Cybersecurity

RESEARCH Open Access

Intrusion detection systems for wireless sensor networks using computational intelligence techniques

Vaishnavi Sivagaminathan[1*], Manmohan Sharma[1] and Santosh Kumar Henge[1]

Abstract

Network Intrusion Detection Systems (NIDS) are utilized to find hostile network connections. This can be accomplished by looking at traffic network activity, but it takes a lot of work. The NIDS heavily utilizes approaches for data extraction and machine learning to find anomalies. In terms of feature selection, NIDS is far more effective. This is accurate since anomaly identification uses a number of time-consuming features. Because of this, the feature selection method influences how long it takes to analyze movement patterns and how clear it is. The goal of the study is to provide NIDS with an attribute selection approach. PSO has been used for that purpose. The Network Intrusion Detection System that is being developed will be able to identify any malicious activity in the network or any unusual behavior in the network, allowing the identification of the illegal activities and safeguarding the enormous amounts of confidential data belonging to the customers from being compromised. In the research, datasets were produced utilising both a network infrastructure and a simulation network. Wireshark is used to gather data packets whereas Cisco Packet Tracer is used to build a network in a simulated environment. Additionally, a physical network consisting of six node MCUs connected to a laptop and a mobile hotspot, has been built and communication packets are being recorded using the Wireshark tool. To train several machine learning models, all the datasets that were gathered—created datasets from our own studies as well as some common datasets like NSDL and UNSW acquired from Kaggle—were employed. Additionally, PSO, which is an optimization method, has been used with these ML algorithms for feature selection. In the research, KNN, decision trees, and ANN have all been combined with PSO for a specific case study. And it was found demonstrated the classification methods PSO + ANN outperformed PSO + KNN and PSO + DT in this case study.

Keywords Network intrusion detection systems (NIDS), Cisco packet tracer, Wireshark tool, Machine learning, PSO, Cybersecurity, Optimization

Introduction

According to Musa et al. (2021), IDSs are "active processes or devices that review device and connection activities for unapproved and disagreeable behavior." IDS are available in three flavors. These categories include HIDS, NIDS, and hybrid-based IDS (Waskle 2020). The HIDS seeks to keep track of internal computer system activity. The NIDS's objective is to dynamically monitor the network traffic in real-time. In order to ascertain any potential network intrusions, the NIDS tries to accomplish that. It tries to do that by using the right detection techniques.

There are three distinct categories: hybrid IDS built on an IDS, exploitation identification, and anomaly detection (Ganesh and Sharma 2021). A collection of specified characteristics or criteria is used in the detection system to identify recognised hazards. The anomaly detection

*Correspondence:
Vaishnavi Sivagaminathan
vaishnavi.ganesh8@gmail.com
[1] Lovely Professional University, Phagwara, India

mechanism detects unidentified attacks on a regular basis. This is achieved by evaluating if the device's state is normal. The IDS classification for anomaly detection is shown in Fig. 1. A hybrid IDS may be able to spot both known and unidentified attacks. The focus of this essay is the NIDS. NIDS uses the entire network's traffic characteristics to detect threats. The NIDS is the subject of this article. NIDS uses the whole network's traffic characteristics to find hazards. The utilization of all capabilities is not necessary for attack detection.

Infiltration is a notion that exists anyplace there is connectivity. Applications comprise Wifi hotspots in big businesses, residential area networks, wireless sensor networks, and the Internet of Things. Securing sensitive data kept in various databases is essential. Customer-related information, such as TINs, dates of birth, and Aadhar card numbers, must be kept safe for this reason. As a result, intrusion detection systems become necessary. It is necessary to have systems for both intrusion detection and prevention (Sivagaminathan and Dr. Manmohan Sharma. 2021a).

DoS attacks, Man in the Middle attacks, sinkhole attacks, selected transmitting attacks, flooded attacks, worm attacks, etc. are just a few examples of the many

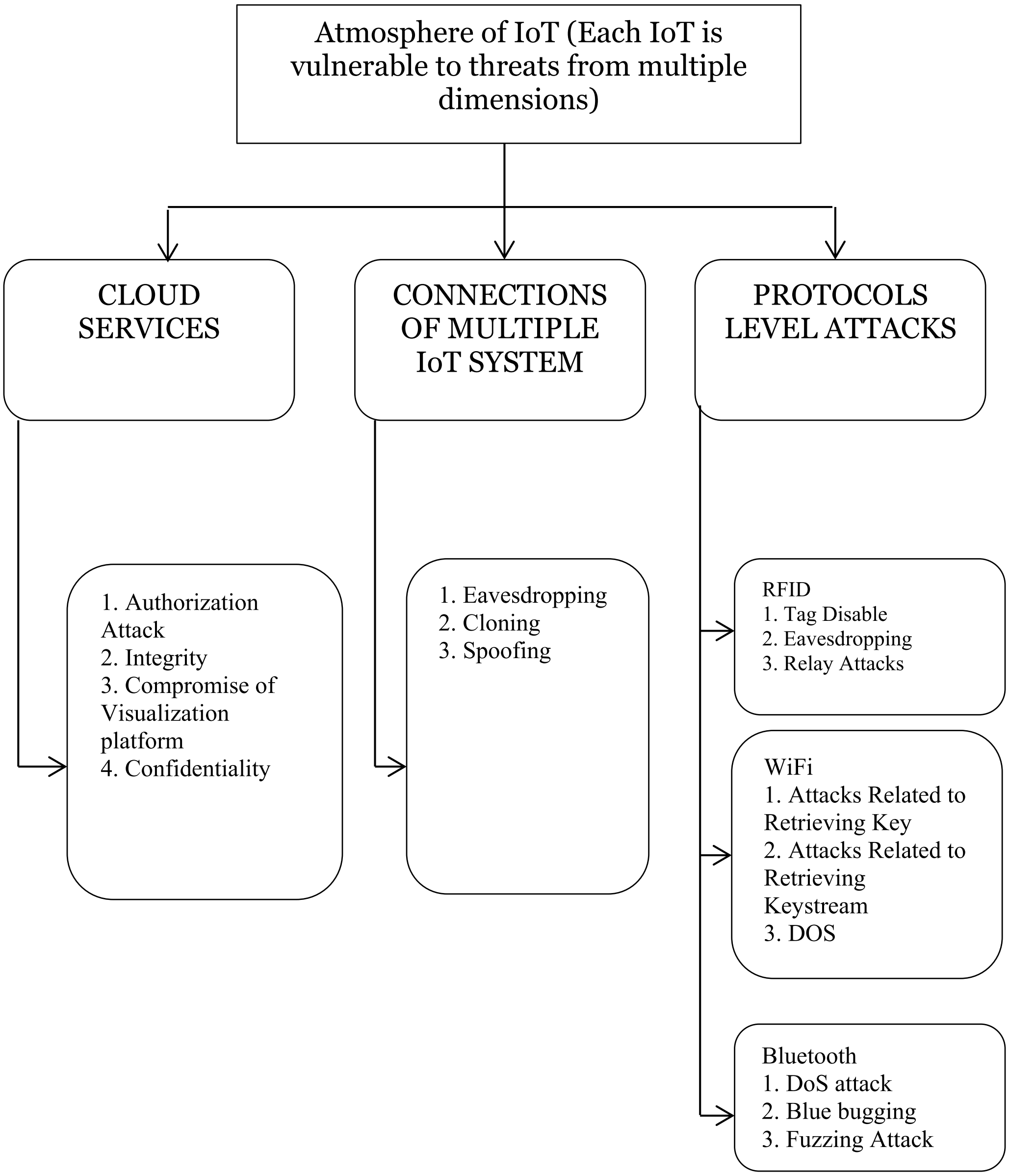


Fig. 1 IoT environment threat dimensions

diverse attack types that may be used. DoS attacks can involve saturating a server with phony information in an effort to jam the networks and block actual traffic from reaching the host. This regularly happens in the world of online business. It's possible for a site to purposefully flood other site's server with fictitious traffic. As a result, intrusion detection and prevention are crucial. (Bang et al. 2020).

Wireless sensors also demand penetration testing. All industries, including those connected to agriculture, business, building roads and traffic networks, the military, telecommunications, and the medical and health fields, employ WSNs. the tracking of patients' locations and the surveillance of elderly patients (Karimipour et al. 2019) are examples of how this is used in the health world.

The following are some IPDS systems that have been created in various fields:

a A commercially available NIDS tool called Snort was used to compare an intrusion detection network system's effectiveness (IDPS) that has been described. All Snort rules Utilize the prefix in the suggested system and randomized indexes techniques, and as during periods of intense network connections, key sequences are developed to decrease the duration of packet sniffing and the probability of false positives (Almomani and M. AL-Akhras 2016).

b Synchronized phasor systems may now identify malicious intrusions with the use of a tool called System for detecting intrusions specific to synchro phasors (SSIDS). It combines a behaviour patterns strategy and a diverse whitelist to detect both known and unidentified attacks. (Abdulaziz et al. 2019).

c To avoid intrusion, a solution known as home region network using ZigBee could use HANIDPS as just an intrusion protection and monitoring system has been developed (Firoz Kabir and Sven Hartmann 2018).

d An IDPS has also been created to safeguard linked automobiles' Controller Area network (CAN) buses. Real-time vehicle data may be provided through the Controller Area Network interface, which links sensing devices and controlling devices in a network for control applications (Yang et al. 2020). A serial automobile bus network is involved.

Threats to IoT settings come in many forms, both physical and virtual. Figure 1 demonstrates the many forms of cyber security included in the IoT process, including cloud services with multiple-system creation, and attack level. All of the above-mentioned categories have a high degree of assault; hence these procedures demand high-security characteristics on several dimensions (Jokar and Leung 2016; Sharma and Moller 2018). Despite the fact that several IoT systems provide poor attack characteristics, protocol-level feature implementations significantly superior than that used by all people. As a result, to prevent any sort of hazard from accessing the defined system, a greater feature is necessary.

The paper will follow the following format: The preparation of datasets utilising two pieces is covered in Sect. "Proposed methodology". Part a involves employing a simulation environment, such as the Wireshark and Cisco Packet Tracer tools. The development of datasets through a real, physical network made with node MCUs is covered in Part b (Jing et al. 2022). Several machine learning classifiers are trained in Sect. "ML classification model training using a variety of methods " utilising the datasets mentioned above and PSO as an optimization strategy. Section "Result and discussion" includes the findings and Discussions.

Proposed methodology

The proposed Methodology is as follows:

A variety of machine learning (ML) models, including Linear Regression, SVM, Decision Trees, Random Forest, k nearest neighbor (knn), Artificial Neural Networks, Adaboost, Naive Bayes classifier, and Bayesian classifiers, among others, are trained using the selected features, as shown in Fig. 2, and their prediction accuracy is determined (Zhao et al. 2022; Zhang et al. 2022a). To further improve the effectiveness of ML classifiers, PSO has also been used as an optimization strategy.

a) Creating datasets with the wireshark tool using a cisco packet tracer simulated network

The technique used in our proposed study was to first construct the network system with the appropriate node layout, as illustrated in Flowchart Fig. 3 (Mushtaq et al. 2022). This node was created using a distinctive network design (Transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems 2022). We set up Cisco Packet Tracer to initialize a model of the whole network architecture for this purpose. We have created a test network environment for this system with 5 source IP addresses, 13 destination IP addresses, and 9 protocols. ARP, BROWSER, DHCP, ICMPV6, IGMPV3, LLMNR, MDNS, NBNS, and SSDP were among the network protocols used (Ravi et al. 2022). Using the Cisco packet tracer simulator, the protocol was started for a duration of 10 min. There were no run time errors while the simulation was running since the run time was properly setup (Mokhtar Mohammadi et al. 2021; Lo et al. 2022)

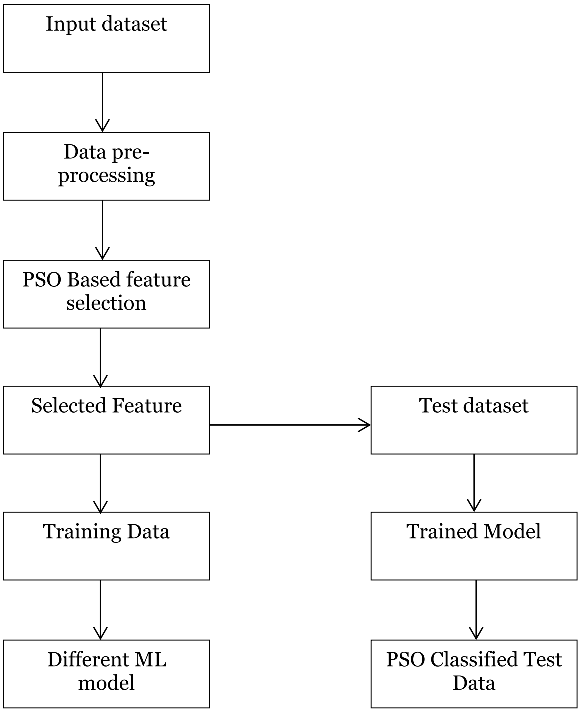


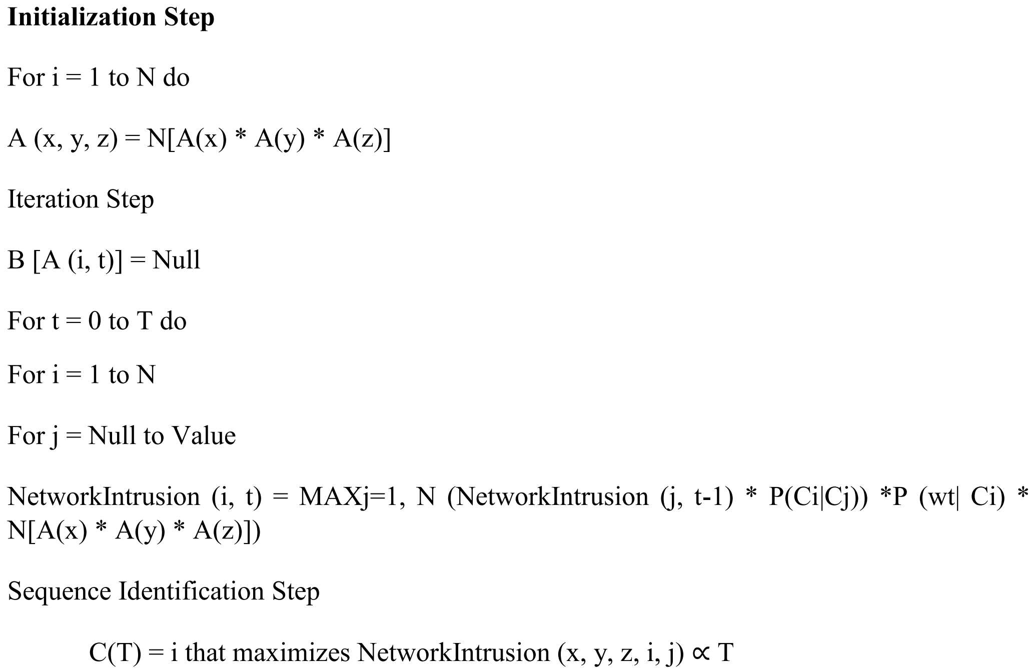
Fig. 2 Operating a better IDS system

through. Once the simulation model was fully modelled, we utilized the Wireshark system to gather data packet values for source, destination IP, and protocols with respect to time, allowing us to initialize the time domain model and create a more accurate and reliable prediction model.

Proposed algorithm

The suggested approach is made to lessen the features of network incursion for effective management of source and destination protocols on the available network bandwidth. Any network, including Bluetooth, 3G, 4G, 5G, Wi-Fi 2.4Ghz or Wi-Fi 33 5Ghz, may use this method. Understanding the method for determining the historical features of incursion flow on the specific network is necessary (Wang et al. 2022a). In order to comprehend the future mutation in the infiltration over any network bandwidth, this analysis is being taught utilizing neural networks (Wang et al. 2020). The method begins with the function A (x, y, z), where x, y, and z represent source IP, destination IP, and intrusion protocols, respectively.

We have I as a variable that identifies the features of an intrusion, j as the likelihood that the intrusion would be discovered, and x, y, and z as parameters that rely on the simulation model's functions (Saba et al. 2022; Maldonado et al. 2022).



```
Initialization Step
For i = 1 to N do
A (x, y, z) = N[A(x) * A(y) * A(z)]
Iteration Step
B [A (i, t)] = Null
For t = 0 to T do
For i = 1 to N
For j = Null to Value
NetworkIntrusion (i, t) = MAXj=1, N (NetworkIntrusion (j, t-1) * P(Ci|Cj)) *P (wt| Ci) * N[A(x) * A(y) * A(z)])
Sequence Identification Step
        C(T) = i that maximizes NetworkIntrusion (x, y, z, i, j) ∝ T
```

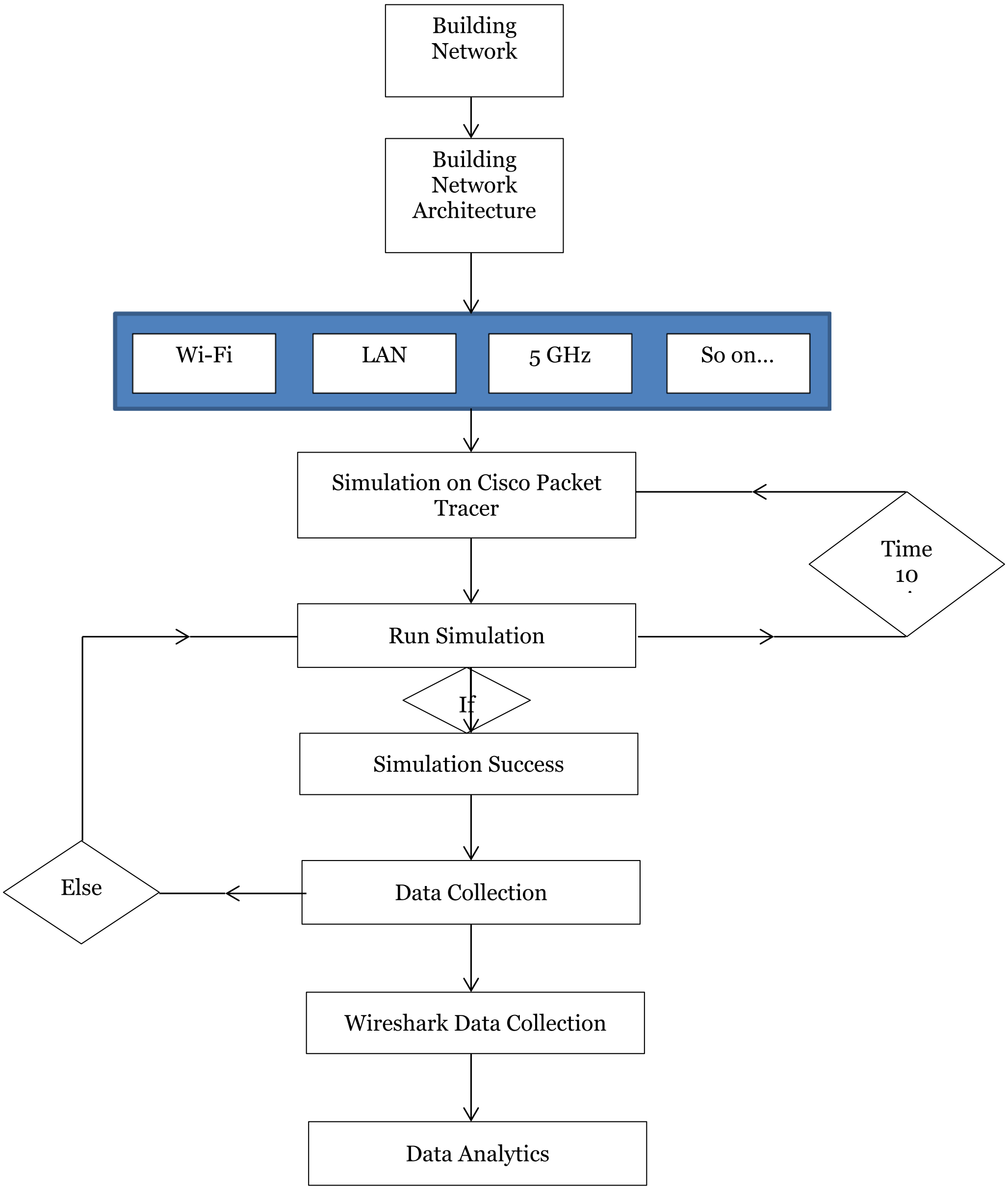


Fig. 3 Demonstrates the entire process of data collecting for any network simulation model

Back trace to find the sequence of Intrusion

The probability of the ideal sequence for source, destination, protocols, incursion, and values attributes is stored in the array Network Intrusion (X, Y, Z, I j). Certain network features will be given probability and weight in C(T) functions (Wang et al. 2022b).

1. Using Cisco Packet Tracer, a network made up of PCs, switches, and routers connected by LAN is built in the simulated scenario. Figure 4 illustrates that (Selection and for Intrusion Detection System et al. 2020).
2. Using the Wireshark tool, 10 min worth of activity on our laptop system, including the aforementioned conversation, is captured in the packets that were transmitted. The Wireshark tool is used to recover the protocols utilised, source IP addresses, destination IP addresses, and the length of communication between specified sources and specific destinations (Detecting botnet by using particle swarm optimization algorithm based on voting system 2020).
3. In order to determine which destination takes the longest, filters are now being used, graphs are being displayed, and each protocol is being examined indi-

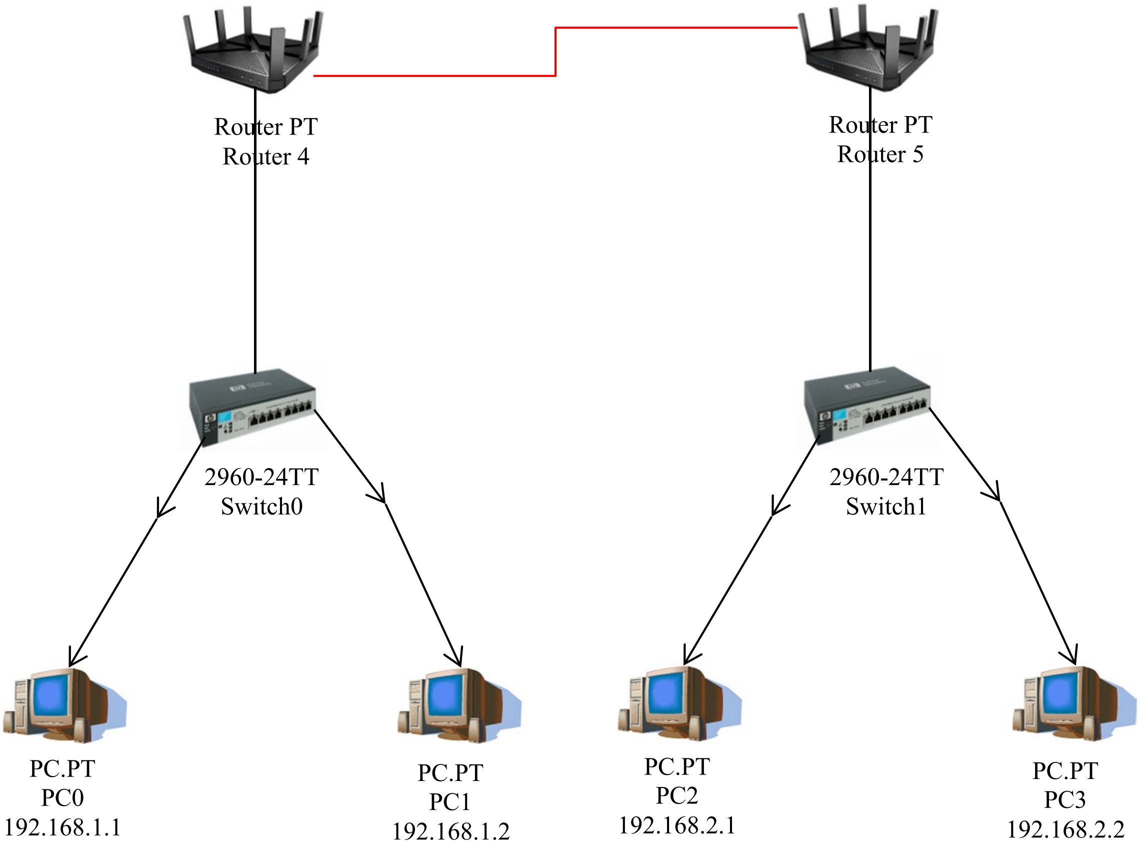


Fig. 4 Showing the test network architecture in Cisco packet tracer

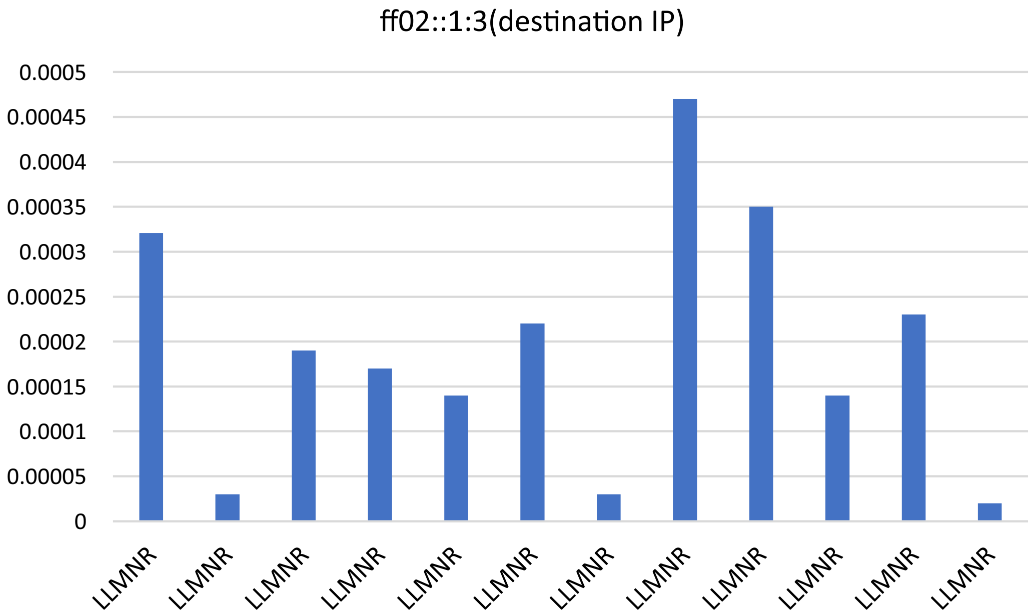


Fig. 5 Shows protocols vs (ff02::1:3) destination IP

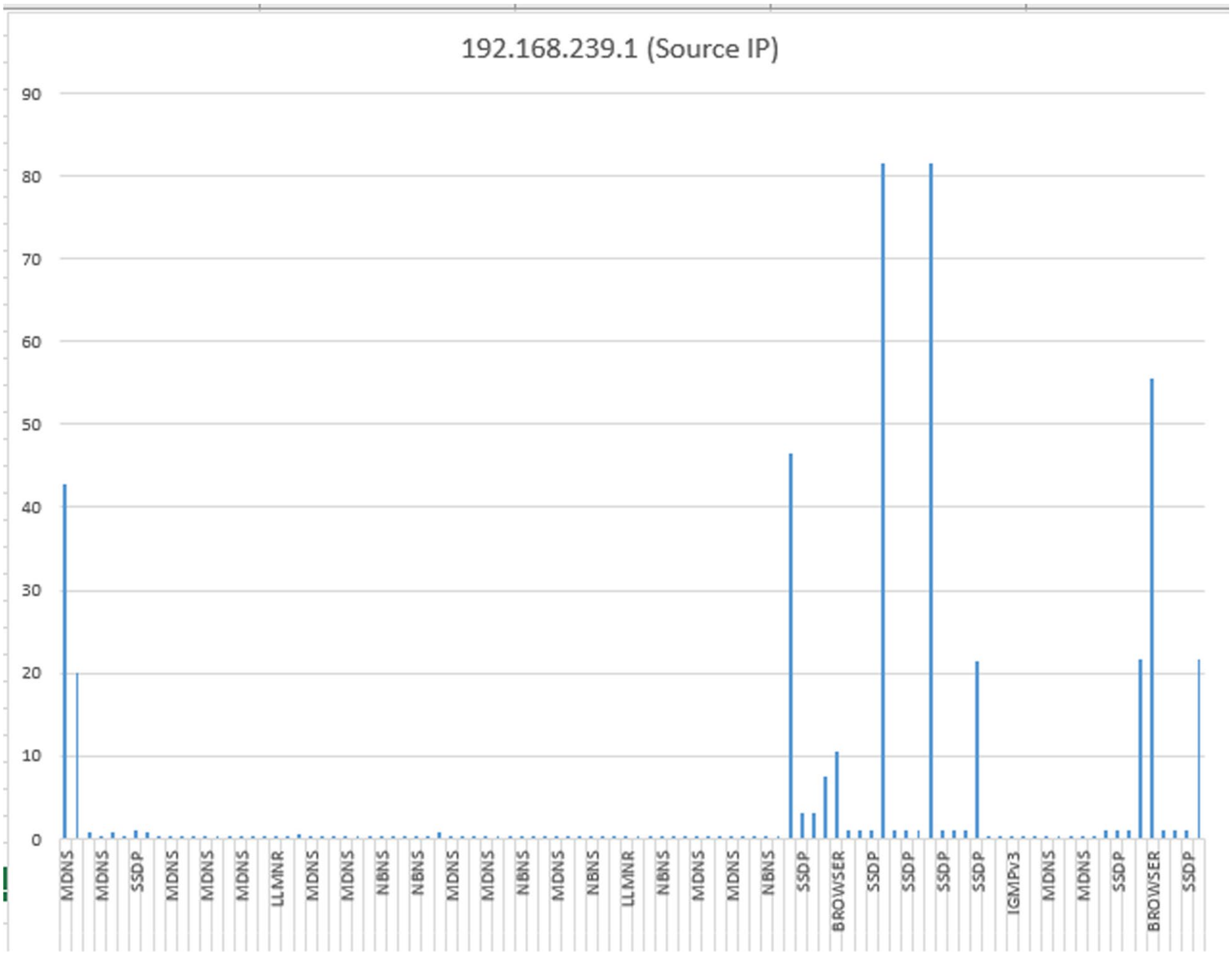


Fig. 6 Shows protocols vs (192.168.239.1) Source IP

vidually (Chohra et al. 2022). The area that is most affected is the one that occupies the majority of the graph's time. When a destination's maximum time is shown, it means the location offered the greatest degree of defense against any odd incoming packets from a source. Consequently, this odd package that just arrived could be an intrusion.

4. We next try to identify the source from where this packet originated to the place where it experienced the most resistance by applying filters to that particular destination. Once more, by finding the source that takes up the greatest space in the graph, the IP address of the suspected intrusion source may be determined.

The information is shown in the following R-plotted graphs, Figs. 5, 6, and 7. (Part a's findings).

The many criteria by which the above graphs are shown include the different Source IPs, Destination IPs, Protocols involved, and the length of time it takes for a certain Protocol to have an effect on a certain Destination IP before having an impact on a particular Source IP. The parameters are shown below:

Figure 4 depicts the network architecture utilised in our testing environment, and Table 3 shows the Source, Destination, and Protocol Dataset in relation to it.

Figure 8 shows the development of wireless sensor networks made up of NS2 nodes.

According to varied data bandwidth communications, it has been discovered that the processing time line for various communication protocols on the specified test environment varies from 0.002 to a maximum of 40 s (Cui et al. 2019). Our research has documented the duration of data packet transmission, which is a result of communication protocols. This observation directly relates to the reliability of intrusion to time and the processing power of the network design, network nodes, or network cloud.

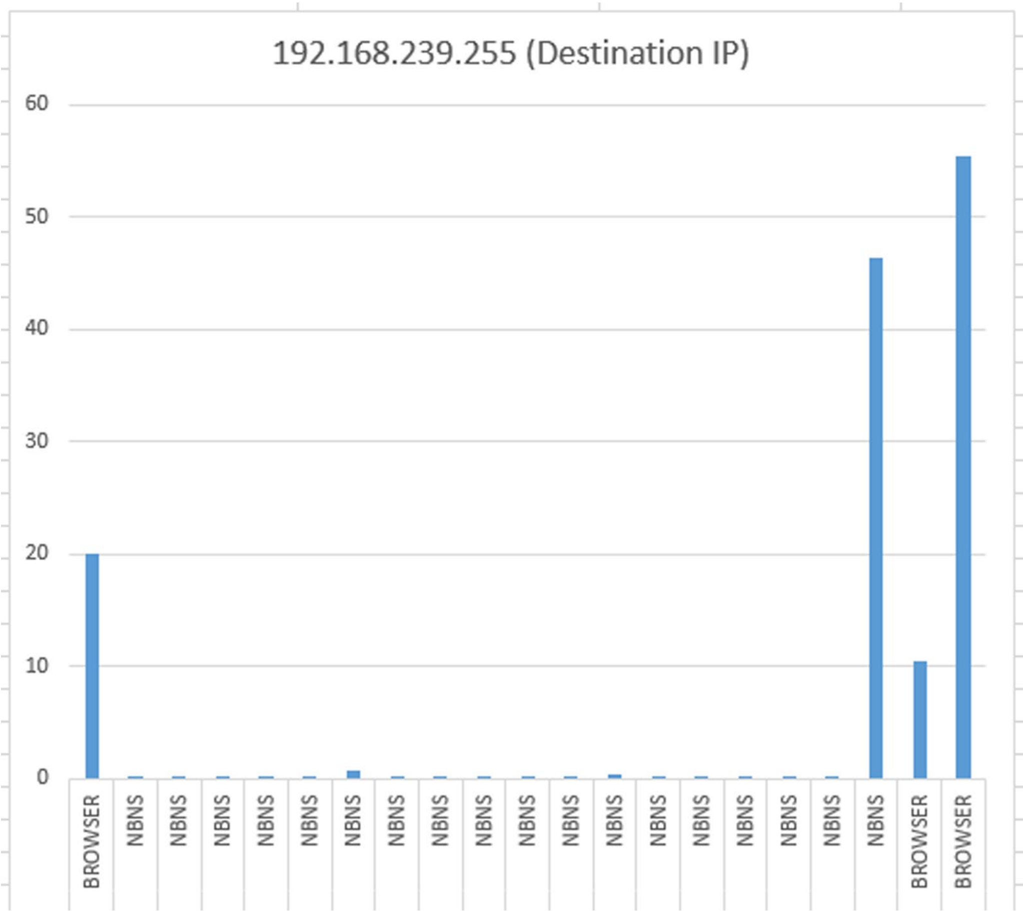


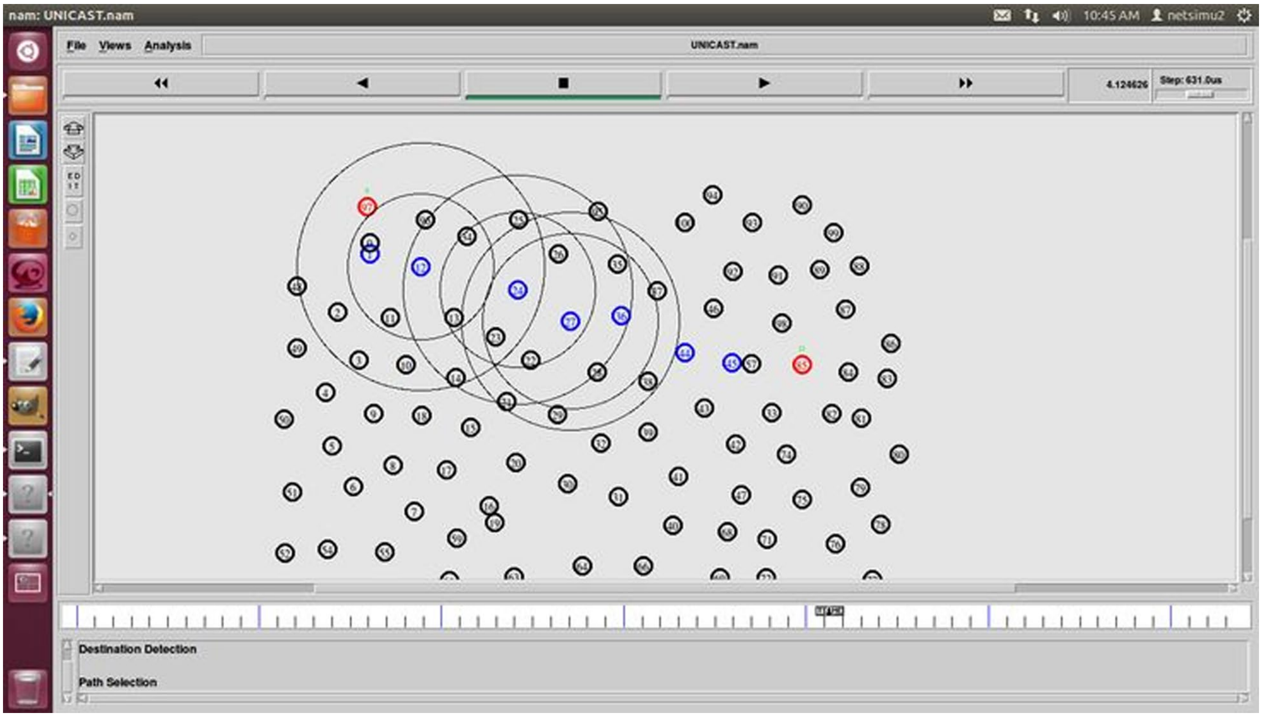
Fig. 7 Shows protocols vs (192.168.239.255) destination IP

b) The development of datasets from a physical network made using five node MCUs, a laptop, and a mobile device

The following was done during the experiment. An internet connection based on a mobile hotspot was made possible by the development of a network of laptops and six node MCUs. The matching node MCUs were then connected to six LEDs. First, normal on and Off buttons from a mobile device with IoT programming were used to switch on and off the LEDs (Gölcük et al. 2020). The Normal Dataset was compiled using the Wireshark software. The IP address of one of the nodes' MCUs was afterwards modified to an extremely long string, allowing some type of intrusion to be introduced (Alazzam et al. 2020; Kitali et al. 2021; Lima et al. 2020). Another dataset—this time an intrusion-induced dataset—was also created using the Wireshark programme. This moment, the node MCU received two successive ON orders followed by two seconds later by two OFF commands. Using the normal and intrusion-induced datasets from each of these datasets, the neural network model was trained. Some datasets were created from scratch, while others come from UNSW and other Kaggle and GitHub sources (Hemmasian et al. 2022).

A physical network was constructed utilising a laptop, a mobile device, and five node MCUs, as illustrated in Fig. 9. Additionally, the dataset was obtained via both harmful and lawful means. These datasets are those that we presently have (Balamurugan et al. 2022).(v). Several types of data caused by viruses are included in a UNSW dataset from GitHub.(vi). The dataset Kddcup 99

(i). A typical dataset created with the Wireshark programmed and a simulated Cisco Packet Tracer network.



Destination Detection

Path Selection

Fig. 8 Creation of wireless sensor networks consisting of nodes in NS2

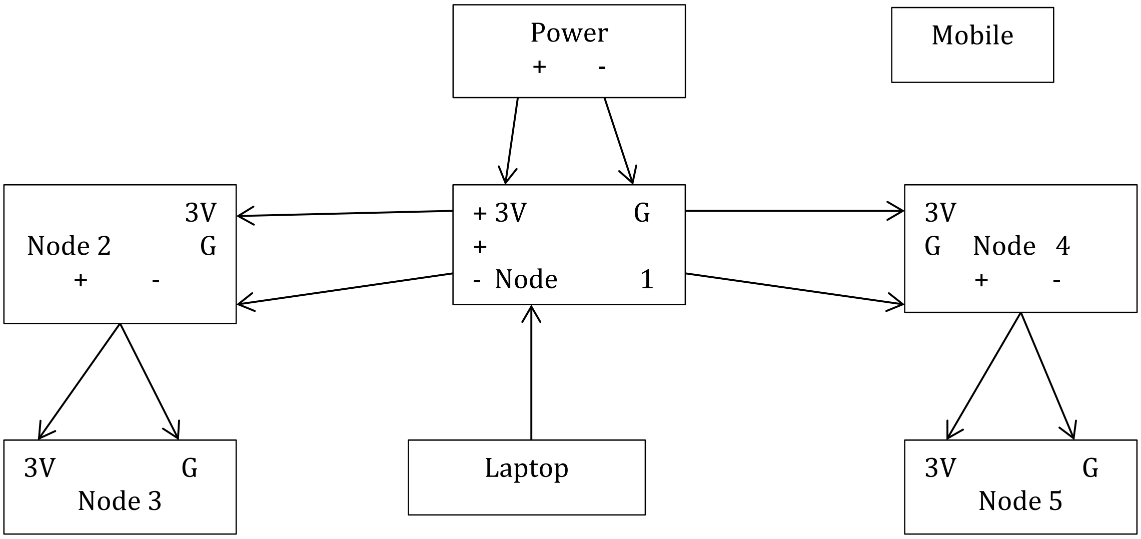


Fig. 9 A physical network made up of a mobile device, a laptop, and five node MCUs was created

(ii). Using node MCUs in wireless networks, a typical dataset for an IoT context was obtained.

(iii). The NSDL dataset from Kaggle is used to train the neural network (which consists of details about various types of attacks)

(iv). The perturbed dataset was created by adding turbulence within the network we built using IoT (Qazi et al. 2022; Zhu et al. 2022).

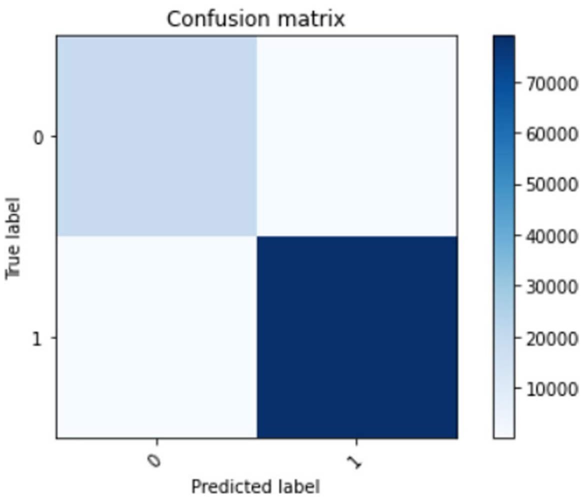


Fig. 10 Confusion matrix plotting for Logistic Regression

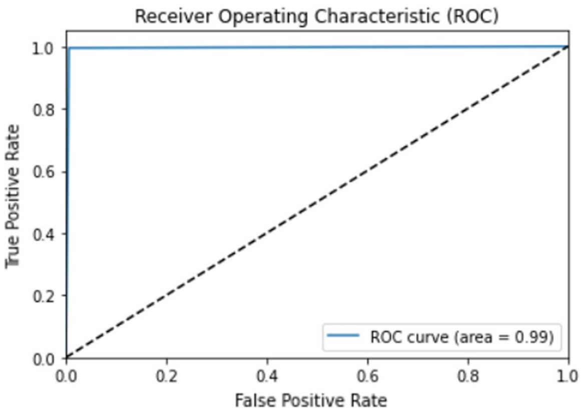


Fig. 11 Receiver operating characteristic (ROC)for logistic regression

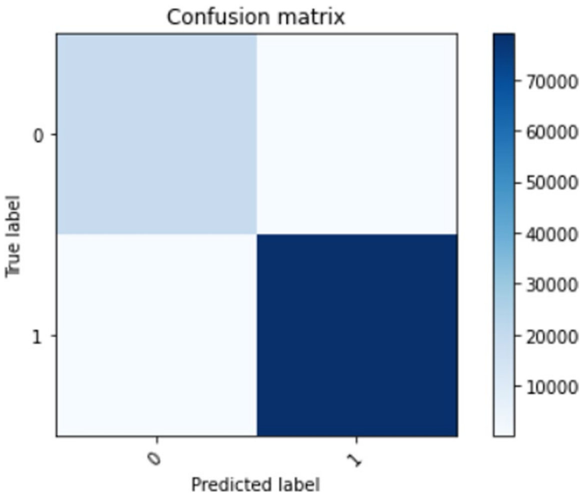


Fig. 12 Plotting confusion matrix for KNN

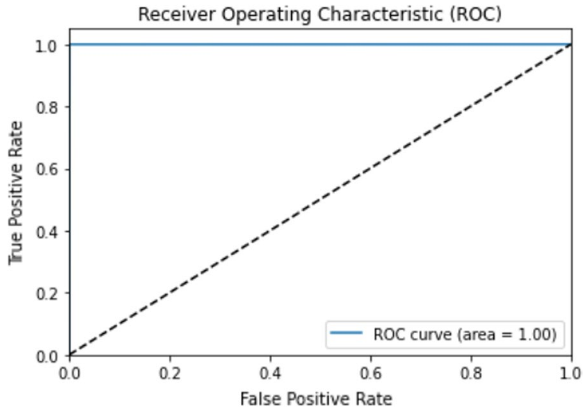


Fig. 13 Receiver operating characteristic (ROC) for KNN

Table 1 Classification report for logistic regression

	Precision	Recall	f1-score	Support
0	0.98	0.99	0.99	19,368
1	1	0.99	1	79,436
Accuracy			0.99	98,804
Average macro	0.99	0.99	0.99	98,804
Avg. weighted	0.99	0.99	0.99	98,804

Table 2 Classification report for KNN

	Precision	Recall	f1-score	Support
0	1	1	1	19,368
1	1	1	1	79,436
Accuracy			1	98,804
Macro avg	1	1	1	98,804
Weighted Avg	1	1	1	98,804

ML classification model training using a variety of methods

These datasets were used to train the various ML classifiers mentioned above, and their rates of accurately detecting hazardous behavior were calculated (Joon and Tomar 2022). Following that, PSO was combined with each of these various ML classifiers, and a comparison study is provided in Results.

Figures 10, 11, 12, and 13 below illustrate the confusion matrix, classification report, and receiver operating characteristic for logistic regression and KNN (Tables 1 and 2).

Table 3 Shows the source, destination and protocol dataset with respect to our test environment of network topology as shown in Fig. 4

Source	Destination	Protocol
192.168.239.1	192.168.239.1	ARP
192.168.239.254	192.168.239.254	BROWSER
fe80::f9fc:ad11:1e14:b75	192.168.239.255	DHCP
VMware_c0:00:08	224.0.0.22	ICMPv6
VMware_fc:23:ae	224.0.0.251	IGMPv3
	224.0.0.252	LLMNR
	239.255.255.250	MDNS
	Broadcast	NBNS
	ff02::1:3	SSDP
	ff02::16	
	ff02::fb	
	VMware_c0:00:08	
	VMware_fc:23:ae	

Table 4 Performance metrics for proposed classifiers

Measure	PSO + DT (%)	PSO + KNN (%)	PSO + ANN (%)
Predictability	98.7	99.6	99.7
Accuracy	75.2	88.4	90.2
Low predictive value (NPV) (Sindhu et al. 2012)	99.5	99.8	99.8
F1 rank	81.7	92.1	94.1

Table 5 Assessment of suggested classifications

Measures	PSO + DT (%)	PSO + KNN (%)	PSO + ANN (%)
Precision (Hoque et al. 2012)	98.5	99.5	99.77
DR	89.5	96.1	97.2
FPR	1.2	0.3	0.02

Table 6 Comparison evaluation of the current system

Authors	Algorithm	Accuracy (%)	FPR (%)
Sindhu, Geeta & Kannan (Guo 2007)	DT	98.2	0.016
Mohammad Sazzadul Hoque (Preeti et al. 2022)	GA	96.4	0.05
Guo	KNN	98.45	0.048
	TCM + KNN	99.4	0.1
Proposed classifier	PSO + DT	98.5	0.011
	PSO + KNN	99.6	0.004
	PSO + ANN	99.78	0.003

Result and discussion

After utilising the aforementioned datasets to train multiple ML classifiers, PSO was used in conjunction with each of these classifiers. A comparison of PSO in conjunction with three of the classifiers—k Nearest Neighbor, Artificial Neural Networks, Decision Trees, are listed here (Tables 3, 4, 5 and 6).

The following was noted when the proposed IDS system and the present IDS were contrasted from various research studies:

Therefore, it can be stated that, when compared to other systems, the suggested IDS, PSO + ANN provides the best accuracy and the lowest FPR (A survey on firefly algorithms et al. 2022; Judy Simon et al. 2022).

Below are some benefits of the various algorithms and technologies used for this study endeavor:

i. Advantages of particle swarm optimization (PSO)

   Popular optimization methods include Particle Swarm Optimization (PSO). The concept behind it is to simulate the behaviour of a flock of birds, with each bird standing in for a particle that seeks for the global optimum. Finding the best answer requires, the method utilises a swarm of particles that fly across the solution space and investigate various options (Ganesh and Sharma 2021).

   PSO continues to be a popular option for many optimization issues despite the development of several other optimization techniques throughout the years. This is because PSO provides a number of benefits over other optimization methods, including: Simple and straightforward to use: PSO is an easy-to-implement optimization method that works with any computer language (Guilherme Ramos et al. 2022).

   - Efficient in terms of computations PSO is a quick and effective optimization approach because it doesn't call for complicated or time-consuming calculations.
   - Effective performance for complicated issues PSO has been demonstrated to be effective for difficult optimization issues with high-dimensional search spaces.
   - Robustness PSO is a robust optimization method, which means it can deal with erratic or noisy objective functions (Wang et al. 2021).

PSO, a well-liked optimization method, has been extensively applied in many different applications, including feature selection (Meysam Valueian et al. 37 2022; Abdallah and Wafa' Eleisah et al. 2022). The approach offers various benefits over other optimization methods, including resilience, strong performance for complicated problems, and simplicity and computing economy.

Different performance measures have been used in studies on numerous contemporary intrusion detection systems (Sivagaminathan and Dr. Manmohan Sharma. 2021b). A number of machine learning algorithms have been studied, including K-Nearest Neighbors, SVM, Discriminant Analysis, Naive Bayes Model, Logistic Regression, Ridge Classifier, and Decision Trees. The functioning of computational intelligence methods including Grey Wolf Optimization (GWO), Firefly Optimization (FFA), Genetic Algorithms, and numerous evolutionary algorithms was also thoroughly researched (Pampapathi et al. 2022).

ii. Advantages of wireshark tool

For 10 minutes, the packets sent through the laptop system were captured using the Wireshark Tool, and a simulation of a LAN server, PCs, and routers was built using Cisco Packet Tracer. We used this information to build our own dataset, which had protocols, source and destination IP addresses, and—most importantly—the amount of time needed to communicate between each source and each destination. We then plotted several graphs to study these interdependencies (Zhang et al. 2022b).

Popular software for recording and examining network data is called Wireshark. To monitor and fix network issues, network administrators, security experts, and network engineers frequently utilize it. Wireshark is a recommended tool for collecting active communication packets for a number of reasons, including:

- Compatibility windows, Linux, and macOS are just a few of the many operating systems that Wireshark supports. Additionally, it supports a large number of networking protocols, giving it a flexible tool for examining various kinds of network data.
- User-friendly interface The Wireshark interface is user-friendly, making it simple to explore and analyses network traffic. Additionally, it offers a number of visualization tools, including packet decoding, protocol dissectors, and graphs, to make it simpler to comprehend the data being gathered.
- Open-source because Wireshark is an open-source programme, it is available for free and may be altered to suit certain requirements. This implies that a sizable user base exists that can offer the tool resources and assistance (Al-Anzi 2022).
- Advanced functions Wireshark has a number of advanced functions.
- Additional features Wireshark has a number of advanced capabilities that make it a strong tool for network analysis and troubleshooting, including packet filtering, protocol analysis, and exporting of recorded data.

Due to its interoperability, user-friendly interface, open-source status, and extensive functionality, Wireshark is a recommended tool for collecting active communication packets (Hassan et al. 2022). These elements make it a flexible and effective tool for network traffic analysis and problem-solving.

iii. Advantages of cisco packet tracer

A network simulation programme called Cisco Packet Tracer offers a visual interface for network design and setup. It is a graphical user interface (GUI)-based programme that enables users to effortlessly drag and drop elements to construct a virtual network environment, such as PCs, switches, routers, and servers. Users may experiment with various setups, test out network situations, and debug network problems with the help of the tool, which is intended to mimic a real-world network environment (Pingale et al. 2022; Choudhary and Kesswani 2020).

On the other hand, NS2 is a discrete event simulator that gives network simulations a command-line interface. In order to construct and configure network components in the virtual environment, users must write code. This necessitates a better comprehension of network protocols, coding principles, and some degree of programming expertise (Rintyarna et al. 2019).

Cisco Packet Tracer and NS2 vary primarily in that the former offers a graphical interface for network simulations while the later necessitates user-written code. Cisco Packet Tracer is therefore a more approachable choice for folks who are unfamiliar with network simulations or who lack a solid experience in programming (Alzubaidi et al. 2020).

Conclusions

In the modern world, network intrusion detection is quite important. Every network is vulnerable to different kinds of assaults. Using the Wireshark tool, data packets were recorded during live communication in the system where a simulation network was built utilising Cisco Packet Tracer, as well as in a real network built using five node MCUs, a laptop, and a mobile device. Datasets caused by intrusions were also gathered from this setup. Along with some standard datasets from UNSW, Kaggle, and GitHub, the acquired datasets were utilised to train numerous ML models. As an optimization method, PSO was used with these ML classifiers. PSO+ANN, PSO+KNN, and PSO+DT were carefully watched and investigated in a case study. With a best accuracy of 99.78 and a lowest FPR of 0.003%, it was discovered that PSO+ANN surpasses PSO+KNN, PSO+DT, and other current IDS.

Potential datasets when trained to the proposed IDS, may employ deep learning approaches for giving better efficient results.

Author contributions

All authors have equally contributed to the research work. All authors read and approved by the final manuscript.

Authors' information

Astt. Proff. Vaishnavi Sivagaminathan working as Assistant Professor in Priyadarshini College of Engineering, Nagpur is undergoing her PhD from Lovely Professional University, Punjab, India in Computer Science and Engineering discipline. As a highly skilled Assistant Professor with more than 12 years of experience delivering lectures, conducting training programs, supervising projects, collecting and processing technical data and conducting research. Her research specializations are artificial intelligence, machine learning, image processing, cyber security and Networking and Security.

Dr. Manmohan Sharma presently serving as Professor in School of Computer Applications, Lovely Professional University, Punjab, INDIA has a vast experience of more than 24 years in the field of academics, research and administration with different Universities and Institutions of repute such as Dr. B.R. Ambedkar University, Mangalayatan University etc. Dr. Sharma has been awarded with his Doctorate degree from Dr. B.R. Ambedkar University, Agra in 2014 in the field of Wireless Mobile Networks. His areas of interest include Wireless Mobile Networks, Adhoc Networks, Mobile Cloud Computing, Recommender Systems, Data Science and Machine Learning etc. More than 50 research papers authored and co-authored, published in International or National journals of repute and conference proceedings comes under his credits. He is currently supervising six doctoral theses. Three Ph.D. and three M.Phil. degrees has already awarded under his supervision. He has guided more than 600 PG and UG projects during his service period under the aegis of various Universities and Institutions. He worked as reviewer of many conference papers and member of the technical program committees for several technical conferences. He is also actively serving several journals related to the field of wireless, mobile communication and cloud computing as editorial board member. He is also member of various professional/technical Societies including Computer Society of India (CSI), Association of Computing Machines (ACM), Cloud Computing Community of IEEE, Network Professional Association (NPA), International Association of Computer Science and Information Technology (IACSIT), and Computer Science Teachers Association (CSTA).

Dr. Santosh Kumar Henge working as Associate Professor in the School of Computer Science and Engineering, Lovely Professional University, Punjab, India. As a highly skilled Associate Professor with more than 16 years of experience delivering lectures, comprised of nearly 8 years of international level teaching experience and more than 8 years of national level experience, conducting training programs, supervising projects, collecting and processing technical data and conducting research. He was awarded a Ph.D. degree from the Department of Computer Science, Kakatiya University. His research specializations are artificial intelligence, machine learning, medical image processing and cyber security which are mainly emphasis on neural-fuzzy hybrid systems, machine learning algorithms, image processing, data mining and wide data analysis. He is also actively serving several AI and cyber security related journals and conferences as editorial board member, organizing committee member, workshop organizer and reviewer.

Funding

There are no funding resources for this research work.

Availability of data and materials

Data is available with the author; it will be made available to researchers as per demand.

Declarations

Ethics approval and consent to participate

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. And the work shown in the paper is original.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Received: 28 December 2022 Accepted: 22 April 2023
Published online: 03 October 2023

References

Abdallah EE, Otoom AF (2022) Intrusion detection systems using supervised machine learning techniques: a survey. Procedia Comput Sci 1(201):205–212. https://doi.org/10.1016/j.procs.2022.03.029

Abdulaziz I Al-issa1, Mousa Al-Akhras1+2, Mohammed S ALsahli1, Mohammed Alawairdhi1 (2019) "Using machine learning to detect DoS attacks in wireless sensor networks." In: IEEE jordan international joint conference on electrical engineering and information technology

Al-Anzi FS (2022) Design and analysis of intrusion detection systems for wireless mesh networks. Digit Commun Net. https://doi.org/10.1016/j.dcan.2022.05.013

Alazzam H, Sharieh A, Sabri KE (2020) A feature selection algorithm for intrusion detection system based on pigeon inspired optimizer. Expert Syst Appl 148:113249. https://doi.org/10.1016/j.eswa.2020.113249

Almasoudy FH, Al-Yaseen WL, Idrees AK (2020) Differential evolution wrapper feature selection for intrusion detection system. Procedia Comput Sci 167:1230–1239. https://doi.org/10.1016/j.procs.2020.03.438

Almomani B, Al-Kasasbeh and M AL-Akhras, (2016) "WSN-DS: a dataset for intrusion detection systems in wireless sensor networks. J Sensors. https://doi.org/10.1155/2016/4731953

Alzubaidi A, Tepper J, Lotfi A (2020) A novel deep mining model for effective knowledge discovery from omics data. Artif Intell Med 104:101821. https://doi.org/10.1016/j.artmed.2020.101821

Asadi M, Jamali MAJ, Parsa S, Majidnezhad V (2020) Detecting botnet by using particle swarm optimization algorithm based on voting system. Future Generat Comput Syst 107:95–111. https://doi.org/10.1016/j.future.2020.01.055

Balamurugan E, Mehbodniya A, Kariri E, Yadav K, Kumar A, Haq MA (2022) Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN). Pattern Recognition Lett 156:142–151. https://doi.org/10.1016/j.patrec.2022.02.013

Bang R, Manish P, Vasu G, Vishal K, Jyoti M, and Sambhaji S (2020) "Redefining smartness in township with internet of things & artificial intelligence: Dholera city." In: E3S web of conferences, vol 170, p 06001. EDP Sciences

Chohra A, Shirani P, Karbab E, Debbabi M (2022) Chameleon: optimized feature selection using particle swarm optimization and ensemble methods for network anomaly detection. Comput Sec 117:102684. https://doi.org/10.1016/j.cose.2022.102684

Choudhary S, Kesswani N (2020) Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 datasets using deep learning in IoT. Procedia Comput Sci 1(167):1561–1573. https://doi.org/10.1016/j.procs.2020.03.367

Cui G, Liu B, Luan W (2019) Neural network with extended input for estimating electricity consumption using background-based data generation. Energy Procedia 158:2683–2688. https://doi.org/10.1016/j.egypro.2019.02.022

Debicha I, Bauwens R, Debatty T, Dricot J-M, Kenaza T, Mees W (2022) and TAD: transfer learning-based multi-adversarial detection of evasion attacks against network intrusion detection systems. Future Generat Comput Syst. https://doi.org/10.1016/j.future.2022.08.011

Deep K (2022) A random walk Grey wolf optimizer based on dispersion factor for feature selection on chronic disease prediction. Expert Syst Appl 206:117864

Firoz Kabir M, Sven Hartmann"(2018) Cyber security challenges: an efficient intrusion detection system design". In : IEEE international young engineers forum

Ganesh V, Sharma M (2021) Intrusion detection and prevention systems: a review. In: Ranganathan G, Chen J, Rocha Á (eds) Inventive communication and computational technologies. Lecture notes in networks and systems, https://doi.org/10.1007/978-981-15-7345-3_71

Guo YL (2007) An active learning-based TCM-KNN algorithm for supervised network intrusion detection. Comput Secur 26:459–467

Gölcük İ, Ozsoydan FB (2020) Evolutionary and adaptive inheritance enhanced grey wolf optimization algorithm for binary domains. Knowledge-Based Syst 194:105586. https://doi.org/10.1016/j.knosys.2020.105586

Hassan IH, Abdullahi M, Aliyu MM, Yusuf SA, Abdulrahim A (2022) An improved binary manta ray foraging optimization algorithm based feature selection and random forest classifier for network intrusion detection. Intell Syst Appl 1(16):200114

Hemmasian A, Meidani K, Mirjalili S, Farimani AB (2022) VecMetaPy: a vectorized framework for metaheuristic optimization in Python. Adv Eng Software 1(166):103092

Hoque M S, Mukit M, Bikas M, & Naser A (2012) An implementation of an intrusion detection system using a genetic algorithm. arXiv preprint arXiv:1204.1336

Imran M, Haider N, Shoaib M, Razzak I (2022) An intelligent and efficient network intrusion detection system using deep learning. Comput Electric Eng 1(99):107764. https://doi.org/10.1016/j.compeleceng.2022.107764

Jing Yu, Ye X, Li H (2022) A high precision intrusion detection system for network security communication based on multi-scale convolutional neural network. Future Generat Comput Syst 129:399–406. https://doi.org/10.1016/j.future.2021.10.018

Joon R, Tomar P (2022) Energy aware Q-learning AODV (EAQ-AODV) routing for cognitive radio sensor networks. J King Saud Univ Comput Inform Sci. https://doi.org/10.1016/j.jksuci.2022.03.021

Karimipour H, Dehghantanha A, Parizi RM, Choo K-KR, Leung H (2019) 'A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids.' IEEE Access 7:80778–80788

Kitali AE, Mokhtarimousavi S, Kadeha C, Alluri P (2021) Severity analysis of crashes on express lane facilities using support vector machine model trained by firefly algorithm. Traffic Injury Prevent 22(1):79–84

Li J, Wei X, Li Bo, Zeng Z (2022) A survey on firefly algorithms. Neurocomputing 500:662–678. https://doi.org/10.1016/j.neucom.2022.05.100

Lima FS, Alves VM, Araujo AC. Metacontrol (2020) A Python based application for self-optimizing control using metamodels. Comput Chem Eng 140: 106979

Lo W, Alqahtani H, Thakur K, Almadhor A, Chander S, Kumar G (2022) A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic. Vehic Commun 35:100471. https://doi.org/10.1016/j.vehcom.2022.100471

Maldonado J, Riff MC, Neveu B (2022) A review of recent approaches on wrapper feature selection for intrusion detection. Expert Syst Appl 18:116822. https://doi.org/10.1016/j.eswa.2022.116822

Mokhtar Mohammadi, Tarik A. Rashid, Sarkhel H.Taher Karim, Adil Hussain Mohammed Aldalwie, Quan Thanh Tho, Moazam Bidaki, Amir Masoud Rahmani, Mehdi Hosseinzadeh, A comprehensive survey and taxonomy of the SVM-based intrusion detection systems. J Net Comput Appl 178: 102983 https://doi.org/10.1016/j.jnca.2021.102983

Musa US, Chakraborty S, Abdullahi MM, Maini T. A review on intrusion detection system using machine learning techniques. In2021 International conference on computing, communication, and intelligent systems (ICCCIS) 2021 Feb 19 (pp. 541-549). IEEE https://doi.org/10.1109/ICCCIS51004.2021.9397121.

Mushtaq E, Zameer A, Khan A (2022) A two-stage stacked ensemble intrusion detection system using five base classifiers and MLP with optimal feature selection. Microproc Microsyst. https://doi.org/10.1016/j.micpro.2022.104660

Pampapathi BM, Guptha N, Hema MS (2022) Towards an effective deep learning-based intrusion detection system in the internet of things. Telemat Inform Reports 7:100009. https://doi.org/10.1016/j.teler.2022.100009

Paria J, Victor C M Leung (2016) "Intrusion detection and prevention for ZigBee-based home area networks in smart grids". In: IEEE Transaction on Smart Grid

Pingale SV, Sutar SR (2022) Remora whale optimization-based hybrid deep learning for network intrusion detection using CNN features. Expert Syst Appl 210:118476. https://doi.org/10.1016/j.eswa.2022.118476

Priyanka S, Dietmar PF Moller (2018)"Protecting ECUs and vehicles internal networks". In IEEE conference

Ramos G, Aguiar AP, Pequito S (2022) An overview of structural systems theory. Automatica 140:110229

Ravi V, Chaganti R, Alazab M (2022) Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. Comput Electric Eng 102:108156. https://doi.org/10.1016/j.compeleceng.2022.108156

Rintyarna BS, Sarno R, Fatichah C (2019) Evaluating the performance of sentence level features and domain sensitive features of product reviews on supervised sentiment analysis tasks. J Big Data 6:1–19

Saba T, Rehman A, Sadad T, Kolivand H (2022) Anomaly-based intrusion detection system for IoT networks through deep learning model. Comput Electric Eng 99:107810. https://doi.org/10.1016/j.compeleceng.2022.107810

Simon J, Kapileswar N, Polasi PK, Elaveini MA (2022) Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm. Comput Electric Eng 102:108190. https://doi.org/10.1016/j.compeleceng.2022.108190

Sindhu SSS, Geetha S, Kannan A (2012) Decision tree-based lightweight intrusion detection using a wrapper approach. Expert Syst Appl 39(1):129–141

Subhash W, Lokesh P and Upendra S (2020) Intrusion detection system using PCA with random forest approach international conference on electronics and sustainable communication systems (ICESC)

Vaishnavi Sivagaminathan, Dr. Manmohan Sharma. "Dynamic communication protocol modelling for intrusion traces using cisco packet tracer integration with wireshark". Design engineering, Aug. 2021a, pp 4583–99, http://thedesignengineering.com/index.php/DE/article/view/3853

Vaishnavi S, Dr. Manmohan S (2021b)"Dynamic communication protocol modelling for intrusion traces using cisco packet tracer integration with wireshark". Design Engineering, Aug. 2021b, pp. 4583–99, http://thedesignengineering.com/index.php/DE/article/view/3853

Valueian M, Vahidi-Asl M, Khalilian A (2022) SituRepair: incorporating machine-learning fault class prediction to inform situational multiple fault automatic program repair. Int J Critic Infrastruct Protect 1(37):100527

Wang W, Jian S, Tan Y, Qingbo Wu, Huang C (2022b) Representation learning-based network intrusion detection system by capturing explicit and implicit feature interactions. Comput Sec 112:102537. https://doi.org/10.1016/j.cose.2021.102537

Wang Z, Li Z, He D, Chan S (2022a) A lightweight approach for network intrusion detection in industrial cyber-physical systems based on knowledge distillation and deep metric learning. Expert Syst Appl 206:117671. https://doi.org/10.1016/j.eswa.2022.117671

Wang S, Wang Q, Bailey N, Zhao J (2021) Deep neural networks for choice analysis: a statistical learning theory perspective. Transp Res Part B: Methodol 148:60–81. https://doi.org/10.1016/j.trb.2021.03.011

Wang M, Yiqin Lu, Qin J (2020) A dynamic MLP-based DDoS attack detection method using feature selection and feedback. Comput Sec 88:101645. https://doi.org/10.1016/j.cose.2019.101645

Yang Y, McLaughlin K, Sezer S, Littler T, Pranggono B, Brogan P, Wang HF (2020) Intrusion detection system for network security in synchrophasor systems

Zhang C, Jia D, Wang L, Wang W, Liu F, Yang A (2022b) Comparative research on network intrusion detection methods based on machine learning. Comput Sec 121:102861. https://doi.org/10.1016/j.cose.2022.102861

Zhang Z, Zhang Y, Guo Da, Yao L, Li Z (2022a) SecFedNIDS: robust defense for poisoning attack against federated learning-based network intrusion detection system. Future Generat Comput Syst 134:154–169. https://doi.org/10.1016/j.future.2022.04.010

Zhao Xu, Huang G, Jiang J, Gao L, Li M (2022) Task offloading of cooperative intrusion detection system based on deep Q network in mobile edge computing. Expert Syst Appl 206:117860. https://doi.org/10.1016/j.eswa.2022.117860

Zhu J, Wang G, Li Y, Duo Z, Sun C (2022) Optimization of hydrogen liquefaction process based on parallel genetic algorithm. Int J Hydrogen Energy. https://doi.org/10.1016/j.ijhydene.2022.06.062

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.