Intelligent Anomaly Detection System for IoT

Diego Angelo Bolatti[1] [0000-0002-8275-4476], Marcelo Karanik[1], Carolina Todt[1] [0000-0001-8429-6141], Reinaldo Scappini [1] [0000-0001-6854-4643], Sergio Gramajo [1] [0000-0001-5091-7931]

[1] Center for Applied Research in Information and Communication Technologies at National University of Technology (UTN), Resistencia Regional Faculty (UTN-FRRe). French St. 414, Resistencia, Province of Chaco, Argentina.
{diegobolatti, mkaranik, carolinatodt, rscappini, sergiogramajo}@ca.frre.utn.edu.ar

Abstract. The growing use of the Internet of Things (IoT) in different areas implies a proportional growth in threats and attacks on end devices. To solve this problem, the IoT systems must be equipped with an anomaly detection system (ADS). This work introduces the design of a hybrid ADS based on the Software-Defined Network (SDN) architecture, which combines the rule-based and Machine Learning-based detection technique. Whereas the rule-based approach is used to detect known attacks with the help of rules defined by security experts. And the Machine Learning approach is used to detect unknown attacks with the help of Artificial Intelligence techniques.

Keywords: IoT, Anomaly Detection, Machine Learning, SDN.

1 Introduction

The Internet of Things (IoT) has been expanding in recent years and this is reflected in the thousands of devices connected every day, which obtain and exchange information through the web. This new paradigm is used in different sectors such as healthcare, transportation, agriculture, entertainment, and education.

The great diversity of communication, devices, technologies, and protocols makes managing the security of an IoT ecosystem a great challenge.

Designers rarely bear in mind security when it comes to IoT devices, and many of them lack essential encryption and authentication capabilities, which has led to a whole new category of attacks explicitly targeting end devices.

To address this issue, several security solutions for IoT have been proposed [1- 2]. Most of these solutions focus on the use of cryptography for preventing external attacks, such as message alteration and eavesdropping.

If some of the sensor nodes are compromised and become internal attackers, cryptographic techniques cannot detect these malicious nodes because the adversary can have a valid key to perform activities within the network.

Usually, attackers establish malicious nodes as legitimate nodes within the network to launch internal attacks, such as data alterations, selective forwarding, jamming, denial of service, and clone attacks. These attacks are destructive to IoT network operations. For this reason, the capability to detect intrusions and malicious activities within IoT networks is critical for maintaining the functionality of the IoT system.

This article introduces the design of an intelligent anomaly detection system for IoT and is organized as follows. The related work is presented in Section 2. The proposal system is introduced in Section 3 and, finally, the discussion and future works are presented in Section 4.

2 Related Work

The anomaly detection system can be the key to solving intrusions because alterations to normal behavior indicate the presence of intentional or unintentional induced attacks on the IoT network.

Implementing an Anomaly Detection System (ADS), Software-Defined Networks (SDN) architecture for instance, offers a good alternative because it provides all the benefits of virtualization, such as agility and cost-effective redundancy, and scalability.

The visibility across the network helps identify malicious actions and take appropriate action, such as quarantines.

Centralizing security control in one entity, such as the SDN controller, has the disadvantage of creating a central point of attack, but SDN can be used effectively to manage the security of the IoT environment if it is implemented securely and appropriately [3-4].

Anomaly Detection can use two detection techniques—rule-based or Machine Learning (ML)-based. The rule-based approach detects anomalies with rules defined by security experts [5] and is ideal to identify known attacks. The benefit of using this technique is that the rules are easily understood and highly accurate.

Generally, the Proposed ADS uses ML techniques [6-7] to identify unknown security attacks. To use ML effectively for cybersecurity purposes, a large amount of properly labeled training data is needed.

However, even when an algorithm has received a large amount of data, it does not ensure that it can correctly identify all new attacks. Therefore, human supervision, experience, and verification are constantly required. Without this process, even a single incorrect entry can cause a "snowball effect" and possibly undermine the solution to the point of failure. The same problem arises if the algorithm only uses its own output data as inputs for further learning. Errors are reinforced and multiplied as the same incorrect results re-enter the solution in a cycle, creating more false positives (incorrectly categorizing clean samples as malicious) and false negatives (marking malicious samples as benign).

To reduce the rate of false positives and negatives, both anomaly detection approaches can be combined, thus obtaining a hybrid system [8-9].

3 Proposal

This work proposes a hybrid anomaly detection system for IoT, which uses rule-based and ML-based with real-time data as input.

In the first part, the rule-based ADS captures the network traffic coming from the end devices through an open flow switch in the gateway, and based on some

predefined rules, classifies the incoming network traffic as normal or abnormal (attack).

After classification, the information is stored in a database allowing that data to be used in the future for training the ML-based anomaly detector.

In the second part, the learning model is trained using the labeled training data set. After training the model, we use the model to validate the classification results performed by the rule-based anomaly detector. The final prediction of the system is obtained by comparing the results of both types of detectors. If one of the systems declares a package as a failure; it will be labeled as an attack.

The anomaly detection system will be installed in the device layer of the reference architecture proposed by the ITU (International Telecommunication Union) [10].

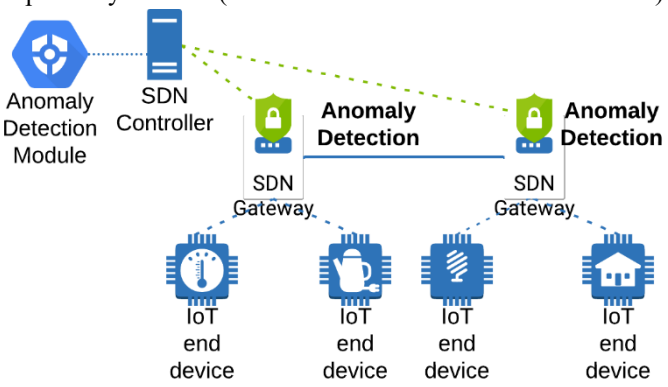

Fig. 1. Architecture of the Intelligent Anomaly Detection System for IoT.

As shown in Fig. 1, the architecture consists of the following four components:

- **IoT end device** with the mandatory capabilities of communication and optional capabilities of sensing, actuation and data capture.
- **Gateway SDN** to connect the different devices to the network trough Low Power Wide Area Networks (LPWAN) such as LoRa, SigFox, NB-IoT, LTE-M, etc.
- **OpenFlow Switches** to monitor the traffic coming from the end devices.
- **SDN Controller** manages and configures the distributed network resources and provides an abstracted view of the network resources to the SDN applications via another standardized interface (i.e., application-control interface) and the relevant information and data models.
- **Anomaly Detection Module** to check the packet for anomalies and add intelligence to the SDN controller to readjust the network and maintaining the policies defined by administrators when detecting the following attacks: Denial of Service (DoS), Data type probe, Battery drain attack, Packet tampering, Jamming, Man in the Middle, and Packet delay.

4 Discussion and Future Work

To solve the security problems of the IoT environment, this article describes an Anomaly Detection System based on two different detection approaches, rule-based

and ML-based, in different instances. The result of both techniques is compared, and if one of the systems detects an anomaly; it will be labeled as an attack. This system combines both human and machine intelligence. And the advantage of using a hybrid system is that reducing the number of false-positive and false-negative rates.

An interesting aspect to analyze is the interactions of the model (SDN Controller - SDN Gateway and SDN Gateway - SDN Gateway). In the first case the SDN Controller defines data flow control rules based on application and SDN gateway traffic. In the second case, SDN Gateways check rules and configuration updates to keep their states synchronized.

In the field of security, ML can play an important role in helping security teams make accurate decisions about security threats and incidents. But ML cannot do the job for the human engineers, developers. There is no magic solution, human experience is always necessary.

The system design is currently being finalized and the next step in this work will be to evaluate and identify the most appropriate Machine Learning technique for the system. As a final step, we intend to test the system in a real-world IoT environment to evaluate its efficiency and viability.

References

1. S. Sridhar and S. Smys, "Intelligent security framework for iot devices cryptography based end-to-end security architecture," 2017 International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, pp. 1-5 (2017).
2. Mathur, A., Newe, T., Elgenaidi, W., Rao, M., Dooly, G., & Toal, D. A secure end-to-end IoT solution. Sensors and Actuators A: Physical vol. 263, pp. 291-299 (2017).
3. Nguyen, Tam N. The challenges in SDN/ML based network security: A survey. arXiv preprint arXiv:1804.03539 (2018).
4. Tsogbaatar, Enkhtur, et al. SDN-Enabled IoT Anomaly Detection Using Ensemble Learning. IFIP International Conference on Artificial Intelligence Applications and Innovations. Springer, Cham (2020).
5. Xie, M., Han, S., Tian, B., & Parvin, S. Anomaly detection in wireless sensor networks: A survey. Journal of Network and computer Applications, 34(4), pp.1302-1325 (2011).
6. Nguyen, T. D., Marchal, S., Miettinen, M., Fereidooni, H., Asokan, N., & Sadeghi, A. R. (2019, July). DÏoT: A federated self-learning anomaly detection system for IoT. In 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), pp. 756-767. IEEE (2019).
7. 2-Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). pp. 0305-0310. IEEE (2019).
8. Thanigaivelan, Nanda Kumar, et al. "Hybrid internal anomaly detection system for IoT: Reactive nodes with cross-layer operation." Security and Communication Networks 2018 (2018).
9. Bhatt, P., & Morais, A. HADS: hybrid anomaly detection system for iot environments. In 2018 International Conference on Internet of Things, Embedded Systems and Communications (IINTEC), pp. 191-196. IEEE (2018).
10. ITU-T Y.4000/Y.2060 (06/2012) Overview of the Internet of Things. http://www.itu.int/ITUT/recommendations/rec.aspx?rec=11559&lang=en.