iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.49383

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Cyber-Physical Simulation

Vipul Tiwari[1], Harini S[2], Rakshith M[3]
Department of CSE, Dayananda sagar college of Engineering, Bangalore, India

Abstract: Integration of the internet into entities of the different domains of human society (such as smart homes, health care, smart grids, manufacturing processes, product supply chains, and environmental monitoring) is emerging as a new paradigm called the internet of things. However .the ubiquitous and wide range iot networks make them prone to cyber attacks. One of the main types of attack is a denial of service, where the attacker floods the network with the large volume of data to prevent nodes from using the services. An intrusion detection mechanism is considered a chief source of protection for information and communication technology. However, conventional intrusion detection methods need to be modified and improved for application to the iot owing to certain limitations, such as resource-constraints devices, the limited memory and battery capacity nodes, and specific protocol stacks.
INDEX: Intrusion detection system, anomaly detection, Internet of things, support vector machine.

I. INTRODUCTION

The concept of Internet of Things (IoT) is based on the integration of uniquely identiable heterogeneous physical objects around us (humans, animals, sensors, instant cameras, vehicles etc.) and the cyber world with the ability to transfer data over a network without requiring human-to-human or human-to-computer interfaces. As illustrated in Figure 1, the applications of the IoT may range from a simple appliance for a smart home to a complex apparatus in a smart grid.

A. Testbed For Power Systems

The IoT provides a tremendous opportunity for societies around the world. Even with different objectives, contrasting IoT applications have an intersection set of characteristics. Broadly speaking, a primary node in IoT has capability to perform three distinct actions; *data collection*, *data transmission*, and *data processing and utilization* the data collection stage, small, memory-constrained and low energy-consumption sensors with a short-range communications capability are employed to collect.

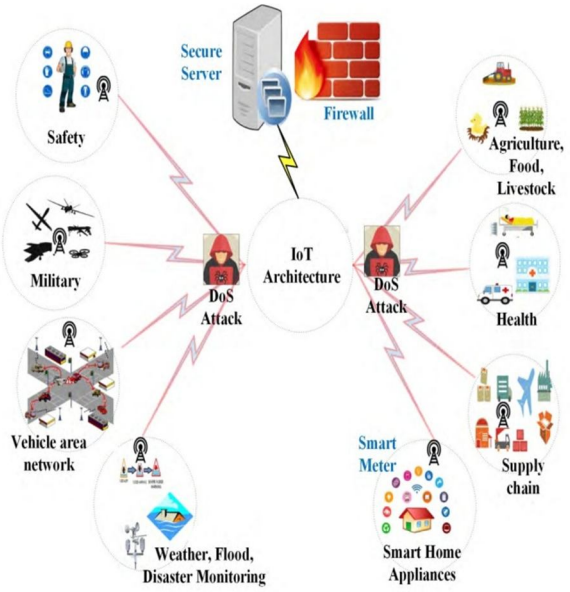
Considering that the development of IDSs for the IoT represents a significant challenge for information security, researchers describe Iot networks in terms of specific characteristics as follows:

1) Unlike traditional networks , where the systems administration deploys IDS agents in networks entities with high computing and storage capacities , the memory capacity, processing power, and battery energy-capacity constraints of IoT network nodes that host IDS agents is challenging.
2) In conventional networks, end systems are directly connected to specific nodes (e.g., wireless access points, switches, and routers) that are responsible for forwarding packets to the destination. In constrast, there are multiple hopes of IoT networks. Regular nodes may simultaneously forward packets and work as end systems. Moreover, in some IoT applications, the network topology regularly changes. The specificity of the topology poses new challenges for IDSs.
3) Protocols used in IoT networks are different from conventional networks, such as IPv6 over Low-power Wireless Personal Area Network(6LoW-PAN),IPv6 Routing Protocol for Low –power and Lossy Networks (RPL) and Constrained Application Protocol(CoAP). Heterogeneity in protocols introduces new weaknesses which result in new challenges for IDS in the IoT.

The characteristics of Iot networks given above limit the design of IDS to an lightweight still efficient enough to secure the network from potential attacks. The term lightweight does not refer to simplicity of the system. It means that the IDS should be able to perform its operations with the available amount of resources in the sensor nodes of the network .Concluding, a lightweight system is the one which can perform in limited energy and computation resources regardless of simplicity .Keeping these definitions in mind,we design a light weight IDS system by avoiding the complex features extraction and feature selection steps. We provide rather uncomplicated and limited number of features to be extracted from raw data .The results show that, this type of system can perform efficiently in discriminating an intrusion in the IOT network.

The proposed scheme is intuitive to perform well in this type of application. However, there is no literature addressing the intrusions detection problem using such a foolproof algorithm. This leaves gap for proposing and analyzing such uncomplicated and intuitive algorithm for these applications rather than utilizing complex statically techniques.

There are many datasets available providing samples DoS attacks under different scenaries including KDD'99, DARPA .CAIDA DDoS, etc. The issue to us these datasets for evaluating our proposed algorithm lies in the attributes in which these datasets are available .the only characteristic of network traffic that is use in our algorithms is the packet arrival rate per node. However, this characteristic of the data is not given in any of the above given dataset. For instance, the dataset KDD'99 represent the data sample in attributes such as protocol type, duration of connection, land etc, but packet arrival rate. This limits our algorithms to be tested utilizing these online available datasets.



An example of IoT applications

A. Motivation

The novelty of this manuscript lies in the design of an ID forIoT networks with the characteristics of lightweight i.e., minimizing cost of system in terms of energy consumption and computational resources. An Ideal IDS system is lightweight enough to be implemented in a sensor node equipped with limited battery capacity and computational resources, still performing efficiently. In this work, this is achieved by elim-inating the complex features extraction from data and thefeature selection steps. Instead of taking different characteristics the proposed IDS rely on only the packet arrivalrate attribute of raw data. Moreover, the complexity of anSVM-based classifier directly depends on the dimensionsof input vector. The higher the dimensions of input vectorthe higher the complexity of SVM. Keeping this in mind,we reduce the dimensions by extracting only 2 to 3 features from input vector. In short, we try to develop lightweight IDS by the following way. We are considering only one attribute,i.e., the packet transmission rate, and extract only 2 to 3features from that attribute. The three features utilized includemean, median and maximum values obtained to perform the classification. Intuitively, these steps reduce the energy and computational cost as compared to a system considering upto 40 complex attributes, such as protocol type, service, land,wrong fragments etc. as given in NSL-KDD dataset. Thisapproach makes the proposed IDS suitable for implementa-tion in sensor nodes of IoT while keeping the efficiency ofsystem satisfactory as illustrated in the experimental results. Furthermore, several researchers have proved that an SVM-based classifier outperform neural networks, k-nearest neighbor, random forest etc. This is the motivation to design our proposed algorithm based on an SVM-based classifier. A performance comparison of SVM-based classifier and other machine learning-based algorithms can also befound in literature supporting this argument.

B. Contributions

Thus, to unlock the IoT potential, we need to improve IoT security and the performance of IDS. In this paper,we are motivated to consider intrusions (and corresponding anomaly-based IDS) accompanied by changes in traffic intensity. This effect is typical for a wide range of attacks in the IoT environment. The main contributions of this paper are as

1) We analyze DoS attacks in the IoT that were reported in the literature and conclude that the consequences of the intrusions include changes in the intensityof the transmitted packets. In some cases, the change in traffic intensity is an attack tool; in other cases, it is a concomitant effect. Analysis reveals the relationship between traffic change profiles and types of intrusion.
2) Intrusion detection on a sensor-by-sensor basis is a challenging problem. At the same time, there is an industrial demand on intrusion detection in devices. In some recent papers it has been declared a low quality of SVM based intrusion detection on a sensor-by-sensor basis. However, in this paper we demonstrate that a foolproof SVM based approach combined with proper statistics and feature engineering provides good perfor mance in various scenarios.
3) Instead of utilizing complex attributes (given in online datasets such as NSL-KDD) of the system, we utilize only one attribute, the packet arrival rate to the sensor node. To the best of authors' knowledge, this work is pioneer considering specifically this attribute for devel oping an IDS for IoT.
4) Based on the above analysis, we develop a support vector machine (SVM)-based classifier for lightweight IDS. The performance of classifier is analyzed for linear, polynomial, and radial-basis kernel functions.
5) Simulation experiments are conducted to verify the choice of SVM parameters and to demonstrate the method's efficiency. The performance of IDS is ana- lyzed in terms of true positive rate, true negative rate, false positive rate, false negative rate, and accuracy and detection time.
6) Furthermore, the performance of proposed SVM- based IDS is compared with other machine learning algorithms-based IDS including neural network, KNN and decision tree. The accuracies comparison of 100 iter- ations of experiments prove the efficiency SVM-based classifier using linear and polynomial kernel functions.
7) Finally, the performance of proposed algorithm is compared with some of the proposed algorithms in liter- ature. The accuracy measure is used to assess how effi- ciently an algorithm can detect the intrusions. The CPU time measure is used to compare the lightweightness measure of different algorithms. The results show that the proposed algorithm is not only lightweight among the given set of algorithms but it also outperforms these algorithms

II. ANALYSIS OF IOT THREATS

A. *Typical Attacks In Iot And Concomitant Effect*

Considering the specific characteristics of IoT networks, an adversary can launch attacks to disrupt the system in many ways. In this paper, we consider the typical attacks reported in the literature. Remark, there are several projects on, and standardization initiatives for, WSNs, which may eventually converge with the Internet of Things (IoT), for example European Union projects of Internet of Things Architecture (IoT-A) have been addressing the challenges of IoT solutions development from the WSNs perspective.A brief description of the typical attacks follows. A brief description of these attacks follows.

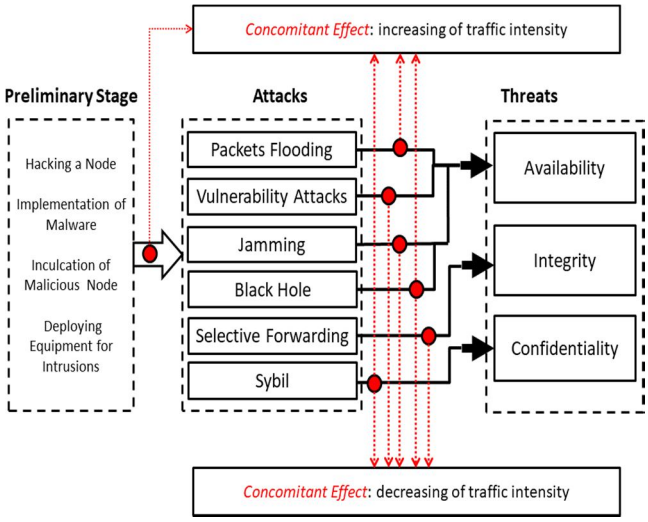
1) *Packets Flooding:* In a wide range of attacks, an intruder can generate a storm of spoofed packets or repeatedly duplicated legal packets. This results in the channels being overloaded, network node buffers overflowing, and in some cases, the goal of the intruder can be the depletion of a network node battery (a vampire attack). However, in all cases, the attack obviously increases traffic intensity.
2) *Vulnerability Attacks:* During a vulnerability attack, some malformed packets are sent to the target to mislead a protocol or an application running under it. It leads to degradation of device functionality, and therefore, data transmission intensity is degraded as well.
3) *Black hole Attack:* A malicious node can attract all the packets by requesting a fresh, misleading route to the destination. Then, it accepts them without forwarding them to the destination.
4) *Jamming:* An intruder transmits a signal and jams net- work working frequencies in a way that decreases the signal-to-noise ratio to a level where the nodes of the wireless network can no longer function. As a result of the attack, a group of nodes becomes isolated and does not generate traffic. Therefore, the attack decreases traffic.
5) *Selective Forwarding:* An intruder drops part of the packets, which leads to information integrity degrada- tion. If an intruder does not replace the legal packets with spoofed packets, that quickly unmasks the intrusion, and then, traffic intensity decreases
6) *Sybil Attack:* A node in an IoT network is compro- mised by adversaries in such a way that it depicts itself with false identities to other nodes. Depending on an intruder's goal, the attack can lead to two scenarios of traffic change. Sham nodes can generate additional traffic, or inhibit the traffic of legal nodes.
7) Sinkhole Attack: In this scenario, a compromised node tries to attract network traffic by advertising false routing information. Subsequently, it can be used to initiate other attacks, like selective forwarding, acknowledge spoofing, altering packets or dropping them etc.

8) Clone Attack: In this situation, adversaries acquire the secret information of nodes and create duplicates of this information in the whole network to mislead data packets. These kinds of attack are very dangerous to wireless sensor networks. Cloned nodes can launch a variety of attacks: black hole, inject false data etc.

9) Wormhole Attack: The adversary can attract and avoid a huge amount of network data by creating a tunnel between two distant nodes in an IoT network. This attack is generally used in conjunction with eavesdropping or selective forwarding.

10) Hello, Flood Attack: In the network, each new node sends ‘‘Hello’’ messages to discover its neighbor nodes.

Also, it broadcasts its route to the base station. Other nodes may choose to route data through this new node ifthe path is shorter. If a malicious node equipped with apower transmitter sends a ‘‘Hello’’ message with attractive conditions, then a lot of nodes choose it for data transmission. However, the packets of these nodes willnever be retransmitted. Therefore, the attack decreases general intensity.



Typical Iot attacks and concomitant effects

Thus, the typical attacks in the IoT are accompanied by changes in traffic intensity. As the result of some attacks, the intensity grows; in others, it declines. There are some cases where the same attack leads to traffic increasing in one location yet decreasing in another. In the preliminary stages of the attack, an intruder usually explores the network looking for vulnerabilities, which can be accompanied by an increase in traffic. The relationships of typical IoT attacks to traffic change are shown . The concomitant effect can be inherent in all components of the CIA triad.

DoS attacks, especially distributed DoS (DDoS) are serious problems in the IoT, which have been inherited from traditional IP networks. An efficient protection against these types of attack does not exist yet; for example, the biggest attack ever, recorded in 2016, left hundreds of thousands of connected devices infected [18]. In the IoT, the situation becomes worse due to the limited resources of IoT devices. In the preliminary stages of an attack, an intruder can generate some traffic to explore a network and identify system bottle- necks. Moreover, fundamentally new attacks on the IoT lead to traffic change, as well.

Thus, observations of traffic intensity can be used for IDS. To design an IDS for the IoT, the representative charac- teristics of low computing power, limited memory capacity, and constrained energy capacity in the nodes should be taken into account. In this paper, we investigate a foolproof and

Lightweight IDS based on an SVM. We show in a series of experiments that by extracting only two or three features froman input sample, the SVM can achieve satisfactory results detecting attacks against the network in a timely manner.

A. IOT Traffic Modeling

Generally, to analyze network behavior, a mathematical model of the traffic is used. Real traffic records are available in particular cases. The models are based on sim- plifying assumptions; however, some often provide a basis for adequate approximations of network behavior, as well as worthwhile insights. The scientific and engineering commu-nity has accepted the following fact: the Poisson process (i.e. exponentially distributed times between packet arrivals) is appropriate for traffic modeling in the IoT as wellas in WSNs, which are considered an essential part of the IoT.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Here, we consider conditions for Poisson process deriva- tion. Let $N(t)$ be the number of packets that have arrived in the time interval $(0, t)$, and let λ be a positive constant. Let usformulate the following four conditions:

1) $N(0) = 0$.
2) Packet arrivals in non-overlapping time intervals are mutually independent.
3) The probability reflecting the number of packet arrivals in the interval $(t, t + h)$ depends only on length h and not on time origin t.
4) For a sufficiently small h, we get equations for the probabilities as follows:

$$P[N(t+h) - N(t) = 1] = \lambda h + o(h)$$
$$P[N(t+h) - N(t) = 0] = 1 - \lambda h + o(h)$$
$$P[N(t+h) - N(t) > 1] = o(h) \quad (1)$$

where $o(h)$ is the quantity as $\lim_{h \to 0} \frac{o(h)}{h} = 0$.

In other words, if interval h is small enough, then the probability of the event ''more than one packet arrival during time h'' is negligibly small.

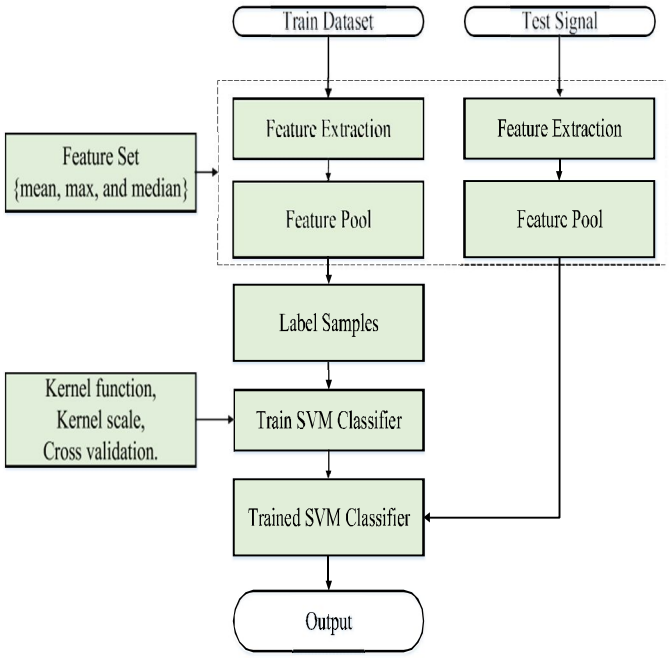
If the four conditions above are met, then the traffic is described by a Poisson process, i.e. the time between packet arrivals is exponentially distributed, and the probabity mass function of N (t) is as follows:

$$P[N(t) = n] = (\lambda t)^n e^{-\lambda t}, \quad n \geq 0. \quad (2)$$

The Poisson process is used in many practical situations. So in this paper, we use it to generate training and testing samples for SVM performance analysis. However, we wouldremark that we do not use special properties of a Poisson probability mass function. Our features are limited by order statistics, mean, and median. So, the proposed approach can be applied even in more general situations.

III. THE PROPOSED INTRUSION DETECTION SYSTEM

The framework of the proposed IDS is given in Figure 3. The two main phases of the system include the training phase and the evaluation phase. Remark, in this paper we consider intrusions accompanied by changing traffic Intensity. However, the proposed approach does not utilize any specific properties of intrusions. Thus, it can be adopted for other cases. In the training phase, a training dataset containing labeled samples is obtained. Features are extracted from these samples in the first stage of this phase to obtain a feature pool. The resulting feature pool along with a vector of labels is then used to train the classifier. After a trained classifier is obtained, it is then presented to classify the unobserved samples from the test dataset. To evaluate the performance of the classifier, similar features used in the training phase are extracted from the test dataset. These unlabeled test samples are then given input to the classifier to obtain the predictedoutput.



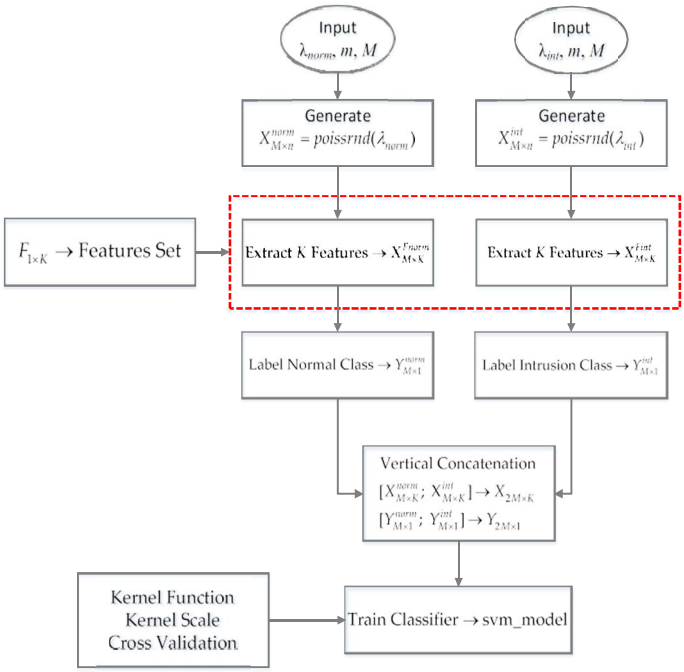
Framework of the proposed support vector machine-based intrusion detection system

A. Support Vector Machine

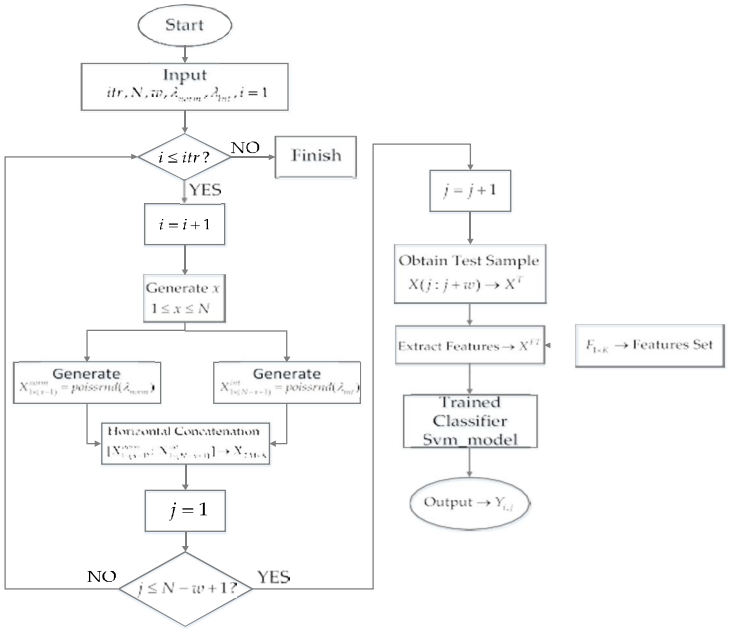
The SVM was developed from the concepts of statically learning theory in the late 1970's. The SVM primarily deals with the two-class classification problems. A linearline,or hyper plane , is constructed as a decision boundary between the datasets of two classes for classification. The data points nearest to the hyper plane, which impart the construction of the hyperplane, are called the super vectors. Hence, the algorithm is a support vector machine. The optimized hyperplanr can be mathematically expressed as

$$w^T x + b = 0 \qquad (3)$$

There are several kernel functions used in an SVM for non-linear pattern classification, such as linear, polynomial, sigmoid, and the radial-basis function (RBF). In this work, three kernel functions (linear, polynomial and RBF) are used.



Flowchart of training phase



Flowchart of testing phase

IV. DISCUSSION

The tradeoff for using only three features as opposed to '40 complex attributes' is related to the issue of feature selection and reduction. The advantage of using only three features is as following:

First, the system processing time canbe reduced due to low time consumption of single attribute acquisition from input data instead of multiple attributes.

Secondly, extracting just 2 or 3 features from that single attribute takes lower time as compared to extraction of upto 40 features from the multiple attributes.

Lastly, the complexity of SVM is also reduced because of utilizing a much lower number of dimensions (features) of input samples. Combining all these effects makes a big difference to the complexity of system. Furthermore, the feature selection stepis omitted in the case of the proposed algorithm. These points can be considered as the positive effects of utilizing the proposed algorithm along with the proposed signal preprocessing model. Nevertheless, the feature selection and reductiontechniques do not necessarily converge to global optimum, and sometimes end up selecting redundant features, which ultimately results in poor performance of classifier

Apparently, the main drawback of the proposed algorithm is that it lacks the ability to detect intrusions which do not have concomitant (increasing or decreasing) effect on the traffic intensity of node. The algorithms which consider the complex 40 features may be able to detect more sophisticatedintrusions. This issue is reserved for future works.

In this paper, we have considered the packet arrival rate, which follow the Poisson distribution, of the traffic intensityto the node. The Poisson distribution is just used for performance evaluation. We use this distribution because it hadbeen offered in papers of authoritative journals. It should be noted that, we do not use specific properties of CDF. Therefore, all expenses will be the same for any othertraffic pattern followed in practice. However, the selected features such as mean, maximum and median, and the proposed detection scheme can be used irrespective of the type of distribution, given the condition that the intrusion or attackhas an increasing or decreasing effect on the traffic intensity(packet arrival rate) to the node.

A. Why need to use Packet Arrival rate Attribute?

As we have explained in Section III, the types of intrusions orattacks considered in this paper are the ones which influencethe traffic intensity. Either the data rate is decreased (e.g. in case of packets flooding attack, jamming attack etc.) or increased (e.g. black hole attack, wormhole attack) whenever any of these intrusions occur.

This means that if the IDS monitor the traffic intensity alone (or more specifically packet arrival rate measure), it may be able to detect these intrusions most of the time. This is our motivation of proposing an IDS which rely on packet arrival rate attribute exclusively to detect the intrusions. This claim is also supported by experimental results given in the paper.

B. Why Need to Extract min, Max and Median Features?

The packet arrival rate is the only attribute of data which is used for intrusion detection in the network. Now, the question is why needed to extract features from this attribute? Why not use this attribute to detect an intrusion using a threshold value? If the packet arrival rate goes higher than the thresholdvalue, it can be considered as intrusion and vice versa. The answer to these questions can be given in a single argument;the threshold value selection is not an easy and reliable way.To find out a threshold for any system needs a continuous monitoring of the network for a long time to get an estimate of the threshold value. Selecting a sub-optimal value of threshold would result in higher miss-detection or false- alarm instances. Moreover, it is believed that the network conditions are not consistent all the times. The nodes may observe variations in packet arrival rate depending on the network conditions i.e., network may be very busy or idle. Therefore, the threshold selection method is not favored for detection and classification application. On the other hand, the machine learning algorithms try to learn the characteristics of the network from a handful amount of historical data. At this point, we have two choices; either directly use the only attribute (packet arrival rate attribute value) as the singleinput, or extract features (minimum, maximum and median values) from this attribute to give input to machine learning-based classifier. In former case, using the single input to theclassifier may degrade the performance of system because of two reasons. First, there may be a single value whichis included in both classes i.e., intrusion and non-intrusion classes. For instance, depending on the network condition,a specific packet arrival rate may or may not be resulted dueto the intrusion in the network. Secondly, if a single value of packet arrival rate attribute is used, the classifier needs to perform detection every time we get a new value. Ultimately,the energy consumption is increased due to the utilizationof computational resources more frequently. In this paper, the minimum, maximum and median values are obtained from the packet arrival rate attribute over a window of time to solve both the problems. For instance, a packet of data is arrived every t seconds to the node.

If this single value isused, then the classifier will perform the classification task every t seconds. On the contrary, if we use a time window $T >> t$, then the classifier has to perform classification every T seconds. This leads to reduce the frequency of utilizingcomputational resources as well as the algorithm converge better as compared to using the first case of utilizing a single attribute alone.

C. Why SVM?

The SVM is favored among other machine learning algorithms because of its efficient performance. The performancecomparison among different machine learning algorithms given in the experimental results section confirms our claim.Furthermore, the light weightness of the proposed algorithm is proved in the experimental results as well.

D. How Do We Get Less Training And Testing Times?

The main reason that the proposed algorithm has the lowest training and testing time is that the other algorithms have additional feature selection properties. They try to select the best subset of features using complex optimization techniques. For instance, GA-SVM utilizes genetic algorithm to choose the best features among given set. Similarly, A-IDS and WFS-IDS algorithms analyze and select the best features using wrapper-based feature selection mechanism. A detailed explanation about these algorithms is out of scope of the current work; therefore, readers are suggested to refer these papers for more details. However, the major reason which reduces the computational time of the proposed algorithm isthe elimination of the feature selection which is the part of training phase only. The testing phase has no feature selection step, and hence,the difference between the testing times of all these algorithmsis very low as given . However, the small differences in training time are reported because of using different algorithms.

E. How do we Get Better Accuracy?

The complexity of the classifier has a direct effect of the complexity and size of input vectors. The simple and small vectors with high discrimination power among different classes are easy to classify by classifier. On the other hand, the higher number of the dimensions with complex relation among features of input vector increases the challenge of classification for classifier. In authors' opinion, the input vector of only 2 dimensions with comparatively low complexity among features are the key factors which lead the classifier to obtain ahighest accuracy of proposed IDS.There are a few control values used in the proposed algorithm. First, the kernel parameter used in the support vector machine. Changing this value may affect the performance of classifier. An optimized value can be obtained by hit and trial. Another value which should be selected carefully is the time window size. As shown in the experimental results, increase in time window size may improve the performance to some extent. Further increase in the time window size may degradethe performance of classifier.

V. CONCLUSIONS AND FUTURE WORKS

The IoT is a promising technology developed for applications ranging from small smart-home systems to large networks, such as smart grids. However, this vast network is exposed to different types of attacks, compromising its reliability. Furthermore, the limitations in the nodes, including memory, computational resources, and battery capacity, challenge net- work security. It is necessary to design a lightweight systemthat can efficiently improve the security of the IoT with the available resources.

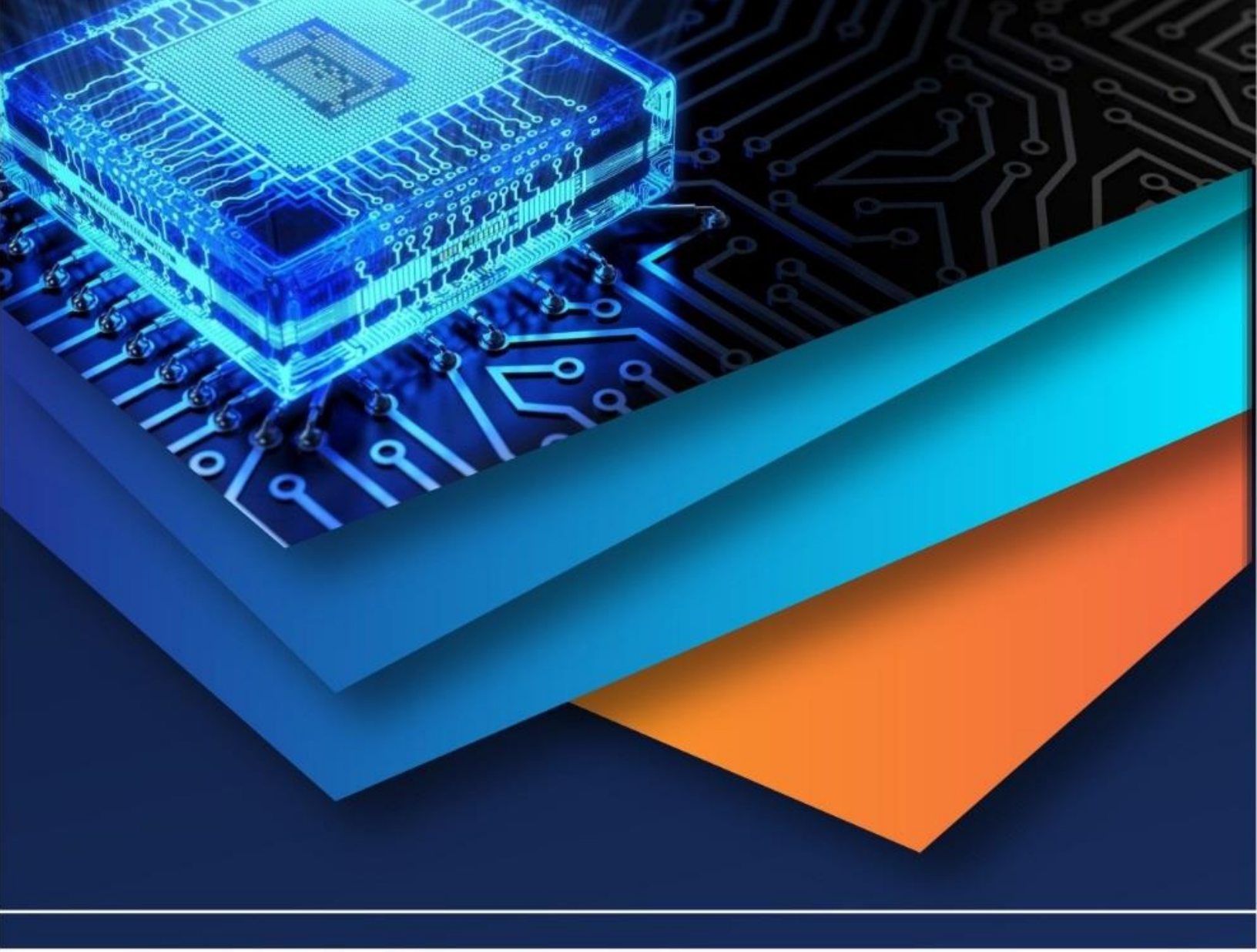
This paper focuses on designing lightweight IDS for anomaly detection in the IoT. A common type of attack, known as DDoS, is the target. The proposed IDS is focuses on two major issues; the attribute of the receiving data used to classify the signal and the machine learning based classifier. The only attributed considered in this paper is the packet arrival rate to the node. For classification purpose, an SVM- based classifier with input given in the form of two or three in complex features is utilized. Through a series of experiments, we prove that these two factors (the packet arrival rate attribute and an SVM-based classifier) can be enough to detect the intrusion in IoT network. Furthermore, we presented a comparative analysis of SVM-based classifier with other machine learning-based classifiers including NN, k-NN and DT to show the advantage of utilizing SVM in terms of accuracy over other techniques. For further proof, we also presented a comparison of pro- posed algorithm with other IDS proposed in literature. The results show that SVM-based IDS can perform satisfactorily in detection of attacks. Also, the lightweightness measure of proposed algorithm is proven in terms of CPU time execution. An investigation of various concomitant effects of attacks and increase in the scope of this IDS system to encompass other types of intrusions, where the effect of changing traffic intensity is not clearly pronounced or masked by intruders, is reserved for future works. Furthermore, concrete details of IDS implementation and intrusions mitigation are definedby application domains and strategy of security perimeter deployment. It is also a direction of our future work.

REFERENCES

[1] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga,''A survey of intrusion detection in Internet of Things,'' J. Netw. Comput. Appl., Apr. 2017.
[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, ''Security, privacy and trust in Internet of Things: The road ahead,'' Comput. Netw., vol. 76, pp. 146–164, Jan. 2015.
[3] D. Singh, G. Tripathi, and A. J. Jara, ''A survey of Internet-of-Things: Future vision, architecture, challenges and services,'' in Proc. IEEE World Internet Things (WF-IoT), Mar. 2014, pp. 287–292.
[4] A. Meddeb, ''Internet of Things standards: Who stands out from thecrowd?'' IEEE Commun. Mag., vol. 54, no. 7, pp. 40–47, Jul. 2016.
[5] H. Sedjelmaci, S. M. Senouci, and T. Taleb, ''An accurate security game for low-resource IoT devices,'' IEEE Trans. Veh. Technol., vol. 66, no. 10, pp. 9381–9393, Oct. 2017.
[6] Y. Fu, Z. Yan, J. Cao, and O. Koné, and X. Cao, ''An automata based intru-sion detection method for internet of things,'' Mobile Inf. Syst., vol. 2017, May 2017, Art. no. 1750637.
[7] M. Roesch et al., ''Snort—Lightweight Intrusion Detection for Networks,''in Proc. Lisa, vol. 99, 1999, pp. 229–238.
[8] T. H. Hai, E.-N. Huh, and M. Jo, ''A lightweight intrusion detection frame-work for wireless sensor networks,'' Wireless Commun. Mobile Comput., vol. 10, no. 4, pp. 559–572, 2010.
[9] Y. Maleh and A. Ezzati, ''Lightweight intrusion detection scheme for wireless sensor networks,'' IAENG Int. J. Comput. Sci., vol. 42, no. 4, pp. 347–354, 2015.
[10] I. Sharafaldin, A. Gharib, A. H. Lashkari, and A. A. Ghorbani, ''Towards a reliable intrusion detection benchmark dataset,'' Softw. Netw., vol. 2017, no. 1, pp. 177–200, 2018.
[11] KDD'99 Dataset. Accessed: Mar. 10, 2018. [Online]. Available: http://www.unb.ca/cic/datasets/index.html
[12] S. U. Jan, V.-H. Vu, and I. Koo, ''Throughput maximization using an SVM for multi-class hypothesis-based spectrum sensing in cognitive radio,'' Appl. Sci., vol. 8, no. 3, p. 421, 2018.
[13] S. U. Jan, Y. D. Lee, J. Shin, and I. Koo, ''Sensor fault classification based on support vector machine and statistical time-domain features,'' IEEE Access, vol. 5, pp. 8682–8690, May 2017.
[14] P. T. Noi and M. Kappas, ''Comparison of random forest, K-nearest neigh- bor, and support vector machine classifiers for land cover classification using sentinel-2 imagery,'' Sensors, vol. 18, no. 1, p. 18, 2018.
[15] J. Deogirikar and A. Vidhate, ''Security attacks in IoT: A survey,'' in Proc. IEEE Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC), Feb. 2017, pp. 32–37.
[16] L. Atzori, A. Iera, and G. Morabito, ''The Internet of Things: A survey,''
[17] Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[18] I. Tomić and J. A. McCann, ''A survey of potential security issues in existing wireless sensor network protocols,'' IEEE Internet Things J., vol. 4, no. 6, pp. 1910–1923, Dec. 2017.
[19] M. D. Donno, N. Dragoni, A. Giaretta, and A. Spognardi, ''DDoS-capable IoT malwares: Comparative analysis and Mirai investigation,'' Secur. Com-mun. Netw., vol. 2018, Feb. 2018, Art. no. 7178164.
[20] V. Shakhov and I. Koo, ''Depletion-of-battery attack: Specificity, mod- elling and analysis,'' Sensors, vol. 18, no. 6, p. 1849, 2018.
[21] F. Farahnakian and J. Heikkonen, ''A deep auto-encoder based approach for intrusion detection system,'' in Proc. IEEE 20th Int. Conf. Adv. Commun. Technol. (ICACT), Feb. 2018, pp. 178–183.
[22] S.-M. Lee, B.-D. Jeong, and S.-B. Suh, ''Method of intrusion detection in terminal device and intrusion detecting apparatus,'' U.S. Patent 8 701 188, Apr. 15, 2014.
[23] J.-P. Ramirez-Paredes, E. A. Doucette, J. W. Curtis, and V. Ayala-Ramirez,''Sensor compromise detection in multiple-target tracking systems,'' Sen-sors, vol. 18, no. 2, p. 638, 2018.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY