Research on Attack and Defense Game Model for Improving the Efficiency of Network Intrusion Detection System

Guohui Zhou
Guangxi Vocational & Technical Institute of Industry, Guangxi 530001, China
*Corresponding author: zhgh1001@126.com

Abstract. The widespread use of wireless networks has expanded people’s ability to obtain information, but its inherent network characteristics make it more vulnerable to cyber-attacks. Existing intrusion detection systems usually only target specific attack methods, but are incapable of other attacks. Based on this research background, taking game theory as the theoretical basis, it analyses the offensive and defensive process in wireless sensor networks, and demonstrates the necessity of implementing an intrusion detection system by analysing model equilibrium solutions. In view of the diversity of attack methods of network intruders, the game model is further improved, and a non-cooperative complete information static game model is established. By analysing the mixed Nash equilibrium solution of the model, the best defines strategy of the intrusion detection system is obtained and the system is balanced. Energy consumption and detection efficiency. Simulation experiment results show that the wireless sensor network intrusion detection system based on offensive and defensive game can not only effectively resist multiple network attacks, but also reduce the energy consumption caused by the intrusion detection system and prolong the service life of the network.

1. Introduction
Wireless sensor networks (WSNs) are one of the hot research fields in recent years. Some characteristics of wireless sensor networks, such as limited energy, low-power computing, and wireless communication, make them face many security threats. When the attacker is inside the network, the firewall as the first line of defines is ineffective. Intrusion detection system (IDS) is the second line of defines for network security, which can detect and prevent attacks from inside and outside. The intrusion detection system designed for wired networks and ad hoc networks cannot be directly used in wireless sensor networks, so it is necessary to design a specific intrusion detection system for wireless sensor networks, and to fully consider the characteristics of wireless sensor networks [1].

Game theory is a mathematical theory that studies the phenomenon of confrontation, which considers gaming, the individual’s predicted behaviour and actual behaviour during the game. The individuals participating in the game all have different goals or interests. In order to maximize their respective interests, each party must consider the various possible action plans of the opponent and choose the most beneficial or reasonable plan for themselves. Combined with the problems in this article, several basic concepts of game theory are defined. Game theory refers to a decision-making subject in a game, by reasonably choosing its own actions, in order to obtain maximum benefits (or utility). It is usually expressed by I=1, 2, ..., n.
2. Intrusion detection system based on game theory

There are N game attackers and defenders interconnected, and the activation state \( x_i \) (I=1, 2, 3, ..., N) of each game attacker takes 0 or 1, respectively representing inhibition and excitement. The state of each game attacker is governed by other game defenders according to the following rules

\[
x_i = f\left(\sum_{j=1}^{N} w_{ij} x_j - \theta_i \right), i = 1,2,\cdots,N
\]  

(1)

Where \( w_{ij} \) represents the strength of the synaptic connection between the game attacker I and the game defender j, or weight; \( \theta_i \) represents the threshold of the game attacker I; \( f(\cdot) \) here takes the step function \( \text{step}(\cdot) \).

Equation (1) can also be understood as the input-output relationship of game attacker I. \( x_j \) is the input of the jth game defender to the ith game attacker; \( x_i \) is the output of the ith game defender; \( \sum_{j=1}^{N} w_{ij} x_j - \theta_i \) is the net input of the ith game attacker. If the threshold is also regarded as a weight, then equation (1) can be rewritten as

\[
x_i = f\left(\sum_{j=0}^{N} w_{ij} x_j \right), i = 1,2,\cdots,N
\]  

(2)

At this time there is \( w_{ii} x_i = -\theta_i, x w_0 = 1 \), which is the original MP model. However, this simple MP model does not consider the effects of time integration, refractory period, and delay and digital-to-analog conversion. If these effects are considered, many variants of the MP model can be developed. They are different in details (that is, parallel distributed processing ideas), but they have many commonalities. Extracting these commonalities can give a fairly general model. Its mathematical expression is

\[
\sigma_i = f\left(\sum_{j=1}^{N} w_{ij} x_j + s_i - \theta_i \right)
\]  

(3)

\[
u_i = f(\sigma_i)
\]  

(4)

\[
y_i = g(\nu_i) = h(\sigma_i)
\]  

(5)

Where \( W_{ij}, x_j, \theta_i \) and have the same meaning as equation (1); \( \sigma_i \) represents the net input of the i-th game attacker, \( s_i \) represents the external input of the i-th game defender, \( u_i \) represents the activation state of the i-th game attacker, \( y_i \) represents the output of the i-th game defender, \( f(\cdot) \) represents the activation rule (activation function) of the game attacker, and \( g(\cdot) \) represents the output rule (conversion function) of the game defender.
3. Network intrusion detection system design

3.1. Three-tier distributed architecture
This system uses a three-tier distributed architecture: network intrusion detector, intrusion event database and Web-based analysis console. In order to avoid unnecessary network traffic, the network intrusion detector and intrusion event database are integrated into a host, and the web server on the host is accessed remotely with a standard browser as an analysis console. The communication between the two is encrypted with HTTPS. Protocol transmission. The location of IDS in the switching network is generally selected as follows: 1. as close to the attack source as possible; 2. as close to the protected source as possible. These locations are usually on the switch in the server area, the first switch after the Internet access router, or the LAN switch on the key protection network segment [2].

3.2. System composition and implementation
The system is deployed in the DMZ (demilitarized zone) zone where the network server is located and is used to monitor network traffic on the Internet and intranet. Using two network cards, the network intrusion detector uses a network card without an IP address to monitor to ensure the security of the network intrusion detection system itself, and accesses the internal network through another network card and assigns the private IP address used by the internal network to it from Intranet access analysis console. By enabling user authentication and access control of the APACHE server and combining with SSL, the access security of the system is guaranteed. The experimental platform used by the system is Red hat Linux 9.0 and various software such as Apache, MM, Mod_ssl, ACID, Phplot, MySQL and so on. The system implementation is shown in Figure 1.

Figure 1. System implementation diagram

3.3. System module design and analysis

3.3.1. Network data engine module. In this system, in order for the network data engine module to accept all the data in the network, the network card is generally set to promiscuous mode, and in promiscuous mode the computer can accept all the information flowing through the network segment. This part of the development used the mature Berkeley Packet Filter (BPF) mechanism and network security tool development library in Linux, namely the packet capture function library Libgamep.
When a data packet reaches the network interface device, the link layer device driver usually transfers it to the system protocol stack for processing. However, when BPF is also listening on the network interface, the driver will first call BPF, BPF will pass the packet to the filter of each monitoring process, these user-defined filters will determine whether a packet is accepted and what should be saved in the data package. For each filter that decides to accept the packet, BPF copies the required data to the buffer connected to it, and then the device driver regains control. At this time, if the target address of the data packet is not the local address, the driver returns from the interrupt process, otherwise, the normal network protocol processing will be performed [3].

3.3.2. Analysis module. The analysis module includes a preprocessing module, a rule matching processing module, and a rule knowledge base. This module is the core part of the intrusion detection system and plays a vital role in the efficient operation of the entire system.

3.4. Intrusion and log database
A good intrusion detection system should not only provide administrators with real-time and abundant alarm information, but also record field data in detail in order to reconstruct certain network events in the future when forensics is needed. The front-end program for database management is usually integrated with the console module. The data source of the database is mainly the data processed by the analysis module, including alarm information and other important information, and the data obtained by the administrator after the conditional query to process the query results, such as the generated local files and format reports [4].

3.5. Intrusion detection data set preprocessing
The training data used in the experiment was taken from the KDDCUP09 data set. In order to facilitate operation, distinguish normal events from attack events, and extract the characteristics of attack events. In the experiment, we first pre-processed the data set. The preprocessing process includes: coding, feature classification, and feature value normalization. The specific methods and steps are shown in Table 1 and Table 2:
Table 1. Protocol type field coding:

| Protocol Type | Field Code |
|---------------|------------|
| TCP           | 1          |
| UDP           | 2          |
| ICMP          | 3          |

Table 2. Attack type coding

| Attack Type       | Field Code |
|-------------------|------------|
| Normal            | 0          |
| Back              | 1          |
| Buffer_overflow   | 2          |
| ftp_write         | 3          |
| Guess_passwd      | 4          |
| Imap              | 5          |
| Ips               | 6          |
| weep              | 7          |
| Land              | 8          |
| Load module       | 9          |
| Multihop          | 10         |
| Neptune           | 11         |
| Nmap              | 12         |
| Perl              | 13         |
| Phf               | 14         |
| Pod               | 15         |
| Ports weep        | 16         |
| Rootkit           | 17         |
| Satan             | 18         |
| Smurf             | 19         |
| Spy               | 20         |
| Ware client       | 21         |
| Ware master       | 22         |
| Dos               | 23         |

In the experiment, in order to facilitate processing and analysis, we normalized the continuous feature values in the data set. Through the normalization algorithm, each continuous feature value in the data set is limited to [0.0, 1.0]. The normalization algorithm is as follows:

$$x = \frac{x - \text{MIN}}{\text{MAX} - \text{MIN}} \quad (6)$$

Among them: x is a continuous numeric variable; MIN and MAX are the minimum and maximum values of the eigenvalues belonging to the x variable, respectively.

3.6. Data center processing method

The main types of attacks in WSN are shown in Table 1. Through the analysis of the main attacks in WSN, the network anomalies caused by these attacks can be summarized: resource consumption and flood attacks will cause network traffic anomalies, resulting in node energy exhaustion; Black hole attacks and counterfeit response attacks will cause packet loss and cause the network to lose its proper role; worm hole attacks, routing information spoofing, tampering or replay attacks, and witch attacks all use network vulnerabilities, resulting in chaotic network routing. Therefore, You can select the network traffic characteristics such as the node's packet sending rate, packet receiving rate and packet loss rate, the routing information such as the start address, destination address and transmission energy of the data packet, and the content characteristics such as the type and length of the data packet as the intrusion characteristics [5].

For anomaly detection algorithms, the detection system needs to store all normal training samples. Feature dimensionality reduction can reduce the amount of data storage and calculation, save energy consumption, and extend network life; for misuse detection algorithms, feature dimensionality reduction can remove redundant features to improve the training speed and classification performance of the classifier.
| Attack type                  | Attack description                                                                 | Attack results                                      |
|-----------------------------|----------------------------------------------------------------------------------|----------------------------------------------------|
| Resource consumption attack | The attacker sends a lot of useless messages the attacker sends a lot of attack messages through flooding | Consume network and node resources                  |
| Flood attack                | The attacker makes other nodes believe that it is the best forwarding option according to the routing algorithm, attracting other nodes to send packets to it | The performance of the entire network is degraded, and normal communication cannot form a network black hole |
| Black hole attack           | The attacker sends the received packet to the other end of the tunnel through the tunnel with little delay, and the other attacker performs a replay attack | Destroys the routing competition condition, so that two distant nodes are considered to be adjacent |
| Wormhole attack             | The attacker induces the sender to send unreliable links or dead links by sending them on these links. | Packet loss                                         |
| Counterfeit response attack | Change the routing information between two nodes                                  | Disordered routing, increased network delay, and uneven network traffic |
| Routing information spoofing, tampering, or playback attacks | An attacking node impersonates the identities of multiple legitimate nodes       | Routing confusion                                   |

4. **Algorithm performance test**

We study the changes in detection rate and false alarm rate when the number of IDS in the network increases. Finally, we compare the performance of our model with other hybrid models. In order to evaluate the effectiveness of the proposed model, a set of metrics were used to make the judgment. Detection rate: indicates the ratio of detected attacks to the total number of attacks. False alarm rate: the rate of misinterpretation of normal connections as abnormal behaviour. The model combining SVM-based anomaly detection and attack signature-based detection can achieve a higher detection rate (about 98%) and a lower false alarm rate (about 3%). Table 4 shows that the model the detection and false positives of attacks.

| Attack form                  | The detection rate | False alarm rate |
|------------------------------|--------------------|------------------|
| Hello flood attack           | 97.21%             | 2.25%            |
| Black hole attack            | 96.82%             | 3.50%            |
| Wormhole attack              | 98.20%             | 4.53%            |
| Selective forwarding attack   | 98.39%             | 5.12%            |

4.1. **Feature processing**

In this paper, based on the MATLAB simulation platform, the game method is used to reduce the dimensionality of the training samples for anomaly detection and misuse detection. The curve of the cumulative contribution rate with the number of games is shown in Figure 3. The test samples are the same as the training samples. The game transformation matrix performs dimension reduction. The selected threshold is 94%. When the cumulative contribution rate is greater than this threshold, stop increasing the game.
Figure 3. The relationship between the number of games and the cumulative contribution rate

As can be seen from Figure 3, when the cumulative contribution rate reaches 94%, anomaly detection extracts 8 dimensions from 41-dimensional features as a game, and misuse detection extracts 6 dimensions as a game, indicating that the game method can effectively achieve feature dimensionality reduction, effectively reducing the amount of calculation [6].

4.2. Cluster intrusion detection

Wireless sensor networks are large-scale networks. The construction of network applications for sensor networks is still in the initial stage, and large-scale physical testing is difficult to implement. Simulation within a certain range has become an important means of verifying some theoretical and technical methods. The intrusion detection system strategy proposed in this paper is built on the intrusion detection module, focusing on the experiment and configuration of the node's intrusion detection layout, and the simplified processing of the underlying data functions and collection processing. In Figure 4, the "+" point is the time point data of the cyber attacker's attack, and the "-" curve is the fitted curve.
Figure 4. Curve fitting diagram of time point

It can be seen from the Degree value in Figure 4 that a quadratic curve is used to fit it. There is a confidence curve on both the left and right sides of the fitting curve. The parameter we pass in the function is 0.005, so this curve is a 95% confidence curve, indicating that 95% of the data falls between these two lines. In this figure, the size of the interval is 4.933, which means that the time interval formed by adding and subtracting 4.9331 from the predicted value will include the real attack time point with a 95% confidence rate [7].

5. Conclusions
In view of the characteristics of low computing power and limited energy in wireless sensor networks, this paper proposes an intrusion detection model based on game theory. Experiments show that the model has a higher average detection rate and a lower average false detection rate, and has the characteristics of low energy consumption, which has certain reference value for solving the problem of intrusion detection in wireless sensor networks.

References
[1] Lin, W. C. Ke, S. W., & Tsai, C. F. Cann: an intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge Based Systems, 7 (8) (2015) 13 - 21.
[2] Min-Joo, K. Je-Won, K., & Tieqiao, T. Intrusion detection system using deep neural network for in-vehicle network security. Plos One, 11 (6) (2016) 16 - 24.
[3] Aburomman, A. A. & Reaz, M. B. I. (2015). A novel svm-knn-pso ensemble method for intrusion detection system. Applied Soft Computing, 38 (5) (2015) 360 - 372.
[4] Faisal, M. A. Aung, Z., Williams, J. R., & Sanchez, A. Data-stream-based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study. Systems Journal IEEE, 9 (1) (2015) 31 - 44.
[5] Hodo, E. Bellekens, X., Hamilton, A., Dubouilh, P. L., Jorkyase, E., & Tachtatzis, C., et al. Threat analysis of iot networks using artificial neural network intrusion detection system. tetrahedron letters, 42(39) (2017) 6865 - 6867.
[6] Bul' Ajoul, W. James, A., & Pannu, M. Improving network intrusion detection system
performance through quality of service configuration and parallel technology. Journal of Computer & System Sciences, 81 (6) (2015) 981 - 999.

[7] Fabi A. K. Alert aggregation based pattern classifier for effective network intrusion detection system. Pediatric Allergy & Immunology, 21 (2) (2015) 368 - 376.