Intrusion Detection for WiFi Network: A Deep Learning Approach

Shaoqian Wang[1,2], Bo Li[1], Mao Yang[1](✉), and Zhongjiang Yan[1]

[1] School of Electronics and Information,
Northwestern Polytechnical University, Xi'an, China
{libo.npu,yangmao,zhjyan}@nwpu.edu.cn
[2] Science and Technology on Communication Networks Laboratory,
Shijiazhuang 053200, China

Abstract. With the popularity and development of Wi-Fi network, network security has become a key concern in the recent years. The amount of network attacks and intrusion activities are growing rapidly. Therefore, the continuous improvement of Intrusion Detection Systems (IDS) is necessary. In this paper, we analyse different types of network attacks in wireless networks and utilize Stacked Autoencoder (SAE) and Deep Neural Network (DNN) to perform network attack classification. We evaluate our method on the Aegean WiFi Intrusion Dataset (AWID) and preprocess the dataset by feature selection. In our experiments, we classified the network records into 4 types: normal record, injection attack, impersonation attack and flooding attack. The classification accuracies we achieved of these 4 types of records are 98.4619%, 99.9940%, 98.3936% and 73.1200%, respectively.

Keywords: Wi-fi network · Network intrusion detection · Deep learning

1 Introduction

With the development of Internet related technology and the enhancement of network demand, WLAN technology has developed rapidly day by day. There are many kinds of Wi-Fi networks, such as home wireless local area network, campus network, enterprise network, etc. Users can use mobile phones to access the Internet at any time, as long as they are in the range of signal reception. However, with the increasing number of wireless network users, the problem of network security is becoming more and more serious. Many large wireless local networks, such as campus network and enterprise network, contain a large number of important information, and any network security problems may cause huge

J.-L. Chen et al. (Eds.): WiCON 2018, LNICST 264, pp. 95–104, 2019.
https://doi.org/10.1007/978-3-030-06158-6_10

losses. In contrast to the wired networks, Wi-Fi network with wireless propagation characteristics is relatively less secure and more vulnerable to attack. Packets are easily intercepted and tampered when they are propagating from source address to destination address. In order to protect the confidentiality, integrity and security of network system resources in a Wi-Fi network, the application of intrusion detection technology is very necessary.

Intrusion Detection System (IDS) can monitor the running status of network and system in real time, and detect various kinds of attack. There have been many studies related to the use of intrusion detection technology in large-scale wireless local area networks such as campus networks and enterprise networks. Deep learning techniques can also be adopted to improve the performance of IDS and classify the attacks from the mass data of the wireless network.

A large number of records including various network attack patterns are important for deep learning techniques. In previous papers, KDDCUP99 [1] and NSLKDD [2] datasets have been used for many times. These two are very classic Wi-Fi network datasets, which have 4 categories and 39 attack types. However, because of the rapid development of network technology, network records more than a decade ago have apparently been unable to adapt to today's Wi-Fi network. In this paper, we use the Aegean WiFi Intrusion Dataset (AWID) [3] to validate our proposed approach. The dataset was published in 2015 and it contains normal records and different attack records. In recent years, more and more research literatures on intrusion detection have cited the AWID dataset.

Kolias et al. [3] used the AWID dataset to perform intrusion detection based on various machine learning algorithms. They introduced AWID and network attack types in great detail, but the accuracy of classification using machine learning techniques is not ideal. Aminanto et al. [4–6] proposed several novel methods to detect impersonation type attack and showed a detection rate of 99.918% and a false alarm rate of 0.012%. But their models can not detect other attacks except impersonation attack. Thing [7] compared the classification accuracies under the SAE model with different activation functions and achieved optimal results based on the Parametric Rectified Linear Unit (PRelu) [8] function. However, in the above-mentioned papers, only two-layer or three-layer models were used in the deep learning model, and no attempt was made in a neural network with more hidden layers.

In this paper, we analyse several kinds of network attacks in Wi-Fi networks and utilize Deep Neural Network (DNN) and Stacked Autoencoder (SAE) to perform attack classification. We validate our approach using AWID dataset after the feature selection. In our experiments, our proposed approach classified the network records into 4 categories, and we achieved great classification accuracies of the injection, flooding and impersonation attacks.

In the rest of this paper, the second part introduces some common network attacks in Wi-Fi networks. The third part introduces the AWID dataset and the data preprocessing. The fourth part introduces our SAE model and DNN model. The fifth section shows the test results and analysis. The sixth part summarizes the full text.

2 Attacks for Wireless Network

Attacks in Wi-Fi networks generally fall into two categories. One is attacks against data confidentiality protection, network access control, and data integrity protection; the other is attacks based on a unique approach to wireless network deployment, design, and maintenance. In addition, network attacks in Wi-Fi networks can also be subdivided into the following seven categories:

2.1 Injection

In a Wi-Fi network, an attacker can implement message injection by installing related attack software. An attacker can implement forged data packets, modify the header or end of the data packet, and can tamper with any field of the data packet. After the packet is injected into the relevant data transmission, the attacker can control the entire transmission process of the message.

2.2 Eavesdropping Adversary and Network Traffic Analysis

Because of the characteristics of Wi-Fi network, its transmission medium is open. Attackers can eavesdrop the network information in Wi-Fi networks through related tools. Even if the message has been encrypted, as long as there are certain rules or vulnerabilities in the message, the attacker can perform analysis and calculation on the information packet to obtain some or all of the messages from the specific message.

2.3 Unauthorized Access

In a Wi-Fi network, signals are transmitted by electromagnetic waves. Within the service area formed by the access point (AP), any wireless terminal may access the AP. Unauthorized access means that the user accesses the wireless terminal device through the AP, but this access is not allowed by the AP. Wi-Fi network encryption and authentication methods need to be improved, there are still some loopholes. The Wi-Fi network uses a unidirectional authentication mechanism, the wireless terminal sends a authentication request to the AP, and the AP does not authenticate the wireless terminal. Unidirectional authentication will give the intruder the opportunity to enter the network through the AP. Illegal users can constantly send authentication requests to AP. A large number of authentication requests can cause AP to be paralyzed and not work properly. And then, the attacker can steal network data or information on the network terminal device after access to the network.

2.4 Session Hijacking

Session hijacking attacks generally consist of two parts. First, the attacker uses some method to force the station (STA) to disconnect from the AP. After that, the attacker will establish a connection with the AP as a faked STA, steal the message session, and control the sending and receiving of the session. Session hijacking attacks are also generally divided into two forms: passive hijacking and active hijacking. Passive hijacking is actually monitoring the data flow between two parties in the background to get sensitive data. Active hijacking is to replace a host in the session with an attacker and take over the conversation.

2.5 Forged AP

AP's MAC address is included in the header of the packet in Wi-Fi networks. The data packet header exists in clear text during data transmission. The attacker can obtain the MAC address of the AP and change his MAC address to the address of a valid AP.

2.6 Man-in-the-Middle Attack

Man-in-the-middle attack is an indirect attack. This attack mode is to place a computer controlled by an intruder between two communication computers that are network-connected through various technical means. This computer is called a "Man-in-the-Middle". This computer can intercept and tamper with the normal network communication data, but both parties of the communication are unaware of it. When host A and B communicate, they are forwarded by host C. There is no real direct communication between A and B. The information transfer between them is done by C as an intermediary. In this way, host C is able to eavesdrop and tamper with the information from the communication, and achieve its own goals by sending the malicious information to A or B.

2.7 Dos

Dos attack is a very serious and most common type of attack in wired networks and wireless networks. Its purpose is to make the network unable to serve legitimate users. Attackers can initiate multiple forms of denial of service attacks. Attackers can broadcast a large number of radio frequency interference signals. The wireless channel is always busy. As a result, legitimate users cannot use the channel to send normal requests. An attacker can also send a large number of invalid association messages to the AP. As a result, the AP resources are exhausted and crashed, and normal wireless access services cannot be provided. This affects the establishment of relationships between other legal STAs and APs.

3 Datasets and Attributes Selecting

AWID dataset is collected in a real local area network. Compared with the dataset generated by simulation software, AWID dataset has higher reliability and authenticity. AWID dataset can be classified into AWID-CLS dataset and AWID-ATK dataset. There are 4 types of labels in AWID-CLS dataset and 16 types of labels in AWID-ATK dataset. In this paper, we select the AWID-CLS-R dataset, which contain 4 classes namely normal, injection, impersonation and flooding. The training dataset contains 1795575 records and the test dataset contains 575643 records. The distribution of normal records and various attack records are shown in Table 1.

Table 1. Data distribution

	Normal	Injection	Impersonation	Flooding
AWID-CLS-R-Trn	1633190	65379	48522	48484
AWID-CLS-R-Tst	530785	16682	20079	8097

The records in AWID have 154 attributes, but not all of them contribute to the training of the model. In addition, there are also some question mark ("?") for unavailable values for the corresponding attributes in the dataset. Therefore, the preprocessing of the datasets is necessary. In the first step, string attribute and the attributes which consist of the same value are removed. In the second step, we removed some attributes according to the amount of the question marks. All the attributes which have too many "?" were removed, while the rest of the question marks in the dataset were set to zero [9] value. Based on these steps, 71 attributes were selected. In the third step, we transformed all the data into numerical values and normalize the attributes. Equation (1) shows the formula of normalizing.

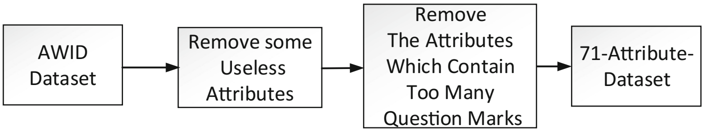
AWID Dataset
Remove some Useless Attributes
Remove The Attributes Which Contain Too Many Question Marks
71-Attribute-Dataset

Fig. 1. Preprocessing of the dataset

$$y_i = \frac{x_i - min(x)}{max(x) - min(x)} \tag{1}$$

In this formula, y_i expresses the normalized value, x_i expresses the attribute values, and $max(x)$ and $min(x)$ express the maximum and minimum values of the attribute x. In the last step, because the size of normal records is much larger than the size of attack records, the amount of normal type records should be reduced. We balanced the train dataset by selecting only 10% of the normal type records randomly. Table 2 shows the data distribution of the final training dataset.

Table 2. Remaining records

Category	Number
Normal	163319
Injection	65379
Impersonation	48522
Flooding	48484

4 Deep Learning Model

In this paper, SAE and DNN are used to build intrusion detection classification models. They both use PRelu as the activation function. In PReLU, parameter a can be learnt during the training phase.

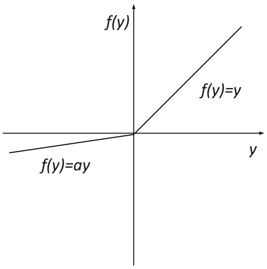

Fig. 2. Parametric Rectified Linear Unit(PRelu)

4.1 Stacked Autoencoder (SAE)

SAE is a deep learning model composed of multi-layered autoencoders. The output of the previous autoencoder can be used as the input of the next autoencoder. SAE is widely used in model pre-training and non-label supervised learning. Figure 3 briefly shows the a single-layer autoencoder. Based on the principle of input equal to output, the input data will be encoded and decoded. After many times of training, the input data encoded result can be used as the input of the next layer.

The SAE model we utilized in this paper is composed of three hidden layers, the number of neurons in each layer are 128, 96 and 64. After the training step, we utilized Softmax regression to classify the records.

4.2 Deep Neural Networks (DNN)

The DNN model is a deep back propagation (BP) neural network model. A larger number of hidden layers provide a higher level of abstraction for the model, and

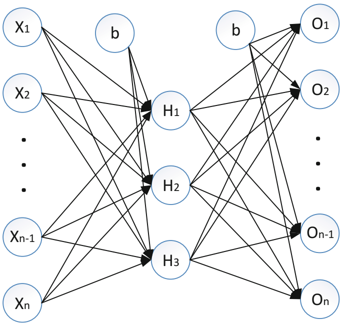

Fig. 3. Autoencoder

improve the ability of the model. In this paper, we use the DNN with more hidden layers to train and test the dataset. We used mini-batch gradient descent and dropout [10] algorithm to further improve the performance of DNN model.

We proposed two kinds of DNN models, one is composed of 3 hidden layers, the number of neurons in each layer are 128, 64 and 32; the other is composed of 7 hidden layers, and the number of neurons in each layer are 94, 112, 128, 96, 72, 48 and 24. They both utilize Softmax regression to classify the records.

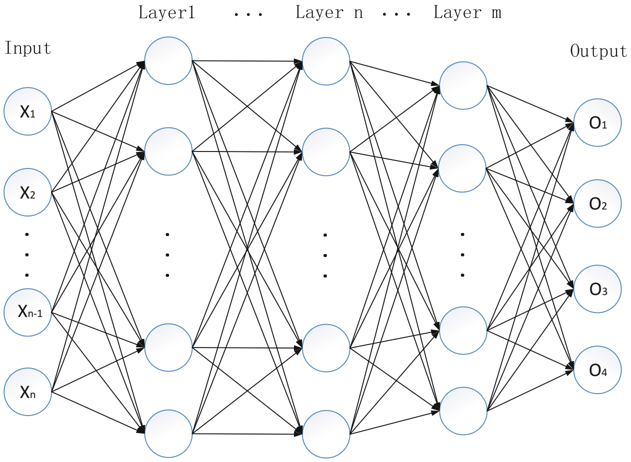

Fig. 4. Deep Neural Network (DNN)

5 Performance Evaluation

Based on SAE and DNN models, training and testing were conducted on 71-attribute dataset. We achieved the classification accuracies of the normal records and the three types of attack records. Tables 3, 4, 5 show the classification results for the three models we proposed.

Table 3. The Evaluation of the SAE using AWID with 71 Attributes

Category	Number	Correctly classified	Incorrectly classified	Classification accuracy (%)
Normal	530785	521477	9308	98.2464
Injection	16682	16681	1	99.9940
Impersonation	20079	16499	3580	82.1704
Flooding	8097	5602	2495	69.1861

Table 4. The evaluation of the 3-hidden-layer DNN using AWID With 71 attributes

Category	Number	Correctly classified	Incorrectly classified	Classification accuracy (%)
Normal	530785	509697	21088	96.0270
Injection	16682	16681	1	99.9940
Impersonation	20079	1278	18801	6.3649
Flooding	8097	5974	2123	73.7804

Table 5. The evaluation of the 7-hidden-layer DNN using AWID With 71 attributes

Category	Number	Correctly classified	Incorrectly classified	Classification accuracy (%)
Normal	530785	522621	8164	98.4619
Injection	16682	16681	1	99.9940
Impersonation	20079	19757	322	98.3963
Flooding	8097	5927	2170	73.1200

By comparing the results showed from Tables 3, 4, 5, it can be found that the classification accuracies of injection type attack are same. We achieved an accuracy of 99.994%, only 1 injection type record was classified incorrectly. Although the impersonation attack is the most challenging to detect, our 7-hidden-layer DNN showed a great classification accuracy of impersonation type attack. The accuracy of impersonation attack is high to 98.3963%, it is a obvious improvement, compared to the 82.1704% and the 6.3649% which we achieved based on the 3-hidden-layer DNN and SAE. The accuracy of flooding attack based on 7-hidden-layer DNN is 73.12%, it is a little lower than the 73.7804% we achieved based on the 3-hidden-layer DNN.

We compared our results against the previous work by Thing [7] as shown in Table 6. Thing [7] tested 2-hidden-layer SAE model and 3-hidden-layer SAE model on AWID dataset. The 2-hidden-layer SAE showed a better performance, and it achieved a accuracy of 99.8050%. Our proposed method showed a drop in the normal record classification by 1.343%, but we achieved a improvement in the classification accuracies of the injection and flooding attacks by 17.2761% and 15.642%, respectively. Our proposed approach has the advantage of detecting injection type attack and flooding type attack.

Table 6. Result comparing

	Normal(%)	Injection (%)	Impersonation (%)	Flooding (%)
Thing [7]	99.8050	82.7179	98.4959	57.4780
Our result	98.4619	99.9940	98.3963	73.1200

6 Conclusion

In this paper, we analyze theoretically the various types of attacks that exist in Wi-Fi networks and proposed a deep learning approach for the attack classification problem. We validate our approach using AWID dataset and select 71 attributes after the feature selection. We adopt SAE and DNN to perform attack classification. The experimental results showed that our 7-hidden-layer DNN model achieved a high accuracy for all categories. The classification accuracy of normal, injection attack, impersonation attack and flooding attack are 98.4619%, 99.9940%, 98.3936% and 73.1200%, respectively.

Acknowledgment. This work was supported in part by the National Natural Science Foundations of CHINA (Grant No. 61771390, No. 61501373, No. 61771392, and No. 61271279), the National Science and Technology Major Project (Grant No. 2016ZX03001018-004, and No. 2015ZX03002006-004), the Fundamental Research Funds for the Central Universities (Grant No. 3102017ZY018), and the Science and Technology on Communication Networks Laboratory Open Projects (Grant No. KX172600027).

References

1. KDDCUP99, Kdd cup99 data set (1999). http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. Accessed 15 Jan 2018
2. NSL-KDD, NSL-KDD data set for network-based intrusion detection systems (2009). http://www.unb.ca/research/iscx/dataset/iscx-NSL-KDD-dataset.html. Accessed 15 Jan 2018
3. Kolias, C., Kambourakis, G., Stavrou, A., et al.: Intrusion detection in 802.11 networks: empirical evaluation of threats and a public dataset [J]. IEEE Commun. Surv. Tutor. **18**(1), 184–208 (2016)
4. Aminanto, M.E., Choi, R., Tanuwidjaja, H.C., et al.: Deep abstraction and weighted feature selection for Wi-Fi impersonation detection [J]. IEEE Trans. Inf. Forensics Secur. **PP**(99), 1–1 (2018)
5. Aminanto, M.E., Tanuwidjaja, H.C., Yoo, P.D., et al.: Wi-Fi intrusion detection using weighted-feature selection for neural networks classifier [C]. In: International Workshop on Big Data and Information Security, pp. 99–104 (2018)
6. Aminanto, M.E., Kim, K.: Detecting impersonation attack in WiFi networks using deep learning approach. In: Choi, D., Guilley, S. (eds.) WISA 2016. LNCS, vol. 10144, pp. 136–147. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-56549-1_12

7. Thing, V.L.L.: IEEE 802.11 network anomaly detection and attack classification: a deep learning approach [C]. In: Wireless Communications and Networking Conference, pp. 1–6. IEEE (2017)
8. He, K., Zhang, X., Ren, S., et al.: Delving deep into rectifiers: surpassing human-level performance on ImageNet classification [J]. pp. 1026–1034 (2015)
9. Larose, D.T.: Data Preprocessing, Discovering Knowledge in Data: An Introduction to Data Mining, pp. 27–40. Wiley (2014)
10. Srivastava, N., Hinton, G., Krizhevsky, A., et al.: Dropout: a simple way to prevent neural networks from overfitting [J]. J. Mach. Learn. Res. **15**(1), 1929–1958 (2014)