An Intrusion Detection System for Detecting Compromised Gateways in Clustered IoT Networks

Nalam Venkata Abhishek, Teng Joon Lim, Biplab Sikdar and Anshoo Tandon
Department of Electrical and Computer Engineering, National University of Singapore
Email: abhishek_nalam@u.nus.edu, eleltj@nus.edu.sg, bsikdar@nus.edu.sg, dcsansh@nus.edu.sg

***Abstract*—It is well known that clustering IoT devices will help to alleviate the network scalability problem in IoT networks. However, clustering also provides an opportunity for an adversary to compromise a set of nodes by simply compromising their gateway. In such scenarios, one of the strategies available to an adversary to degrade the performance of a network is by corrupting the packets to be forwarded by the gateway. In this paper, a centralized detection system for detecting the presence of such a malicious gateway is proposed. The proposed system uses the packet drop probability as a means to monitor the gateways. An algorithm is presented to design the key parameters of the proposed system. Results are presented to verify the detection statistics and show the effectiveness of the system.**

I. Introduction

With the ability to automate everything around us and to the potential to generate extra revenue, the popularity of Internet of Things (IoT) is increasing day by day. Many applications like smart grid, smart home, intelligent transport system, etc. can be realized using IoT [1]. With more than fifty billion devices estimated to be connected to the Internet by 2020 [2], there is a need to revisit many issues like scalability, security, etc. To achieve the network scalability objective, researchers in the past have developed various clustering techniques [3]–[5]. In the case of a clustered network, each cluster is assigned a gateway which forwards the packets to and from the base station, assuming that a cellular architecture is used to provide Internet access to the IoT nodes. A node with superior resources is chosen as a gateway. Capturing or compromising the gateway would affect all the nodes in the cluster, and therefore, gateway security attacks need to be guarded against.

Inadequate hardware and energy resources inherent in IoT devices make them prone to various attacks [6]–[8] and also make it difficult to deploy many traditional security algorithms. Employing Intrusion Detection Systems (IDS) is therefore necessary to detect any malicious activity, in addition to other defenses like secured pairing, integrity verification and secured architectures. The three strategies for the deployment of an IDS are [8]:

1) **Centralized Intrusion Detection (CID) System:** The IDS is located at the base station (in case of a cellular architecture) or the access point (in case of wireless LANs). This approach adds extra latency to the network but helps in prolonging the battery life of the IoT device.
2) **Distributed Intrusion Detection (DID) System:** The IDS is located in every IoT device. No extra latency is incurred but it negatively impacts the lifetime of the IoT device.
3) **Hybrid Intrusion Detection (HID) System:** There are two types of such systems. The first one is where the IDS is hosted by the cluster head or the gateway. The second one is where additional nodes called monitor nodes are deployed to detect changes in the network.

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

One of the ways to degrade the performance of the network is by compromising the gateways and corrupting the communication between the nodes and the base station. Researchers in the past have tried to investigate the behavior of such nodes [9]–[14]. In [9], [10] the data is received over two different paths, and the two received messages are compared to determine the presence of any malicious forwarding node or relay (referred to as a gateway in this paper). In [11], tracing bits (whose location is not known to the gateway) are embedded into each packet sent by the node to detect the presence of malicious gateways. An optimization algorithm is also presented where the number of tracing bits and parity bits have to be balanced. In [13]–[16] the detection systems require the sensor nodes to listen to specific tracing signals for detection, which will lead to additional consumption of energy and bandwidth. **Machine learning algorithms presented in [17] can also be used to detect such malicious gateways but the performance is limited by the size of training data. Further, injecting packets into the network to build the training data may be difficult.** In [18], the author has proposed a mechanism which exploits the signal (sent to the relay by the node) overheard at the destination to classify the relay.

In this paper, the detection system presented does not require any training data and is based on theoretical foundations that have not been throughly explored in the existing literature. In comparison to a previous work in [19] we now propose a detection system which does not require the information to be sent to the base station (or the access point) via multiple paths (or via multiple relays). The key novelty behind the IDS proposed in this paper is to monitor the gateways by monitoring the downlink channel of the network.

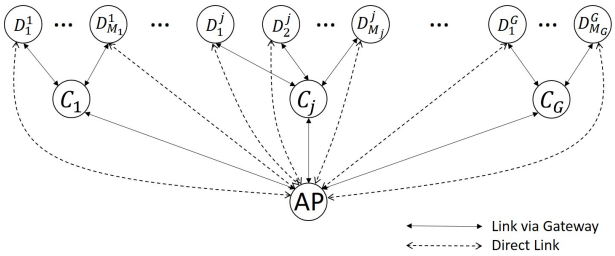

Fig. 1: Network Model Illustration.

Such scenarios with downlink channel being equally active as uplink are common in IoT networks that employ sensors, actuators and controllers for providing their services (e.g. Intelligent traffic lighting system [20]). Secondly, we use a side channel from the IoT device to the base station which will be elaborated upon later in the paper. Lastly, we present a method to estimate the parameters of the adversary required for the detection system.

The rest of the paper is organized as follows. In Section II, the network and the adversary models are described. In Section III, we propose the detection system, derive the expressions for the false alarm and miss detection probabilities, and design the key parameters of the system. In Section IV, results are presented to verify the detection statistics and show the effectiveness of the system. In Section V, we provide some concluding remarks and directions for future research.

II. System Model

A. Network Model

An IoT network with M IoT devices is considered. These devices are assumed to be clustered into G groups with each group having its own gateway. The IoT devices exchange information with a secured access point (AP) via the gateway. A set of IoT devices $\mathcal{M}_j = \{D_i^j, i = 1, \cdots, M_j\}$ have the device C_j as their gateway. Each device is connected to only one gateway i.e. $M_i \cap M_j = \emptyset$, for all $i \neq j$. All the nodes in the network use CSMA as the MAC protocol. The network model is illustrated in Fig. 1. One possible way to implement such a model is to follow the IEEE 802.11ah specification where the gateways in the network operate as "decode and forward" relays [21]. The dashed lines representing direct links between IoT devices and the AP are low-rate connections that may be enabled by the longer range of the HaLow system.

Whether the system is implemented with HaLow technology or not, it is assumed that every IoT device has the ability to directly communicate with the access point wirelessly. Before the IoT device associates itself with the access point, it will disassociate itself from its gateway. The same channel will be used by the proposed detection system which will be elaborated upon in Section III.

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 average packet drop probability (PDP) of a packet received by an IoT device D_i^j is assumed to be known and denoted by α_{ij} (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.

B. Adversary Model

We now describe the strategy employed by the adversary. Suppose that gateway C_j is compromised by the adversary. The adversary tries to disrupt the communication between the access point and IoT devices connected to C_j. This is achieved by corrupting a packet which needs to be forwarded either to the access point (uplink) or an IoT device (downlink), or both. In general, a received packet is said to be corrupted when at least one of the bits is received in error. The adversary can achieve this by executing either one or both of the following strategies:

1) The attacker can corrupt the channel pilots which are used for channel estimation and equalization. By sending modified pilots, the estimated channel will be incorrect and incorrect decoding of the bits in the payload will occur with a high probability. Such an attack has a low probability of detection because the transmitted PHY-layer frame appears to be valid.
2) The attacker can flip some of the bits of the physical layer payload. Such an attack is easier to implement than the one above, but is also easier to detect since the received PHY-layer frame will fail the cyclic redundancy check (CRC) almost surely.

A corrupted packet will be dropped and will have to be retransmitted. By deliberately introducing bit (and therefore packet) errors, the attacker can adversely impact the battery lifetime of the IoT devices and at the same time degrade the performance of the network as measured by other quality of service parameters such as throughput and delay.

Assume that there are g compromised gateways. Hence, the probability of a randomly selected gateway being compromised is given by:

$$q = \frac{g}{G}. \tag{1}$$

Each compromised gateway is assumed to corrupt the packet to be forwarded with a probability p. In the presence of such an attack, a packet can be dropped either due to the network non-idealities or the action of the gateway. Hence, the packet drop probability observed by an IoT device D_i^j communicating to the AP via malicious gateway is given by:

$$\beta_{ij} = p + (1 - p)\alpha_{ij} \tag{2}$$

III. Intrusion Detection System

In this section, we present our intrusion detection system (IDS) which is to be established at the access point. The IDS will identify the presence of any malicious gateway implementing the attack mentioned in Section II-B. In the

presence of an attack, it is evident from (2) that the PDP increases due to the malicious nature of the gateway. Hence, we use the observed PDP as a decision statistic to identify a malicious gateway. The IDS algorithm for gateway C_j performs a binary hypothesis test with the following hypotheses:

- H_0: Gateway C_j is not compromised
- H_1: Gateway C_j is compromised.

Given the description of the adversary in Section II-B, the prior probabilities of the hypotheses are:

$$P(H_0) = 1-q \quad (3)$$
$$P(H_1) = q. \quad (4)$$

The intrusion detection system requires the IoT devices to execute the following additional tasks:

1) All the IoT devices will track the number of packets dropped at their respective ends.
2) A set of devices $\mathcal{S}_j \subseteq \mathcal{M}_j$ will regularly update the access point about the observed number of packets dropped using the side channel mentioned in Section II-A. The design of $\mathcal{S}_j$ will be discussed later in the paper.

A. Detection Algorithm

We now derive the IDS for gateway C_j. Denote the number of downlink packets dropped by the IoT device D_i^j out of a total of N packets by N_{ij} (where $i = 1, 2, \cdots, S_j$). Since the packet drops are assumed to be independent under H_0, the probability distributions of $N_{ij}, i \in \{1, \cdots, S_j\}$ follow the binomial distribution and are defined as follows:

$$P(N_{ij} = k|H_0) = \gamma_{0,ij}(k) = \binom{N}{k}(\alpha_{ij})^k(1-\alpha_{ij})^{N-k} \quad (5)$$

We can assume that the wireless channels used by the nodes in the network are independent. Using this assumption the probability distributions of the variables $N_{ij}, i \in \{1, \cdots, S_j\}$ are independent. The joint probability distribution is now defined below, where $N_j = [N_{1j}, \cdots, N_{S_jj}]$ and $n_j = [n_{1j}, \cdots, n_{S_jj}]$.

$$P(N_j = n_j|H_0) = \prod_{i=1}^{S_j} \gamma_{0,ij}(n_{ij}). \quad (6)$$

Similarly, in the presence of an attack on gateway C_j, the individual distributions of the variables $N_{ij}, i \in \{1, \cdots, S_j\}$ are:

$$P(N_{ij} = k|H_1) = \gamma_{1,ij}(k) = \binom{N}{k}(\beta_{ij})^k(1-\beta_{ij})^{N-k} \quad (7)$$

where β_{ij} is defined in (2). The joint distribution of the variables $N_{ij}, i \in \{1, \cdots, S_j\}$, in the presence of an attack on C_j that randomly chooses packets to corrupt with probability p, is:

$$P(N_j = n_j|H_1) = \prod_{i=1}^{S_j} \gamma_{1,ij}(n_{ij}). \quad (8)$$

The Likelihood ratio test (LRT) [22], which is known to maximize the probability of detection for any given probability of false alarm, gives us the detection rule. The likelihood ratio is denoted by $L(n_j)$. The LRT decides in favor of H_1 if and only if the following holds:

$$L(n_j) = \frac{P(N_j = n_j|H_1)}{P(N_j = n_j|H_0)} > \gamma \quad (9)$$

$$\Rightarrow \prod_{i=1}^{S_j} \frac{(\beta_{ij})^{n_{ij}}(1-\beta_{ij})^{N-n_{ij}}}{(\alpha_{ij})^{n_{ij}}(1-\alpha_{ij})^{N-n_{ij}}} > \gamma \quad (10)$$

$$\Rightarrow \prod_{i=1}^{S_j} a_{ij}^{n_{ij}} > \gamma b \quad (11)$$

$$\Rightarrow W_j = \sum_{i=1}^{S_j} n_{ij}\log(a_{ij}) > \log(\gamma b) = T_j \quad (12)$$

where,

$$a_{ij} = \frac{\beta_{ij}}{\alpha_{ij}(1-p)} \text{ and } b = \left(\frac{1}{1-p}\right)^{NS_j}.$$

The design of the threshold T_j will be discussed in a later section.

We now derive the maximum likelihood estimates (MLE) of the probabilities p and q [23]. The MLE will be based on the joint probability distribution of the variables $N_j, j \in \{1, \cdots, G\}$. The probability mass function $P(N_j = n_j) = \gamma_j(n_j)$ can be calculated as follows $\forall j \in \{1, 2, \cdots G\}$:

$$\begin{aligned}\gamma_j(n_j) =& P(N_j = n_j|H_0)P(H_0) \\ &+ P(N_j = n_j|H_1)P(H_1) \\ =& (1-q)\prod_{i=1}^{S_j}\gamma_{0,ij}(n_{ij}) + q\prod_{i=1}^{S_j}\gamma_{1,ij}(n_{ij}) \end{aligned} \quad (13)$$

The joint probability mass function of the variables $N_j, j \in \{1, \cdots, G\}$ is now defined below:

$$P(N_1 = n_1, \cdots, N_G = n_G) = \prod_{j=1}^{G}\gamma_j(n_j) \quad (14)$$

By maximizing the PMF in (14), we can estimate the probabilities p and q. One of the possible ways to find the values of p and q is by **solving the problem numerically**. The estimated values are given by $\hat{p}$ and $\hat{q}$.

B. Performance of the IDS

To characterize the performance of the IDS for gateway C_j using the decision rule in (12), one generally uses the false alarm (P_j^{FA}) and miss detection (P_j^{MD}) probabilities. Using the expressions of these probabilities, the system parameters S_j and T_j are also designed to minimize P_j^{MD} for a given maximum allowable P_j^{FA}. The probability that the detection system decides on H_1 in the absence of an attack is defined as the false alarm probability. The probability that the detection system decides on H_0 in the presence of an attack is defined as the the miss detection

probability. In this subsection, we derive the expressions for these two probabilities, for an ideal case where probability p is estimated without error, as follows:

$$P_j^{FA} = P(W_j > T_j|H_0) \tag{15}$$

$$P_j^{MD} = P(W_j \leq T_j|H_1). \tag{16}$$

For sufficiently large N, the binomially distributed variables $N_{ij}, i \in \{1, \cdots, S_j\}$ become approximately Gaussian due to the Central Limit theorem under both the hypotheses. In other words, under H_0, $N_{ij} \sim \mathcal{N}(N\alpha_{ij}, N\alpha_{ij}(1-\alpha_{ij}))$ and under H_1, $N_{ij} \sim \mathcal{N}(N\beta_{ij}, N\beta_{ij}(1-\beta_{ij}))$, as $N \to \infty$. The sum W_j in (12) then becomes a linear combination of i.i.d. Gaussian random variables, and is itself Gaussian. The mean and variance of W_j under hypothesis H_0 are $\mu_{j,h0}$ and $\sigma^2_{j,h0}$ respectively and under hypothesis H_1 are $\mu_{j,h1}$ and $\sigma^2_{j,h1}$ respectively. These are easily shown to be:

$$\mu_{j,h0} = \sum_{i=1}^{S_j} N\alpha_{ij} \log(a_{ij})$$

$$\sigma^2_{j,h0} = \sum_{i=1}^{S_j} N\alpha_{ij}(1-\alpha_{ij})(\log a_{ij})^2$$

$$\mu_{j,h1} = \sum_{i=1}^{S_j} N\beta_{ij} \log(a_{ij})$$

$$\sigma^2_{j,h1} = \sum_{i=1}^{S_j} N\beta_{ij}(1-\beta_{ij})(\log a_{ij})^2.$$

Hence, the approximate values of P_j^{FA} and P_j^{MD} can be calculated as:

$$P_j^{FA} = Q\left(\frac{T_j - \mu_{j,h0}}{\sigma_{j,h0}}\right) \tag{17}$$

$$P_j^{MD} = 1 - Q\left(\frac{T_j - \mu_{j,h1}}{\sigma_{j,h1}}\right) \tag{18}$$

where,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{u^2}{2}\right) du.$$

C. Threshold Design

Since the IoT devices have limited battery storage, it is desirable to have only a subset of them to report their N_{ij} in order to limit the adverse impact on the battery lifetime. This would also limit the number of side channels required from the IoT devices to the AP. To find the minimum number of IoT devices that should report to the access point about their gateway, we solve the following optimization problem:

$$\text{Minimize } S_j \tag{19}$$

$$\text{Subject to } P_j^{FA} \leq \epsilon_1 \tag{20}$$

$$P_j^{MD} \leq \epsilon_2. \tag{21}$$

Since the constraints are not elementary expressions, we propose to solve the problem numerically. To estimate the optimum value of S_j, we first initialize the set $\mathcal{S}_j$ to $\mathcal{M}_j$. Then, using the Neyman-Pearson lemma [24], we find the threshold that minimizes the miss detection probability and also satisfies Constraint (20). According to this lemma, the miss detection probability is minimized when $P_j^{FA} = \epsilon_1$. If the value of P_j^{MD} obtained satisfies the Constraint (21), then the device which has the least battery life is removed from $\mathcal{S}_j$. After this, the process is repeated for the new set $\mathcal{S}_j$. This will continue till the Constraint (21) is violated, at which point the algorithm stops. The cardinality of the set before the last device was removed is the optimum value of S_j. **The performance of this proposed algorithm will be discussed in our future work.**

Sub case	RMSE ($\hat{p}$)	RMSE ($\hat{q}$)
(1)	0.0364	0.0480
(2)	0.0273	0

TABLE I: RMSE - Estimates of Adversary parameters

IV. Results

In this section, we present a number of simulation results. The simulations were performed using MATLAB. We first present the effectiveness of the estimation algorithm using the root mean square error (RMSE) for a network setup having one access point, four gateways and four IoT devices under each gateway. In the network adopted, two out of the four gateways are malicious. Hence, from (1) it is evident that q is set to 0.5. The value of N is set to 50. The downlink SNR used for generating the results is $20dB$ for all the nodes. We consider two sub cases in this scenario:

1) Probability p is set to 0.25.
2) Probability p is set to 0.75.

The values of $\hat{p}$ and $\hat{q}$ obtained over 50×10^4 Monte Carlo simulations for both the sub cases are shown in the histogram plotted in Figure 2. The RMSE obtained for both the sub cases are tabulated in Table I. From the RMSE values obtained, it is evident that the residual variance between the actual value and estimated values is significantly less.

We now present our simulation results to verify the derived detection statistics in (17) and (18). For the same, we used a network which has one access point, two gateways and five IoT devices associated with each gateway and placed equidistant from their respective gateways. One of the two gateways in the network is malicious. The downlink SNR used for generating the results is $20dB$ at all the nodes. To verify the false alarm and miss detection probabilities in (17) and (18), we obtained the simulated probabilities by averaging over 10^6 Monte Carlo simulations for the scenario where the attack probability p was set to 0.2 and the value of N to 100. In this case, all the IoT devices are used in the IDS algorithm. The results are plotted for the following sub cases:

1) Probability p is estimated using the method presented in Section III-A.
2) Probability p is assumed to be perfectly known.

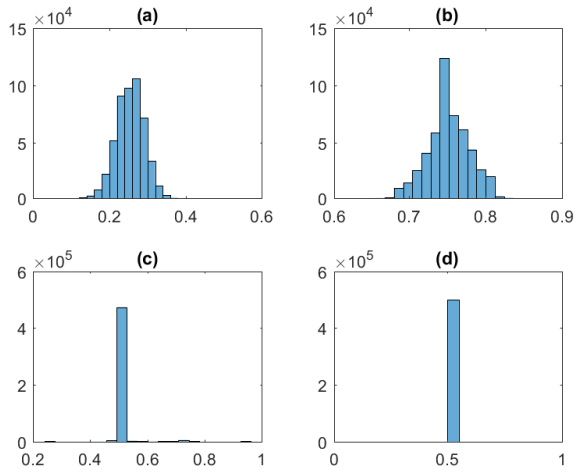

Fig. 2: (a) Histogram of $\hat{p}$ when actual values of p and q are 0.25 and 0.5. (b) Histogram of $\hat{p}$ when actual values of p and q are 0.75 and 0.5. (c) Histogram of $\hat{q}$ when actual values of p and q are 0.25 and 0.5. (d) Histogram of $\hat{q}$ when actual values of p and q are 0.75 and 0.5.

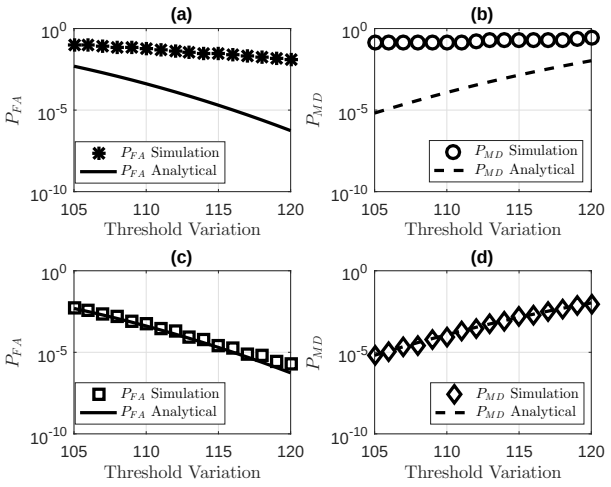

Fig. 3: (a) Simulated and Analytical P_{FA} using estimated p. (b) Simulated and Analytical P_{MD} using estimated p. (c) Simulated and Analytical P_{FA} using perfectly known p. (d) Simulated and Analytical P_{FA} using perfectly known p.

The false alarm probability curve corresponds to the unattacked gateway and the miss detection curve corresponds to the compromised gateway. The probabilities obtained using the simulation results and the analytical results calculated using the approximations derived in (17) and (18) for the scenario are shown in Fig. 3. It can be observed from Fig. 3(c) and 3(d) that the false alarm and miss detection probabilities obtained using (17) and (18) are reflected accurately in the simulation results when the probability p is assumed to be perfectly known. Whereas in Fig. 3(a) and

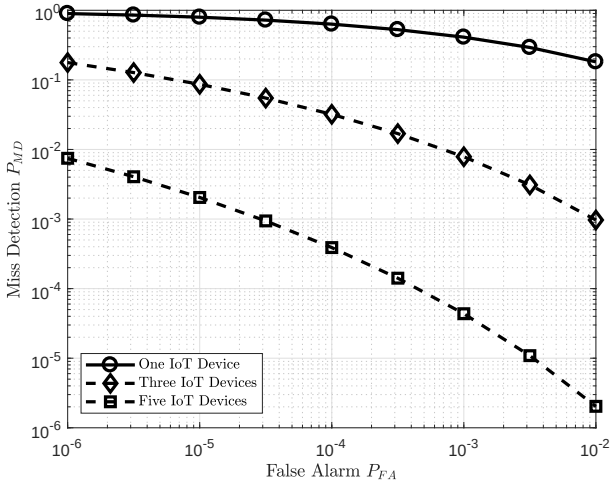

Fig. 4: Performance of the IDS - comparison. Attack Probability is set to 0.2.

3(b) where the probability p is being estimated, the false alarm and miss detection probabilities seem to deviate from the analytically obtained values. This is mainly due to the erroneously obtained $\hat{p}$ **because of the finite sample size (N).**

We now present the effect of incorporating more nodes in the detection system using a network which has one access point, one gateway and five IoT devices associated with the gateway. The attack probability p is set to 0.2. The downlink SNR used for generating the results is $20dB$ for all the nodes. We consider three sub cases in this scenario:

1) Only one IoT Device is used in the IDS algorithm.
2) Three IoT devices are used in the IDS algorithm.
3) Five IoT devices are used in the IDS algorithm.

Using the derived analytical results in (17) and (18), we have presented the variation of the miss detection probability w.r.t. various false alarm probabilities in Fig. 4. It can be observed from both the figures that for a given false alarm probability, the miss detection probability decreases as the number of nodes increases.

To prove the effectiveness of the proposed IDS, we compared it with the detection system presented in [18]. The network setup adopted for comparison has one access point, one gateway and five IoT devices placed equidistant from the gateway. It can be observed from [18] that for false alarm probabilities ranging from 10^{-3} to 10^{-1}, the miss detection probabilities vary between 10^{-3} and 10^{-1}. To compare the performance of our IDS, we used the analytical approximations derived in (17) and (18). We varied the false alarm probabilities for the attack probabilities 0.1, 0.15 and 0.2 to calculate the corresponding miss detection probability. The obtained results are shown in Fig. 5. It is evident from the figure that for our proposed detection system, when the attack probability is greater than 0.1, we obtain lower miss

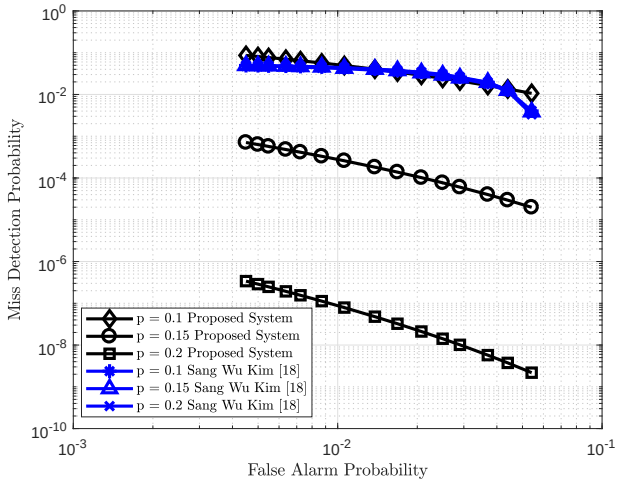

Fig. 5: Performance of the IDS - comparison

detection probabilities for the same false alarm probabilities.

V. Conclusion and Future Directions

A novel approach for detecting an adversary who is corrupting the communication between an IoT device and the access point by compromising the gateway is presented. The condition for detection is derived using the likelihood ratio test and is based on the number of packets dropped by the IoT devices. The estimates for the probabilities p and q are obtained using Maximum Likelihood Estimation. An algorithm for designing the key parameters for optimum performance of the system is presented. Results presented verify the derived statistics when the probability p is assumed to be perfectly known and also prove the effectiveness of the system by comparing with previous work.

In this paper, we assume that the packet is corrupted at the PHY layer. As a part of our future work, we would consider an attack where the adversary is changing the data without affecting the protocol. In this paper, it is also assumed that the IoT devices are secure i.e. they are not compromised by the adversary. As a part of our future work, we will evaluate the effectiveness of this algorithm when a fraction of the devices are compromised and update incorrect information about the gateway to the access point. **We have not considered the situation where the malicious gateways can affect the uplink packets of the IoT devices. We will be addressing this problem in our future work.**

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] 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

[3] 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.

[4] O. Younis and S. Fahmy, "Heed: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on mobile computing*, vol. 3, no. 4, pp. 366–379, 2004.

[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on wireless communications*, vol. 1, no. 4, pp. 660–670, 2002.

[6] 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 (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015.

[7] 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.

[8] 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.

[9] S. Dehnie, H. T. Sencar, and N. Memon, "Detecting malicious behavior in cooperative diversity," in *Information Sciences and Systems, 2007. CISS'07. 41st Annual Conference on*. IEEE, 2007, pp. 895–899.

[10] R. Cao, E. Graves, T. F. Wong, and T. Lv, "Detecting substitution attacks against non-colluding relays," in *Global Communications Conference (GLOBECOM), 2013 IEEE*. IEEE, 2013, pp. 1856–1861.

[11] T. A. Khalaf, S. W. Kim, and A. E. Abdel-Hakim, "Tradeoff between reliability and security in multiple access relay networks under falsified data injection attack," *IEEE transactions on information forensics and security*, vol. 9, no. 3, pp. 386–396, 2014.

[12] C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.-F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks [wireless sensor networks]," in *Wireless Communications and Networking Conference*, vol. 4. IEEE, 2005, pp. 1927–1932.

[13] Y. Mao and M. Wu, "Tracing malicious relays in cooperative wireless communications," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 2, pp. 198–212, 2007.

[14] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 4, pp. 744–757, 2010.

[15] L.-C. Lo, W.-J. Huang, R. Y. Chang, and W.-H. Chung, "Noncoherent detection of misbehaving relays in decode-and-forward cooperative networks," *IEEE Communications Letters*, vol. 19, no. 9, pp. 1536–1539, 2015.

[16] L.-C. Lo and W.-J. Huang, "Misbehavior detection without channel information in cooperative networks," in *Vehicular Technology Conference (VTC Fall), 2011 IEEE*. IEEE, 2011.

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

[18] S. W. Kim, "Physical integrity check in cooperative relay communications," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6401–6413, 2015.

[19] C. Jia and T. J. Lim, "Detecting cluster head attacks in heterogeneous wireless sensor networks," in *Vehicular Technology Conference (VTC Spring), 2017 IEEE*. IEEE, 2017.

[20] 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.

[21] "802.11ah-2016 - 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," 2017.

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

[23] ——, "Fundamentals of statistical signal processing. vol 1, estimation theory," 1993.

[24] J. Neyman and E. Pearson, "On the problem of the most efficient tests of statistical hypotheses," *Philosophical Transactions of the Royal Society*, vol. 231, pp. 289–337, 1933.