ScienceDirect

Advances in Engineering Software

Volume 169, July 2022, 103126

Detection and prevention of man-in-the-middle attack in iot network using regression modeling

N. Sivasankari [a], S. Kamalakkannan [b]

Show more

https://doi.org/10.1016/j.advengsoft.2022.103126

Get rights and content

Abstract

Security is the primary concern in any IoT application or network. Due to the rapid increase in the usage of IoT devices, data privacy becomes one of the most challenging issue to the researcher. In IoT applications, such as health care, smart homes or any wearables, transmission of human's personal data is more frequent. Man-in-the-Middle attack is one in which outsiders eavesdrops the communication between two trusted parties and steal the important information such as password, personal identification number, etc., and misuse it. So, this paper proposes a Regression Modelling technique to detect and mitigate the attack to provide attack-free path from source to destination in an IoT network. Three machine learning techniques Linear Regression (LR), Multi-variate Linear Regression (MLR) and Gaussian Process Regression (GPR) used and performance of these three algorithms analyzed on various metrics and shown Gaussian Process Regression provide higher rate for detecting the attacks and produces the lower rate for misclassification of attacks.

Introduction

Today we live in the digital era. Internet enters every human life in the world. Due to the popularization of internet, the next advancement 'Internet of Things' comes into existence. That is, one device will be able to communicate with other device without human intervention. Study shows that IoT market starts with 2 billion objects interconnected in the year 2006 and at 2020 it increased to 200 billion. The drastic growth is due to the intelligence of IoT devices, so it is adapted in almost every field like education, health care, agriculture, finance, smart home, smart cities, smart vehicle, etc., IoT environment consist of heterogeneity of devices, networks, protocols, and standards. No network is free from security threats and vulnerability. The security loopholes of IoT system create various security threats to the different IoT layers. Since IoT is involved in many areas such as medical, power plant, and home automation, attacks on such crucial applications may cause severe consequences. OWASP published several in-build vulnerabilities, i.e., weak passwords, insecure network and cloud services, usage of outdated components, insecure default setting, data transfer and storage of IoT devices can allow the attackers easily to penetrate the system.

Regarding IoT, attacks generalized into four categories: Physical Attacks - targets the hardware of an IoT system, Network Attacks - used to extract large amount of data remotely, Encryption - finding the encryption key and steal the data and Software attack - accessing the entire software system by installing malware, virus, phishing, injecting malicious code. The following are the various common cyber threat attacks in IoT:

Botnets: Botnets are collection of compromised computers remotely controlled by cybercriminals to carry out various swindles and cyber-attacks such as stealing private information, exploitation of data, phishing emails, and DDoS attacks. The rapid growth of IoT, led to more devices connected to the Internet and increase the attack vector possibilities. Botnets as well as Things Bot have two common characteristics: internet enabled and transfer data automatically via a network. They are difficult to detect because the user has no knowledge that the device is compromised. Botnets follows command-and-control model in which central server controls the bots in the network.

Man-in-the-Middle: Man- in- the- Middle (MitM) attacks occurs when the hacker breaches communication between two end system by injecting a malicious node between the legitimate nodes or by targeting the communication protocols in IoT network. Through the MitM concept, the hackers can alter the traffic flow, reconfigure the network topology, create fake identities, and generate malicious and false information to compromise an IoT system. The variants of MitM attack are eavesdropping, Sybil attack, Wormhole attacks, Identity replication attack, Node replication attacks, etc.,

Eavesdropping attack is possible due to unsecured communication link to access personal data between two end devices. It is also known as sniffing or snooping attack.

If a weakened connection between an IoT device and server found, an attacker might be able to intercept network traffic and steal the possibly sensitive information that IoT devices transmit over enterprise networks.

Wormhole attack is an internal attack which is hard to identify. Attackers listens the activities of network without altering it.

Sinkhole attack creates network traffic by sending route request to neighbor node. It transmits fake information and collapses the entire network communication. It is the most destructive routing attacks in IoT environment.

Social Engineering: Social Engineering is the act of manipulating user and getting their confidential and sensitive information and gain illegal access to data. Attackers executes social engineering easily in IoT devices because IoT devices usually collect large volume of information, especially personal identification in case of wearables, health care to provide personalized and friendly services.

Denial of Services: DoS attack are common attacks in IoT systems. This happens when a requested service or resources is unavailable to the users. In a Distributed Denial of Service (DDoS) attack, many malicious systems are involved to attack one target. DoS attack can be possible in each layer of communication and it is shown in Table 1.

Privilege escalation: Attackers gain access to IoT resources which are protected from user or an application by exploiting flaws in design, device bugs or operating system bugs or through configuration of application-software.

Brute Force Password Attack: In Brute-force attacks, access to the device is possible due to the weakness of IoT device passwords.

Firmware hijacking: Firmware hijacking makes the attackers to hijack the device and download the malicious software. It is made possible, when an IoT devices download the firmware updates from an illegitimate source.

Physical tampering: In an IoT devices deployed environment, where the enterprise fails to control the device and the people who can access it, there exists physical threats. Moreover, globally, attacks emerge due to continues rapid expansion of IoT. Attackers make use of compromised IoT nodes to gain access to network and move more deeper into it by passing variety of security controls. Finally, attackers can send sensitive information to themselves via IoT devices.

Ransomware: Ransomware is one of the well-known bad attacks in IoT. Hackers can encrypt the critical data of the user and demand a ransom for decrypting the same. For example, the intruders can tamper a smart health care system and send a notification to the owner to pay a ransom. It can also use to attack IIoT.

In IoT network, various attacks are possible and it leads to security and privacy issues. Implementing legacy network attack detection techniques is not possible due to the resource constraints of IoT devices and of different protocols used. The proposed work focuses on detecting End-point Man-in-the-Middle (MitM) attack using regression analysis:

- Simulating an IoT nodes and generating both normal and adversary (MitM) data traffic using NS2 tool.

- Three machine techniques such as Linear Regression (LR), Multilinear Regression (MLR) and Gaussian Process Regression (GPR) applied to collected data set.
- Performance of techniques analyzed with both positive and negative measures.
- Proved that Gaussian Process Regression technique provides greater accuracy in detecting the attack while identifying the path between the source and the destination.
- The main contribution of the proposed work is as follows:
- To enhance privacy in IoT network by detecting Man-in-the-Middle attack.
- No need of central controller to detect the attack. Hence, each source node in IoT LAN finds attack free path (without MitM node) to the destination node on its own.
- Provides a higher detection rate of attack and lower false measures.

The remaining of the paper organized as follows: Section2 includes Literature survey regarding various approaches for enhancing security in IoT networks. Section3 depicts proposed attack detection framework. Section4 discusses the experimental results of the proposed work and Section5 concludes the paper.

Section snippets

Literature survey

The previous studies related to enhancing security in IoT environment is depicted in the Table2 [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11]

From the survey, it is clear that IoT environment still vulnerable to many attacks and researches are going on in many aspects. This research work is focused on detecting Man-in-the-Middle attack specific to end nodes attacker in IoT environment.…

Proposed work

As the name implies, in Man-in-the-Middle attack, attackers play a role between two legitimate users as shown in Fig1. In this, attackers eavesdrop the communication link and listen the conversation between two targets. Man in the Middle attack is possible in two ways: 1) by placing an adversary node between the legitimate nodes or 2) by injecting malicious code or software on the target host machine.

For instance, think where a malicious user takes the control of heat monitoring device and…

Experiments and results

This section explains the performance metrics used in the proposed work and the findings of the regression modeling illustrated.

True Positive (TP) rate refers the attacks correctly predicted as attacks, True Negative (TN) rate refers the normal traffic predicted correctly as normal, False Positive (FP) refers the wrong identification of non-attack traffic as malicious, False Negative (FN) refers the wrong identification of attack as non-attack. P' and N' refers the total number of instances…

Conclusion

This paper provides solution to detect and mitigate MitM attack in IoT network. For adversary node detection, this work proposed Regression modeling to find the attack-free route from source to the destination. Three machine learning regression techiques LR, MLR and GPR are implemented and perfomance of each techniques are analyzed

based on various metrics. Packet loss ratio and throughput of each classifier is also estimated and analyzed. Results shows that among the three, the performance of…

Declaration of Competing Interest

None.…

Sivasankari Nitiynandan, born in Puducherry on 13th September 1985. She received the BCA degree in Computer Applications and MCA degree in Computer Application from Pondicherry University, India in 2005 and 2008 respectively. Currently she is working as a Teaching Fellow in Anna University, Chennai and pursuing her part-time research in VISTAS, in the field of securing Internet of Things application using Machine Learning techniques. Her areas of interest are IoT, Machine Learning, Network…

Recommended articles

References (11)

G. Hatzivasilis *et al.*
WARDOG: awareness Detection Watchdog for Botnet Infection on the Host Device
IEEE TRANS SUSTAINABLE COMPUT (2021)

Ryan Heartfield *et al.*
Anatolij Bezemskij, and Emmanouil Panaousis, “self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning
IEEE Trans Inf Forensics Secur (2021)

Weizhi Meng *et al.*
Enhancing medical smartphone networks via blockchain-based trust management against insider attacks
IEEE Trans Eng Manage (2020)

A. Mourad *et al.*
Ad-hoc vehicular fog enabling cooperative low-latency intrusion detection
IEEE INTERNET OF THINGS J (2020)

Hamed Haddad Pajouh, Reza Javidan, Raouf Khayami, Ali Dehghantanha, And Kim-Kwang Raymond Choo, “A two-layer dimension...

There are more references available in the full text version of this article.

Cited by (17)

On the control of microgrids against cyber-attacks: A review of methods and applications
2024, Applied Energy

Show abstract

A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain
2023, Internet of Things (Netherlands)

Show abstract

Novel modified ANFIS based fuzzy logic model for performance prediction of FRCM-to-concrete bond strength

2023, Advances in Engineering Software

Show abstract

A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions

2022, Internet of Things (Netherlands)

> *Citation Excerpt :*
>
> ...Various approaches have been developed for the prediction and detection of the attack. Machine learning-based approaches for intrusion detection have begun to produce more and more successful results [28]. Malware is software that harms or provides unauthorized access to devices, websites, or networks for data breaches, identity theft, and espionage without the user's knowledge....

Show abstract

Enhancing IoT Security: An Innovative Key Management System for Lightweight Block Ciphers

2023, Sensors

Detection and Mitigation of Active Attacks in Ethereum Blockchain (EBC)-IoMT Based Smart Contract

2023, SSRN

View all citing articles on Scopus

Sivasankari Nitiynandan, born in Puducherry on 13th September 1985. She received the BCA degree in Computer Applications and MCA degree in Computer Application from Pondicherry University, India in 2005 and 2008 respectively. Currently she is working as a Teaching Fellow in Anna University, Chennai and pursuing her part-time research in VISTAS, in the field of securing Internet of Things application using Machine Learning techniques. Her areas of interest are IoT, Machine Learning, Network Security, and Wireless Sensor Network.

Dr. S. Kamalakkannan received his M.Sc Computer Science Degree from Bharathidasan University, M.Phil. Computer Science Degree from Periyar University, and Ph.D. in Computer Science from Vels Institute of Science, Technology & Advanced Studies (VISTAS) Tamil Nadu, India. He is currently working as Associate Professor, Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India, which is a well-known university. He has 17 years of teaching experience in both UG and PG level. His-research interest includes Data Mining, Big Data Analytics, and Block Chain Technology. He has produced five M.Phil. Research scholars. He has published more than 35 research articles in various international journals such as Scopus and UGC referred journal. He serves as an Examiner in various Universities and Colleges. He received Best Young Scientist award and Best Faculty award.

View full text