SEMI-SUPERVISED MACHINE LEARNING APPROACH FOR PROBE ATTACK

1A. Hasini, 2S. Keerthipriya, 3V. Srilaxmi, 4Mrs.K. Anuranjani,

[1,2,3]Students,[4]Assistant professor
Department of CSE, BIHER

***Abstract*- The quick spread of computer networks has altered how network security is seen. The ease of accessibility makes computer networks vulnerable to many hacking attacks. There are various and possibly catastrophic threats to networks. Researchers have so far created intrusion detection systems (IDS) that can recognise assaults in a variety of situations. There are several techniques that may be used to identify abuse and anomalies. Since various types of ecosystems are best served by different techniques, many of the technologies presented are complimentary to one another. Several intrusion detection systems have been developed to defend against these threats used. The Intrusion Detection System (IDS) is a system that gathers and examines network data to find various assaults conducted against network components. We built the model using the KDDcup99 data set. In this article, a three-layer architecture for probe attack detection is suggested. Dimensionality reduction is accomplished via Principal Component Analysis. Duplicate samples were also taken out of the training data set. Finally, we used a line chart to compare the effectiveness of each classifier. The new intrusion detection technology presented in this research is utilised to survey and categorise them. The detection theory and a few operational components of intrusion detection make up the taxonomy.**

INTRODUCTION

A system of linked sensor nodes that communicate wirelessly or through wires to exchange perceived data. a unit that consists of one or more sensors and, optionally, one or more actuators and has networking and processing capabilities for detected data. A sensor node is made up of several nodes of the same type that are physically scattered and interact with one another. Each of these nodes has a transceiver, an energy source, a microprocessor (microcontroller) that processes sensor signals, a sensing element (sensor), and a microprocessor. Sensor nodes with the required sensors are dispersed throughout the item, making it feasible to collect data about the object and manage operations that occur on it.In the past, we have discussed conventional WSN applications for data collection and processing. These apps have one unique data collection point, called the sink, which makes them unique. However, in some applications, sensor nodes must also communicate with one another in order to share data. Because of this, multiple WSN organisational strategies for sensor node interaction exist. Network topologies are the name for these designs. Star, tree, and mesh are the three basic types of network topologies for WSNs. Various WSN standards support various network topologies.

LITERATURE REVIEW

NL-IDS: Trust Based Intrusion Detection System for Network layer in Wireless Sensor Networks Umashankar Ghugar, Jayaram Pradhan IEEE 2021.

From the last few years, security in wireless sensor network (WSN) is essential because WSN application uses important information sharing between the nodes. There are large number of issues raised related to security due to open deployment of network. The attackers disturb the security system by attacking the different protocol layers in WSN we have proposed a trust based intrusion detection system (NL-IDS) for network layer in WSN to detect the Black hole attackers in the network. To analyze the performance of NL-IDS, we have simulated the model in MATLAB R2015a, and the result shows that NL-IDS is better than Wang et al. [11] as compare of detection accuracy and false alarm rate.

Analyzing the Vulnerability of Wireless Sensor Networks to a Malicious Matched Protocol Attack George D. O'Mahon, Philip J. Harris, Colin C. Murphy IEEE 2021.

Safety critical, Internet of Things (IoT) and space-based applications have recently begun to adopt wireless networks based on commercial off the shelf (COTS) devices and standardized protocols, which inherently establishes the security challenge of malicious intrusions. Malicious intrusions can cause severe consequences if undetected, including, complete denial of services

Abnormal-Node Detection Based on Spatio-Temporal and Multivariate-Attribute Correlation in Wireless Sensor Networks Nesrine Berjab, Hieu Hanh Le, Chia-Mu Yu, Sy-Yen Kuo, Haruo Yokota IEEE 2021.

In wireless sensor networks (WSNs), data can be subject to malicious attacks and failures, leading to unreliability. This vulnerability poses a challenge to environmental monitoring applications by creating false alarms. To guarantee a trustworthy system, we therefore need to detect abnormal nodes. In this paper, we propose a new framework for detecting abnormal nodes in clustered heterogeneous WSNs.

Secure Knowledge and Cluster-Based Intrusion Detection Mechanism for Smart Wireless Sensor Networks Amjad Mehmood, Akbar Khanan, Muhammad Muneer, Salwani Abdulla, Khairul Akram Ariffin, Houbing Song IEEE 2021.

Wireless sensor networks, due to their nature, are more prone to security threats than other networks. Developments in WSNs have led to the introduction of many protocols specially developed for security purposes. Most of these protocols are not efficient in terms of putting an excessive computational and energy consumption burden on small nodes in WSNs. This paper proposes a

knowledge-based context-aware approach for handling the intrusions generated by malicious nodes. The system operates on a knowledge base, located at the base station, which is used to store the events generated by the nodes inside the network.
Threshold Tuning-Based Wearable Sensor Fault Detection for Reliable Medical Monitoring Using Bayesian Network Model Haibin Zhang, Jiajia Liu, Nei Kato IEEE 2021.
As the medical body sensor network (BSN) is usually resource limited and vulnerable to environmental effects and malicious attacks, faulty sensor data arise inevitably which may result in false alarms, faulty medical diagnosis, and even serious misjudgment. Thus, faulty sensory data should be detected and removed as much as possible before being utilized for medical diagnosis-making. Most available works directly employed fault detection schemes developed in traditional wireless sensor network (WSN) for body sensor fault detection. Extensive online dataset has been adopted to evaluate the performance of our fault detection scheme, which shows that our scheme possesses a good fault detection accuracy and a low false alarm rate.
A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation Cong Pu, Sunho Lim IEEE 2021.

Due to the lack of centralized coordination, physical protection, and security requirements of inherent network protocols, wireless sensor networks (WSNs) are vulnerable to diverse denial-of-service (DoS) attacks that primarily target service availability by disrupting network routing protocols or interfering with on-going communications. In this paper, we propose a light-weight countermeasure to a selective forwarding attack, called SCAD, where a randomly selected single checkpoint node is deployed to detect the forwarding mis behavior of malicious node. The proposed countermeasure is integrated with timeout and hop-by-hop retransmission techniques to quickly recover unexpected packet losses due to the forwarding misbehavior or bad channel quality. We also present a simple analytical model and its numerical result in terms of false detection rate.
Energy Efficient Detection-Removal Algorithm for Selective Forwarding Attack In Wireless Sensor Networks T.R Sreelakshmi, G.S Binu IEEE 2021.

Wireless sensor networks (WSNs) propose the promise of a flexible, low cost solution for monitoring critical infrastructure. Sensor networks have been recommended for applications such as traffic monitoring, military and battlefield surveillance. Wireless sensor networks are more prone to security attacks due to their broadcasting nature of the transmission medium and unattended deployment of nodes in hostile and unfriendly areas where they are not protected as compared to wired networks. Attackers can deploy various types of security attacks to obstruct the security of WSNs. Network layer attacks are more severe since if the routing information is disregarded, disturbances may bring about routing loops, changing of routes etc. Selective forwarding attack is a type of active attack affecting network layers that selectively drops or refuses to forward the data packets. This paper discusses about an energy efficient detection-removal algorithm for effective detection of selective forwarding attack in a clustered WSN scenario. The impact of the malicious node in network parameters like packet delivery ratio, throughput, residual energy of network and end to end delay are analyzed.

False Data Injection Prevention in Wireless Sensor Networks using Node-level Trust Value Computation B. Sreevidya, M. Rajesh IEEE 2021.

Wireless Sensor Networks are extensively used in developing applications for surveillance, habitat monitoring, border security, intrusion detection etc. Most of these applications require secure data transmission among the nodes of the network. Out of the different types of attacks a data critical application faces, False Data Injection attacks are the most damaging one. So prevention of False Data Injection attacks is a crucial aspect while building data critical wireless sensor network applications. Researchers have suggested cryptographic schemes like RSA, ECC for the prevention of False Data Injection Attacks. The proposed work aims on using trust parameter of every nodes to distinguish malicious and non-malicious nodes and use only trusted nodes to forward the packet to destination thus by prevention FDI attacks. Simulation is carried out with the help of Network Simulator 2 (NS2). The results shows the energy consumption is less in the proposed scheme compared to the cryptographic technique

Heterogeneous statistical QoS provisioning over 5G mobile wireless networks Author: Xi Zhang ;Wenchi Cheng ; Hailin Zhang Published in: IEEE Network (Volume: 28, Issue: 6, Nov.-Dec. 2021)

in this article we propose a novel heterogeneous statistical QoS provisioning architecture for 5G mobile wireless networks. First, we develop and analyze the new heterogeneous statistical QoS system model by applying and extending the effective capacity theory. Then, through the wireless coupling channels, we apply our proposed heterogeneous statistical QoS architecture to efficiently implement the following powerful 5G-candidate wireless techniques: 1) device-to-device networks; 2) full-duplex networks; and 3) cognitive radio networks, respectively, for providing heterogeneous statistical delay-bounded QoS guarantees. Finally, using the simulation experiments we show that our proposed architecture and schemes significantly outperform the existing traditional statistical delay-bounded QoS provisioning schemes in terms of satisfying the heterogeneous delay-bounded QoS requirements while maximizing the aggregate system throughput over 5G mobile wireless networks.

PROPOSED SYSTEM

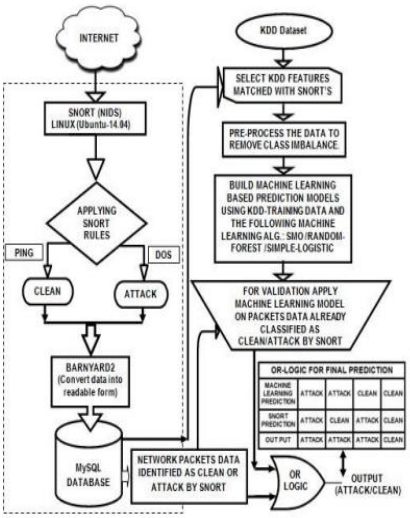
Convolutional neural networks (CNN, or ConvNet) are a kind of deep neural networks used most frequently to analyse visual vision in deep learning. They also go by the names shift invariant or translation invariant due to its shared-weights design. They are used in a variety of fields, including financial time series, image and video recognition, recommender systems, image classification, and image segmentation.

Multilayer perceptrons are regularised variants of CNNs. Fully linked networks, or multilayer perceptrons, are those in which every neuron in one layer is connected to every neuron in the following layer. These networks are vulnerable to overfitting data because

of their "fully-connectedness." Adding some kind of magnitude measurement of weights to the loss function is a typical method of regularisation. CNNs tackle regularisation differently; they make use of the data's hierarchical structure to piece together more complicated patterns out of smaller, simpler ones. CNNs are therefore at the lower end of the connectivity and complexity spectrum.

Because of how closely the connection network between neurons mimics the arrangement of the animal visual cortex, biological processes served as an inspiration for CNN. Only in the constrained area of the visual field known as the receptive field do individual cortical neurons respond to inputs. Different neurons' receptive areas partially overlap one another to fill the whole visual field.

Comparatively speaking to other image classification algorithms, CNNs employ a minimal amount of pre-processing. This implies that the filters, which were manually designed for traditional techniques, are learned by the network. This feature design's independence from past knowledge and human effort is a significant benefit.



MODULE DESCRIPTION

There are 8 components in the system.

They are

- Incoming packet
- Packet Capture
- Packet scanner
- Packet analyzer
- Labeling
- Training model
- Prediction:
- Output

Incoming packet: Our project is directly connected to the network, and we transfer online packets to a packet scanner.

Packet Capture: Many packets are transmitted from source to destination in real-time networking. Live network packets are gathered in this module and sent to the pre-processor module. Machine learning holds that data should be sorted or clustered based on its attributes or qualities, such as the protocols employed by packets.

Packet scanner: We utilize a packet scanner to scan the packet once it has been captured. Scannable packets are the most crucial component of our system.

Packet analyzer: Sniffer is another name for a packet analyzer. Sniffers catch each packet as data streams pass across the network, decode the packet when necessary to reveal the values of its different fields, and then analyse the content in accordance with specifications.

Labeling: Labeling is used to specify the appropriate packet.

Training model: The training model includes a collection of trained data sets that are used to identify attacks in packets.

Prediction: We estimate whether the packet is a regular packet or an abnormal packet based on the training model.

Output: We produce output in the form of an abnormal packet based on the prediction (i.e. normal or abnormal).

CONCLUSION

The scientific community and business organisations are equally interested in intrusion detection at the moment. Based on a suggested taxonomy and examples of previous and present initiatives, we have provided background information on the state-of-the-art of IDS at the moment. This taxonomy also emphasises new research and effectively addresses both earlier and more recent discoveries. Each of its techniques has pros and cons of its own. We think that no one criterion can be employed as a full defence against infiltration into a computer network. It does not exist in a single form that can be applied as a universal defence against all potential assaults. Building and maintaining computer systems and networks that are resistant to assaults is both technically challenging and expensive. The method to be used is dependent

FUTURE SCOPE

Other machine learning algorithms should be taken into account in future study to find more effective ways to apply the classification methodology to the datasets. It is advised that more study be done on other parameters that might increase detection accuracy.

REFERENCES:

[1]Harshal Waghmare, Radha Kokare, Detection and Classification of Diseases of Grape Plant Using Opposite Colour Local Binary Pattern Feature and Machine Learning for Automated Decision Support System, 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)
[2]Hulya Yalcin, Plant Phenology Recognition using Deep Learning: Deep-Pheno.
[3]Emanuel Cortes, Plant Disease Classification Using Convolutional Networks and Generative Adversial Networks.
[4][I.Gogul, V.Sathiesh Kumar, Flower Species Recognition System using Convolutional Neural Networks and Transfer Learning, 2017 4th International Conference on Signal Processing, Communications and Networking (ICSCN -2017), March 16 18, 2017, Chennai, INDIA.
[5]S. Sankaran, A. Mishra, R. Ehsani, and C. Davis, A review of advanced techniques for detecting plant diseases, Computers and Electronics in Agriculture, vol. 72, no. 1, pp. 113, 2010.
[6]P. R. Reddy, S. N. Divya, and R. Vijayalakshmi, Plant disease detection techniquetoola theoretical approach, International Journal of Innovative Technology and Research, pp. 9193, 2015.
[7]A.-K. Mahlein, T. Rumpf, P. Welke et al., Development of spectral indices for detecting and identifying plant diseases, Remote Sensing of Environment, vol. 128, pp. 2130, 2013
[8]Dong Pixia and Wang Xiangdong, Recognition of Greenhouse Cucumber Disease Based on Image Processing Technology, Open Journal of Applied Sciences, vol. 3, pp. 27-3, Mar. 2013.
[9]S. Arivazhagan, R. Newlin Shebiah, S. Ananthi and S. Vishnu Varthini, Detection of unhealthy region of plant leaves and classification of plant leaf diseases using texture features, Commission Internationale du Genie Rural(CIGR) journal, vol. 15, no. 1, pp. 211-217, 2013.
[10]Sachin D. Khirade and A. B. Patil. Plant Disease Detection Using Image Processing. International Conference on Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on, pp. 768-771. IEEE, 2015.

Plagiarism Scan Report

Report Generated on: Feb 16,2023

0% Plagiarised	100% Unique
Total Words:	407
Total Characters:	2695
Plagiarized Sentences:	0
Unique Sentences:	27 (100%)

Content Checked for Plagiarism

ABSTRACT

The quick spread of computer networks has altered how network security is seen. The ease of accessibility makes computer networks vulnerable to many hacking attacks. There are various and possibly catastrophic threats to networks. Researchers have so far created intrusion detection systems (IDS) that can recognise assaults in a variety of situations. There are several techniques that may be used to identify abuse and anomalies. Since various types of ecosystems are best served by different techniques, many of the technologies presented are complimentary to one another. Several intrusion detection systems have been developed to defend against these threats used. The Intrusion Detection System (IDS) is a system that gathers and examines network data to find various assaults conducted against network components. We built the model using the KDDcup99 data set. In this article, a three-layer architecture for probe attack detection is suggested. Dimensionality reduction is accomplished via Principal Component Analysis. Duplicate samples were also taken out of the training data set. Finally, we used a line chart to compare the effectiveness of each classifier. The new intrusion detection technology presented in this research is utilised to survey and categorise them. The detection theory and a few operational components of intrusion detection make up the taxonomy.

INTRODUCTION

A system of linked sensor nodes that communicate wirelessly or through wires to exchange perceived data. a unit that consists of one or more sensors and, optionally, one or more actuators and has networking and processing capabilities for detected data. A sensor node is made up of several nodes of the same type that are physically scattered and interact with one another. Each of these nodes has a transceiver, an energy source, a microprocessor (microcontroller) that processes sensor signals, a sensing element (sensor), and a microprocessor. Sensor nodes with the required sensors are dispersed throughout the item, making it

feasible to collect data about the object and manage operations that occur on it.

In the past, we have discussed conventional WSN applications for data collection and processing. These apps have one unique data collection point, called the sink, which makes them unique. However, in some applications, sensor nodes must also communicate with one another in order to share data. Because of this, multiple WSN organisational strategies for sensor node interaction exist. Network topologies are the name for these designs. Star, tree, and mesh are the three basic types of network topologies for WSNs. Various WSN standards support various network topologies.

No Plagiarism Found

Page 1 of 2