INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG20-TD1885

STUDY GROUP 20

Original: English

Question(s): 6/20 Virtual, 6-16 July 2020

TD

Source: Rapporteur Q6/20

Title: Baseline text for proposed new work item to develop a Technical Report of Intelligent Anomaly Detection System for IoT

Purpose: Discussion

Contact: Dr. Abdulhadi AbouAlmal Tel: +971501818540
Etisalat Group, UAE E-mail: draboualmal@gmail.com

Keywords: IoT, Security, Anomaly detection, Machine Learning

Abstract: This TD contains the baseline text for proposed new work item to develop a Technical Report of Intelligent Anomaly Detection System for IoT.

Please see below.

International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(6 July 2020)

Y.STR-IADIoT
Proposal of an Intelligent Anomaly Detection System for IoT

Summary

This technical report contains a proposal of an Intelligent Anomaly Detection System for IoT to detect and alert unusual activities in the IoT network traffic.

Keywords

IoT, Security, Anomaly detection, Machine Learning.

Change Log

This document contains Version 1 of the ITU-T Technical Report on "*Proposal of an Intelligent Anomaly Detection System for IoT*" approved at the ITU-T Study Group 20 meeting held in Geneva, 6-16 July 2020.

Editors:

Diego Bolatti
National Technological University
Argentina
Tel:
Fax:
Email: dbolatti@frre.utn.edu.ar

Marcelo Karanik
National Technological University
Argentina
Tel:
Fax:
Email: marcelo@frre.utn.edu.ar

Carolina Todt
National Technological University
Argentina
Tel:
Fax:
Email: carolinatodt@gmail.com

CONTENTS

Page

Technical Report ITU-T Y.STR-IADIoT

Technical Report ITU-T
Proposal of an Intelligent Anomaly Detection System for IoT

Summary

This technical report contains a proposal of an Intelligent Anomaly Detection System for IoT to detect and alert unusual activities in the IoT network traffic.

Scope

This document describes a proof of concept of an Intelligent Anomaly Detection System for IoT.

References

[1] Debar H, Dacier M, Wespi A. Towards a taxonomy of intrusion-detection systems. Computer Networks 1999; 31(8):805–822.

[2] Pajouh, H. H., Javidan, R., Khayami, R., Ali, D., & Choo, K. K. R. (2016). A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Transactions on Emerging Topics in Computing.

[3] Sciforce. 2019. Anomaly Detection—Another Challenge For Artificial Intelligence. Available at: <https://medium.com/sciforce/anomaly-detection-another-challenge-for-artificial-intelligence-c69d414b14db>.

Terms and definitions

Terms defined elsewhere

This Technical Report uses the following terms defined elsewhere:

[TBD]

Terms defined here

This Technical Report defines the following terms:

[TBD]

Abbreviations

AI	Artificial Intelligence
ML	Machine Learning
IoT	Internet of Things
ADS	Anomaly Detection System

Background

The Internet of Things is a fast expanding network of smart heterogeneous objects. It refers to the physical devices that are capable of communicating with other physical devices. Unlike the wireless sensor networks, IoT is connected to worldwide Internet that exposes it to global intrusion in addition to wireless attacks inside an IoT network. It is protected by cryptographic and network security

techniques, but they are vulnerable to internal and external attacks. The IoT devices are resource constrained in terms of limited storage, battery, limited transmission range and processing. We also need a system, which can identify the anormal behavior and trigger an alarm in anormal scenario to take appropriate preventive measure. Hence, an Anomaly Detection System plays an important role to prevent such cyberattacks in IoT.

The Anomaly Detection System is a software and/or hardware entity to automate the detection of abnormal activities that attempt to compromise the integrity, confidentiality, or availability of a system with the following functionality [1]:

- Monitor the network traffic or behavior of systems.
- Automatically recognize unauthorized and malicious activities in a network/system.
- Trigger the alarms on recognizing the malicious activity.

Anomaly detection can be done using the concepts of Machine Learning. Machine learning is a subset of artificial intelligence that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. ML techniques, such as supervised learning, unsupervised learning, and reinforcement learning, have been widely adopted in the network security landscape.

Motivation

Why anomaly detection is important for IoT Security?

Attack and anomaly detection in the Internet of Things infrastructure is a rising concern in the domain of IoT. With the increased use of IoT infrastructure in every domain, threats and attacks in these infrastructures are also growing commensurately.

The first line of defense for IoT devices is based on security techniques such as cryptographic authentication and secure construction of network topology. However, some attackers still launch malicious attacks on IoT devices through data analysis. Anomaly Detection is considered as the second line of defense, which plays an important role in ensuring the security of IoT devices [2]. Anomaly detection detects and identifies Denial of Service, Data Type Probing, Malicious Control, Malicious Operation, Scan, Spying and Wrong Setup are such attacks and anomalies which can cause an IoT system failure.

Why use Machine Learning for Anomaly Detection?

Machine Learning comes in, offering help in many aspects [3]:

- **Automation:** AI-driven anomaly detection algorithms can automatically analyze datasets, dynamically fine-tune the parameters of normal behavior and identify breaches in the patterns.
- **Self-learning:** AI-driven algorithms constitute the core of self-learning systems that are able to learn from data patterns and deliver predictions or answers as required.
- **Real-time analysis:** ML solutions can interpret data activity in real time. The moment a pattern isn’t recognized by the system, it sends a signal.
- **Scrupulousness:** Anomaly detection platforms provide end-to-end gap-free monitoring to go through minutiae of data and identify smallest anomalies that would go unnoticed by humans
- **Accuracy:** ML enhances the accuracy of anomaly detection avoiding nuisance alerts and false positives/negatives triggered by static thresholds.
- **Data processing:** Machine learning tools allow you to process a large amount of data, making it ideal for an anomaly detection module.

Challenges and Requirements of ADS in IoT

Challenges

Anomaly detection system challenges in the IoT application scenario:

- **Dynamic threat landscape.** New IoT devices are released on a daily basis. A significant fraction of them have security vulnerabilities. Exploits targeting vulnerable devices are also being developed by adversaries at a similarly high pace. This makes the threats against IoT devices highly dynamic and ever-increasing.
- **Resource limitations.** IoT devices have limited capabilities: available memory, computing resources and energy often making it infeasible to perform on-device detection.
- **IoT device heterogeneity and false alarms.** Behaviors of different IoT devices are very heterogeneous, so that anomaly detection techniques easily raise false alarms. However, to be useful in practice, anomaly detection systems must minimize false alarms.
- **Scarcity of communications.** IoT devices generate only little traffic, often triggered by infrequent user interactions.

Requirements

The ADS for IoT should meet the following set of requirements:

- The deployment of ADS in IoT should not introduce new vulnerabilities to the system.
- The ADS should be self-managed to detect hardware and software changes automatically.
- It should be self configure and self adaptive to the configuration changes.
- The ADS should be able to cope up with the system failure and be able to recover in the same conditions as before the failure.
- The ADS should detect anomalies with the lowest usage of system resources.
- The ADS should run continuously, and remain transparent to the system as well as to the users.
- It should monitor itself to detect whether it has been compromised by an attacker, and must be able to protect itself from unauthorized access or attacks.
- The ADS should detect the anomalies with low processing and communication overhead.
- The mobility of IoT devices should not affect the detection accuracy.
- It should be interoperable with other ADSs.
- It should be scalable in order to efficiently process the large number of IoT devices.
- The ADS should be able to detect a variety of anomalies with fewer false positive and false negative rates.
- The ADS should provide automated responses to suspicious activities without any human intervention.
- The ADS should not only detect anomalies but also localize the source of anomalies.

Conclusion and proposals

Based on the reasons foresaid in the motivation section, a “Intelligent Anomaly Detection System” is proposed, to detect and alert unusual activities in the IoT network traffic. The system will use machine learning algorithms to detect abnormal network behaviors. This detection systems provides security as a service and facilitates interoperability between various network communication protocols used in IoT.

_____