



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379



9940 572 462



6381 907 438



ijircce@gmail.com



www.ijircce.com

Wireless Network Attacks Using Supervised Machine Learning Techniques

Sunderwaran.S, Pavithra.k, Pooja.S, Logeswari.S, D. Nirmala

Student, Department of ECE, T.J.S. Engineering College, Chennai, Tamil Nadu, India

Student, Department of CSE, T.J.S. Engineering College, Chennai, Tamil Nadu, India

Student, Department of CSE, T.J.S. Engineering College, Chennai, Tamil Nadu, India

Student, Department of CSE, T.J.S. Engineering College, Chennai, Tamil Nadu, India

Assistant Professor, Department of ECE, T.J.S. Engineering College, Chennai, Tamil Nadu, India

ABSTRACT: Network attacks pose a significant threat to the security and integrity of computer networks. The ability to predict and prevent these attacks is crucial for maintaining a secure network environment. Supervised machine learning techniques have emerged as effective tools for network attack prediction due to their ability to analyse large amounts of network data and identify patterns indicative of malicious activity. We present a comprehensive analysis of supervised machine learning techniques for the prediction of network attacks. We collect and pre-process the data, extracting relevant features and transforming them into a suitable format for machine learning algorithms.

We evaluate the performance of these algorithms. We investigate the interpretability of the trained models to gain insights into the underlying patterns and characteristics of network attacks. This allows network administrators to understand the nature of attacks and develop appropriate defences strategies. Additionally, we discuss the challenges and limitations associated with the application of supervised machine learning techniques in the domain of network attack prediction, such as the need for real-time analysis and the emergence of sophisticated evasion techniques.

KEYWORDS: Wireless Networks, Network Security, Intrusion Detection, Cyber Attacks, Supervised Learning, Machine Learning.

I. INTRODUCTION

The most devastating and complicated attack in a wireless sensor network is the Wormhole attack. In this attack, the attacker keeps track of the packets and makes a tunnel with other nodes of different communication networks, and thus the attacker passes the packets through this tunnel. And the outsider attack can be prevented by authentication and encryption techniques by launching a Sybil attack on the sensor network. In WSN the routing protocols in network has a unique identity. The figure demonstrates Sybil attack where an attacker node AD' is present with multiple identities.

II. OBJECTIVES

Use supervised machine learning algorithms to detect unauthorized access or malicious activities within a wireless network. This could involve classifying network traffic into normal and abnormal categories, allowing for the identification of potential security threats. Train supervised machine learning models to identify anomalous behavior or patterns within wireless network traffic. This could help in detecting previously unseen attacks or deviations from normal network behavior Utilize supervised machine learning techniques to classify different types of network traffic, such as distinguishing between web browsing, email communication, streaming media, etc. This classification can aid in understanding network usage and identifying potentially malicious activities.

III. LITERATURE SURVEY

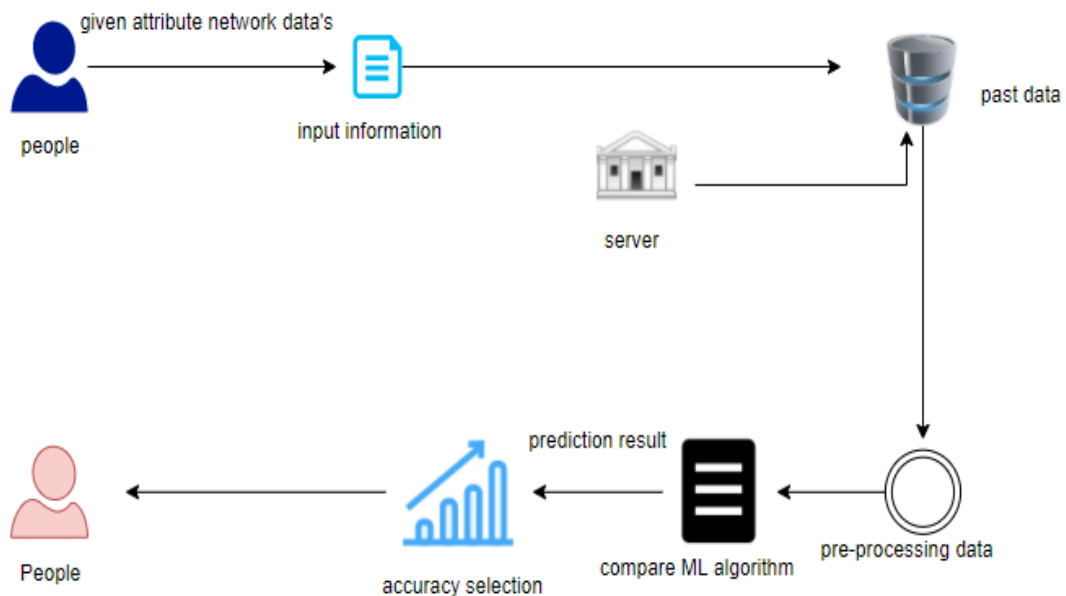
Title: Evaluation of Machine Learning Algorithms for Intrusion Detection System in WSN

Author: Mohammed S.Alsahli, Marwah M.Almasri, Mousa Al-Akhras, Abdulaziz I.Al-Issa, Mohammed Alawairdhi

Year: 2021

Technology has revolutionized into connecting “things” together with the rebirth of the global network called Internet of Things (IoT). This is achieved through Wireless Sensor Network (WSN) which introduces new security challenges for Information Technology (IT) scientists and researchers. This paper addresses the security issues in WSN by establishing potential automated solutions for identifying associated risks. It also evaluates the effectiveness of various machine learning algorithms on two types of datasets, mainly, KDD99 and WSN datasets. The aim is to analyze and protect WSN networks in combination with Firewalls, Deep Packet Inspection (DPI), and Intrusion Prevention Systems (IPS) all specialized for the overall protection of WSN networks. Multiple testing options were investigated such as cross validation and percentage split. Based on the finding, the most accurate algorithm and the least time processing were suggested for both datasets.

IV. SYSTEM ARCHITECTURE



V. IMPLEMENTATION

Framework Django is a web framework from Python language. Django provides a library and a collection of codes that can be used to build websites, without the need to do everything from scratch. But Framework Django still doesn't use the Model View Controller (MVC) method. Django-RESTful is an extension for Django that provides additional support for building REST APIs. You will never be disappointed with the time it takes to develop an API. Django-RESTful is a lightweight abstraction that works with the existing ORM/libraries. Django-RESTful encourages best practices with minimal setup.

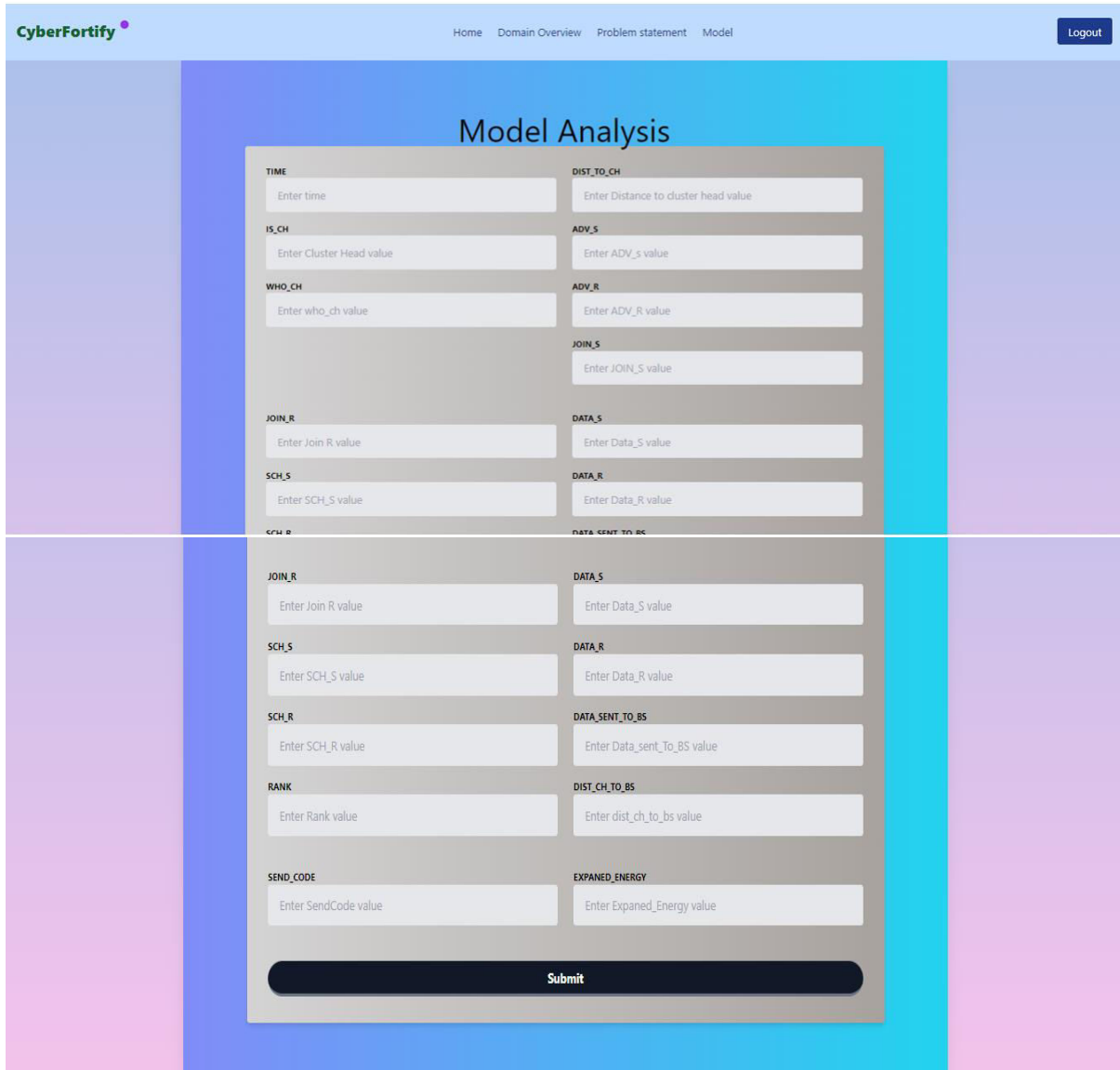
Start Using an API

1. Most APIs require an API key. ...
2. The easiest way to start using an API is by finding an HTTP client online, like REST-Client, Postman, or Paw.
3. The next best way to pull data from an API is by building a URL from existing API documentation.

Parameters

- **rule** (*str*) – The URL rule string.
- **endpoint** (*Optional[str]*) – The endpoint name to associate with the rule and view function. Used when routing and building URLs. Defaults to `view_func.__name__`.
- **view_func** (*Optional[Callable]*) – The view function to associate with the endpoint name.

VI. RESULTS



The screenshot shows a web application interface for 'Model Analysis'. The interface includes a navigation bar with 'Home', 'Domain Overview', 'Problem statement', and 'Model' links, and a 'Logout' button. The main content area contains a form with the following fields:

- TIME: Enter time
- DIST_TO_CH: Enter Distance to cluster head value
- IS_CH: Enter Cluster Head value
- ADV_S: Enter ADV_s value
- WHO_CH: Enter who_ch value
- ADV_R: Enter ADV_R value
- JOIN_S: Enter JOIN_S value
- JOIN_R: Enter Join R value
- DATA_S: Enter Data_S value
- SCH_S: Enter SCH_S value
- DATA_R: Enter Data_R value
- SCH_R: Enter SCH_R value
- DATA_SENT_TO_BS: Enter Data_sent_To_BS value
- RANK: Enter Rank value
- DIST_CH_TO_BS: Enter dist_ch_to_bs value
- SEND_CODE: Enter SendCode value
- EXPANDED_ENERGY: Enter Expanded_Energy value

A 'Submit' button is located at the bottom of the form.

VII. CONCLUSION

The analytical process started from data cleaning and processing, missing value, exploratory analysis and finally model building and evaluation. The best accuracy on public test set is higher accuracy score will be find out by comparing each algorithm with type of all WSN Attacks for future prediction results by finding best connections. This brings some of the following insights about diagnose the network attack of each new connection. To presented a prediction model with the aid of artificial intelligence to improve over human accuracy and provide with the scope of early detection. It can be inferred from this model that, area analysis and use of machine learning technique is useful in developing prediction models that can helps to network sectors reduce the long process of diagnosis and eradicate any human error.

REFERENCES

1. Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717-2727.



2. Bhattacharyya, A., Kalita, J. K., & Kar, S. (2020). A Survey on Intrusion Detection System Using Machine Learning Techniques. *Wireless Personal Communications*, 110(3), 1217-1248.
3. Fortino, G., Parisi, D., Pirrone, V., & Russo, W. (2018). A machine learning approach for the detection of TCP SYN flood attacks. *Future Generation Computer Systems*, 86, 920-934.
4. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning* (Vol. 1). MIT press Cambridge.
5. Gupta, R., Gupta, B. B., & Joshi, R. C. (2019). Intrusion detection system using machine learning and deep learning techniques: A review. *Journal of Network and Computer Applications*, 128, 82-103.
6. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436-444.
7. Li, K., Li, J., & Yang, X. (2019). Detecting DoS attacks using a stacked autoencoder-based ensemble learning method. *Future Generation Computer Systems*, 90, 246-256.
8. Raza, M. A., & Shafiq, M. Z. (2019). An Efficient Intrusion Detection System Based on Ensemble Machine Learning Algorithms for Improving the Performance of Wireless Network. *Wireless Personal Communications*, 109(2), 915-939.
9. Saxena, S., & Upadhyay, H. (2020). A Comprehensive Study on Machine Learning-based Intrusion Detection Techniques for Wireless Sensor Networks. *Wireless Personal Communications*, 110(2), 821-850.
10. Sharafaldin, I., Lashkari, A. H., & Ghorbani, A. A. (2018). Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In *Proceedings of the 4th International Conference on Information Systems Security and Privacy* (pp. 108-117).



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details