INTERNATIONAL JOURNAL ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 10th Nov 2021. Link :http://www.ijiemr.org/downloads.php?vol=Volume-10&issue=ISSUE-11

DOI: 10.48047/IJIEMR/V10/I11/01

Title **Machine Learning Based Intelligent Intrusion Classification System for IoT Gateway Communication**

Volume 10, Issue 11, Pages: 1-9

Paper Authors

Mrs. V. Sree Ranganayaki, Dr. A. Ramesh Babu

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Machine Learning Based Intelligent Intrusion Classification System for IoT Gateway Communication

Mrs. V. Sree Ranganayaki[1] and Dr. A. Ramesh Babu[2]

[1]Research Scholar, Chaitanya Deemed to be University, Telangana, India.

[2]Professor, Chaitanya Deemed to be University, Telangana, India.

[1]sreeranganayaki5@gmail.com

[2]rameshadloori@gmail.com

Abstract -Internet of Things(IoT) is a next generation of Internet in that every object in the universe connect, communicate with sensor devices through Internet. In that inter-connected communication devices as well as sensor devices share the data through IoT gateway for a relevant application like whether forecasting, healthcare, smart city, disaster management are providing without human interaction. IoT enhances comfortable for human being even security is one of the challenging tasks. Intrusion detection system (IDS) will protect IoT devices from intruders. Now a day i.e in this era, as per user requirement and day-to-day increasing new innovative technologies as IoT, cloud computing, big data analytics, AIapplications implementation a network traffic will be generating a heavy data. To manage these data intrusion detection system is essential technique to detect, collect analyze the data is transmission through IoT gateway network. It is essential to improve the accuracy as well speed of intrusion detection system model by applying machine learning approach to detect IoT systems and gateway network to protect from cyber-attacks. In this paper providing a detailed study of Intrusion detection system (IDS) classification system for IoT gateway communication to protect IoT gateway by machine learning algorithms ina intelligent fashion.

Keywords –Internet of Things(IoT), gateway, Intrusion Detection System(IDS), cloud computing, big data.

1 - INTRODUCTION

Internet of Things(IoT) is a next generation of Internet is embedded with communication devices for sensingobjects that are nearby sensor devices. These sensor devices are low power,less bandwidth and life time ofthese sensor devices are very short and cannot replace batter frequently. Thesedevices connect,communicate and exchange data with other devices in a IoT gateway network. Mostlythe sensordevices are gather information from objects and send to Internet through IoT gateway forfurther processing this collected data and finally results can appear for end user by viewing mobile phone [1].

These IoT sensor devices are of two types homogenous and heterogeneous. In homogenous sensor devices the energy levels are same whereas in heterogeneous sensor devices the different energy levels[2]. The sensor devices having the capability of connect, collect for real-time application data of the remotely physical devices. The data collected by these Sensor devices are providing a provision of make intelligent decision for efficiently managingthe Internet of Things applications. Even it is requirement to design an intelligentsecurity mechanism for protecting Internet of Things against cyber-attacks for protect the data of a particular application.

It is motivation for taking consideration of implement of certain intrusion detection system by polar machine learning algorithms for IoT gateway network. Internet of Things are popular for developing applications for real-time smart systems,smart cities applications, automation of smart homes, smart health care etc. with technological challenges. Mostly these IoT devices and gateway network are attacked by physically accessing throughnetwork by malicious attacks. These IoT devices are connect and communicate with wirelessnetwork for that intruder attackers can easily eradicate communication channels. Due to minimal energy levels, minimal computation of resources of IoT devices, for implement ofadvancement security features not possible[3,4,5].

Internet of Things(IoT) SystemIoT for development real-time applications like home automation, industrial automation,city applications etc are by implemented IoT involving with various protocols and communication technologiesThe following figure shows the corresponding network technologies with protocols for related network technologies for efficient create, management of IoT applications[6].

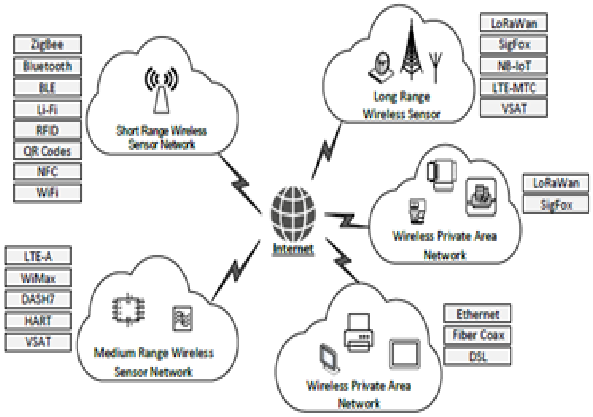

ZigBee
Bluetooth
BLE
Li-Fi
RFID
QR Codes
NFC
WiFi
Short Range Wireless Sensor Network
Long Range Wireless Sensor
LoRaWan
SigFox
NB-IoT
LTE-MTC
VSAT
Internet
Wireless Private Area Network
LoRaWan
SigFox
LTE-A
WiMax
DASH7
HART
VSAT
Medium Range Wireless Sensor Network
Wireless Private Area Network
Ethernet
Fiber Coax
DSL

Fig- Internet of Things(IoT) system model with accessing application through protocols and related network technologies.

2- LITERATURE SURVEY

In the area of IoT security various survey have been carried out. In our literature review focusing
on security on IoT application by Machine Learning algorithms.

In[7] authors discuss about machine learning algorithms for related to IoT security and also privacy. The authors identify limited bandwidth and computation power of IoT devices and lack of implementation of machine learning algorithms solutions towards IoT networks.

In [8,9] authors discussed about possibility of machine learning algorithms for to detect intrusion in IoT networks. Implement of machine learning algorithms for in Intrusion Detection Systems detect anomalies for classification of traffic.

In[10] authors discuss about types of ID related algorithms where implement on MANET for detect an attack in IoT network through some principles.

In[11] authors proposed a hybrid data processing of implementation by Nature inspired computing algorithms. These algorithms are inspiration of nature and model for solving computational problems in real-time environment. Authors apply hybrid algorithm by GWO and CNNalgorithms. This model achieve better accurate results while comparison to other IDS's algorithms.

3- INTERNET OF THINGS(IOT) THREATS AND ATTACKS

IoT systems are suffering from different security issues the reasons are first, IoT devices are low powered battery device and having minimum energy levels, not possible to replace, rechargebattery frequently. For the IoT systems is a challenging task for providing a securityfeature for against malicious attacks because IoT sensor devices are collect sensingdata that is highly useful for IoT applications. Second, IoT systems are connect communicate in networkcommunicating with diverse protocols, Third IoT devices are insecure in physical.IoT network connect to the IoT gateway network for applications like automation of home, smart lighting, smart parking in city applications, smart agriculture, HVAC systems applications based on IoT efficiently. All these development of application sensors, communication technologies and protocols involved for development of applications.IoT gateway connect to IoT devices through Internet for global communication [12,13].

Owing to limitations of processing, less battery energy capability of Internet of Thingsdevices, the intruder, hacker make IoT gateway network un-usable to connect to SoftAp. This causeof all communication network to eavesdropping and man in middle (MiTM) attack for a certaincommunications. IoT devices interact and integration with intelligent technology for communicate withreal physical environment for enabling interacting with various objects[14].

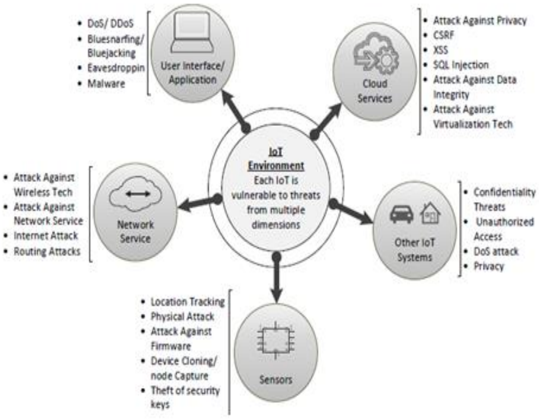


Fig – Internet of Things(IoT) with various attacks

4- ATTACKS AGAINST INTERNET OF THINGS (IOT) PROTOCOLS

Internet of Things(IoT) based protocols are light weight protocols for limited energy, limited data rate and less computing power enable devices. The following protocols based attacks for IoT technologies as follows[15,16,17].

4.1. Radio Frequency Identification (RFID) -

RFID system contain two components i.e. tags and readers. The reader is one of the device in RFID, that having one or more antenna uses radio waves for receiving signals from RFID tag. Tags are use radio waves to connect, communicate of their identify to readers. The readers are passive or active mode. Passive tags are battery less they are power by reader. Active tags are powered by battery. Various attacks against RFID are tag disable, modification of tag, snooping, relay attack etc.

4.2. Zigbee

Zigbee is a IoT protocol used to communicate to IoT devices for the reasons of low less cost, less power consumption. The major security threats for Zigbee networks are sniffing, replay attack, eavesdropping etc.

4.3. Bluetooth

Bluetooth is a protocol for sending and receiving through 2.4GHz wireless link. It is one of the security protocols of IoT network and connectivity of short-range in between 1-100 meters distance, supports low-power, low-cost, wireless transmissions for electronic devices.The PIN crack is the major attacks of Bluetooth, MAC spoofing, bluebagging,fuzzing attack, worm attack, DoS Attacks.

4.4. Near Field Communication

NFC is a communication protocols in IoT. It provide communication for distance of 4cm between two electronic devices in a network. NFC provide a low-speed connection for use of bootstrap and is capability for wireless communications support. The attacks against NFC technologies are summarized are eaves dropping, data corruption, data modification, data insertion etc.

4.5. Routing Protocol for Low Power and Lossy Network (RPL)

RPL protocols is designed for point-to-point communication, multi-point communication, point-to-multiple-point communications based on IPv6. The RPL will work on Destination oriented directed acyclic graph(DODAG) is a special type of protocol that join tree as well as mesh topologies. The attacks against RPL are sinkhole attack, wormhole attack, blackhole attack, hellow flooding attack etc.

4.6. 6LoWPAN

6LoWPAN is Internet protocol(IPv6) for low-power wireless personal area networks designed for resource-constrained device communication for low-power objects innetworks of IPV6. To achieve 6LoWPAN apply method of fragmentation at adaption layer. Attacksagainst 6LoWPAN are fragmentation attack, authentication attack, confidentiality attack etc.

5-INTRUSION DETECTION SYSTEM(IDS)

Intrusion Detection System (IDS) can be a device or it can be software application for monitoringa network for protect malicious activity. The IDS system having generalized structure that contain (i) the module of data gathering collects the data prove for data attack (ii) attacks of processing of data detects by data attack (iii) providing of report for attach mechanism.Intrusion Detection System(IDS) contain three components they are monitoring, analysis & detection, alarms. The monitoring module detect alarms, network traffic and patterns. The analysis module using various methods especially Machine learning algorithms are suitable as well as dominant for data examination for anomalousbehavior and attacksfor IoT devices in IoT network environment[17,18].

5.1 Machine Learning (ML) Techniques for IDS

Machine learning techniques are classified into supervised learning and un-supervised learning.

Again supervised learning classified into Naive Bayes (NB) Classifier,K-Nearest Neighbor (KNN),Decision Trees (DTs),Support Vector Machines (SVMs),Ensemble Learning (EL),Random Forest (RF),k-Means Clustering,Principle Component Analysis(PCA). The un-supervised learning classifiedinto K-means clustering, principle component analysis(PCA).

5.2 Naive Bayes (NB) Classifier

NB classifier popular of supervised learning algorithm as per Bayes to solve classification problems. The application of NB is for classification of training dataset. This algorithm is classification method that predicts as per probability of an object. Naïve means occurrence of the features is independent of various features. Bayes' means it depends on Bayes' theorem of principle.

The formula for Bayes' theorem as follows.

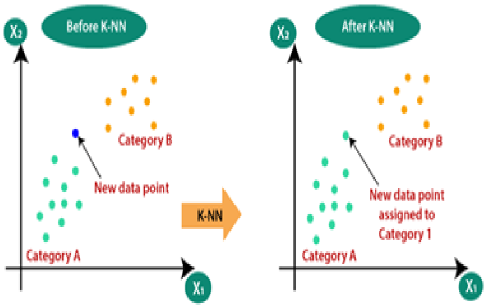
$$P(A)|\, B) = \frac{P(B|A)P(A)}{P(B)}$$

Where,

P(A|B) is a probability of hypothesis A for event B.
P(B|A) is a probability of hypothesis is true.

5.3 K-Nearest Neighbor (KNN)

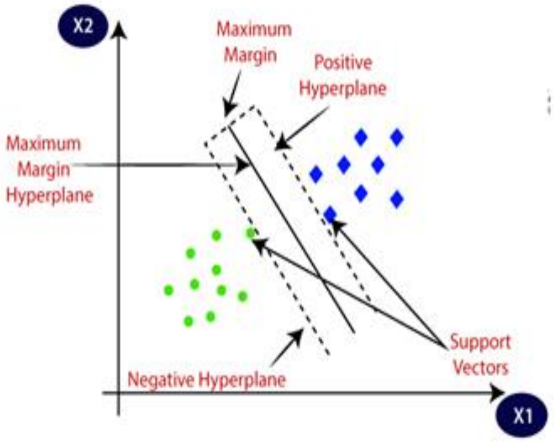
KNN is supervised machine learning algorithm. K-NN assuming the similarities of new data and put new data in category that is similarity to the available one. K-NN mostly used for classification problems. KNN not need any parameters for executing. To measure distance between neighbors using Euclidean distance. The KNN classifier algorithms used to classify data instance as per relative distance. K-NN do not make any assumptions on underlying data for that known as non-parametric algorithm. And also it do not learn from the training set instead it stores the dataset in the time of classification and perform actions on that dataset.



Decision Tree is in the category of supervised learning algorithms applyingto solve the problems ofclassification and regressio. It is classifiers like tree structure of internal nodes are treated as feature ofdataset, branches are treated as decision rules, each leaf treated as outcome.In Decision tree contain two nodes are decision node, leaf node. Decision nodes for take any decision where leaf nodes are not containany next branches.It is well known as decision tree as it is equal to a tree. It will exactly start with root nodeand extend branches like a tree data structure. To construct a tree use classification and regression tree algorithm(CART).

5.4 Support Vector Machine(SVM)

SVM is in the category of supervised machine learning algorithms. Used for classification and also regression problems. The aim of SVM make a decision boundary that segregate n-dimensional space. The decision boundary is hyperplane. To create hyperplane SVM chosen the extreme points for creation by applying super vector machine algorithm. The diagram shows two various categories that are classified using hyperplane.



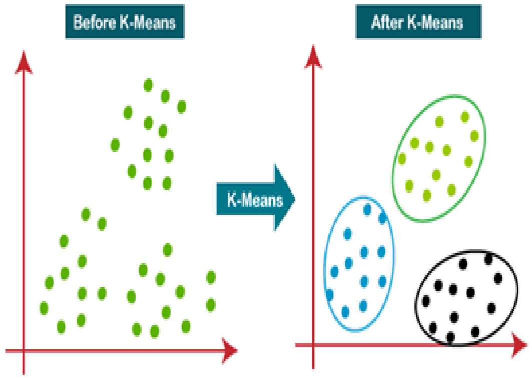
5.5 Random Forest (RF) Algorithm

Random forest is a well known machine learning algorithm based on supervised learning algorithms. It will apply for classification and regression problems in machine learning. This

algorithm combine multiple classifiers to solve a complex problems for improving of performance of the given model.Random forest is a well known classifier that consists a no. of decision trees on subsets of dataset and takes average to improving datasets' predictive accuracy. Manufacturers are not concentrate on security of devices because devices are low power hardware equipment. IoT devices are not enabled devices for heavy computational tasks.

5.6 K-Means Clustering Algorithm

It is in category of Un-supervised learning algorithms used to grouping the un-labeled datasets into various clusters. K defining the no. of pre-defined clustering that used tobe creating in that particular process if K=2 i.e. two clusters, K=3 i.e. three clusters.K-means algorithm perform two type of tasks i.e. determine the best value for K centriodsby iterative process. Assign every data point to near of K-center. Which points arenearest to the K-center will be create a cluster.



5 -CONCLUSIONAND CHALLENGES

In this we study and research works have been provided for IDS for Internet of Things platform. Even there a lot of open challenges and issues for providing security of devices in IoT gateway network. The IoT gateway network possessing homogeneousDevices(sensor device energy levels are same) and also heterogeneous (sensor device energy levels are different) type of devices. For that researchershaving challenge to conclude the type of protocols are defined for overall protection of IoT devices. Another challenge related to intrusion detection in IoT gateway networks are as follows. A quality of dataset should collect for IoT based IDS is essential. That type of datasets will contains an efficient network size for data flow for related label. The IoT data lack in provide require features like label missing, not sufficient network features. Creating and providing actual IoT datasets for solving the problems in real-time environment forchallenging for IoT gateway network. There is a requirement for essential security solution for IoT. The machine learning algorithms based IDS is have developed for providing essential IoT security. In this paper a survey on machine learning algorithms for Intrusion Detection techniques for IoT device and networks are briefly discussed. The attacks on IoT protocols and network discussed in brief in literature survey.

Finally we conclude that research should explore their future research for protection of IoT devices i.e. low battery, low processing capability devices against attacks in IoT network for that it is essential to provide certain improvement of machine learning algorithms that are suitable for security of these type of IoT devices.

REFERNCES

[1]Corcoran, Peter. "The Internet of Things." *IEEE Consumer Electronics Magazine, Jan 2016.*

[2]Fan, Tongrang, and Yanzhao Chen. "A scheme of data management in the Internet of Things." *2010 2nd IEEE InternationalConference on Network Infrastructure and Digital Content*. IEEE, 2010.

[3]Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." *IEEE Transactions on emerging topics in computing* 5.4 (2016): 586-602.

[4]Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." *2016 49th Hawaii International Conference on System Sciences (HICSS)*. IEEE, 2016.

[5] Adat, Vipindev, and Brij B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." *Telecommunication Systems* 67.3 (2018): 423-441.

[6]Jasim, Nabaa Ali, Haider TH, and Salim AL Rikabi. "Design and Implementation of Smart City Applications Based on the Internet of Things." *International Journal of Interactive Mobile Technologies* 15.13 (2021).

[7]Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning. arXiv**2018**, arXiv:1801.06275.

[8] Xiao, L.; Wan, X.; Lu, X.; Zhang, Y.; Wu, D. IoT security techniques based on machine learning. arXiv**2018**, arXiv:1801.06275.

[9]. Buczak, A.L.; Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutor. **2015**, 18, 1153–1176.

[10] Kumar, S.; Dutta, K. Intrusion detection in mobile ad hoc networks: Techniques, systems, and future challenges. Secur. Commun. Netw. **2016**, 9, 2484–2556.

[11]Garg, S.; Kaur, K.; Kumar, N.; Kaddoum, G.; Zomaya, A.Y.; Ranjan, R. A hybrid deep learning-based model for anomaly detection in cloud datacenter networks. IEEE Trans. Netw. Serv. Manag. **2019**, 16, 924–935.

[12]Siddiqui, Shams Tabrez, et al. "Security threats, attacks, and possible countermeasures in internet of things." *Advances in data and information sciences*. Springer, Singapore, 2020. 35-46.

[13]Alaba, Fadele Ayotunde, et al. "Internet of Things security: A survey." *Journal of Network and Computer Applications* 88 (2017): 10-28.

[14]Krejčí, Radek, Ondřej Hujňák, and Marek Švepeš. "Security survey of the IoT wireless protocols." *2017 25th Telecommunication Forum (TELFOR)*. IEEE, 2017.

[15] Krejčí, Radek, Ondřej Hujňák, and Marek Švepeš. "Security survey of the IoT wireless protocols." *2017 25th Telecommunication Forum (TELFOR)*. IEEE, 2017.

[16] Dragomir, Dan, et al. "A survey on secure communication protocols for IoT systems." *2016 International Workshop on Secure Internet of Things (SIoT)*. IEEE, 2016.

[17] Tabassum, Aliya, Aiman Erbad, and Mohsen Guizani. "A survey on recent approaches in intrusion detection system in iots." *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2019.