Ph.D. Research Proposal

Doctoral Program in "Department Name"

QoS Provisioning Via Intrusion Detection and Prevention for Wireless Networks Using Intellectual Approaches

by

<Name of the Candidate>

<Reg. No of the Candidate>

<Supervisor Name>

<Date of Submission (DD MM 20YY>

I. INTRODUCTION / BACKGROUND

The intrusion detection is one of the several security mechanisms to secure the IoT from the intruders. In general, there exist two significant methods to detect the intrusion in IoT network. They are signature or misuse detection based method and another one is anomaly based method. In the signature based method, intruders are identified using the set of predefined malicious patterns and attack signatures [3]. Based on these parameters, signature based method detects the intruders. On the other hand, anomaly based method detects the intruders based on the deviation from the normal behaviour of the devices [4]. However, these two methodologies have issues that are: signature based method cannot able to detect the unknown attack and anomaly based method have high false positive rate because of its inefficiency in intrusive and abnormal behaviours. In order to overwhelm these issues in traditional signature and anomaly based methods, hybrid IDS method is evolved [5]. The hybrid IDS method has combine advantage and evades the disadvantages of both IDS method.

The security risks are only concerning within the network, it is also formed and recognized from surroundings also. A set of most widely studied security requirements are follows:

- **Authentication –**

  This is mainly applied between the trusted third party and the specific device. This is a single step to prevent any intrusions in network and this is advice the mobile device to know its security behavior and credentials to avoid malicious activities. This must ensure without knowing the security credentials, access or communication is not permitted.

- **Confidentiality –**

  This requirement ensures whether the data transmitted from the source node is confidential or not because communication link is unsecure and attackers may receive the sensitive data through that link.

- **Integrity –**

This is one of the essential security requirement when design the secure network which defines the originality of the source node. Hereby, any mobile node can verify the originality of data from the source node.

- **Privacy –**

  Privacy preservation is a great demand in network for all mobile users and node privacy must be preserved. This requirement guarantees the secrecy of data while transmitting the sensitive to the destination node via multi-hop communication.

- **Trustworthiness –**

  This security feature must be required for any kind of network or system. Since source node must ensure the relay nodes before going to transmit the data. This results that data can be transmitted to the adjacent nodes without any privacy leakage. It is classified into two classes: Direct and Indirect.

- **Non-repudiation and Accountability –**

  This requirement represents the behavior of individual system that must be supports data collection and transmission operations.

- **Availability –**

  This requirement must ensures that the resources for processing security operations for devices.

1.1 Research Outline & Scope

QoS provisioning and also energy consumption is an important issue in wireless networks. It is achieved by the way of stopping the entries of malicious and compromised mobile users in mobile ad hoc network. In this specialty, energy efficiency, detection rate, false positive rate and delay are taking into account significant criteria. There are several systems, and methods have been proposed to detect interruptions and prevent it throughout the network. Unfortunately, enhancements are still on-demand to increase the detection rate and decrease the false positive rate. In addition to deal with the performance improvement of the Wireless Networks in terms of QoS metrics as packet delivery ratio and throughput.

1.2 Research Objectives

The main research objectives of this research work are follows,

- To analyze the current workings about Security for QoS Provisioning and define the security issues and limits on each work.
- To protect the environment fully and addressing all the security issues in the recent literature
- To design the newfangled and active security framework that can be applicable for real-world Wireless Networks with high solid and dynamic mobile nodes.
- To give immediate action about the detected intrusions throughout the network, which avoid the further malicious activities among the mobile nodes
- To reduce number of false events in the network by improving QoS of the network and to protect the network from malicious access and achieve all other performance measures.

All the aforementioned objectives are satisfied in this research work.

1.1 Applications / Use cases

At this moment, Wireless Networks has huge amount of potential to work on many applications. In below, there are very few applications are given as a reference,

- **Healthcare Applications -** Distributing information among vehicles fin real-time
- **Military Applications -** Wireless Networks allow for battle communications (military) in order to maintain information. For instance, planes, tanks and soldiers
- **Education Applications -** Conferences and Virtual Classrooms
- **Industrial Applications -** Nowadays, Wireless Networks is used for commercial application developments. For instance, disaster relief applications.

II. RESEARCH GAPS

2.1 Common Problem Statement

From the earlier approaches, detecting intrusion is a tedious task due to the following reasons: (1). Current approaches are not identifying the attackers directly in the network and the number of malicious activities over the time is relatively high. (2). Lack of absolute choice of the method to detect any kind of security attacks. (3). Absence of relevant feature set identification according to the transmitted packets. (4). some of the methods result high detection rate and low false positive rate, but it is a time consuming operation, and (5). It does not completely remove the intrusions in network. Further, some of the problems highlighted to improve QoS that is follows:

- Absence of routing attacks (e.g. spoofing attack) detection in low alarm rate.
- Low scalability and not practical to implement in a real-time.
- Huge amount of loss of messages (low PDR).
- Many of the times intrusion is not prevented, but only detected.
- High message communication and computation overheads.

2.2 Problem Definition

Elwahsh et al. [1] have designed neutrosophic intelligent system using self-organized feature maps (SOFM) and genetic algorithm (GA). In neutrosophic system, rules are generated in terms of symbols instead of numerical values in which attack packets are identified by membership, non-membership, and indeterminacy degrees. In this work, KDD dataset used and it cannot be directly used for intrusion detection. Hence SOFM is presented here to define neutrosophic variables and then neutrosophic rules generated using GA algorithm. Finally packets are classified normal and abnormal.

Problems

- In this paper, authors proposed generalized neutrosophic set to solve uncertainty issue, but it is always not suitable for complex applications like intrusion detection
- Detection delay rate is large when processing with GA.
- For accurate classification, we require to define the threshold values according to packet header information

Proposed Solutions

- In this work, we proposed HMM, which solve uncertainty issue, our proposed scheme is suitable for intrusion detection system
- Detection delay rate is minimized with the use of C4.5 with LightNet Architecture, which require minimum training time and testing time

Vimala et al. [2] have proposed Adaptive Fault Tolerant Mobile Agent based Intrusion Detection System is proposed, which runs by KDD Dataset. At first, attacks classification is implemented using TSVID algorithm, which is used RBF kernel and iterative learning scheme. Then classification is executed using NNIDS that uses neural network approach. Finally DF-IDS is implemented to give the successful classification. Results shows that the TSVID gives better performance than NNIDS, and DFIDS related to accuracy and error rate.

Problems Defined

- Preprocessing (data normalization) is required to reduce the false positive rate and increase the level of detection rate.
- TSVID algorithm does not perform well, when we have huge dataset and more noise so it is tricky for decision making

Solutions Proposed

- In preprocessing, we execute two steps: encoding and normalization, which shows our novelty in this paper to improve the detection rate
- Our proposed scheme can work well in both large scale and small scale datasets

Kavitha et al. [3] proposed a new intelligent framework called INDIA, which is referred as intruder node detection and isolation in Wireless Ad Hoc Networks. There are three processes are invoked in this work such as feature extraction, feature optimization and classification. Feature extraction is implemented using trust value (direct trust, indirect trust and total trust) computation of each node. Then feature optimization is implemented using particle swarm optimization (PSO). Finally optimized set of features are classified using neural network.

Problems Defined

- The speed of IDS is important element, which is very less in this work for trust value computation is done by any third party since itself compute trust value does not effective.

Solutions Proposed

- Detection delay metric considered in this work to show our proposed scheme has obtained better performance

Feng et al. [4] introduced a plug and play device for DDoS attacks detection and capture tool is also considered here to acquire packets from nodes. Deep learning model (deep neural network) is proposed to detect attacks, then convolutional neural network (CNN) is proposed to detect XSS attacks and long short term memory (LSTM) is proposed to detect SQL attacks. The proposed scheme is implemented using NS2 simulator and tested for KDD dataset.

Problems Defined

- Plug and play device is cost effective and small computation power , which leads to low scalability and bringing this tool for IDS is not practical

Solutions Proposed

- We proposed C4.5 with LightNet for IDS, which consume less computational power

Zhang et al. [5] have proposed two algorithms for intrusion detection in networks such as improved PCA (Principal Component Analysis) and Gaussian Naïve Bayes Algorithm. An improved version of PCA minimize data pollution problem. Total number of weighted principal components is 12, which are selected using sequential selection. Feature dimensionality reduction is implemented by enhanced PCA and the user behavior is classified using Gaussian naïve bayes algorithm.

Problems Defined

- Runtime of improved PCA is typically large since improved PCA does not select optimum set of features for classification
- Gaussian naïve bayes algorithm for packets classification is less but detection rate is not high
- In preprocessing, min-max normalization is applied, which is simple algorithm which does not support for time series packets information.

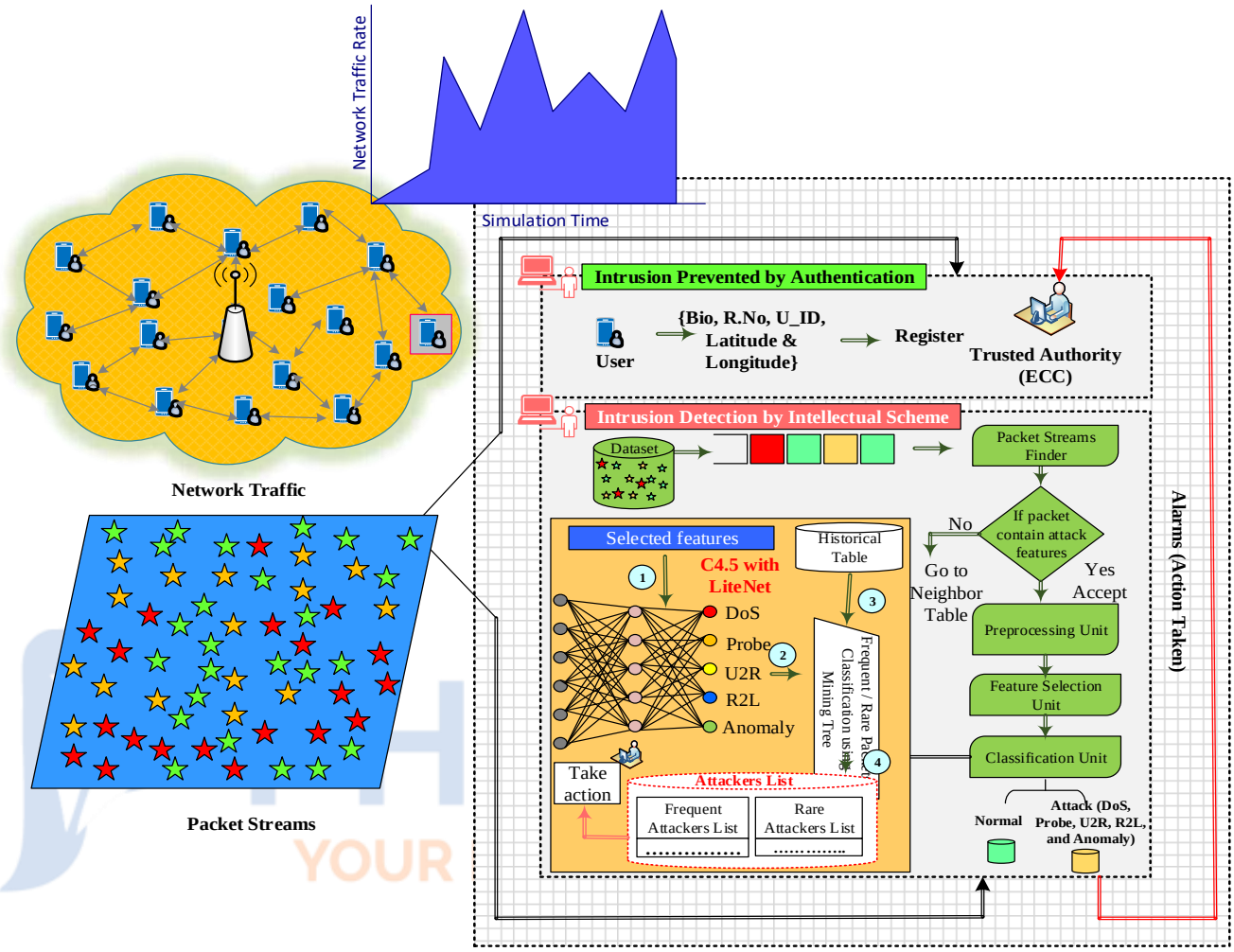
Solutions Proposed

- C4.5 with LightNet is used for packets classification, which gives high detection rate and effective IDS
- In preprocessing logarithmic normalization and encoding schemes are considered, which is time series and suitable for any application.

III. RESEARCH CONTRIBUTIONS

In our work, we have overwhelmed the problems in the existing IDS in the IoT network. Our work considers the NSL KDD dataset to perform the intrusion detection where we concentrate on detecting four different attacks such as DoS, Probe, U2R and R2L. We concentrated on hybrid IDS model using hybrid machine learning algorithm. Here, both signature and anomaly based approaches are proposed. The processes involved in the proposed IDS & IPS model are discussed as follows:

SYSTEM ARCHITECTURE



Each unit in intrusion detection engine is described in detail as follows:

Packet Streams Finder –

In this unit, an incoming packet from the mobile user is arrived, which is classified into either normal or attack based on the packet header information and threshold value. Due to massive arrival rate of network traffic, packets threshold value may change frequently. Hence, constant threshold does not suitable and it leads to incorrect outcome. So it must be adaptive and required to dynamic for classifying attack patterns. To mitigate this issue, Tsallis Entropy is used and also threshold level of node is calculated based on the percentage of the successful PDR of

the particular node.

For packet classification, Hidden Markov Model controller is used, which considers the input variables from the packet header. In this, environmental parameters are considered as the *SNR and bandwidth*. If the packet is classified as 'Normal', then it is put into the neighbor node table and allows the node to access the resources. Otherwise, the packet is passed to remaining three units to find the category of attack (DoS, U2R, R2L, and Anomaly) and also check the attack is frequent or rare.

Data Preprocessing –

In this unit, two operations are held such as Packet Encoding and Data Normalization. Generally speaking, dataset consists of features in an abbreviated form (eg. RSTO). In packet encoding, abbreviation is transformed into numerical values (binary value) for ease of classified. For example, RSTO is assigned with binary value 00. In normalization step, two techniques are used such as Logarithmic and Linear. In logarithmic all features are transformed into some specific and accepted range, whereas linear step cap the packet feature in the range of 0 and 5.

Feature Selection –

Set of features are selected using Human Mental Search Optimization. In this C4.5 lightnet algorithm, hidden layer clusters the incoming data using the **Human Mental Search (HMS)** algorithm. This process is performed to reduce the high feature dimensionality of the data packet. In the output layer, it classified into six classes as DoS, Probe, U2R, R2L, Anomaly and Normal

The unknown (anomaly) attack packet from the signature based IDS is processed in the anomaly based IDS framework. The attacks information is transmitted to the alarm module where alarm is provided to the system administrator.

Performance Evaluation

To evaluate the performance of the proposed IDS & IPS model, we have considered following performance metrics,

- Detection Rate (%)
  - Number of packets
- False alarm rate (%)
  - Number of packets
- Sensitivity (%)
  - Number of packets
- Specificity (%)
  - Number of packets
- F-Measure (%)
  - Number of packets
- Computation time (ms)

IV. RESEARCH NOVELTIES

- Our work initially filters the traffic initially in order to handle the huge packet stream from the IoT traffic. Thus reduces the overhead introduced during IDS model.
- We have considered environment related parameters (SNR and Bandwidth) during anomaly based IDS model in order to differentiate the abnormal and intrusive packet features. For this purpose, we have utilized HMM algorithm.
- We utilized C4.5 with LightNet to detect the intruders in the signature based system. Here, we classify the incoming packet in order to reduce the high dimensional feature set. Thus reduces the time during the intruder detection in the signature based system.

V. PREVIOUS WORKS & LIMITATIONS

Paper 1

Title – A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks

Concept

The authors in this paper presented the two layer mechanism to detect the intrusion in IoT network. This paper introduced the PCA and LDA to reduce the dimensionality of the features in the NSL KDD dataset. Initially, PCA is utilized to reduce the feature and further LDA is utilized to produce final reduced feature set. The reduced feature set is further processed in the naïve bayes and KNN algorithm to detect the intrusion. Here, naïve bayes is initially classifies the normal and anomaly. At last, KNN is utilized to detect the intrusion in IoT network.

Limitations

- The utilized classifiers such as k-NN and naïve bayes don't provide accurate result in intrusion detection. Since, naïve bayes provides result based on the probability of intruders and k-NN cannot able to handle the outliers of the intruder datasets.
- This paper achieves low detection rate, it is because of ineffective feature reduction procedures during intrusion detection. Since, the proposed PCA lose significant features due to its ineffective principal components (multi-dimensional mean, square distance of features) selection procedures.

Paper 2

Title - DL-IDS: a deep learning–based intrusion detection framework for securing IoT

Concept

The authors in this paper have concentrate on the deep learning based model to secure the IoT environment. It utilized NSL KDD dataset to detect the attacks from the IoT traffic. This paper consists of three different phases that are preprocessing, feature selection and classification. In preprocessing, it utilized the minkowsi distance based method to remove the redundant data from the dataset. Here, the spider monkey optimizer algorithm is used to select the optimal features. The optimal features from the dataset are further processed in the stacked deep polynomial network is used to detect the intruder.

Paper 3

Title – A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks

Concept

In this paper, the ensemble model based hybrid intrusion detection is performed on the IoT botnet dataset. It contains four different phases to detect the intrusion that are preprocessing, feature selection, signature based IDS and anomaly based IDS. Here, the features are selected using the information gain based algorithm. Then the selected features are transmitted to the signature based IDS model where the c5 classifier is used. And, in anomaly based model one class SVM is utilized to detect the intrusion. Then for the newly detect attacks, it generates attack signature for further processes.

Limitations

- The utilized one class SVM cannot able to handle the huge dimensional dataset that tends to result in low detection rate.

Paper 4

Title – Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks

Concept

This paper proposes the anomaly based intrusion detection model using the NSL KDD dataset features. Here, three different processes are executed that are preprocessing, feature selection and classification. The preprocessing is performed where data in the dataset are converted to the respective numeric values. And then, PCA algorithm is utilized to select the features from the preprocessed data. Then the selected features are processed using the GA based fuzzy classifiers where GA is used to select the optimal parameters for the SVM algorithm. Based on the selected features, it detects the attacks in the NSL KDD dataset.

Paper 5

Title – A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network

Concept

This paper detects the intrusion with the aid of the hybrid IDS model ISCX-UNB dataset. It initially performs the anomaly based IDS model where the anomalous packet and normal packets are classified. Here, the four different classifiers are used to detect the anomaly based IDS that are SVM, decision tree, random forest and gradient boosting tree. And, the misuse detection model is performed using the convolutional LSTM algorithm. In this features are extracted using the convolutional algorithm and then extracted features are classified using the LSTM algorithm.

Limitations

- Here, the incoming packets are first processed in the anomaly based IDS model where high feature dimensionality of the incoming packet streams is not reduced. Thus introduce high computation time and also degrades the detection rate.

Paper 6

Title – Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms

Concept

In this paper, the anomaly IDS model is utilized to detect the intruders on the NSL-KDD and ISCXIDS2012 datasets. This paper utilized the hybrid algorithm to detect the intrusions that are optimization and machine learning algorithms. It initially preprocesses the data packet and then performs feature selection, classification processes. Here, the feature selection process is executed using the artificial bee colony (ABC) optimization algorithm. Based on the selected features, adaboost machine learning algorithm detects the intruders in the network.

Paper 7

Title – An Intrusion Detection System for Connected Vehicles in Smart Cities

Concept

In this paper, the hybrid based intrusion detection is performed on the NSL KDD dataset. Here, the incoming data are initially processed into the preprocessing phase. In preprocessing stage, data packet is transmitted into the numeric form. Further preprocessed data packet is processed in hybrid based intrusion detection model. It utilized two different algorithms to detect the attacks in the dataset. The utilized algorithms are deep belief network and decision tree. The decision tree algorithm provides final detected attacks in the NSL KDD dataset.

Paper 8

Title – Deep Belief Network enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things

Concept

In this paper, the authors have pointed out the deep belief network to detect the intrusion in the IoT environment. It follows three different processes to perform the intrusion detection that are preprocessing, feature extraction and classification. In preprocessing, it executes the normalization process. And then the significant features from the dataset are extracted from the dataset. And the significant features from the dataset are processed in the deep belief network. Deep belief network classifies the intruders data packets from the normal data packets.

Limitations

- The process of matching the signature for incoming packet with the database signature induces tedious processing. Thus degrades the attack detection accuracy and consumes more time.

Paper 9

Title - A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer

Concept

The authors in this paper introduced the intrusion detection system with the aid of the feature selection on KDD cup 99, NSL KDD and UNSW datasets. Here, the intrusion attacks are detected using the feature selection based algorithm. Here, the pigeon inspired optimization algorithm is utilized to select the features from the dataset. The continuous binary cosine model is utilized. Based on these methods, this paper detects the attacks in the dataset.

Paper 10

Title - A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine

Concept

In this paper, intrusion detection scheme is based on the misuse detection based model (signature). In this, KDD99 and UNSW-NB15 datasets are utilized to detect the intrusion based on the signature of the attacks. This paper utilized the kernel principal component analysis algorithm to reduce the feature dimensionality and extracts features for intrusion detection. Here, extreme learning machine algorithm is utilized for intrusion detection. It has hybrid kernel functions such as RBF and polynomial kernel for detection. Further, this paper optimized the parameters of the ELM using the DE with GSA algorithm.

Limitations

- Feature dimensionality reduction is performed by selecting optimal features afore to the intrusion detection process. However, it doesn't suitable for the non-linear based high dimensional dataset. Thus in turn results in low accuracy during the intrusion detection. In this, kernel PCA is used to reduce the feature dimensionality which doesn't exhibit better performance under high dimensional data. Since, the size of the kernel matrix increases quadratically when increase in the data.

Paper 11

Title – Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks

Concept

The authors in this paper proposed the hybrid intrusion detection scheme on NSL-KDD and CICIDS 2017 dataset. This paper utilized both misuse detection (signature) and anomaly detection approaches for intrusion detection. Here, signatures in the repository are constructed in tree format using suffix tree. For the received packet, in signature based repository pattern matching method is utilized to detect the attacks. For the unknown signature patterns, received packets are transmitted to the anomaly detection engine where deep recurrent neural network is utilized to detect the intrusion. For the malicious packets, signatures are generated using the signature generation engine.

Limitations

- Here, the signatures are stored in the form of tree using suffix tree algorithm. This doesn't provide better performance under high dimensional data environment. Since, it constructs suffixes for single string instead of set of string.

Paper 12

Title – Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network

Concept

The authors in this paper proposed the intrusion detection system using the optimization and deep learning algorithms. The genetic algorithm is improved using the elite retention strategy. Here, the improved genetic algorithm is used to select the optimal number of hidden layers and number of neurons in each layer in deep belief network. The proposed deep belief network is

used to detect the intrusion in the IoT environment. For intrusion detection purpose, it utilized the NSL KDD dataset.

Limitations

- The proposed intrusion detection framework doesn't provide low detection rate. It is because of processing of all features (41) in dataset which also contain irrelevant features such as duration, land and hot. The processing of these features consume more time. Thus, this paper cannot able to detect the intruder on time.

Paper 13

Title - A New Architecture for Network Intrusion Detection and Prevention

Concept

This paper presents an investigation, involving experiments, which shows that current network intrusion, detection, and prevention systems (NIDPSs) have several shortcomings in detecting or preventing rising unwanted traffic and have several threats in high-speed environments. It shows that the NIDPS performance can be weak in the face of high-speed and high-load malicious traffic in terms of packet drops, outstanding packets without analysis, and failing to detect/prevent unwanted traffic. A novel quality of service (QoS) architecture has been designed to increase the intrusion detection and prevention performance.

Paper 14

Title – Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection

Concept

Various intrusion detection techniques are used, but their performance is an issue. Intrusion detection performance depends on accuracy, which needs to improve to decrease false alarms and to increase the detection rate. To resolve concerns on performance, multilayer perceptron, support vector machine (SVM), and other techniques have been used in recent work.

Such techniques indicate limitations and are not efficient for use in large data sets, such as system and network data. The intrusion detection system is used in analyzing huge traffic data; thus, an efficient classification technique is necessary to overcome the issue.

Paper 15

Title – An Industrial Network Intrusion Detection Algorithm Based on Multi-Feature Data Clustering Optimization Model

Concept

In this work an industrial network intrusion detection algorithm based on multi-feature data clustering optimization model, where the weighted distances and security coefficients of data are classified based on the priority threshold of data attribute feature for each node in the network, given that the data modules in the industrial network environment are diverse and easy to diagnose, restore and rebuild. The proposed algorithm can effectively improve the detection rate and real-time performance of detecting abnormal behavior for the multi-feature data in industrial networks. The novel features are twofold, to rapidly select a node with high-security coefficient as the cluster center, and match the multi-feature data around the center into a cluster.

BIBLIOGRAPHY

Elwahsh, H., Gamal, M., Salama, A. A., & El-Henawy, I. M. (2018). A Novel Approach for Classifying MANET Attacks with a Neutrosophic Intelligent System based on Genetic Algorithm. Security and Communication Networks, 2018, 1–10.

Vimala, S., Khanaa, V., & Nalini, C. (2018). A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks. Cluster Computing.

Kavitha, T., Geetha, K., & Muthaiah, R. (2019). India: Intruder Node Detection and Isolation Action in Mobile Ad Hoc Networks Using Feature Optimization and Classification Approach. Journal of Medical Systems, 43(6).

Feng, F., Liu, X., Yong, B., Zhou, R., & Zhou, Q. (2018). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks.

Zhang, B., Liu, Z., Jia, Y., Ren, J., & Zhao, X. (2018). Network Intrusion Detection Method Based on PCA and Bayes Algorithm. Security and Communication Networks, 2018

Pajouh, H.H., Javidan, R., Khayami, R., Dehghantanha, A., & Choo, K.R. (2019). A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks. IEEE Transactions on Emerging Topics in Computing, 7, 314-323.

Otoum, Y., Liu, D., & Nayak, A. (2019). DL-IDS: a deep learning–based intrusion detection framework for securing IoT. Transactions on Emerging Telecommunications Technologies.

Khraisat, Gondal, Vamplew, Kamruzzaman, & Alazab. (2019). A novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks. Electronics, 8(11), 1210.

Pradeep Mohan Kumar, K., Saravanan, M., Thenmozhi, M., & Vijayakumar, K. (2019). Intrusion detection system based on GA-fuzzy classifier for detecting malicious attacks. Concurrency and Computation: Practice and Experience, e5242.

Khan, M. A., Karim, M. R., & Kim, Y. (2019). A Scalable and Hybrid Intrusion Detection System Based on the Convolutional-LSTM Network. Symmetry, 11(4), 583.

Mazini, M., Shirazi, B., & Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University - Computer and Information Sciences.

Aloqaily, M., Otoum, S., Ridhawi, I. A., & Jararweh, Y. (2019). An Intrusion Detection System for Connected Vehicles in Smart Cities. Ad Hoc Networks.

Balakrishnan, N., Rajendran, A., Pelusi, D., & Ponnusamy, V. (2019). Deep Belief Network enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things. Internet of Things, 100112.

Alazzam, H., Sharieh, A., & Sabri, K. E. (2020). A Feature Selection Algorithm for Intrusion Detection System Based on Pigeon Inspired Optimizer. Expert Systems with Applications, 113249. doi:10.1016/j.eswa.2020.113249

Lv, L., Wang, W., Zhang, Z., & Liu, X. (2020). A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. Knowl. Based Syst., 195, 105648.

Kaur, S., & Singh, M.J. (2019). Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks. Neural Computing and Applications, 1-19.

Zhang, Y., Li, P., & Wang, X. (2019). Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network. IEEE Access, 7, 31711-31722.

Bulrajoul, W., James, A., & Shaikh, S. (2019). A new Architecture for Network Intrusion Detection and Prevention. IEEE Access, 1–1.

Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance Comparison of Support Vector Machine, Random Forest, and Extreme Learning Machine for Intrusion Detection. IEEE Access, 6, 33789–33795.

Liang, W., Li, K.-C., Long, J., Kui, X., & Zomaya, A. Y. (2019). An Industrial Network Intrusion Detection Algorithm based on Multi-Feature Data Clustering Optimization Model. IEEE Transactions on Industrial Informatics, 1–1.