u. Hence, for a higher K_u, a more accurate estimate is obtained, which is to be expected.

B. Intrusion Detection System Unicast - Downlink Packets

In this part of the section, we present the IDS for detecting an adversary affecting the unicast downlink packets. The intrusion detection system requires the IoT devices to execute the following additional tasks:

- Each IoT device D_j tracks the number of packets dropped (N_{dj}), out of the past K_d packets, due to a CRC check fail.
- **All the IoT devices will regularly update the trusted node about N_{dj}.**

1) Conditional Probability Distributions of Decision Statistics: We can assume the packet drops to be independent in the absence of an attack. When there is no attack, the packets are dropped with probability $\alpha_{dj}, j \in \{1, \cdots, M\}$ (i.e. the downlink PDP in the absence of attack), and hence the probability distribution of the variables $N_{dj}, j \in \{1, \cdots, M\}$ under H_0 are given as follows:

$$P(N_{dj} = k|H_0) = \binom{K_d}{k}(\alpha_{dj})^k(1-\alpha_{dj})^{K_d-k} \tag{15}$$

for $k \in \{1, \cdots, P_j\}$. When the relay is compromised, the PDPs of the devices increase to $\beta_{dj}, j \in \{1, \cdots, M\}$ which are given by:

$$\beta_{dj} = \delta_{dj} + (1-\delta_{dj})\alpha_{dj} \tag{16}$$

where $\delta_{dj}, j \in \{1, \cdots, M\}$ are unknown random variables. Using this, the probability distribution of the variables $N_{dj}, i \in \{1, \cdots, M\}$ under H_1 are given as follows:

$$P(N_{dj} = k|H_1) = \binom{K_d}{k}(\beta_{dj})^k(1-\beta_{dj})^{K_d-k} \tag{17}$$

for $k \in \{1, \cdots, P_j\}$. Similar to the uplink case, we can assume that the variables $N_{dj}, j \in \{1, \cdots, M\}$ are independent. Hence, the joint probability distribution under H_0 and H_1 is now defined below, where $N_d = [N_{d1}, \cdots, N_{dM}]$ and $n_d = [n_{d1}, \cdots, n_{dM}]$.

$$P(N_d = n_d|H_0) = \prod_{j=1}^{M} P(N_{dj} = n_{dj}|H_0). \tag{18}$$

Similarly, the joint probability distribution under H_1 is

$$P(N_d = n_d|H_1) = \prod_{j=1}^{M} P(N_{dj} = n_{dj}|H_1). \tag{19}$$

2) Detection Algorithm: Since the probability distribution of N_d under H_1 involves unknown random variables $\hat{\delta}_{dj}, j \in \{1, \cdots, M\}$, we now derive the detection algorithm using GLRT where the unknown variables are replaced by their MLEs $\hat{\delta}_{dj}, j \in \{1, \cdots, M\}$. This will be further elaborated on in Section III-B3. Since the probability distributions of N_d under both the hypotheses are similar to N_u, the detection algorithm obtained using GLRT decides in favor of H_1 when

$$S_d = \sum_{j=1}^{M} S_{dj} > \log(\gamma_d) = \Gamma_d \tag{20}$$

where $S_{dj} = n_{dj}\log(a_{dj}) + K_d\log(1-\hat{\delta}_{dj})$ and $a_{dj} = \frac{\hat{\beta}_{dj}}{\alpha_{dj}(1-\hat{\delta}_{dj})}$. $\hat{\beta_{dj}} \triangleq \hat{\delta}_{dj} + (1-\hat{\delta}_{dj})\alpha_{dj}$ is the MLE of β_{dj}.

3) Probability Estimation: The MLE of the probabilities $\delta_{dj}, j \in \{1, \cdots, M\}$ are obtained by maximizing (19) over $\delta_{dj}, j \in \{1, \cdots, M\}$. The MLE of δ_{dj} is obtained by setting the derivative of $P(N_{dj} = n_{dj}|H_1)$ with respect to δ_{dj} to zero, under the constraint that $\delta_{dj} \geq 0$, i.e.,

$$\hat{\delta}_{dj} = \max\left(0, \frac{\frac{n_{dj}}{K_d} - \alpha_{dj}}{1-\alpha_{dj}}\right). \tag{21}$$

for $j \in \{1, \cdots, M\}$. Since the expression in (21) is similar to (10), the bounds on the mean ($\hat{\mu}_{dj}$) and the variance ($\hat{\sigma^2}_{dj}$) of $\hat{\delta}_{dj}, j \in \{1, \cdots, M\}$ can be obtained and are as follows:

$$\hat{\mu}_{dj} \geq \delta_{dj} \tag{22}$$

$$\hat{\sigma^2}_{dj} \leq \frac{\beta_{dj}(1-\delta_{dj})}{K_u(1-\alpha_{dj})}. \tag{23}$$

It can be seen from (23) that the variance decreases as we increase K_d. Hence, for a higher K_d, a more accurate estimate can be expected, as in the unicast uplink case.

C. Intrusion Detection System - Broadcast Packets

In this part of the section, we present the IDS for detecting an adversary affecting the broadcast packets. The Intrusion Detection System requires the network to possess the following features:

- At regular intervals, to detect the presence of a malicious relay, each device D_j is required to send the feedback sequence $B_{ij}, i = \{1, 2, \ldots, K_b\}$ about every packet received. If the i^{th} packet is received successfully by D_j, then $B_{ij} = 0$, otherwise $B_{ij} = 1$.
- All the IoT devices will regularly update the trusted node about the observed number of packets dropped out of the past K_b packets. Therefore, the feedback received from the devices about the i^{th} packet is given by:

$$B_i = \{B_{i1}, \cdots, B_{iM}\}$$

1) Conditional Probability Distributions of Decision Statistics: The probability distribution of B_{ij}, in the absence of an attack, is given as follows:

$$P(B_{ij} = k|H_0) = (\alpha_{dj})^k(1-\alpha_{dj})^{(1-k)} \tag{24}$$

for $i \in \{1, \cdots K_b\}$, $j \in \{1, \cdots M\}$ and $k \in \{0, 1\}$. In the absence of an attack, we can assume that the packet drops by

different devices are independent. Hence, the variables $B_{ij}, i \in \{1, \cdots K_b\}$ and $j \in \{1, \cdots M\}$ are independent and the joint probability distribution under H_0 is:

$$P(B = b|H_0) = \prod_{i=1}^{P} \prod_{j=1}^{M} (\alpha_j)^{b_{ij}} (1 - \alpha_j)^{1-b_{ij}}$$

where $B = \{B_1, \cdots, B_{K_b}\}$ and $b = \{b_1, \cdots, b_{K_b}\}$. In the presence of an attack, if the i^{th} packet is corrupted by the adversary, it will be dropped by all the devices. Hence, the variables $B_{ij}, j \in \{1, \cdots, M\}$ cannot be independent. However, $B_i, i \in \{1, \cdots, K_b\}$ can be assumed to be independent from the assumption that the wireless channel is memoryless over time. Hence, the joint probability distribution under H_1 is given as follows:

- Firstly, we define the probability distribution of B_i. When the adversary does not corrupt the packet, the probability we observe B_i is given by the product of individual probability distributions of $B_{ij}, j \in \{1, \cdots, M\}$. However, when the adversary corrupts the packet, the packet will be dropped by all devices. Hence, the probability mass function of B_i is given as follows:

$$P(B_i = b_i|H_1) = (1 - \delta_b) \prod_{j=1}^{M} (\alpha_{dj})^{b_{ij}} (1 - \alpha_{dj})^{1-b_{ij}} + \delta_b \prod_{j=1}^{M} b_{ij} \quad (25)$$

- Since $B_i, i \in \{1, \cdots, K_b\}$ are independent, the joint probability distribution is given as follows:

$$P(B = b|H_1) = \prod_{i=1}^{P} P(B_j = b_j|H_1) \quad (26)$$

where $B = \{B_1, \cdots, B_{K_b}\}$ and $B = \{b_1, \cdots, b_{K_b}\}$.

2) Detection Algorithm: Since the probability distribution of B under H_1 involves an unknown random variable δ_b, we use the GLRT to obtain the decision rule. The parameter δ_b is now replaced with its MLE, $\hat{\delta}_b$. This will be further elaborated on in Section III-C3. The detection algorithm decides in favor of H_1 when

$$\frac{P(B = b|H_1)}{P(B = b|H_0)} > \gamma_b. \quad (27)$$

This can be simplified as follows:

$$S_b = K_b \log(1 - \hat{\delta}_b) + n_b \log(a_b) > \log(\gamma_b) \ = \Gamma_b \quad (28)$$

where $a_b = \frac{\hat{\beta}_b}{\alpha_b(1-\hat{\delta}_b)}$, $\alpha_b = \prod_{j=1}^{P} \alpha_{dj}$, $\hat{\beta}_b = \hat{\delta}_b + (1 - \hat{\delta}_b)\alpha_b$ and $N_b = n_b$ is the number of packets dropped by all the devices. To obtain the probability distribution for S_b required to define the detection statistics, the probability distribution of n_b is required. The same under H_0 is defined as follows:

- The probability that a specific packet is dropped by all the devices, under H_0, is equal to $\prod_{j=1}^{M} \alpha_j (\triangleq \alpha_b)$
- The probability that N_b packets are dropped by all the devices (out of the past K_b packets) is given as follows:

$$P(N_b = k|H_0) = \binom{K_b}{k} (\alpha_b)^k (1 - \alpha_b)^{K_b - k} \quad (29)$$

Similarly, under H_1, the probability distribution of N_b is given as follows:

$$P(N_b = k|H_1) = \binom{K_b}{k} (\beta_b)^k (1 - \beta_b)^{K_b - k} \quad (30)$$

where $\beta_b \triangleq \delta_b + (1 - \delta_b)\alpha_b$ is the probability that a specific packet is dropped by all the devices under H_1.

3) Probability Estimation: The MLE of the probability δ_b is obtained by maximizing (26) over δ_b. Hence, the MLE of δ_b is obtained by setting the derivative of $P(B = b|H_1)$ with respect to δ_b to zero, under the constraint that $\delta_b \geq 0$, i.e.,

$$\hat{\delta_b} = \max\left(0, \frac{\frac{n_b}{K_b} - \alpha}{1 - \alpha_b}\right). \quad (31)$$

Since the expression in (31) is similar to (10), the bounds on the mean ($\hat{\mu_b}$) and the variance ($\hat{\sigma_b^2}$) of $\hat{\delta}_{dj}$ can be obtained and are as follows:

$$\hat{\mu_b} \geq \delta_b \quad (32)$$

$$\hat{\sigma_b^2} \leq \frac{\beta_b(1 - \delta_b)}{K_b(1 - \alpha_b)}. \quad (33)$$

It can be seen from (33) that the variance decreases as we increase K_b. Hence, for a higher K_b, a more accurate estimate can be expected.

D. Performance Characteristics of the Algorithms

To evaluate the performance of the algorithm in (9), we use the false alarm and missed detection probabilities. The probability that the detection system decides on H_1 in the absence of an attack is defined as the false alarm probability (P_{FA}^k). The probability that the detection system decides on H_0 in the presence of an attack is defined as the missed detection probability (P_{MD}^k). We therefore have

$$P_{FA}^k = P(S_k > \Gamma_k|H_0) \quad (34)$$

$$P_{MD}^k = P(S_k \leq \Gamma_k|H_1). \quad (35)$$

for $k \in \{u, d, b\}$.

Firstly, we consider the unicast case. Using the expressions obtained for the estimated attack probabilities, the expressions obtained for the variables $S_{dj}, j \in \{1, \cdots, M\}$ and $S_{uj}, j \in \{1, \cdots, M\}$ are of the following form:

$$F = \begin{cases} n_t \log\left(\frac{n_t(1-\alpha_t)}{\alpha_t(K_t - n_t)}\right) + K_t \log\left(\frac{K_t - n_t}{K_t(1-\alpha_t)}\right), & \text{if } \frac{n_t}{K_t} > \alpha_t \\ 0, & \text{if } \frac{n_t}{K_t} \leq \alpha_t \end{cases}$$

We know that the probability distribution of n_t is binomial ($\mathcal{B}(\alpha_t, K_t)$) but finding the distribution of F is not trivial. Hence, it is difficult to find distribution of the variables $S_{dj}, j \in \{1, \cdots, M\}$ and $S_{uj}, j \in \{1, \cdots, M\}$ and therefore S_u and S_d. Exact analytical expressions for the detection statistics are thus unavailable. Note that the attack probabilities are zero under H_0, and so P_{FA}^u and P_{FA}^d are independent of the adversary parameters. However, for the threshold chosen to meet the desired false alarm probability value, the corresponding missed detection probability is a function of the attack probabilities. The proposed IDS's performance in terms of the missed detection probability will still be acceptable as long as

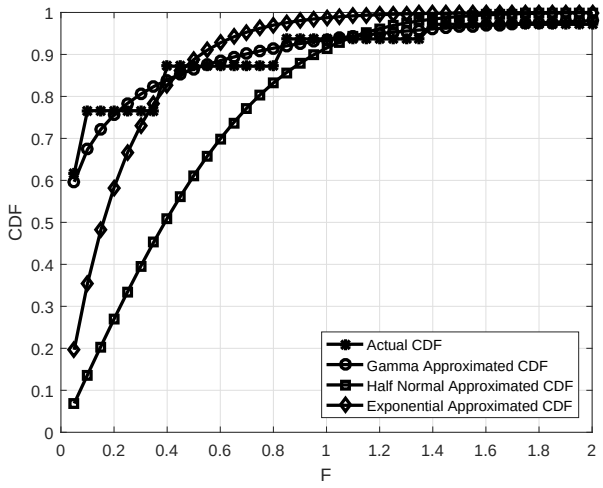

Fig. 2: Distribution Fitting Comparison

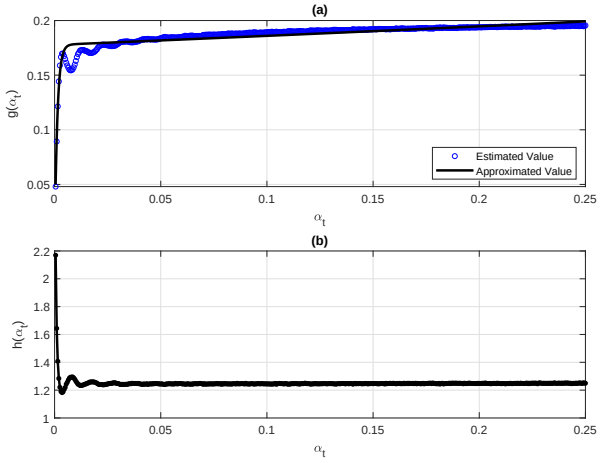

Fig. 3: (a) Shape parameter, $g(\alpha_t)$, variation with α_t. (b) Inverse scale parameter, $h(\alpha_t)$ variation with α_t.

attack probabilities are not too small, which we can assume to be true since otherwise, the attack would not be effective. Therefore, to find the thresholds, we need the expressions for false alarm probability for which the probability distributions of the variables S_u and S_d under H_0 are required.

Since the closed form distribution of F (under H_0) cannot be found, we approximate it with a Gamma distribution. The Gamma distribution can be a good fit because by adjusting its two parameters (shape parameter and inverse scale parameter), we can get PDFs of many different shapes for non-negative random variables, which F is. The same can be observed in Fig. 2, for $\alpha_t = 0.05$, where the discrepancy between the cumulative distribution function (CDF) of Gamma distribution fit and the actual CDF of F is less as compared to the other distributions. Therefore, once we find the parameters of the best fit Gamma distribution for F, we can then derive P_{FA}^u and P_{FA}^d, and hence the thresholds Γ_u and Γ_d necessary to achieve a desired false alarm probability.

We now numerically obtain the expressions for the parameters of the Gamma distribution of F, the shape parameter given by $g(\alpha_t)$ and the inverse scale parameter $h(\alpha_t)$. We followed the below procedure for the same:

- For every possible value of α_k generate 10^7 values of n_t for a fixed $K_t(= 100)$.
- Evaluate the corresponding value of F using the above values.
- For each α_t, using the generated 10^7 values of F, we fit it to Gamma distribution and obtain the corresponding parameters.

The values of $g(\alpha_t)$ and $h(\alpha_t)$ obtained as we vary α_t are shown in the Fig. 3(a) and 3(b). It can be observed from the plots that $h(\alpha_t)$ does not change much with varying α_t. Hence, we propose the value of $h(\alpha_t)$ to be constant (over α_t) and equal to 1.25 (the mean obtained) for $K_t = 100$. The expression for $g(\alpha_t)$ as a function of α_t is as follows:

$$g(\alpha_t) = 0.1777e^{0.4565\alpha_t} - 0.189e^{-786.1\alpha_t} \tag{36}$$

Using (36), we now approximate $S_{dj}, j \in \{1, \cdots, M\}$ and $S_{uj}, j \in \{1, \cdots, M\}$ as Gamma random variables (in the absence of attack i.e. under H_0) as shown below:

$$S_{uj} \sim \Gamma(g(\alpha_{uj}), 1.25) \tag{37}$$

$$S_{dj} \sim \Gamma(g(\alpha_{dj}), 1.25) \tag{38}$$

for $j \in \{1, \cdots, M\}$. Using the expressions obtained for S_u and S_d in (9) and (20) and the distributions obtained for $S_{dj}, j \in \{1, \cdots, M\}$ and $S_{uj}, j \in \{1, \cdots, M\}$ under H_0, the distributions for S_u and S_d under H_0 are as follows:

$$S_u \sim \Gamma(\alpha_\Gamma^u, 1.25) \tag{39}$$

$$S_d \sim \Gamma(\alpha_\Gamma^d, 1.25) \tag{40}$$

where $\alpha_\Gamma^u = \sum_{j=1}^{M} g(\alpha_{uj})$ and $\alpha_\Gamma^d = \sum_{j=1}^{M} g(\alpha_{dj})$.

For the broadcast case, it can be seen that the expression for S_b is similar to F. Hence, we approximate S_b with a Gamma distribution in the absence of attack as shown below:

$$S_b \sim \Gamma(\alpha_\Gamma^b, 1.25) \tag{41}$$

where $\alpha_\Gamma^u = g(\alpha_b)$.

E. Threshold Design

To obtain the threshold for the IDSs presented in (9), (20) and (28) the below procedure can be followed:

1) **For any given detection system, either the false alarm probability or the missed detection probability is fixed to obtain the parameters. In this paper, since we do not possess the analytical expressions for the missed detection probability, we use the false alrarm probability expressions for setting the threshold.**
2) **The desired false alarm probability, equal to ρ, is fixed and is user defined i.e. $P_{FA}^k = \rho, k \in \{u, b, d\}$.**
3) **Using (39), (40) and (41) we can now obtain the thresholds Γ_u, Γ_d and Γ_b by using the cumulative distribution function of the Gamma distribution such that**

$$P(S_k > \Gamma_k | H_0) = \rho, k \in \{u, b, d\}. \tag{42}$$

Device	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
α_{uj}	0.06	0.24	0.13	0.97	0.09	0.07	0.02	0.12
δ_{uj}	0.2	0	0	0	0.1	0	0	0.2

TABLE II: Parameters of the Devices - Unicast

Device	α_j
D_1	0.2547
D_2	0.2374
D_3	0.1272

TABLE III: Parameters of the Devices - Broadcast

The expressions for P_{FA} in (39), (40) and (41) depend on the number of devices reporting the feedback about the relay. If only the set $\mathcal{A} \subset \mathcal{D}$ of devices have reported, the expressions can be changed in negligible time and new threshold can be estimated. Therefore, the IDS presented in this paper can adapt to the feedback received automatically.

IV. Results

It can be observed from (9) and (20) that the detection algorithms for unicast uplink and downlink packets are similar. Hence, we present the results for the unicast uplink and broadcast cases only. We demonstrate the following, using simulations performed in MATLAB, in this section:

1) The upper bound to the variance of the estimated attack probabilities and the simulated variance are compared.
2) The expressions obtained for the false alarm probabilities are validated.
3) The impact of the adversary parameters on the performance of the proposed IDSs.
4) The performance of the IDSs proposed in the presence of compromised IoT devices.
5) **The performance of the IDS in (9) is compared against a naive scheme. The same can be extended to the IDSs in (20) and (28) and therefore not discussed.**

For the unicast scenario, we use a network setup with one access point, one relay and eight IoT devices associated with the relay. The value of K_u is 100. The simulated natural PDPs and attack probabilities on every device are given in Table II. For the broadcast scenario, we use a network setup with one access point, one relay and three IoT devices associated with the relay. The value of K_b is 100. The device PDPs used for generating the results are available in Table III.

A. Variance of the MLE Estimates

To demonstrate that the variance of the MLE estimate is close to the upper bound on its variance, for the unicast case, we ran the following steps:

- For a given value of δ_{u1}, we determine the number of packets dropped for the IoT Device D_1.
- We then calculate $\hat{\delta}_{u1}$ using (10).

Similarly, for the broadcast case, we ran the following steps to obtain the simulated variance of the MLE estimate of δ_b:

- For a given value of δ_b, we determine the number of packets dropped by all the IoT Devices.

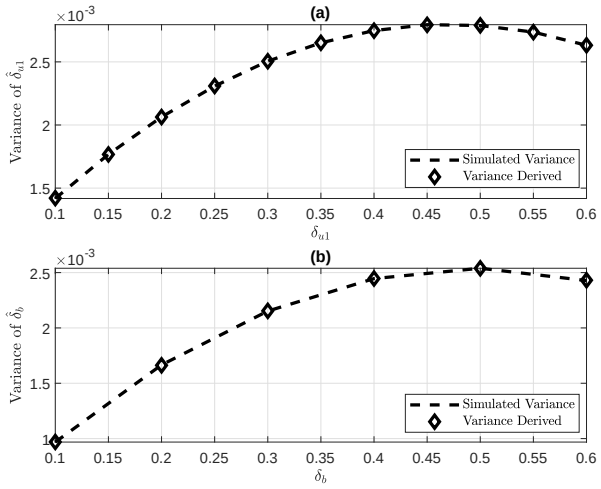

Fig. 4: (a) Sample Variance and Upper Bound of the Variance of attack probability $\hat{\delta}_{u1}$ (vs) δ_{u1} (b) Sample Variance and Upper Bound of the Variance of attack probability $\hat{\delta}_b$ (vs) δ_b.

- We then calculate $\hat{\delta}_b$ using (31).

The sample variances of $\hat{\delta}_b$ and $\hat{\delta}_{u1}$, for a given δ_b and δ_{u1}, are calculated using the estimates obtained from 10^7 Monte Carlo simulations. The results obtained are plotted in Fig. 4. It can be seen that the upper bound calculated is very close to the real estimated value for both the cases.

B. Performance Characteristics

Firstly, we validate the expressions obtained for P^u_{FA} and P^b_{FA}. For the same, we calculate P^u_{FA} and P^b_{FA} using the Gamma approximation (we term these as approximate P^u_{FA} and P^b_{FA}) and also using simulations (we term these as simulated P^u_{FA} and P^b_{FA}). To calculate the simulated P^u_{FA}, the following steps were followed:

- We setup the network using H_0, i.e., all the values of $\delta_{uj}, j \in \{1, \cdots, M\}$ are equal to zero. In every iteration, using simulations, we determine the number of packets dropped for every IoT Device and then calculate $\hat{\delta}_{uj}, j \in \{1, \cdots, M\}$ using (10).
- We then plug in the values in (9) and compare with a pre-defined threshold (Γ_u) to decide H_0 or H_1.

To calculate the simulated P^b_{FA}, the following steps were followed:

- We setup the network using H_0, i.e., the value of δ_b is equal to zero. In every iteration, using simulations, we determine the number of packets dropped by all devices.
- The values of $\hat{\delta}_b$ is calculated using (31).
- We then plug in the values in (9) and compare with a pre-defined threshold (Γ_b) to decide H_0 or H_1.

The simulated P^u_{FA} and P^b_{FA} values are obtained by averaging over 10^7 such Monte Carlo simulations. The results obtained are shown in Figure 5. It can be observed from Figure 5(a) that the discrepancy between the simulated P^u_{FA} and approximated P^u_{FA} is very small. The discrepancy observed between the approximated P^b_{FA} and the simulated P^b_{FA}, as can be observed

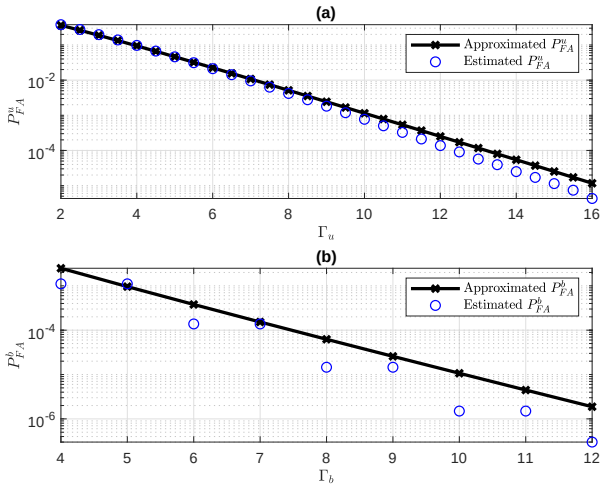

Fig. 5: (a) Approximated and Simulated P^u_{FA} (b) Approximated and Simulated P^b_{FA}.

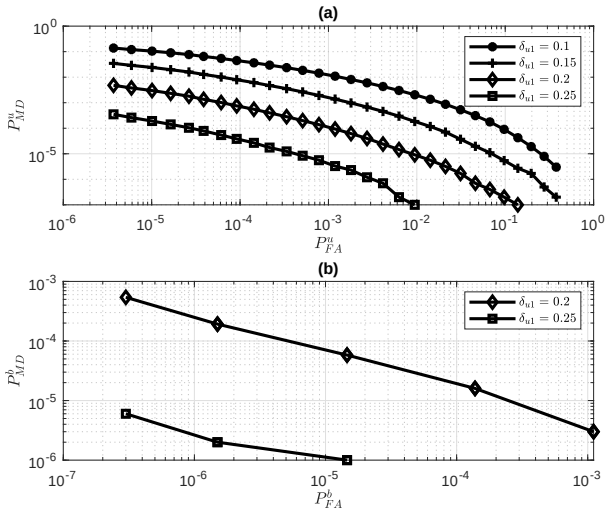

Fig. 6: (a) P^u_{MD} (vs) P^u_{FA} for different δ_{u1} (b) P^b_{MD} (vs) P^b_{FA} for different δ_b.

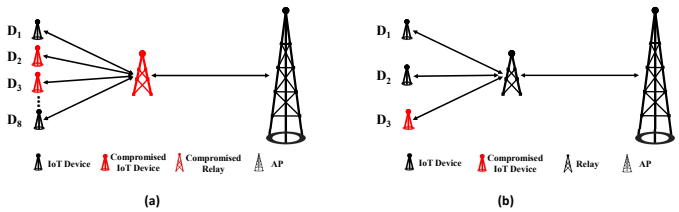

Fig. 7: (a) Adversary - Unicast (b) Adversary - Broadcast.

in Figure 5(b), at a few threshold (Γ_b) values is because we approximated a discrete random variable S_b with Gamma distribution.

A similar approach was carried out for obtaining the simulated P^u_{MD} and P^b_{MD} values with the only difference being that the network is setup using H_1. For the unicast case, to demonstrate the effect of the attack probability on P^u_{MD}, we varied δ_{u1}. For the broadcast case, we varied δ_b. The results obtained, shown in Fig. 6, depict that missed detection probability decreases with increasing attack probability for both the cases. Hence, there is a trade-off between the adversary's choice of attack probabilities and the probability of the attack being discovered. It can be observed that, the values of S_b and S_u increase in the presence of attack with an increase in the values of the attack probabilities. Hence, the gap between the values of S_b and S_u in the presence of attack and absence of attack increases. Therefore, for the same threshold, we can expect a better performance.

C. Performance in the presence of compromised IoT devices

In this section, we will be demonstrating the performance of the IDSs for possible adversary models other than the one mentioned in Section II-B. For the unicast case, we present the results for the uplink packets since the same can be extended for the downlink packets (due to the similarities in the IDSs).

1) Unicast IDS: Consider the network in Figure 7(a) where the adversary has compromised the relay R and devices D_2 and D_3. The adversary can now use the compromised relay to compromise the performance and use the compromised devices to send favourable readings about the relay and try to influence the IDS. In such a scenario, the feedback received from the devices is stated below:

- The set of IoT devices which are not compromised $\{D_1, D_4, \cdots, D_8\}$ transmit the readings observed at their respective end to the IDS computer.
- The set of IoT devices which are compromised $\{D_2, D_3\}$ falsify their feedback to indicate that the relay is not malicious. This can be achieved by generating the feedback using their individual probability distribution obtained under H_0 i.e. using (1).

To demonstrate the performance of the IDS in (9), we used the scenarios in Table IV. The performance characteristics obtained for the IDS in (9) are plotted in Fig. 8. It can be seen that the IDS is able to detect the attack even in the scenario 1 where only one affected device, D_1, is sharing honest feedback, with a detection probability almost equal to one. Therefore, the IDSs presented in (9) can be used to detect an adversary who has compromised the relay and a subset of IoT devices.

2) Broadcast IDS: Consider the network in Figure 7(b) where the adversary has compromised the device D_3 but not the relay. The adversary can now use the compromised device to send false readings about the relay and try to influence the IDS. To obtain the simulated false alarm probability, the following steps were followed:

- The devices D_1 and D_2 are transmitting the actual (and authentic) reading and D_3 is transmitting false readings. The false readings are generated in order to influence the IDS to classify the relay as malicious. The feedback is generated to make it appear that the device D_3 is experiencing a packet drop rate equal to δ_{mb}.
- In every iteration, using simulations, we determine the number of packets dropped by all IoT devices.
- The values of $\hat{\delta}_b$ is calculated using (31).

	δ_{u1}	δ_{u4}	δ_{u5}	δ_{u6}	δ_{u7}	δ_{u8}
Scenario 1	0.2	0	0	0	0	0
Scenario 2	0.2	0	0.1	0	0	0
Scenario 3	0.2	0	0.1	0	0	0.2

TABLE IV: Attack Probabilities

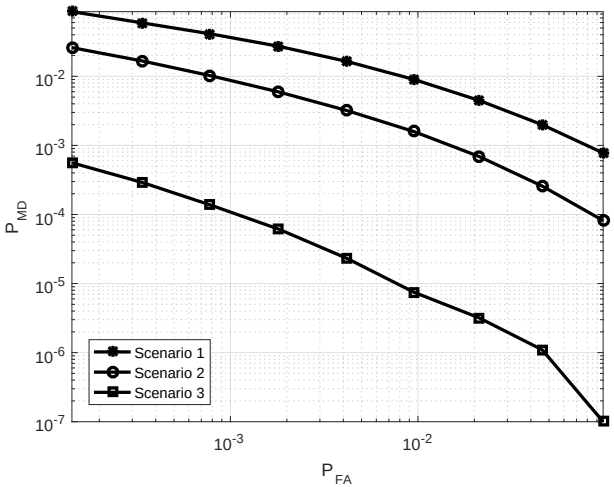

Fig. 8: Simulated P^u_{MD} (vs) P^u_{FA} for different scenarios

- We then plug in the values in (9) and compare with a pre-defined threshold (Γ_b) to decide H_0 or H_1.

The results obtained are plotted in Figure 9(a). Let us consider another scenario where the device D_2 is also compromised along with D_3. To obtain the false alarm probability for this scenario we followed similar approach with the only difference being that the device D_2 also generates false readings similar to D_3. The results obtained are plotted in Figure 9(b). From both the scenarios it can be concluded that the performance of the detection algorithm degrades with increasing number of compromised devices and/or increasing δ_{mb}. However, the performance will be reasonably good unless the number of compromised devices exceeds the number of the authentic devices and/or the value of δ_{mb} is large.

D. Comparison with a naive scheme

In this part of the section, we compare the detection algorithm obtained in (9) against a naive scheme based on the average number of packets retransmitted. The detection algorithm can be perceived as an aggregation of the feedback received from the IoT devices. The most common aggregation operator that can be used when such feedback is available is the average operator. In such a case the detection algorithm is implemented as follows:

1) **We first determine the average number of packets retransmitted $N_{ua} = \frac{1}{M}\sum_{j=1}^{M} N_{uj}$.**
2) **We then compare N_{ua} obtained in the previous step with a preset threshold (Γ_a) to determine if the relay is malicious or not i.e. we decide H_1 if and only if**

$$N_{ua} > \Gamma_a \tag{43}$$

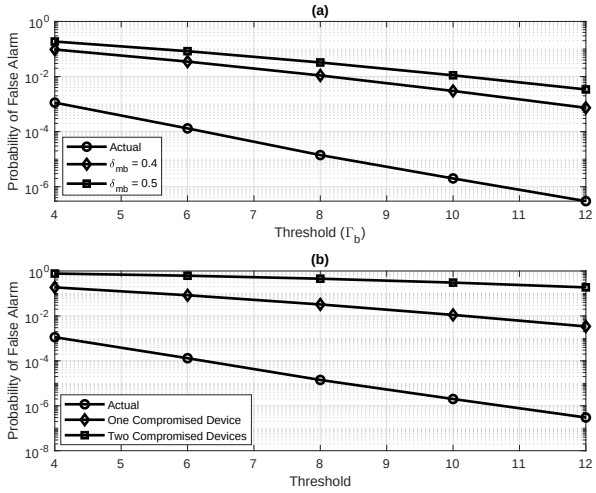

Fig. 9: (a) Simulated False Alarm Probability for varying δ_{mb} (b) Simulated False Alarm Probability for increasing number of compromised devices where $\delta_{mb} = 0.5$.

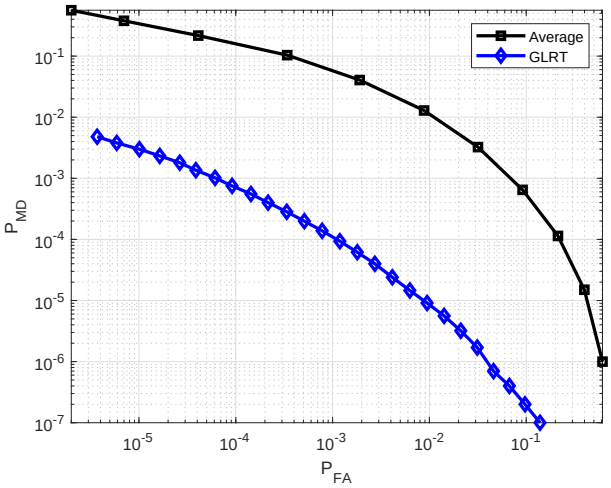

Fig. 10: Comparison with a naive scheme

The performance characteristics of our detection scheme in (9) and the detection scheme in (43) are plotted in Figure 10. The device PDPs used for generating the results are available in Table II. It can be seen from Figure 10 that our detection scheme outperforms the one presented in (43).

V. Conclusion and Future Work

A. Conclusion

A novel approach for detecting an adversary who has compromised the relay and corrupting the communication between an IoT device and the access point was presented. The detection method was derived using the generalized likelihood ratio test. To detect an adversary affecting unicast uplink packets, the detection rule was based on the number of unicast packets re-transmitted by the IoT devices and dropped at the relay. To detect an adversary affecting unicast downlink

packets, the detection rule was based on the number of unicast packets dropped by the IoT devices. To detect an adversary affecting broadcast packets, the detection rule was based on the number of broadcast packets dropped by all IoT devices. The adversary parameters (i.e. the attack probabilities) were obtained using maximum likelihood estimation. Results presented demonstrated the performance of the detection systems. We are able to achieve a negligible false alarm and missed detection probability for most cases. The tightness of the upper bound variance (of the MLEs) to the simulated variance (of the MLEs) was presented. The expressions obtained for the false alarm probabilities were validated using simulations. It was observed that the expressions obtained differed from the simulated values only very slightly. The performance of the IDSs for the case of adversaries who have compromised a subset of the IoT devices was also presented.

B. Directions for Future work

The unicast IDSs can be influenced when a situation similar to Figure 7(b) (where a subset of IoT devices are compromised) is considered. This can be done by generating the feedback using the probability distributions in (3) and (17). In such a case, the unicast IDSs presented in this paper would be misguided and hence would classify the relay as malicious. The broadcast IDS can be influenced when a situation similar to Figure 7(a) (where a subset of IoT and the relay are compromised) is considered. The compromised IoT devices are transmitting favorable feedback in order to influence the decision of the IDS. In such a case, the IDS presented in this paper has a good chance that it would be misguided and hence would classify the relay as authentic. Therefore, an interesting future work would be to identify an alternate approach to detect such attacks. Another strategy for an adversary to drain the batteries of the IoT devices, is by making the IoT devices transmit redundant packets at a high rate. By doing so, the awake time of the IoT devices increases and thus their battery life is adversely impacted. Therefore, another interesting future work would be to detect such adversaries using feedback based on the channel access time.

REFERENCES

[1] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, "A vision of iot: Applications, challenges, and opportunities with china perspective," *IEEE Internet of Things journal*, vol. 1, no. 4, pp. 349–359, 2014.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[3] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *Services, 2015 IEEE World Congress on*. IEEE, 2015, pp. 21–28.

[4] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*. IEEE, 2015.

[5] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," 2011. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[6] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer communications*, vol. 30, no. 14, pp. 2826–2841, 2007.

[7] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the internet of things," *Ad Hoc Networks*, vol. 32, pp. 17–31, 2015.

[8] M. Hossain, S. R. Islam, F. Ali *et al.*, "An internet of things-based health prescription assistant and its security system design," *Future Generation Computer Systems*, vol. 82, pp. 422–439, 2018.

[9] D. Azariadi, V. Tsoutsouras, S. Xydis, and D. Soudris, "Ecg signal analysis and arrhythmia detection on iot wearable medical devices," in *2016 5th International conference on modern circuits and systems technologies (MOCAST)*. IEEE, 2016, pp. 1–4.

[10] M. Collotta, L. L. Bello, and G. Pau, "A novel approach for dynamic traffic lights management based on wireless sensor networks and multiple fuzzy logic controllers," *Expert Systems with Applications*, vol. 42, no. 13, pp. 5403 – 5415, 2015.

[11] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, 2017.

[12] M. Zamani and M. Movahedi, "Machine learning techniques for intrusion detection," *arXiv preprint arXiv:1312.2177*, 2013.

[13] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," *Ad hoc networks*, vol. 11, no. 8, pp. 2661–2674, 2013.

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

[15] S. Lim and L. Huie, "Hop-by-hop cooperative detection of selective forwarding attacks in energy harvesting wireless sensor networks," in *Computing, Networking and Communications (ICNC), 2015 International Conference on*. IEEE, 2015, pp. 315–319.

[16] C. Tumrongwittayapak and R. Varakulsiripunth, "Detecting sinkhole attack and selective forwarding attack in wireless sensor networks," in *Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on*. IEEE, 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 Systems Journal*, 2016.

[18] F. Gara, L. B. Saad, and R. B. Ayed, "An intrusion detection system for selective forwarding attack in ipv6-based mobile wsns," in *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017, pp. 276–281.

[19] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the rpl-based internet of things," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, p. 794326, 2013.

[20] W. Meng, "Intrusion detection in the era of iot: Building trust via traffic filtering and sampling," *Computer*, vol. 51, no. 7, pp. 36–43, July 2018.

[21] N. Sehatbakhsh, M. Alam, A. Nazari, A. Zajic, and M. Prvulovic, "Syndrome: Spectral analysis for anomaly detection on medical iot and embedded devices," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, April 2018, pp. 1–8.

[22] H. Haddad Pajouh, R. Javadian, R. Khayami, A. Dehghantanha, R. Choo *et al.*, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in iot backbone networks," *IEEE Transactions on Emerging Topics in Computing*, 2016.

[23] D. H. Summerville, K. M. Zach, and Y. Chen, "Ultra-lightweight deep packet anomaly detection for internet of things devices," in *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*, Dec 2015, pp. 1–8.

[24] N. V. Abhishek, T. J. Lim, B. Sikdar, and A. Tandon, "An intrusion detection system for detecting compromised gateways in clustered iot networks," in *2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability*. IEEE, 2018, pp. 1–6.

[25] N. V. Abhishek, A. Tandon, T. J. Lim, and B. Sikdar, "Detecting forwarding misbehavior in clustered IoT networks," in *14th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (ACM Q2SWinet 2018)*, Montreal, Canada, Oct. 2018.

[26] R. Ratasuk, N. Mangalvedhe, and A. Ghosh, "Extending lte coverage for machine type communications," in *Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on*. IEEE, 2015, pp. 193–197.

[27] A. Tandon, T. J. Lim, and U. Tefek, "Sentinel based malicious relay detection scheme for wireless iot networks," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Dec 2018, pp. 1–6.

[28] S. M. Kay, "Fundamentals of statistical signal processing: Detection theory, vol. 2," 1998.

[29] S. M. Kay, "Fundamentals of statistical signal processing. vol 1, estimation theory," 1993.