Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 7, pp. 2067–2075
DOI : 10.47974/JDMSC-2080

A traffic-based anomaly detection protocol for security enhancement of nodes in IoT networks

Shahid Ul Haq *
Ash Mohammad Abbas †
Department of Computer Engineering
Aligarh Muslim University
Aligarh 202002
Uttar Pradesh
India

Abstract

An Internet of Things (IoT) constitutes a network of diverse entities, referred to as 'things', interconnected via a wide area network such as the Internet. The extensive connectivity to the broader Internet introduces potential security vulnerabilities within an IoT network. Consequently, there exists a probability of malicious devices targeting the IoT network. As such, it becomes imperative to monitor the behavior of IoT devices to detect and isolate malicious nodes within the network. This paper introduces a traffic-based anomaly detection protocol aimed at enhancing the security of nodes within an IoT network. The protocol's foundation lies in the traffic generated by devices within the IoT network. The efficacy of the proposed protocol is evaluated through simulation-based performance analysis. The observations indicate a reasonable success rate in the detection of anomalous nodes by the protocol.

Subject Classification: *Primary 68M12, Secondary 90B18.*

Keywords: *Internet of Things, Networks, Protocols, Anomaly detection, Traffic, Security, Nodes.*

1. Introduction

An Internet of Things (IoT) is a complex system that encompasses a multitude of devices. These devices are interconnected through various communication channels, which can be either wired or wireless. This intricate network facilitates the exchange of data, thereby enabling

* *E-mail:* **shahidulhaq.lone@gmail.com (Corresponding Author)**
† *E-mail:* **am.abbas.ce@amu.ac.in**

seamless interaction and coordination among the devices [1]. In the IoT architecture, the participating devices frequently exhibit constraints related to physical dimensions, communication reach, computational capabilities, and energy expenditure. These limitations are inherent due to the need for compactness, energy efficiency, and the specific operational requirements of the IoT ecosystem. In the IoT framework, devices are interconnected with expansive networks, predominantly the Internet. This connectivity paradigm exposes IoT devices to a spectrum of security vulnerabilities [2]. Furthermore, an IoT network may encompass a diverse array of nodes. A subset of these nodes may exhibit anomalous behavior. In such networks, nodes exhibiting non-standard behavior are typically classified as anomalies. The identification of these anomalies is crucial for maintaining optimal network communication. Nonetheless, the development of an anomaly detection protocol for an IoT network presents significant challenges due to the diverse constraints inherent to the devices [3].

The implementation of anomaly detection within an IoT network appears to be a prerequisite for the establishment of a secure IoT environment [4]. An integral role of an Anomaly Detection System (ADS) within a network infrastructure is to safeguard against nodes exhibiting abnormal behavior [5]. For the IoT networks, a diverse array of methodologies for the detection of anomalous nodes has been proposed in [6]. In Singh et al, [7] a Source Redundancy Management and Host Intrusion Detection system is introduced, encompassing both heavy and lightweight detection modules. The detection module, characterized by its minimalistic design, operates within a confined local environment and demonstrates superior energy conservation characteristics.

In Li et al, [8] a novel Anomaly Detection for IoT (ADRIoT) scheme, based on edge computing principles, is introduced. The detector is trained via an unsupervised learning approach, utilizing an autoencoder variant of the Long Short Term Memory (LSTM) model. In Liu et al, [9], a Deep Anomaly Detection (DAD) model, based on federated learning methodologies, specifically designed for IoT networks, is presented. The model employs Convolutional Neural Networks (CNN) for the extraction of salient features, and utilizes Long Short-Term Memory (LSTM) for the identification of anomalies. In Moustafa, Turnbull, and Choo [10], a method for intrusion detection in IoT systems is introduced, employing the analysis of statistical attributes.

The study in Kumar et al., [11] introduces a method termed as Collaborative Anomaly Detection for Smart Homes. This approach

employs autoencoders to discern both high-frequency and low-frequency traffic patterns. In An et al., [12], an edge intelligence-based anomaly detection framework for HTTP traffic is proposed. The framework employs a combination of clustering and classification techniques for anomaly identification. In Kumar et al., [13], an anomaly detection mechanism for IoT system logs, is proposed. The mechanism discerns irregular log patterns for the identification of anomalies. In Rosero-Montalvo [14], an anomaly detection framework is developed for resource-constrained IoT devices.

In this paper, we propose a protocol for the detection of anomalous nodes in an IoT. The protocol executes the propagation of anomalous node activity data to adjacent nodes within the network structure. Each node persistently scrutinizes inbound traffic from adjacent nodes and updates the information about the behavior of nodes accordingly. The significant contributions of the paper are as follows:

- We introduce a protocol designed for the identification of anomalies within an IoT network. The protocol operates on the principle of mutual observation among adjacent nodes, based on the analysis of traffic patterns generated within a specified temporal interval.
- We conduct a performance assessment of the proposed protocol via simulation. The protocol demonstrates effectiveness in identifying anomalous nodes that generate traffic exceeding standard thresholds.

The subsequent structure of the paper is as follows: Section 2 introduces the proposed protocol for anomaly detection. Section 3 gives a comprehensive analysis of the proposed protocol. Section 4 presents the results and discussion. The last section presents the conclusion and future work.

2. Proposed Protocol

In the proposed scheme, nodes are categorized into three distinct classifications: normal, grey, and anomalous. A node that consistently generates traffic within specified boundaries is defined as a normal node. A node that surpasses these traffic thresholds for a defined temporal interval is identified as a grey node. A node that sustains its status as a grey node for a predetermined time span is classified as an anomalous

node. Every node in the network contains three separate lists of nodes: a neighbor node list, a grey list, and an anomalous list.

Let $TrafficNode_j$ represent the traffic generated by a neighboring node j. The outputs, $GrList_i$ and $AnmList_i$, correspond to the grey and anomalous lists of node i, respectively. The traffic threshold is denoted by *Threshold*. The list $NghbrList_i$ stores all the neighbors of a specific node i. The timeout is represented by *Timeout*. Initially, the $GrList_i$ and $AnmList_i$ of node i are empty. If a neighboring node j generates traffic $TrafficNode_j >$ *Threshold* for a duration *Timeout*, it is added to the $GrList_i$. If the node i continues to receive a traffic $TrafficNode_j >$ *Threshold* from neighbor j, which is included in a $GrList_i$, then the node is moved to the $AnmList_{i..}$

Algorithm 1: Finding grey and anomalous nodes at node i.

```
Input: TrafficNode_j // Traffic of node j
Output: GrList_i, AnmList_i
GrList_i ←null
AnmListi ←null
while True do
    if TrafficNode_j >= Threshold for Timeout then
        Add Node_j to GrList_i
        if TrafficNode_j >= Threshold for Timeout then
            Add Node_j to AnmList_i
        end if
    end if
    if GrList_k and AnmList_k received then
        for Node_j in NghbrList_i do
            if Node_j in GrList_k then
                Add Node_j to GreyList_i
            end if
            if   Node_j in AnmList_k then
                Add Node_j to AnmList_i
            end if
        end for
    end if
Send GreyList_i and AnmList_i to neighbors
end while
```

After receiving $GrList_k$ and $AnmList_k$ from a neighboring node k, a node examines whether its neighbor j, which is in the received $GrList_k$

from neighbor k, is sending too much traffic too fast, i.e $TrafficNode_j \geq Threshold$ for a *Timeout*. If yes, it adds the address of the node j to the $GrList_i$ that it maintains. If the address of a neighboring node j is in the $AnmList_k$ which it receives from other neighbor k, then it adds the address of the node k in its $GrList_i$ and observes the behavior of the neighboring node j. If the traffic received from node j is beyond a threshold, i.e. $TrafficNode_j > Threshold$ during a *Timeout*, it adds the node to the $AnmList_i$. Whenever there is any update in the $GrList_i$ or $AnmList_i$, it sends the corresponding lists to its neighbors in $NghbrList_i$. The major steps are summarized in Algorithm 1.

3. Characterization of Traffic and Classification of Nodes

In this section, we first conduct a characterization of the traffic propagated by an individual node. Following this, we explain the methodology for designating nodes within an IoT network as normal, grey, or anomalous, based on the characteristic of the traffic they generate.

3.1 *Characterization of Traffic*

Assume the bit-length of a packet transmitted by a node is denoted as B. Given that a node produces x packets within a temporal interval I, the resultant traffic can be calculated as follows:

$$\tau = \frac{xB}{I} \tag{1}$$

Given that each packet possesses a bit-length denoted as B. If a node generates x_1 packets of length B_1 bits, x_2 packets of length B_2 bits, up to x_k packets of length B_k bits during respective time intervals I_1, I_2, …, I_k. The mean traffic generated by the node can be calculated as follows:

$$\tau = \frac{\sum_{i=1}^{k} x_i B_i}{\sum_{i=1}^{k} I_i} \tag{2}$$

We now discuss the procedure for categorizing a node into one of three distinct classes: normal, grey, or anomalous.

3.2 *Classifying Anomalous Nodes*

Let τ_{th}^{g} be the traffic threshold, which upon exceeding, a node transitions into a grey state. A node is considered a normal node if the inequality $0 \leq \tau \leq \tau_{th}^{g}$ is satisfied. Similarly, a node is designated as grey if

the traffic generated by it during two successive time intervals is greater than the grey traffic threshold, i.e $\tau > \tau_{th}^{g}$ for $t \in [0, I]$ and $t \in [I, 2I]$.

A node in a grey state is classified as anomalous when the traffic it produces surpasses the anomalous traffic threshold, τ_{th}^{a}, within a specified timeout period, I_0. So a node in a grey state is classified as anomalous if, $\tau > \tau_{th}^{a}$ for $t \in [2I, 2I + I_0]$, where $I_0 \geq I$ and $\tau_{th}^{a} > \tau_{th}^{g}$.

4. Results and Discussion

A 1000-node IoT network is instantiated within a 1000m × 1000m area, each node possessing a 10m range. Node positions are randomly determined. Nodes are subsequently classified as normal, grey, or anomalous, based upon the traffic they generate.

Figure 1 presents the mean count of anomalous nodes in correlation with the proportion of grey nodes, under varying anomalous traffic thresholds. Grey nodes are introduced into the network randomly, ensuring the ratio of grey nodes to total nodes does not surpass the defined maximum limit. An observed correlation exists wherein the mean count of anomalous nodes increases in response to an increase in the upper limit fraction of permissible anomalous nodes. An increase in the upper limit increases the likelihood of a node sustaining its grey status throughout a specified timeout interval, consequently resulting in an increase in the quantity of anomalous nodes

Figure 2 presents the mean count of anomalous nodes against the traffic threshold, relative to different proportions of anomalous nodes. The data shows a decrement in the average anomalous nodes as the traffic threshold increases. Upon increasing the traffic threshold to 20 Mbps, the anomalous node count becomes insignificant. This can be attributed to the fact that an increased traffic threshold facilitates a node in transmitting an increased volume of traffic, thereby diminishing the likelihood of a node being identified as an anomalous node.

Figure 3 shows the instantaneous enumeration of anomalous nodes in correlation with the epoch number for varying ratios of anomalous nodes. The instantaneous enumeration represents the quantity of anomalous nodes detected at a specific instance of epoch. The quantity of anomalous nodes per epoch is based upon the node-generated traffic. It is observed that a larger permissible proportion of grey nodes in the networks corresponds to a relatively larger quantity of anomalous nodes, and inversely so.

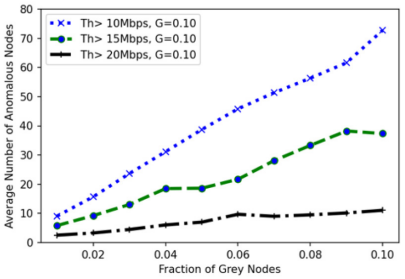

Figure 1

Mean count of anomalous nodes relative to grey node fraction

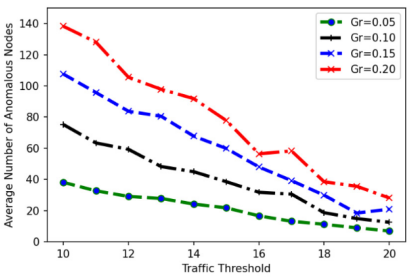

Figure 2

Mean count of anomalous nodes relative to the anomalous traffic threshold

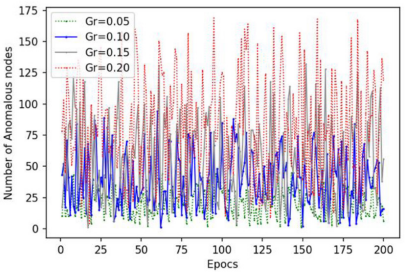

Figure 3

Anomalous node counts per epoch under different anomalous fractions

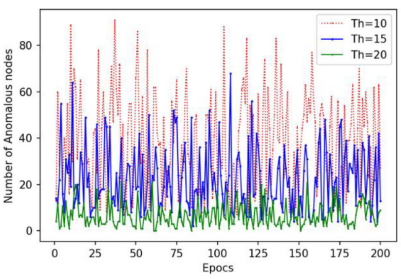

Figure 4

Anomalous node counts per epoch under varying traffic thresholds

Figure 4 represents the count of anomalous nodes detected at a specific instance of epoch. As previously stated, the instantaneous quantity of anomalous nodes is intrinsically tied to the traffic volume produced by the nodes within a specific epoch. A decrease in traffic threshold value increases the number of anomalous nodes, and reciprocally, a behavior also observed in Figure 2.

5. Conclusion and Future work

This study introduces a traffic-based protocol designed for anomaly detection to enhance the security of nodes within IoT networks. Performance evaluation was conducted via simulations. The findings indicate a direct correlation between the average count of detected

anomalous nodes and the maximum permissible proportion of such nodes. Furthermore, a decrease in the anomalous traffic threshold, beyond which a node is classified as anomalous, also increases the average count of detected anomalous nodes. Future research will explore various aspects of this work, including the development of methodologies for route reorganization in IoT networks that circumvent anomalous nodes.

References

[1] L. Babun, K. Denney, Z. B. Celik, P. McDaniel, and A. S. Uluagac, "A survey on iot platforms: Communication, security, and privacy perspectives," *Computer Networks*, vol. 192, pp. 108040 (2021).

[2] S. Chaudhary and P. K. Mishra, "Ddos attacks in industrial iot: A survey," *Computer Networks*, vol. 236, pp. 110015 (2023).

[3] M. N. Khan, A. Rao, and S. Camtepe, "Light-weight cryptographic protocols for iot-constrained devices: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4132–4156, March (2021).

[4] Lin, Xin-Xue, Phone Lin, and En-Hau Yeh. "Anomaly detection/prediction for the internet of things: State of the art and the future." *IEEE Network,* vol. 35 (1), pp. 212-218, (2020).

[5] A. Chatterjee and B. S. Ahmed, "Iot anomaly detection methods and applications: A survey," Internet of Things, vol. 19, pp. 100568 (2022).

[6] A. Sgueglia, A. DiSorbo, C.A. Visaggio, and G. Canfora, "A systematic literature review of iot time series anomaly detection solutions," *Future Generation Computer Systems*, vol. 134, pp. 170–186 (2022).

[7] V. Singh, G. Sharma, R. C. Poonia, N. K. Trivedi, and L. Raja, "Source Redundancy Management and Host Intrusion Detection in Wireless Sensor Networks", Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), vol. 14, pp. 43-47, (2021)

[8] R. Li, Q. Li, J. Zhou, and Y. Jiang, "Adriot: An edge-assisted anomaly detection framework against iot-based network attacks," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 10 576–10 587, July (2022).

[9] Y. Liu, S. Garg, J. Nie, Y. Zhang, Z. Xiong, J. Kang, and M. S. Hossain, "Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6348–6358 (2020).

[10] N. Moustafa, B. Turnbull, and K. -K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things," *IEEE Internet of Things Journal,* vol. 6, no. 3, pp. 4815–4830 (2018).

[11] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication.", *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 4, pp. 499-507, (2019).

[12] Y. An, F. R. Yu, J. Li, J. Chen, and V. C. M. Leung, "Edge intelligence (ei)-enabled http anomaly detection framework for the Internet of Things (IoT)," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3554–3566, March (2021).

[13] A. Kumar, P. Dadheech, V. Singh, L. Raja, and R. C. Poonia, "An enhanced quantum key distribution protocol for security authentication.", *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 4, pp. 499-507, (2019).

[14] P.D. Rosero-Montalvo, Z. Istvan, P. Tozun, and W. Hernandez, "Hybrid anomaly detection model on trusted iot devices," *IEEE Internet of Things Journal*, vol. 10, no. 12, pp. 10959–10969, June (2023).

Received March, 2024