IEEE.org IEEE *Xplore* IEEE SA IEEE Spectrum More Sites

Donate Cart Create Account Personal Sign In

Browse My Settings Help

Access provided by:
Vels Institute of Science Technology & Advanced Studies (VISTAS)

Sign Out

Access provided by:
Vels Institute of Science Technology & Advanced Studies (VISTAS)

Sign Out

All

ADVANCED SEARCH

Conferences > 2023 International Conference...

Detection of Man in The Middle Attack in 5G IOT using Machine Learning

Publisher: IEEE

Cite This PDF

Arul Stephen. C ; A. Vijayalakshmi ; J. Broody ; J.Sri Sathishkumar ; Ebenezer Abishek.B ; Sathish Kumar P **All Authors** •••

1
Cites in Paper

79
Full Text Views

Alerts

Manage Content Alerts
Add to Citation Alerts

Abstract

Document Sections

Show Full Outline ▾

Authors

Figures

References

Citations

Keywords

Metrics

Downl

PDF

Abstract:
Detection is therefore a vital element of any wireless network's security solution. Consequently, a dependable wireless intrusion detection system capable of identifying ... **View more**

Metadata

Abstract:
Detection is therefore a vital element of any wireless network's security solution. Consequently, a dependable wireless intrusion detection system capable of identifying Man-in-the-Middle attacks within the Internet of Things is shown here. In this study, empirical evidence is presented to support the notion that a Man-in-the-Middle attack results in a much longer delay than other forms of attacks. In order for organizations to properly protect their sensitive data, they require a way of forecasting MITM attacks that is both faster and more accurate. Our investigations into this occurrence will be oriented on enhancing our preparedness for future attacks of a similar sort. To identify Man-in-the-Middle (MITM) attacks, we examined a number of machine learning algorithms and evaluated them by applying them to a log collection gathered from Internet of Things devices. A variety of performance measures for models were the subject of study. The GNB methodology requires much less time for both prediction and testing than other methods such as KNN and Random Forest. With a probability of 99.6 percent, GNB is extremely likely to be true. As a result, the GNB method is enough for assessing the presence or absence of an MITM attack..

Published in: 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET)

Date of Conference: 23-24 November 2023

DOI: 10.1109/ICRASET59632.2023.10420166

More Like This

Date Added to IEEE *Xplore*: 08 February 2024

Publisher: IEEE

▸ **ISBN Information:**

Conference Location: B G NAGARA, India

Contents

I. Introduction

IoT refers to communication between devices or the cloud by certain standards. The use of wireless sensor nodes to connect various devices to the IoT using 5G technology enhances bandwidth and reduces latency. With the increasing demand of Iota, the number of devices connected to the network increases, resulting in various network or data security attacks, leading to the loss of personal information to unauthorized persons. A unique ID is used to connect various devices to a particular network. This network employs different topologies like star, mesh, and bus for interconnecting various devices. Clustering techniques are employed to group various network components depending on the coverage area. Applications that involve health monitoring or wildlife monitoring require time-to-time sensed information from the concerned nodes. The information is sensed and sent to the sink via the cluster head. In the case of clustering, the dates are aggregated and shared through the gateway node. The nodes must have a sufficient energy level which is the threshold value to transmit the information in case of node failure Alternative paths are chosen for the transferring of information[1]. The sensed data is averaged and sent to the edge node such that energy utilization is reduced. There are resource constraints in various sensor devices connected through wireless mode, like hidden terminal problems, out of reach since it is a dynamic environment. With the integration of 5G the application of IoT is sure to increase in the days to come. With the implementation of 5G, which is expected to be in 2023, the vulnerabilities due to the integration of technology are going to be a difficult task since security is a major issue in all aspects. Thus, encryption and decryption techniques are to be used to preserve data from various attacks, either passive or active. Despite the various advantages, there are a few disadvantages in terms of security issues.

Sign in to Continue Reading

Authors

Figures

References

Citations

Keywords

Metrics

More Like This

A discrete addressing scheme for Wireless Sensor Networks based Internet of Things
2016 Twenty Second National Conference on Communication (NCC)
Published: 2016

A Comprehensive Study on Machine Learning Algorithms for Wireless Sensor Network Security
2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)
Published: 2020

Show More

IEEE Account

- Change Username/Password
- Update Address

Purchase Details

- Payment Options
- Order History
- View Purchased Documents

Profile Information

- Communications Preferences
- Profession and Education
- Technical Interests

Need Help?

- **US & Canada:** +1 800 678 4333
- **Worldwide:** +1 732 981 0060
- Contact & Support

About IEEE *Xplore* | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies