# A Novel Intrusion Detection Method for WSN

Sijia Wang [a], Qi Li and Yanhui Guo

Beijing University of Posts and Telecommunications, Beijing, 100876, China

[a]1024883269@qq.com

**Keywords:** WSN, Feature extraction, Intrusion detection, SVM.

**Abstract.** Wireless sensor network (WSN), which combines the technology of sensor, embedded system and wireless communications, has become increasingly popular and important in our lives. Security is an important issue for WSN. In this paper, we propose a novel method to detect the attacks in WSN. Our method composes of two important stages: offline training and online testing. In the offline training stage, we collect enough training samples, extract the features and then train the models. In the online testing stage, we extract the features of the captured network packets and compare them with the trained models. The hierarchical system could dramatically reduce the amount of online training without sacrificing the detecting accuracy. We deploy the proposed approach in a wireless sensor network for forest monitoring to evaluate its performance. The experiments show that our method performs better compared to the traditional methods.

## Introduction

Recently, WSN has received increased attention [1, 2]. The powerful capabilities of data acquisition and processing make WSN widely be applied to military, anti-explosion, environment, medical treatment, household, industry and other fields. However, with WSN going deep into our lives, the security issues become one of the important factors of limiting the development of WSN, so the intrusion detection for WSN is very important [3,4]. However, the known methods have some shortcoming. Various security and mechanisms have been proposed and discussed by researchers to ensure the security in WSN. In Ref. [5], the authors design a novel message observation mechanism (MoM) to detect and defense the Dos attack. In Ref. [6], the authors focused on security of WSN with the conclusion that the security of significant systems should be continually reassessed to take new detections into account. The level of security needed from the application should also be marked when preferring hardware. However, each of the solutions has its own drawback. Most of the research majorly worked on the innovation and optimization of the detection module. Therefore, we introduce a new kind of feature selection method. Then, we propose a kind of intrusion detection technology for WSN based on SVM algorithm. The main contribution of this paper is that we take into full account the characteristics of WSN. And the characteristics can also be used in other modules.

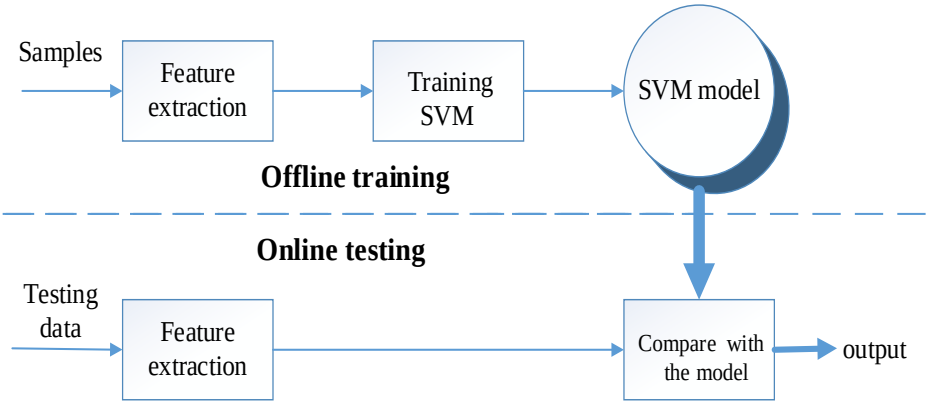


Fig.1 The framework composes of two stages: offline training and online testing.

**Framework Overview**

As is shown in Fig.1, the proposed intrusion system is composed of two important stages: offline training and online testing. In the offline training stage, we collect enough training samples, extract the features and then train the SVM model for both normal and abnormal conditions. In the online testing stage, we extract the features for the captured network packets and compare with the trained models. Then the system make a decision whether the situation is abnormal or not.

**Feature Extraction**

Feature extraction is one of the most important issues in abnormity detection. A lot of previous researches have paid attention to extract behavioral characteristic of the network. However, only few work focused on WSN. In this paper, we introduce some features for WSN.

(1) Num_frame

We define num_frame as the total number of received data frames in a second.

$NF_i = \sum_{j=0}^{i} frame_j - \sum_{j=0}^{i-1} frame_j$

In the expression, $\sum_{j=0}^{i} frame_j$ denotes the total number of frames in the time interval (0, *i*). Therefore, $NF_i$ represents the total number of frames during the *i* second. The Dos attack for WSN often lead to the increased frame density.

(2) Total_load

We define total_load as the traffic throughput of WSN in a second.

$TL_i = \sum_{j=0}^{i} packet\_size_j - \sum_{j=0}^{i-1} packet\_size_j$

In the expression, $\sum_{j=0}^{i} packet\_size_j$ represents the sum of the lengths of all the packets in the time interval (0, *i*).

(3)Num_AP_sent

We define num_AP_sent as the number of frames sent by AP in one second.

$NS_i = \sum_{j=0}^{i} frame\_AP\_sent_j - \sum_{j=0}^{i-1} frame\_AP\_sent_j$

In the expression, $\sum_{j=0}^{i} frame\_AP\_sent_j$ represents the number of frames sent by AP in the time interval (0, *i*).

(4) Num_AP_recv

We define num_AP_recv as the number of frames received by AP in one second.

$NR_i = \sum_{j=0}^{i} frame\_AP\_recv_j - \sum_{j=0}^{i-1} frame\_AP\_recv_j$

In the expression, $\sum_{j=0}^{i} frame\_AP\_recv_j$ represents the number of frames received by AP in the time interval (0, *i*).

(5) Rate_packet_loss

We define rate_packet_loss as the ratio of the number of lost packets and frame rate.

$RL_i = \frac{\sum Loss_{packets}}{NF_i}$

In the expression, $\sum Loss\_packets$ represents the number of lost packets in the i second. We detect the lost packets by using sequence control fields of the frame header.

(6) Subtract_sent_recv

We define subtract_sent_recv as the difference between the number of frames received by STA and the number of frames sent by STA in a second.

$$SU_i = \left(\sum_{j=0}^{i} frame_{STA_{recv\,j}} - \sum_{j=0}^{i-1} frame_{\mathrm{STA}_{recv\,j}}\right) - \left(\sum_{j=0}^{i} frame\_STA\_sent_j - \sum_{j=0}^{i-1} frame\_\mathrm{STA}\_sent_j\right)$$

In the expression, $\sum_{j=0}^{i} frame\_STA\_recv_j$ is the number of frames received by STA, and $\sum_{j=0}^{i} frame\_STA\_sent_j$ represents the number of frames sent by STA. In normal conditions, the two values are equal basically. When the Dos attacks occur, along with illegal STA packets or AP packets, the two values vary greatly.

(7) Frame_duration

We define frame_duration as the average of the three maximum frame duration in a second.

$$FD_i = \frac{\sum \max\_10(duration)}{10}$$

In the expression, $\sum \max\_10(duration)$ represents the sum of the ten maximum frame duration during the *i* second. When duration attack occurs, the value of frame duration is unusually high.

(8) Rate associate

We define rate associate as the ratio of the number of response frames which are correlated successfully to the number of request frames.

$$RA_i = \frac{\sum asso\_res\_success}{\sum asso\_req}$$

In the expression, $\sum asso\_res\_success$ represents the number of response frames which are correlated successfully during the *i* second, and $\sum asso\_req$ represents the number of request frames during the *i* second.

(9)Rate_identify

We define rate_identify as the ratio of the number of response frames which are authenticated successfully to the number of request frames.

$$RI_i = \frac{\sum idtf\_res\_success}{\sum idtf\_req}$$

In the expression, $\sum idtf\_res\_success$ represents the number of response frames which are authenticated successfully during the *i* second, and $\sum idtf\_req$ represents the number of request frames during the *i* second. When a Dos attack occurs, especially with the flooding attack and the certification flooding attack, the rate_identify falls sharply. So we define rate_identify as a basic characteristic of attack detection.

## Abnormal detection based on SVM

In the passage, intrusion detection for WSN detects attacks by SVM. The intrusion detection model is shown in Fig.2.

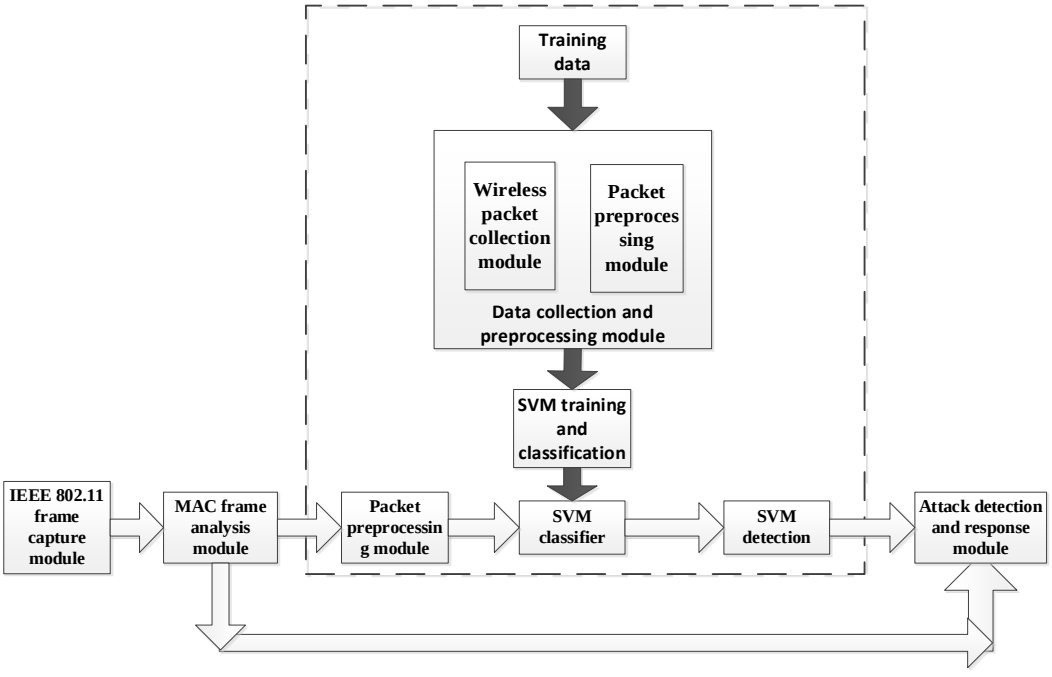


Fig.2 Intrusion detection model for WSN

Based on the above model, the paper realizes an intrusion detection system, including the following functional modules:

SVM training related module:

The functions of the module are to train SVM module by using training data and get the SVM classifier.

IEEE 802.11 frame capture module:

The module sets the wireless network card to be listening mode, calls the C library by using wireless packet capture technology and sniff and capture the wireless packet messages in limited regions.

MAC frame analysis module:

The first step is to strip the MAC frame from the captured message information and remove the loading parts. Secondly, classify these MAC frames according to the type field, subtype field and other frame header parameters by the primary analysis of MAC frame. Finally, analyze the number of different kinds of supervisory frames.

Packet preprocessing module:

The function of this module is to extract and count the values of the parameters of different detected features for SVM classifier to detect the attacks.

SVM attack detection module:

The module is used to detect attacks by analyzing attack characteristics for WSN. And this module is the core module of attack detection system for WSN.

Intrusion detection and response module:

After obtaining the results, the response mechanism starts, handle it with appropriate action and output the detection results.

## Experiments

In this session, we did some experiments to evaluate the performance of the proposed method. In the experiments, we put the attack host in the region of WSN, and then the attack host send a lot of attack data packets in the WSN space. And we write the results of our system and Snort-Wireless to log files. Then, we analyze and compare the attack detection results in log files.

Table 1. Comparison between our method and Snort-Wireless

| Attack | Detection rate of our system | False alarm rate of our system | Detection rate of Snort -Wireless | False alarm rate of Snort -Wireless |
|---|---|---|---|---|
| Authentication Flood Attack | 95.0% | 3.6% | 90.0% | 4.6% |
| Deauthentication Flood Attack | 92.1% | 5.2% | 91.5% | 4.5% |
| Association Request Flood Attack | 90.9% | 2.7% | 87.6% | 3.3% |
| Disassociation Flood Attack | 90.2% | 4.8% | 88.7% | 4.4% |
| Beacon Flood Attack | 95.6% | 2.9% | 90.1% | 4.1% |
| Probe Request Flood Attack | 92.3% | 1.2% | 91.9% | 2.5% |
| Duration Attack | 98.1% | <1% | 97.8% | 1.5% |

As is shown in Table 1, our method performs better than Snort-Wireless. That is because most of the features extracted in Snort-Wireless are the same as that in wireless local-area network. Numerous nodes in WSN are not taken into consideration in Snort-Wireless. Thus, we introduce some new features of WSN to improve the detecting accuracy.

## Conclusions

Because of the defect of security technologies adopted by WSN, WSN is facing great challenges. The main studies and contributions in this paper are as followings:

We introduce a feature set to detect attacks for WSN based on the research on the attacking characteristics.

We propose a kind of intrusion detection technology for WSN based on SVM algorithm. And the experiment tells us that our method has higher detecting accuracy.

**Acknowledgement**

This work is supported by the National Natural Science Foundation of China Project (61302087, 61401038).

**References**

[1] Kali Linux, http://www.kali.org [J]. Retrieved from the web, 2014.

[2] M. Erol-Kantarci and H. T. Mouftah , "Wireless sensor networks for cost-efficient residential energy management in the smart grid",IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 314-325, 2011

[3] "ZigBee alliance examining Japan\'s new smart home recommendations [online] Available: http: // www. smartmeters.com/the-news/3449-zigbee-alliance

[4] F. Benzi , N. Anglani , E. Bassi and L. Frosini,"Electricity smart meters interfacing the households",IEEE Trans. Ind. Electron., vol. 58, no. 10, pp. 4487-4494, 2011

[5] Yi-ying Zhang, Xiang-zhen Li, Yuan-an Liu, “The detection and defence of Dos attack for wireless sensor network” , Elsevier Journal of China Universities of Posts and Telecommunications, Volume 19, Supplement 2, October 2012, Pages 52-56.

[6] Shashikala, C. Kavitha, “A Survey on Secured Routing Protocols for Wireless Sensor Network”, IEEE ICCCNT'12, Coimbatore, India, 26-28th July 2012.