Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 10, Issue. 4, April 2021, pg.17 – 21

IOT Security Vulnerabilities and Predictive Signal Jamming Attack Analysis in LoRaWAN

S. E. Viswapriya; S. Dinesh; D. Viswa Ravi Teja
Assistant Professor, Student, Student
Department of Computer Science, SCSVMV University, Kanchipuram, India
seviswapriya@kanchiuniv.ac.in
DOI: 10.47760/ijcsmc.2021.v10i04.003

Abstract- Application Layer Distributed Denial of Service (DDoS) attacks are very challenging to detect and mitigate. HTTP jamming, XML attack, DNS attacks, etc, are the various possible application layer attacks. The HTTP jamming is the most common and renowned application layer attack. There are various research solutions proposed by validating against HTTP jamming using tools such as Golden Eye, LOIC, proprietary tools, etc. The similar characteristics of the real Time HTTP jamming attack will not be exhibited by the HTTP jamming attacks. Various methods were used to defend these attacks based on distributed schemes with certain difficulties to count the packets or duplicates sent by a node due to lack of communication infrastructure. In order to mitigate packet flood and replica flood attacks, two limits are used respectively. The claim-carry-and- check will notice the violation of both the limits easily. The inconsistency check against full claims is trivial. This is applicable to work in a distributed system. It will tolerate a little number of attackers for collision.
Keywords:- Jamming attacks, HTTP, IOT Security.

I. Introduction

We get denial of service by a new attack, the Ad Hoc Jamming Attack, when used against all on demand ad hoc networks routing protocols. The attacker either broadcasts a lot of Route Request packets for node ID who is not in networks, or sends a lot of DATA packets to consume the bandwidth so as to congest in links in this attack. The main scope of this project comes under Data Analysis, Dataset Pre-processing, Training the Model, Testing of Dataset. An explosion of data in all forms and from every region of the world has been brought by evolution of deep learning. This is termed as big data, is drawn from sources like social media, internet search engines, e-commerce platforms, and online cinemas, etc. We can access easily and can share the large amount of data through finite applications like cloud computing.

II. Literature Survey

According to Kiwon Hong et al, SDN-Assisted Slow HTTP DDoS Attack Defense Method has been used to determine the attack. A web server to be unavailable due to a Slow HTTP Distributed Denial of Service (DDoS) attack, Because of its traffic patterns are similar to those of legitimate clients it is difficult to detect in a network. They also proposed a network- based Slow HTTP DDoS attack defense method which is assisted by a Software-Defined Network (SDN) that can detect and mitigate Slow HTTP DDoS attacks in the network. Simulation results show that the proposed Slow HTTP DDoS attack defense method successfully protects web servers against Slow HTTP DDoS attacks.

According to Qiao Yan, F. Richard et al, they have done Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments. They discussed the new trends and characteristics of DDoS attacks in cloud computing, and provide a comprehensive survey of defense mechanisms against DDoS attacks using SDN. This can help to understand how to make full use of SDN's advantages to defeat DDoS attacks in cloud computing environments and how to prevent SDN itself from becoming a victim of DDoS attacks, which are important for the smooth evolution of SDN-based cloud without the distraction of DDoS attacks.
According to Bharti Nagpal, As with Pratima Sharma et al, they have done DDoS Tools: Classification, Analysis and Comparison. It is recognized that DDoS attack tools and techniques are emerging as effective, refined, and complex to indicate the actual attackers. Due to the seriousness of the problem many detection and prevention methods have been recommended to deal with these types of attacks. This paper aims to provide a better understanding of the existing tools, methods and attack mechanism. In this paper, we commenced a detailed study of various DDoS tools. This paper can be useful for researchers and readers to provide the better understanding of DDoS tools in present times.

III. Existing System

This paper aims to explore the security vulnerabilities of IoT devices particularly that use Low Power Wide Area Networks (LPWANs). In this work, LoRaWAN based IoT security vulnerabilities are scrutinized and loopholes are identified. An attack was designed and simulated with the use of a predictive model of the device data generation. The paper demonstrated that by predicting the data generation model, jamming attack can be carried out to block devices from sending data successfully. This research will aid in the continual development of any necessary countermeasures and mitigations for LoRaWAN and LPWAN functionality of IoT networks in general. The existing system proposes a framework to determine packet sniffing and eavesdropping in building attack profiles for a target LoRaWAN device, which is achieved by analyzing the Traffic and identifying exploitable trends. Compare the effectiveness of continuous and targeted DoS attacks on IoT devices in a LoRaWAN environment. Proposition for remedies to the attack scenarios carried out, and discussion on the implications of such mitigations.

IV. Proposed System

The proposed system presents a period-based defense mechanism (PDM scheme is based on the periods and uses a blacklist to efficiently prevent the data jamming attack, by checking the data packet floods at the end of each period in order to enhance the throughput of burst traffic. Therefore, it can guarantee the Quality of Service (QoS) of burst traffic. As a result of which many data packets are forwarded at a high rate for the whole duration. Flood attacks are launched by malicious or selfish nodes. Malicious nodes, which can be the nodes purposely setup by the opponent or subverted by the opponent via mobile phone worms

begin attacks to congest the network and misuse the resources of other nodes. Selfish nodes may also develop flood attacks to increase their communication throughput. In DTNs, a single packet usually can only be carried to the destination with chances smaller than 1 due to the opportunistic connectivity

Advantages

- Reduce false alarm probability.
- Cost reduction for its users.
- Higher accuracy.
- Opaqueness since routers need not be involved.
- Successfully minimize the amount of traffic.

V. Actual Work Implementation of Modules Exploratory Data Analysis

• Exploratory Data Analysis (EDA) is the first step in data analysis process.
• It allows to get closer to the certainty that the future results will be valid, correctly interpreted, and applicable to the desired business contexts.
• Such level of certainty can be achieved only after raw data is validated and checked for anomalies, ensuring that the data set was collected without errors.

Preprocessing

• If the data is missing from the dataset, then we can use the library called Scikit Learn preprocessing.
• It contains a class called Imputer which will help us take care of the missing data.
• We split our dataset into two sets
  - A Training set
  - A Test set
• A general rule of the thumb is to allocate 80% of the dataset to training set and the remaining 20% to test set. For this task, we will import test train split from model selection library of scikit

Feature engineering

• Filter methods are generally used as a preprocessing step.
• Pearson's Correlation: It is used as a measure for quantifying linear dependence between two continuous variables X and Y. Its value varies from -1 to +1.
• LDA: Linear discriminant analysis is used to find a linear combination of features that characterizes or separates two or more classes (or levels) of a categorical variable.
• ANOVA: ANOVA stands for Analysis of variance. It is similar to LDA except for the fact that it is operated using one or more categorical independent features and one continuous dependent feature. It provides a statistical test of whether the means of several groups are equal or not.
• Chi-Square: It is a statistical test applied to the groups of categorical features to evaluate the likelihood of correlation or association between them using their frequency distribution.

Prediction

• Once training is complete, it's time to see if the model is any good, using Evaluation.
• Evaluation allows us to test our model against data.
• This metric allows us to see how the model might perform against data.
• This is meant to be representative of how the model might perform in the real world.

• Once done with evaluation, it's possible that to see if we can further improve our training in any way.

VI. Results and Discussions

This section explains about various results and descriptions.

	MI_dir_L5_weight	MI_dir_L5_mean	MI_dir_L5_variance	MI_dir_L3_weight	MI_dir_L3_mean	MI_dir_L3_variance	MI_dir_L1_weight	MI_dir_L1_mean	MI_dir_L1_
0	1.000000	566.0	0.000000e+00	1.000000	566.0	0.000000e+00	1.000000	566.0	0.00
1	1.996585	566.0	5.820766e-11	1.997950	566.0	5.820766e-11	1.999316	566.0	0.00
2	2.958989	566.0	0.000000e+00	2.975291	566.0	5.820766e-11	2.991729	566.0	5.8
3	3.958979	566.0	0.000000e+00	3.975285	566.0	0.000000e+00	3.991727	566.0	1.1
4	4.914189	566.0	1.164153e-10	4.948239	566.0	5.820766e-11	4.982654	566.0	5.8

5 rows × 116 columns

Fig 1

	MI_dir_L5_weight	MI_dir_L5_mean	MI_dir_L5_variance	MI_dir_L3_weight	MI_dir_L3_mean	MI_dir_L3_variance	MI_dir_L1_weight	MI_dir_L1_mean	MI_dir_L1_
0	1.000000	75.000000	0.000000	1.000000	75.000000	0.000000	1.000000	75.000000	
1	1.106002	61.437635	19.497725	1.260128	63.096451	36.858761	1.638356	65.844478	
2	2.105991	60.754994	10.754895	2.260121	61.726414	22.915699	2.638352	63.629278	
3	3.105975	60.511916	7.416684	3.260111	61.196857	16.520386	3.638348	62.631771	
4	4.105965	60.387240	5.658644	4.260104	60.915911	12.899777	4.638346	62.064377	

5 rows × 116 columns

Fig 2

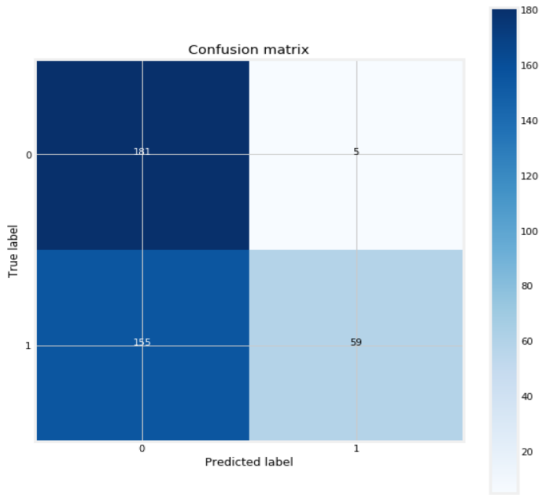

Fig 3

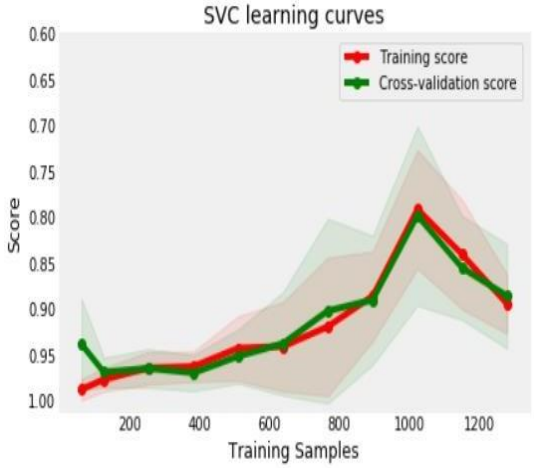

Fig 4

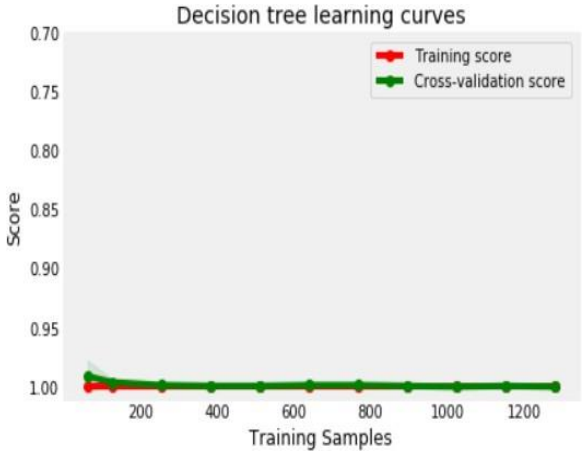

Fig 5

CONCLUSION

Reduce the flood attacks by employing rate limitation and probabilistically detect the number of attackers by developing the claim-carry-check. The learning automata algorithm is used to detect the approximate counting number of packets which are violating the rate limits. This works is implemented in a distributed manner. Also, it can tolerate a little number of attackers to collude. They easily reduce the throughput of burst traffic by comparing with the simple threshold. Hence, the main aim to enhance the throughput of burst traffic under the data jamming attack. This is achieved by using proposed scheme and it also gives guarantee the QOS compared to old scheme.

REFERENCES

[1]. S. Umarani, D. Sharmila, ‘‘Predicting Application Layer DDoS Attacks Using Machine Learning Algorithms”, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.8, No.10, 2014, pp. 1912-1917.

[2]. Shahanaz Begum I, Geetha Ramani G, “DDoS Attack detection and Prevention in Private Cloud Environment “, International Journal of Innovations in Engineering and Technology (IJIET), Vol.7 Issue.3, Oct 2016, pp. 527- 531.

