Cyber-Attacks Prediction in IoT Environment

Arwa Alamoudi

Problem Definition

The basic concept and view of the Internet is expanding and including more things than what we got used to. The idea that computers and mobile phones are connected to the Internet opened the door for more “things” to be connected also. For example, television and coffee machine in the domain of smart home, printer and sensor in workplace, car and smart watch and many others, this is simply the meaning of Internet of Things (IoT).

Internet of Things (IoT) is communication networks of a variety of things or objects around us that have the ability to send and receive data and information with each other through unique addressing scheme to achieve a service or goal without the need of human-to-human and human-to-computer interaction [1].

According to IoT Analytics, the number of things connected to the Internet is increasing rapidly. In 2016, there were around 4.7 billion things connected and it is estimated to reach to nearly 11.6 billion and 21 billion IoT devices in 2021 and 2025 respectively [2]. This rapid growth of numbers of IoT devices help IoT organizations and customers benefit by allowing them to access information from anywhere at anytime on any device as well as automating a lot of tasks thus saving customers time and money [3].

Besides all the IoT applications benefits, a lot of challenges arise including but not limited to the potential of security threats. As the number of connected devices increase, the probability of cyber-attacks also increases [4]. This is due to the face that some IoT devices are not operated by humans and are connected wirelessly to each other which make them more vulnerable and thus more prone to attacks. An example of potential attack in smart home domain when an intruder penetrates the lighting system and gets access to the data generated by its sensors, this data can be translated into valuable information such as if a person being at home or not [5]. The infected area can be expanded to include other connected devices in the same network. Therefore, any vulnerability in any IoT device on a network may function as a backdoor for attackers to enter, access and gather credential information [3].

There are many types of cyber-attacks that can affect an IoT system, common types are denial of Service (DoS), Data Type Probing, Malicious Control, Malicious Operation, Scan, Spying and Wrong Setup.

The main goal of this project is to build a model that acts as a secure and robust infrastructure for IoT systems through predicting attacks in network transmissions, hence protecting user’s privacy and security.

Dataset

The dataset used in this project collected from kaggle [6] provided by Pahl et al [7]. The data was collected from different simulated IoT environments using Distributed Smart Space Orchestration System (DS2OS). It contains communications between different IoT nodes within the environments, these nodes represent light controller, thermometer, movement sensors, washing machines, batteries, thermostats, smart doors and smart phones. Each environment has different organization and different combination and number of nodes/services.

The dataset consists of 13 features and 357,952 traffic traces between different IoT nodes, 10,017 of them were classified as anomalous traffic traces in one of the following seven types of cyber-attack:

1. Denial of Service (DoS): when an attacker prevents a user from accessing a service as a result of overwhelming its resources [8].
2. Data Type Probing: when a malicious node (service) writes anomalous data types than the expected one [7].
3. Malicious Control: when a malicious node tries to take control over original node [7].
4. Malicious Operation: when a malicious node performs anomalous operation than the expected one [7].
5. Scan: it's a pre-attack or scouting activities to scan the network and discover the devices before attacking [9].
6. Spying: when a malicious node reads values and information without the knowledge or permission of the individuals [7].
7. Wrong Setup: when a malicious node accesses another node in the wrong room [7].

Table 1 illustrates features' names, types, and a brief description about each one.

Table 1 The list of Features Repressing each Communication

Name	Type	Description
Source ID	Categorical - Nominal	Represents the source node ID in the environments, for example: lightcontrol2, movement4
Source Address	Categorical - Nominal	Represents the address of the source node, for example: /agent2/lightcontrol2, /agent4/movement4
Source Type	Categorical - Nominal	Represents the source node functionality, for example: /lightControler, /movementSensor
Source Location	Categorical - Nominal	Represents the location of the source node within the environment, for example: BedroomParents, Kitchen
Destination Service Address	Categorical - Nominal	Represents the address of the destination node, for example: /agent2, /lightcontrol2
Destination Service Type	Categorical - Nominal	Represents the destination node functionality, for example: /lightControler, /movementSensor
Destination Location	Categorical - Nominal	Represents the location of the destination node within the environment, for example: BedroomParents, Kitchen.
Accessed Node Address	Categorical - Nominal	Represents the address of the accessed node, for example: /agent11/battery4/charge

Accessed Node Type	Categorical - Nominal	Represents the type of the accessed data node in the data of the destination service, for example: /basic/number, /sensorService
Operation	Categorical - Nominal	Represents the operation performed between source node and destination node, for example: read, write.
Value	Type-specific	Represents the value that gets exchange between source node and destination node, for example: true, 20.3942
Timestamp	Numerical - Discrete	A value that represents a timing in which the operation was performed, for example: 1520117968332
Normality	Categorical - Nominal	Represents the nature of the traffic if it's normal or not with a detail of the type of attack, for example: normal, anomalous(malitiousControl)

References

[1] Atzori, L., Iera, A. and Morabito, G., 2010. The internet of things: A survey. Computer networks, 54(15), pp.2787-2805 [Accessed 18 April 2020].

[2] Iot-analytics.com. 2020. State Of The Iot 2018: Number Of Iot Devices Now At 7B – Market Accelerating. [online] Available at: <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> [Accessed 18 April 2020].

[3] IoT Agenda. 2020. What Is Iot (Internet Of Things) And How Does It Work?. [online] Available at: <https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT> [Accessed 18 April 2020].

[4] Razzaq, M.A., Gill, S.H., Qureshi, M.A. and Ullah, S., 2017. Security issues in the Internet of Things (IoT): a comprehensive study. International Journal of Advanced Computer Science and Applications (IJACSA), 8(6), pp.383-388 [Accessed 18 April 2020].

[5] Abomhara, M., 2015. Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility, 4(1), pp.65-88 [Accessed 18 April 2020].

[6] Kaggle.com. 2020. DS2OS Traffic Traces. [online] Available at: <https://www.kaggle.com/francoisxa/ds2ostraffictraces> [Accessed 18 April 2020].

[7] Pahl, M.O. and Aubet, F.X., 2018, November. All eyes on you: Distributed Multi-Dimensional IoT microservice anomaly detection. In 2018 14th International Conference on Network and Service Management (CNSM) (pp. 72-80). IEEE.

[8] F-secure.com. 2020. Article: What Is... Denial-Of-Service (Dos) | F-Secure. [online] Available at: <https://www.f-secure.com/v-descs/articles/denial-of-service.shtml> [Accessed 18 April 2020].

[9] Security.radware.com. 2020. What Is A Network Scan? | Radware — Ddospedia. [online] Available at: <https://security.radware.com/ddos-knowledge-center/ddospedia/network-scan/> [Accessed 22 April 2020].