The Korean Institute of
Communications and
Information Sciences

Available online at www.sciencedirect.com
ScienceDirect
ICT Express 6 (2020) 353–356
www.elsevier.com/locate/icte

Users emulation attack management in the massive internet of things enabled environment

Samuel D. Okegbile[a,b,*], Olabisi I. Ogunranti[c]

[a] Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa
[b] Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria
[c] Longbridge Technologies, Nigeria

Received 10 December 2019; received in revised form 19 June 2020; accepted 23 June 2020
Available online 3 August 2020

Abstract

Users' emulation attacks are a prominent denial of service attack capable of degrading the entire performance of the network. In this paper, the detection and control of users' emulation attacks in the massive internet of things networks were considered. An efficient power-based signal to interference ratio (SIR) approach was proposed to characterize the attackers' behavior in the system. The trust list table was also adopted to further improve the detection of malicious nodes (MNs). The proposed approach shows an improved performance when compared with the conventional energy detection based approach which did not capture the channel interference in the system modeling. Through the received SIR, MNs can be identified owing to the higher transmission power required to disrupt the network.

Keywords: Emulation attack; Internet of things; Malicious user; Success probability; Trust list table

1. Introduction

Security in Internet of Things (IoT) enabled devices and environment is an important issue due to the ability of the intruders or malicious users to compromise the IoT enabled systems in the absence of adequate and sufficient security measures. It is hence not surprising that the area has recently been attracting a myriad of attention. As reported in [1], about twenty-four million devices are expected to be connected as IoT devices by the year 2020. Most of these devices carry sensitive data and information and the need to ensure data security, integrity, and confidentiality remains an important issue. IoT devices must be protected against sophisticated attacks as this is important to ensure confidentiality and integrity for next-generation devices [2].

Massive IoT networks contain devices connected together for appropriate transmissions and receptions and such networks are susceptible to user's emulation attacks. The user's emulation attack means a typical malicious device pretends to be a legitimate device with the aim of securing illegal access to the network. With access to the network, such an attacker can compromise the entire network or compromise data and information residing at few nodes. Although, IoT devices are resource-limited, identifying their security needs and requirements are very important for the next generation devices [3]. However, most of the preliminary security mechanisms are inappropriate for IoT networks when energy consumption, scalability, and processing power is important while user's emulation attacks are known to be a prominent denial of service attack which is capable of degrading the entire performance of the network. Hence, we consider the detection and control of users' emulation attacks in massive IoT networks.

A software-defined network gateway approach was proposed in [4] to enhance centralized control in the IoT network. Similarly, the authors in [3] proposed a physical unclonable function-based lightweight security system for IoT environment. Existing efforts have shown that security in IoT still remains a major challenge [5]. Blockchain solutions were proposed in [5], though such solutions involve high computation energy and delay. The authors in [6] adopted a Neyman–Pearson composite hypothesis test to identify the presence of

[*] Corresponding author at: Department of Electrical, Electronic and Computer Engineering, University of Pretoria, South Africa.

E-mail addresses: samokegbile@gmail.com (S.D. Okegbile), olabisiogunranti@gmail.com (O.I. Ogunranti).

Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2020.06.005

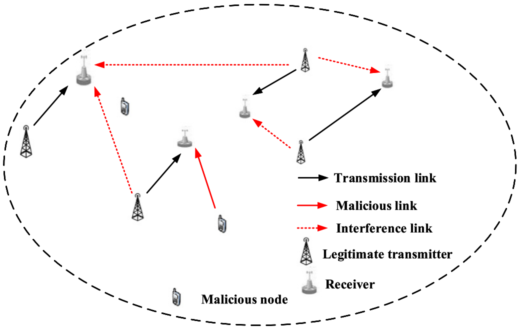

Fig. 1. IoT devices location.

primary user (PU) emulation attacks in the cognitive radio network. A game theory approach was also adopted to differentiate between the real PU and the PU emulation attack in [7]. Similarly, energy detection approach was considered in [8,9] while various efficient IoT security measures and architectures were discussed in [10–12]. The importance and goals of trust management in IoT were further discussed in [11]. To the best of our knowledge, users' emulation attacks in massive IoT networks have not received the deserved attention despite its importance. This paper hence presents a security mechanism capable of preventing users' emulation attacks in massive IoT. Our approach relies on the use of the signal to interference ratio (SIR) received from a typical node and the trust list table to detect malicious users. The spatial distributions of nodes are well captured in the analysis. The approach is energy efficient and is suitable for the dynamic nature of the massive IoT networks.

2. System model

We considered a typical environment where legitimate transmitting devices (LTDs) are distributed following Poisson point process (PPP) Φ of intensity μ with each LTD ($L_i \in \Phi$) assumed to be located at the origin of a disk of radius R, where R is the coverage region radius of any LTD. Each LTD communicates with its corresponding receiver located uniformly at a distance r_L ($r_L \leq R$) from the origin of the disk. In a massive IoT, many legitimate transmitters will be connected to their respective receivers as shown in Fig. 1, hence, interference is experienced at any typical receiver from other active LTDs. Although each receiver is uniformly distributed within R of its paired LTD, static positional information has been shown in [13] to provide a close approximation of the dynamic nature of such a network. As a result of this, we considered a SIR threshold-based approach where the transmission of any LTD is successful if the received SIR at the corresponding paired receiver is at least a predefined SIR threshold ψ, i.e.

$$T_{suc} = P(SIR \geq \psi). \tag{1}$$

It is worth noting that in such a network, a malicious device can disrupt the network in two ways:

- Single node disruption (SND) — A typical malicious device pretends to be the LTD thereby transmitting malicious information to the paired receiver. By accepting malicious data from the device, the information in such a receiver is corrupted, hence compromising data integrity at such a receiver.
- Network disruption — A typical malicious device pretends to be an LTD and transmits with a transmit power $P_{mal} > P_L^{\max}$ with the intention of disrupting the network activities by causing higher interference in the entire network. $P_L^{\max}$ is the maximum allowable transmit power for any LTD.

We assumed that $P_L^{\max}$ is carefully selected to ensure transmission success at any receiver from its paired LTD, while ensuring that the aggregate interference I_{agg} in the channel is below the pre-defined interference threshold I_d in the absence of noise. The conditions for network stability are given as follows:

- Transmit power of each LTD $P_L \leq P_L^{\max}$,
- Aggregate interference in any channel $I_{agg} \leq I_d$.

Assumption 1. Any typical malicious node (MN) influences the network with $P_{mal} > P_L^{\max}$.

Remarks. If any MN transmits with $P_{mal} \leq P_L^{\max}$, such a MN cannot disrupt the network stability and any receiver cannot determine whether such intending transmitting node is LTD or MN using the SIR level. This type of attack will be detected using the trust list table presented in the next section. SND can be determined using the trust list table — a table that contains information about previous activities of all transmitting nodes.

3. Analysis

We now provide an analysis of the proposed scheme in this section. We first considered first-level verification, i.e. SIR threshold-based analysis, and then presented the use of a trust list table for capturing single node disruption cases as second-level verification.

Assumption 2. MNs are detected based on the received SIR at the user emulation detector (UED) and the previous records of nodes on the trust list table. The UED can be any node designated to remove MN per time.

The received SIR at the UED located at distance $r_L \leq R$ from any LTD and MN can be expressed as

$$SIR_{UED}^{L} = \frac{P_L g_L x_L^{-\eta}}{I_{agg}}, \tag{2}$$

$$SIR_{UED}^{M} = \frac{P_{mal} g_M x_M^{-\eta}}{I_{agg}}, \tag{3}$$

where $x_L^{-\eta}$ and $x_M^{-\eta}$ are the Euclidean distances to the UED from the tagged LTD and MN respectively of path loss exponent η. From [9], Rayleigh fading is assumed hence fading parameters g_L and g_M are distributed with unit mean, i.e. $E[g_L] = E[g_M] \sim \exp(1)$ [13]. From (1),

$$T_{suc}^{L} = P(SIR_{UED}^{L} \geq \psi), \tag{4}$$

$$T_{suc}^{M} = P(SIR_{UED}^{M} \geq \psi). \tag{5}$$

3.1. The proposed SIR based detection scheme

From (2) and (3), the detection rule is obtained as

$$|T^L_{suc} - T^M_{suc}| \le \zeta, \tag{6}$$

where ζ is the predefined threshold for node identification. The probability of successfully emulating LTD is

$$P_{suc} = Pr\{|T^L_{suc} - T^M_{suc}| \le \zeta\}. \tag{7}$$

By applying the Markov inequality rule, (7) is given as

$$P_{suc} \ge 1 - \frac{|E[T^L_{suc}] - E[T^M_{suc}]|}{\zeta}. \tag{8}$$

Now we derive expression for T^L_{suc} and T^M_{suc}.

$$T^L_{suc} = P\Big(\frac{P_L g_L x_{L,0}^{-\eta}}{I_{agg}} \ge \psi\Big) = P\Big(\frac{P_L g_L x_{L,0}^{-\eta}}{\sum_{L_i\in\Phi\setminus L_k} P_L g_L x_L^{-\eta}} \ge \psi\Big), \tag{9}$$

$$T^M_{suc} = P\Big(\frac{P_M g_M x_M^{-\eta}}{I_{agg}} \ge \psi\Big) = P\Big(\frac{P_M g_M x_M^{-\eta}}{\sum_{L_i\in\Phi} P_L g_L x_L^{-\eta}} \ge \psi\Big), \tag{10}$$

where $x_{L,0}$ is the distance between the UED and the test LTD $L_k \in \Phi$. With Rayleigh fading assumption,

$$T^L_{suc} = E\Big[\exp\Big(\frac{\psi}{P_L x_{L,0}^{-\eta}} I_{agg}\Big)\Big]. \tag{11}$$

Eq. (11) is the Laplace transform (LT) of I_{agg} evaluated at $s = \frac{\psi}{P_L x_{L,0}^{-\eta}}$. The LT of the I_{agg} is obtained as

$$T^L_{suc} = \mathcal{L}_{I_{agg}}(s) = E\Big[\exp\Big(-s\sum_{L_i\in\Phi} P_L g_L x_L^{-\eta}\Big)\Big]$$
$$= E\Big[\prod_{L_i\in\Phi}\exp(-sP_L g_L x_L^{-\eta})\Big]. \tag{12}$$

Through the use of the probability generation functional of PPP, $\mathcal{L}_{I_{agg}}$ is obtained through some algebraic manipulations at $\eta = 4$ as

$$T^L_{suc} = \mathcal{L}_{I_{agg}}(s) = \exp\Big[-\pi\mu\frac{\sqrt{\psi r_L^{\eta}}}{sinc(0.5)}\Big]. \tag{13}$$

Similarly, T^M_{suc} is obtained at $z = \frac{\psi}{P_{mal} x_M^{-\eta}}$ as

$$T^M_{suc} = \exp\Bigg[-\pi\mu\frac{\sqrt{\frac{\psi P_L}{P_{mal} r_L^{-\eta}}}}{sinc(0.5)}\Bigg] \tag{14}$$

At each instance of $|T^L_{suc} - T^M_{suc}| > \zeta$, the MN is detected and removed from the system by the UED. The trust list table is subsequently updated. The probability of detection can be expressed as

$$p_d = Pr(|T^L_{suc} - T^M_{suc}| > \zeta\ |H_1), \tag{15}$$

where H_1 depicts the hypothesis that MN is present.

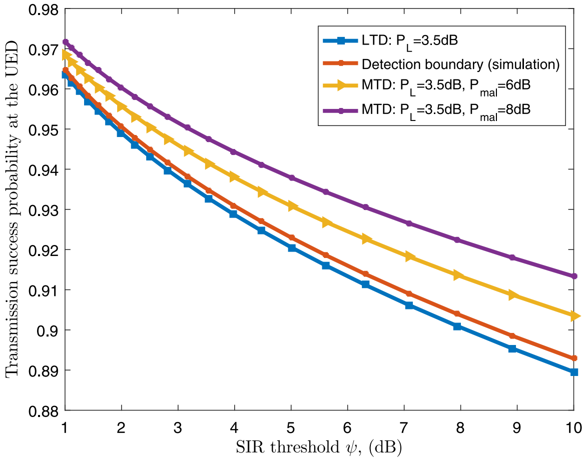

Fig. 2. User identification using SIR ($\mu = 0.03, r_L = 0.5$).

3.2. Trust list table

In a case where the MN transmits with $P_{mal} \le P_L^{\max}$, the receiver checks the trust list table to observe the past records of the potential transmitting pair. If there is a record of previous malicious activities for such a potential transmitting pair, the receiver dismisses the transmission request from the transmitting node and update the trust list table accordingly. In summary, the MN can be detected following Algorithm 1. After a certain number of rejections from the receivers, such a transmitting node is declared harmful to the system by the UED.

4. Results and simulation

We now present the results of the analysis presented in this paper. The received SIRs at the UED from the LTD and MN are not the same owing to the higher transmission power required to disrupt the network. Hence, nodes transmission power can be used to differentiate between LTDs and MNs as shown in Fig. 2. MNs are expected to generate higher SIRs at the UED with an increase in their transmit powers. Hence, any node with higher success probability at the UED above the detection boundary is categorized as MN.

Algorithm 1 Detection of malicious device

```
1: Initialization: If $P \ll P_L^{\max}$, go to 6 else 2
2: If $P \le P_L^{\max}$, go to 3 else 6
3: Check the transmitting node previous activities on the trust
   list table
4: If a device has previous malicious activity, go to 6 else 5
5: Accept the connection and update the trust list table
6: Reject the connection and update the trust list table
7: Repeat 2 to 6 until no service is required
```

The value of parameter ζ determines the performance of the detection approach as shown in Fig. 3. As ζ increases, it becomes difficult to properly differentiate between LTD and MN. Hence, ζ must be set to a very small value to ensure high detection accuracy. Our proposed approach shows improved

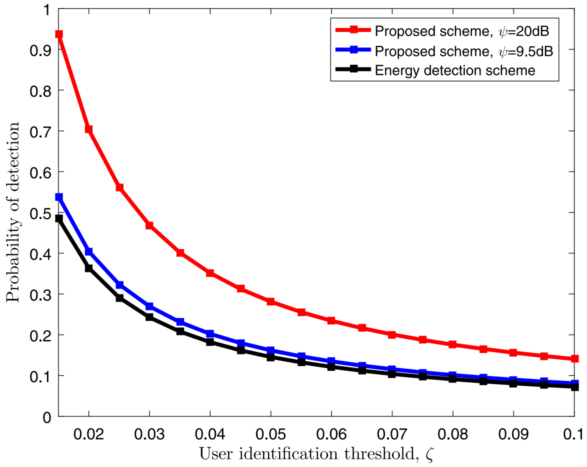

Fig. 3. Effect of users' intensity over marked probability ($P_L = 3.5$ dB, $P_{mal} = 6$ dB, $\mu = 0.03$, $r_L = 0.5$).

performance over the energy detection approach (especially when the value of ζ is very low), where interference in the network is usually neglected.

As shown in Algorithm 1, the trust list table plays an important role in detecting MNs in the system. Based on Assumption 1, any MN needs to transmit with $P_{mal} > P_L^{\max}$ to disrupt the network. This can be detected by the proposed SIR scheme. However, when $P_{mal} \leq P_L^{\max}$, UED cannot detect MNs. Such attacks can be detected following Algorithm 1. Hence, during any MN first transmission, the truth list table is updated against its next attempt. Receivers that remain unsatisfied after their connections with any transmitting node can also update such on the trust list table to assist future decision makings of other receiving nodes.

5. Conclusion

This paper presents tractable analysis capable of detecting the presence of MNs in massive IoT networks. The proposed approach has been demonstrated to be capable of capturing the presence of MNs through the signal received at the receivers and UED. In the future, we will investigate other possible attacks such as jamming attack and spectrum data falsification attack in IoT.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[2] S. Sidhu, B.J. Mohd, T. Hayajneh, Hardware security in IoT devices with emphasis on hardware trojans, J. Sens. Actuator Netw. 8 (3) (2019) 42.

[3] M. Uddin, A.S. Shanta, M.B. Majumder, M.S. Hasan, G.S. Rose, Memristor crossbar PUF based lightweight hardware security for IoT, in: 2019 IEEE International Conference on Consumer Electronics, Las Vegas, 2019, pp. 1–4.

[4] P. Bull, R. Austin, E. Popov, M. Sharma, R. Watson, Flow-based security for IoT devices using an SDN gateway, in: 2016 IEEE International Conference on Future Internet of Things and Cloud, Vienna, 2016, pp. 157–163.

[5] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, Kona, 2017, pp. 618–623.

[6] I. Gupta, O.P. Sahu, Mitigating primary user emulation attacks using analytical model, in: 2019 Engineering Vibration, Communication and Information Processing, Singapore, 2019, pp. 219–227.

[7] S.A. Yazdi, M. Ghazvini, Countermeasure with primary user emulation attack in cognitive radio networks, Wirel. Pers. Commun. 108 (4) (2019) 2261–2277.

[8] S.C. Lin, C.Y. Wen, W.A. Sethares, Two-tier device-based authentication protocol against PUEA attacks for IoT applications, IEEE Trans. Signal Inf. Process. Netw. 4 (1) (2017) 33–47.

[9] Z. Jin, S. Anand, K.P. Subbalakshmi, Detecting primary wheuser emulation attacks in dynamic spectrum access networks, in: IEEE International Conference on Communications, Dresden, 2009, pp. 1–5.

[10] C. Stergiou, K. Psannis, B. Gupta, Y. Ishibashi, Security, privacy and efficiency of sustainable cloud computing for big data and IoT, Sustain. Comput. Inform. Syst. 19 (2018) 174–184.

[11] A. Tewari, B. Gupta, Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework, Future Gener. Comput. Syst. 108 (2020) 909–920.

[12] O.O. Olakanmi, A. Dada, An efficient privacy-preserving approach for secure verifiable outsourced computing on untrusted platforms, Int. J. Cloud Appl. Comput. 9 (2) (2019) 79–98.

[13] S.D. Okegbile, B.T. Maharaj, A.S. Alfa, Interference characterization in underlay cognitive networks with intra-network and inter-network dependence, IEEE Trans. Mob. Comput. (2020) http://dx.doi.org/10.1109/TMC.2020.2993408.