IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PHYSICAL LAYER SECURITY: DETECTION OF ACTIVE EAVESDROPPING ATTACKS

[1]Girija V, [2]Poovarasan G, [3]Vidhya Sri G, [4]Dr.G. Singaravel.

[1,2,3]Student, B-Tech-Information-Technology, K.S.R College of Engineering, Tiruchengode, Tamilnadu, India.

[4]Head of the Department, B-Tech-Information-Technology, K.S.R College of Engineering, Tiruchengode, Tamilnadu, India.

Abstract:

Frothy Disturbance Intrusion Detection Systems (FIDSs) can help detect and prevent security attacks using the Support Vector Machine (SVM) algorithm. Recognizing the importance of FIDS in protecting various domains linked to the internet, we concentrate on adapting traditional intrusion detection methods for the landscape, which faces challenges such as resource constraints and limited memory and battery capacity. Our study entails the creation of a lightweight attack detection technique that uses a supervised machine learning-based FIDS using the SVM algorithm. We use simulations to demonstrate the usefulness of the proposed SVM-based FIDS classifier, which uses a combination of two or three complex features and achieves satisfactory classification accuracy and detection time. This strategy has the ability to enhance application security by effectively addressing the particular.

Keywords: Edge Computing, Frothy Disturbance, Distributed Systems, FIDs, SVM.

1. Introduction

In the realm of cybersecurity, conventional Intrusion Detection Systems (IDS) face significant challenges from the growing complexity and sophistication of network attacks, particularly with regard to imbalanced network traffic. Traditional IDS often fail to detect and respond effectively to anomalies when datasets are unbalanced and the distribution of malicious and legitimate activity is skewed [3]. To overcome these limitations, this work presents a novel strategy that makes use of Transformer-based transfer learning techniques. Proposed IDS aims to increase its flexibility and capacity to generalize to scenarios such as unbalanced network traffic by leveraging Transformer models, which have shown to be highly effective in sequence processing tasks. By improving the accuracy and efficacy of intrusion detection in the face [4]. IDS are defenses in the dynamic field of cybersecurity, serving as vigilant watchdogs against a multitude of potential dangers within digital networks. A crucial component of the defense against malicious activity, unauthorized access, and potential security breaches is an intrusion detection system (IDS) [11]. As a sophisticated surveillance system, IDS continuously keeps an eye on network traffic, looking for patterns and behaviors that may indicate potential security threats [6]. Because it integrates anomaly detection, heuristic analysis, and signature-based detection, IDS are critical to enhancing the resilience of digital infrastructures [7].

2. Literature Survey

A literature survey is a crucial part that provide a thorough analysis of the literature, conference proceedings, and research papers that have already been published and examine the use of SVM to identify physical layer hazards. Sort the literature review according to the main themes, techniques, datasets, and outcomes of the experiments.

Alfred Hero et al. (2023) produced, the cybersecurity is crucial, but security measures are not keeping up with the more skilled attackers who aim to compromise cyber systems. Beyond the conventional defenses like firewalls, password protection, and single point-of-attack defenses, new vulnerabilities have emerged with the advent of massively dispersed systems like the IoT [2].

Mansi Bhavsar et al. (2023) introduced, the Internet of Things, or "Internet of Things," is a vast field with many applications, including transportation, the military, healthcare, agriculture, and many more. It connects different physical items through the Internet. Since those apps deal with issues that arise in real time, they are becoming more and more well-liked [8].

Masoud Abdan and Seyed Amin Hosseini Seno (2022) applied, an assault on the network layer that mimics routing protocols is called a wormhole attack. Several machine learning techniques are used to conduct the classification, including naïve Bayes (NB), convolutional neural network (CNN), decision tree (DT), support vector machine (SVM), linear discrimination analysis (LDA), and closest neighbor (KNN) [9].

Mingfang Li and Zheng Dou (2023) proposed, the range of IoT device kinds and access techniques, it is still vital to solve the security issues we are currently facing. The next generation of IoT networks may benefit from simplified security solutions provided by physical layer security (PLS) [10].

Christantus O. Nnamaniv et al. (2023) proposed, the use of intelligent reflecting surfaces (IRS) carried by unmanned aerial vehicles (UAVs) to securely collect data from wireless sensor networks. Eve, the eavesdropper, is hiding close to Bob, the primary receiver [5].

QUN WANG et al. (2022) proposed, the rapid expansion of Internet-connected systems has given rise to a number of difficulties, including problems with spectrum scarcity that call for effective spectrum sharing (SS) solutions [13].

3. Existing System

Since radio propagation is unrestricted, wireless communication is extensively accessible. Data communication is now feasible and simple as a result. On the other side, unauthorized users may compromise the security of the data being delivered to authorized users. Existing System makes the network vulnerable to hacking, eavesdropping, and information jamming, among other threats. Physical layer security, or PLS, is one of the most promising security methods to prevent eavesdroppers from listening in on wireless network traffic. System serves as a substitute to the complex and computationally demanding cryptographic techniques and algorithms. There has been an exponential rise in research interest in PLS because to its potential to leverage the properties of wireless channel. One of the main characteristics of the broadcast route is its randomization. Due to the previously mentioned qualities, signals [1].

4. Proposed System

The suggested system is a FIDS that is intended to meet the unique issues of protecting varied domains connected with the internet, particularly those with limited resource availability and memory and battery capacity. The system is built around a well-designed sensor network that serves as the backbone for deploying the FIDS. The system uses the Ad-hoc On-demand Distance Vector (AODV) routing protocol for efficient communication and includes a lightweight attack detection method that employs a supervised machine learning-based FIDS using the SVM algorithm. The system's modules include building the sensor network, producing AODV packets with an emphasis on energy efficiency, identifying permitted and unauthorized ports, and controlling data transfer while checking the correctness of received packets. Simulations demonstrate the proposed system's classification accuracy and detection time, demonstrating its potential to improve application security by efficiently addressing the special restrictions of intrusion detection in resource-constrained contexts.

4.1 Constructing Sensor Network Module

Module creates and organizes the sensor network, which serves as the foundation for the FIDS. Entails creating the topology, configuring nodes, and implementing communication protocols for the sensor network. The goal is to build a strong and efficient network infrastructure that will facilitate the implementation of the intrusion detection system [12].

4.2 Find Authorized and Unauthorized Port

Module distinguishes between authorized and unauthorized ports in the sensor network. It is likely to include a method for monitoring and analyzing network traffic, as well as scanning communication ports for irregularities [13]. Detecting illegal ports is critical for identifying potential security concerns, and this adds to the system's total intrusion detection capacity [14].

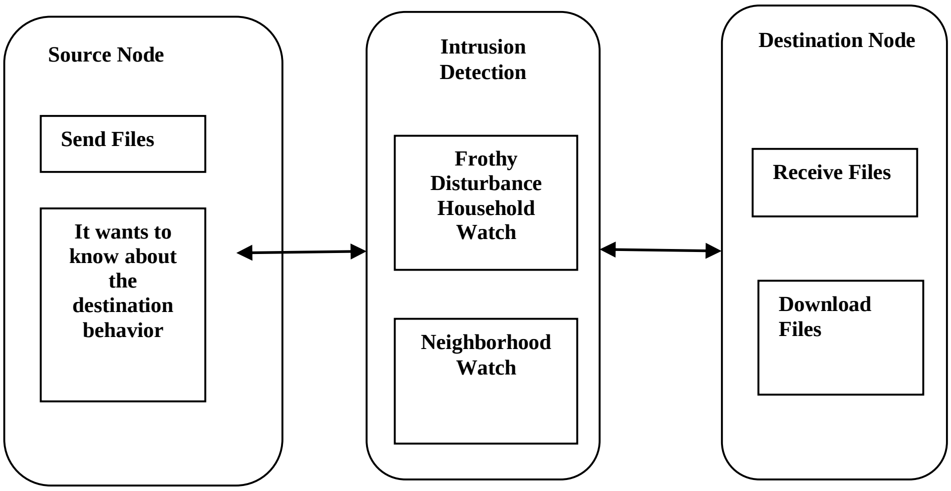

Figure 4.1 Block diagram of FIDS

4.3 Data Transmission and Verification Receiving the Valid Packet

The data transmission module controls information flow in the sensor network. It entails the transfer of AODV packets and other pertinent information. The verification process guarantees the integrity and authenticity of received packets [15]. Module is expected to use the SVM technique indicated in the abstract for successful intrusion detection [16]. Valid packets are processed further, whereas suspicious or unauthorized packets initiate appropriate security steps [17], [18].

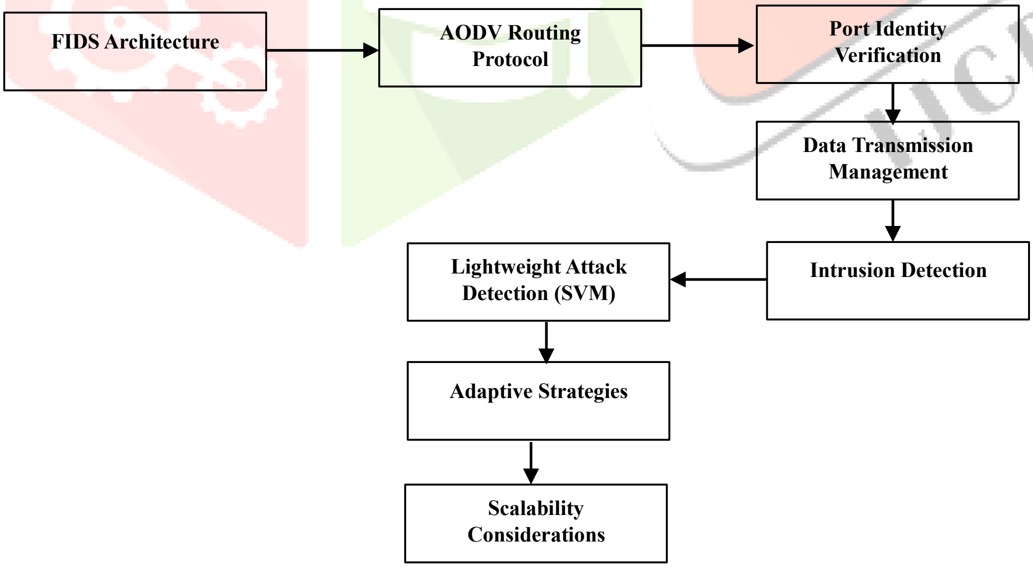
FIDS Architecture
AODV Routing Protocol
Port Identity Verification
Data Transmission Management
Intrusion Detection
Lightweight Attack Detection (SVM)
Adaptive Strategies
Scalability Considerations

Figure 4.2 FIDS Architecture

5. Algorithm Details

A well-liked supervised machine learning model for categorization and prediction of unknown data is called SVM. Many academics claim that SVM is a very accurate text categorization method. It is also often used to the categorization of emotion [19], [20]. For example, we may train a model to categorize incoming data into the positive and negative review categories if we have a dataset with data already pre-labeled into these two groups. In order for the model to assess and categorize unknown data into the categories that were present in the training set, we train it on a dataset [21]. SVM is a technique for linear learning. It determines the best hyper-plane to distinguish between two classes. As a supervised classification model, it seeks to improve classification performance on test data by maximizing the distance between the nearest training point and either class [22].

```
from sklearn.svm import SVC
# Instantiate SVM classifier
svm_model = SVC (kernel='linear', C=1.0)
# Train the model
svm_model.fit (X_train, y_train)
# Make predictions
svm_predictions = svm_model.predict(X_test)
```

6. Result Analysis

The table that follows compares the accuracy of a suggested algorithm with an existing one for the FIDS with SVM for the Internet of Things. The recently suggested approach shows a significant improvement with an accuracy of 88%, while the current algorithm only manages a recognition accuracy of 75%. This significant improvement in accuracy highlights the effectiveness of the suggested lightweight attack detection approach, which makes use of signature criteria, supervised machine learning, and anomaly-based detection.

Table 6.1 Comparison table of Existing System and Proposed System

Algorithm	Accuracy
Existing System	75
Proposed System	88

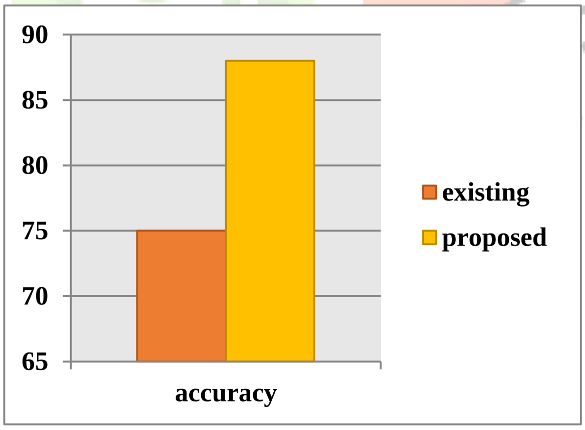

Figure 6.1 Comparison graph *of* Existing System and Proposed System

7. Conclusion and Future Work

To summarize, the created FIDS provides a comprehensive solution optimized for safeguarding varied domains integrated with the internet, particularly those confronting resource limits and limited memory and battery capacity. The suggested system efficiently fulfills the special requirements of identification of intrusions in resource-constrained contexts by integrating a well-constructed sensor network with a lightweight attack detection method based on the SVM algorithm. The simulation results demonstrate the system's efficiency, with remarkable performance in terms of classification accuracy and detection time.

The FIDS may be extended and improved in the future. To begin, investigating the integration of alternative machine learning algorithms alongside the Support Vector Machine (SVM) could provide a comparison analysis to choose the most appropriate method for various scenarios. Furthermore, the system may benefit from scalability considerations to support larger and more complicated sensor networks. Further study could also focus on developing adaptive algorithms that dynamically modify intrusion detection parameters in response to the network's changing features and possible threats.

8. References

[1] Abraham Sanenga, Galefang Allycan Mapunda, Tshepiso Merapelo Ludo Jacob, Leatile Marata, Bokamoso Basutli and Joseph Monamati Chuma 2020, “An Overview of Key Technologies in Physical Layer Security”, Entropy, Vol. 22, DOI: doi:10.3390/e22111261.

[2] Alfred Hero, Soummya Kar, Jose Moura, Joshua Neil, H. Vincent Poor, Melissa Turcotte, 2and Bowei Xi 2023, “Statistics and Data Science for Cybersecurity”, Harvard data science review, DOI: 10.1162/99608f92.a42024d0.

[3] Alon Hillel-Tuch 2021,” Data Siphoning Through Advanced Persistent Transmission Attacks At The Physical Layer”, SSRN, Hillel-Tuch, Alon, Data Siphoning Through Advanced Persistent Transmission Attacks At The Physical Layer. Available at SSRN: https://ssrn.com/abstract=3890371, DOI: http://dx.doi.org/10.2139/ssrn.3890371.

[4] Asadullah Momand, Sana Ullah Jan and Naeem Ramzan 2023,” A Systematic and Comprehensive Survey of Recent Advances in Intrusion Detection Systems Using Machine Learning: Deep Learning, Datasets, and Attack Taxonomy”, Journal of Sensors, Article ID. 6048087, DOI: https://doi.org/10.1155/2023/6048087.

[5] Christantus O. Nnamani, M. R. A. Khandaker, and M. Sellathurai 2022, “UAVaided jamming for secure ground communication with unknown eavesdropper location,” IEEE Access, vol. 8, pp. 72 881–72 892.

[6] Fang Xu, Sajed Ahmad, Muhammad Naveed khan, Manzoor Ahmed, Salman Raza, Feroz Khan, Yi Ma and Wali Ullah Khan 2023, “Beyond encryption: Exploring the potential of physical layer security in UAV networks”, Journal of King Saud University - Computer and Information Sciences, vol. 35, Issue No. 8.

[7] Lamia Alhoraibi, Daniyal Alghazzawi, Reemah Alhebshi and Osama Bassam J. Rabie 2023, “Physical Layer Authentication in Wireless Networks-Based Machine Learning Approaches”, Sensors, vol. 23(4), 1814, DOI: https://doi.org/10.3390/s23041814.

[8] Mansi Bhavsar, Kaushik Roy2, John Kelly and Odeyomi Olusola 2023,” Anomaly-based intrusion detection system for IoT application”, Discover Internet of Things, DOI: https://doi.org/10.1007/s43926-023-00034-5.

[9] Masoud Abdan and Seyed Amin Hosseini Seno 2022, “Machine Learning Methods for Intrusive Detection of Wormhole Attack in Mobile Ad Hoc Network (MANET)”, Wireless Communications and Mobile Computing, Article ID 2375702, DOI: https://doi.org/10.1155/2022/2375702.

[10] Mingfang Li and Zheng Dou 2023, ”Active eavesdropping detection: a novel physical layer security in wireless IoT”, EURASIP Journal on Advances in Signal Processing, DOI: https://doi.org/10.1186/s13634-023-01080-5.

[11] Monette H. Khadr, Hany Elgala, Michael Rahaim, Abdallah Khreishah, Moussa Ayyash and Thomas Little 2021, “Machine learning-based security-aware spatial modulation for heterogeneous radio-optical networks”, Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, DOI: https://doi.org/10.1098/rspa.2020.0889.

[12] Nnamani, Christantus O., M. R. Khandaker, and M. Sellathurai 2021, “Secrecy rate maximization with gridded UAV swarm jamming for passive eavesdropping”, IEEE Global Commun. Conf. (GLOBECOM), 2021, pp. 01–06.

[13] QUN WANG, HAIJIAN SUN, ROSE QINGYANG and ARUPJYOTI BHUYAN”, When Machine Learning Meets Spectrum Sharing Security: Methodologies and Challenges”, IEEE Open Journal of the Communications Society, vol. 3, r 10.1109/OJCOMS.2022.3146364.

[14] Rajendran T, Abishekraj E and Dhanush U 2023, “Improved Intrusion Detection System That Uses Machine Learning Techniques to Proactively Defend DDoS Attack”, ITM Web of Conferences, DOI: https://doi.org/10.1051/itmconf/20235605011.

[15] Robin Gassais, Naser Ezzati- Jivan, Jose M. Fernande, Daniel Aloise and Michel R. Dagenais 2020, “Multi-level host-based intrusion detection system for Internet of things”, Journal of Cloud Computing: Advances, Systems and Applications, DOI: https://doi.org/10.1186/s13677-020-00206-6.

[16] Subrato Bharati and Prajoy Podder 2021, “Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions”, Security and Privacy Challenges in Internet of Things and Mobile Edge Computing, Article ID. 8951961, DOI: https://doi.org/10.1155/2022/8951961.

[17] Tiep M. Hoang, Alireza Vahid, Hoang Duong Tuan, and Lajos Hanzo 2023, “Physical Layer Authentication and Security Design in the Machine Learning Era”, IEEE Communications Surveys & Tutorials, pp. (99):1-1, DOI: 10.1109/COMST.2024.3363639.

[18] Vinay Gugueoth, Sunitha Safavat, Sachin Shetty 2023, “Security of Internet of Things (IoT) using federated learning and deep learning — Recent advancements, issues and prospects”, The Korean Institute of Communications and Information Sciences, vol. 9, Issue No. 5, Pages: 941-960.

[19] Weiping Shi, Xinyi Jiang, Jinsong Hu, Abdeldime Mohamed Salih Abdelgader, Yin Teng, Yang Wang, Hangjia He, Rongen Dong, Feng Shu and Jiangzhou Wang 2022,” Physical layer security techniques for data transmission for future wireless networks”, Security and Safety, vol. 1, 2022007, DOI: https://doi.org/10.1051/sands/2022007.

[20] Wenli Duso1, MengChu Zhou and Abdullah Abusorrah 2022, “A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges”, IEEE/CAA Journal of Automatica Sinica, Volume 9 Issue 5, doi: 10.1109/JAS.2022.105548.

[21] Yong Wang, Jinsong Xi and Tong Cheng 2021, “The Overview of Database Security Threats’ Solutions: Traditional and Machine Learning”, Journal of Information Security, DOI: 10.4236/jis.2021.121002.

[22] Yu Zhang, Shuangrui Zhao, Ji He,[1,2]Yuanyu Zhang, Yulong Shen and Xiaohong Jiang 2023,” A Survey of Secure Communications for Satellite Internet Based on Cryptography and Physical Layer Security”, IET Information Security, Article ID 5604802, DOI: https://doi.org/10.1049/2023/5604802.