ISSN: 1738-9976
Vol. 10, No. 11, November 2016

IJSIA

International Journal of Security and Its Applications

International Journal of
Security and Its Applications
IJSIA

SERSC
Science & Engineering Research Support soCiety

IJSIA International Journal of Security and Its Applications Vol.10 No.11 SERSC

International Journal of Security and Its Applications
Vol. 10, No. 11 (2016), pp.131-142
http://dx.doi.org/10.14257/ijsia.2016.10.11.12

A Novel Intrusion Detection Approach Based on Chaos Theory in Wireless Sensor Networks

Xinling Kong[1*], Yonghong Chen[2], HuiTian[3], Tian Wang[4], Yiqiao Cai[5]

[12345] *School of Computer Science and Technology, Huaqiao University, Xiamen 361021, China*
E-mail: [1]kxling712@163.com, [2]djandcyh@163.com

Abstract

With the development of technology, wireless sensor networks (WSNs) has been widely used in military, political, medical and other fields, their characteristics of data-centric become increasingly prominent. In this paper, a data-oriented intruding detection method based on chaos theoy is proposed. We use the theory of chaotic system to analyze the internal rules of the sensory data and predict the data by RBF neural network firstly, then make an initial detection of false injected data attack according to whether the difference between the predicted and actual value is more than the threshold, finally confirming the attack by checking whether the number of abnormal within the cycle lies in the corresponding range. Experimental results show that RBF neural network predict sensory data more accurate, our approach can effectively distinguish the abnormal events caused by the attack or environmental factors and has high intrusion detection accuracy.

Keyword*: wireless sensor networks; intrusion detection; false injected data attack; RBF neural network; chaotic time series.*

1. Introduction

Wireless Sensor Networks (WSNs) is a kind of network that has plenty of tiny devices sensing and collecting detailed information about the physical environment. Owing to their easy and cheap deployment features, they are used for many different fields of science, health, military, sensing and gather data respecting various activities. To ensure the safety of the wireless sensor networks become more and more important[1].

Intrusion is a behavior which attempts to access, process information, or to damage the system in the case of unauthorized thus making the system not reliable and available. Intrusion detection provides a deterrence for intruder, recognize patterns of known attacks, identify abnormal activities by observing and investigating system and user activities[1].

Most of the existing wireless sensor network intrusion detection systems (IDS) using statistical analysis, such as hidden Markov model, data mining and game theory. These schemes improve the detection accuracy in some extent, but they have poor real-time performance. Other method like using Arma(2,1) model[2]and extended Kalman filter(EKF)[3] to predict future states, determining abnormal by comparing the difference between predicted and actual values. Although both of them make full use of the wireless sensor network's characteristics of sensory data, they are not good at finding the internal rule of data, can't predict the data accurately, contributing to false positive rate and false negative rate.

To overcome the shortcomings of above approach and improve the effectiveness of intrusion detection, we propose an intrusion detection method based on chaos theory to

[1] Xinling Kong is the corresponding author

ISSN: 1738-9976 IJSIA

detect the false injected data attack as Fig. 1 shows. Definitely there must be a deviation between the normal and abnormal data. First we analysis the relationship between different time data based on the theory of chaotic time series, then using RBF neural network to predict their future states after the phase space reconstruction and set threshold value by the predicted data, if the monitored value lies outside of the predicted normal range there may be an abnormal behavior, what's more, the number of abnormal occurrence in each cycle will be saved, we compute the corresponding range of the abnormal occurrence next cycle by the saved record, finally, malicious activities are determined if the number of abnormal behaviors within the cycle out of the range.

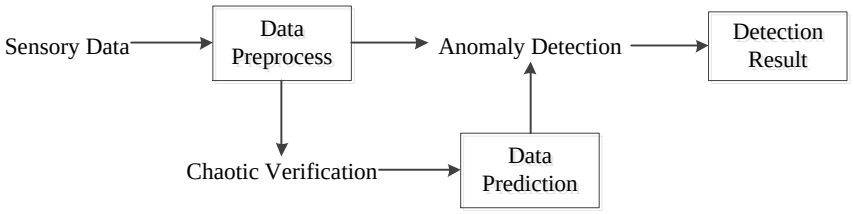


Figure 1. Detection Model

The remainder of the paper is organized as follows: in Section 2 existing anomaly detection algorithms for cluster based WSNs are outlined. A detailed description of our detection scheme is provided in Section 3. Section 4 introduced the obtained simulation results in details, conclusions are given in Section 5, followed by acknowledges.

2. Related Work

There are many intrusion detection method based on anomaly detection in hierarchical, cluster-based WSNs. Bo Sun et[3] all presented a method to detect false injected data. Specifically, by monitoring behaviors of its neighbors and using EKF to predict their future states, each node aims at setting up a normal range of the neighbors' future transmitted aggregated values, and further apply an algorithm of combining cumulative summation and generalized likelihood ratio to increase detection sensitivity, but the EKF has the drawback of filter divergence, it will lead to an inaccurate prediction. In [4] a traffic prediction-based intrusion detection technology is proposed. In[5] presents an intrusion detection based on statistics anomaly in WSNs, by establish models for some system characteristics in normal state of the sensor nodes, and detects the intrusion through the deviation degree of observed values to normal model.

Compared with other intrusion detection method, our scheme have three innovation point, First, based on the anomaly detection technology, make full use of WSN's feature based on sensory data, and detection carried out by Base station(BS) reduced the energy consumption of network nodes, Second, apply the chaos theory , the inner change rule of nonlinear system's movement is well described, built the RBF neural network data forecasting model, avoid subjective prediction, improve accuracy and effectiveness of the prediction. Third, preliminary detect anomaly by comparing whether the actual data exceeds the forecasting range, and achieve effective detection by comparing the number of abnormal occurrence within the cycle is beyond the range which calculated similar to confidence interval. This method can eliminate the false positive which result from abnormal environment, improved the detection's accuracy and credibility greatly. A lot of simulation experiments have done to evaluate the detection algorithm.

3. System Model

3.1 WSNs Model

From the point of view of data collection, wireless sensor network can be divided into two categories: the query type and the source driven. In a source-driven WSN, SNs (sensor nodes) sense the environment at a fixed rate and periodically transmit sensing data to the BS. In a query-based WSN, a query is issued by the BS proactively or reactively, SNs in the feature areas collect data and forward data to the BS in response to the query. This paper focuses on source-driven WSNs [6]. Our network and data aggregation model as Fig. 2 shows.

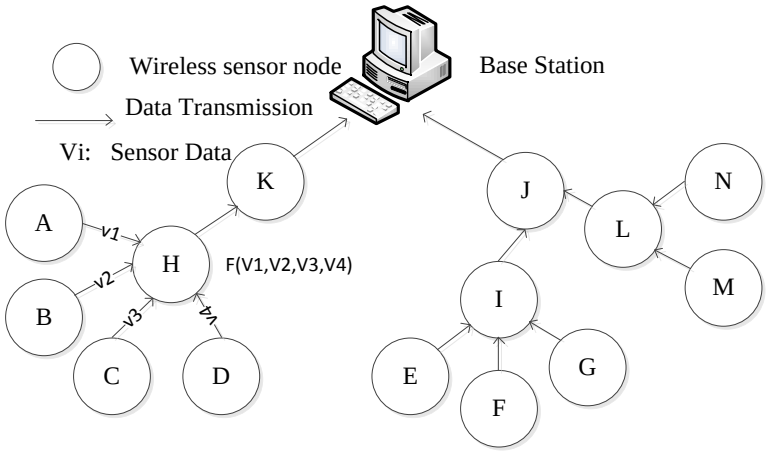


Figure 2. Wireless Sensor Network Model

Motion, location, direction, size, temperature, humidity, radiation, can be monitored by a source-driven WSNs. These variables have a correlation in time, so we can use this feature to predict the next moment data and judge the abnormal according to weather the difference between the actual and the predicted data is greater than the threshold. Natural phenomenon is a result of many factors, the WSN plays an important role in monitoring natural environmental, their sensing data is more likely to be nonlinear. Therefore, it is available to study the objective rules of data according to chaos theory.

Our detection scheme consists of the following parts.

3.2 Data Preprocessing

In this paper, we first compute the data value which the cluster head receive with different aggregation functions, and describe the average aggregation in detail. As Fig. 2 shows each N_i represents one sensor node and transmits value v_i to its parent node.

We set the expectation of each v_i is $E(v_i) = u_i$ and the variance of each v_i is $\mathrm{var}(v_i) = o_i^2$. Suppose that with a probability 0 < p < 1, a packet on each link is lost. Let a random variable X denote the aggregated value of node N , We analyze the probability function[3] of X : P_X

$$P_X\begin{cases}(1-P)^2, if X=\dfrac{\sum_{i=1}^{n} v_i}{n}\\ (1-P)^{n-1}, if X=\dfrac{\sum_{i=1\wedge i\neq 1}^{n} v_i}{n-1}\\ (1-P)^{n-1}, if X=\dfrac{\sum_{i=1\wedge i\neq 1}^{n} v_i}{n-1}\\ \cdots,\cdots\end{cases} \tag{1}$$

To save space, we omit the deduction process. Denote $E(v_i)=\mu$ and. $\text{var}(v_i)=\sigma^2$ Therefore, considering the impact of packet loss, collision, etc.,

$$E(X)=\sum_{m=0}^{n}(1-p)^{n-m}p^m\frac{n!}{m!(n-m)!}\mu \tag{2}$$

$E(X)$ denotes the aggregated value at cluster node N under the average aggregate function.

Assuming the size of the sliding time window is n, the cluster head (CH) receives the data sequence $x_1, x_2, x_3, \cdots x_{n-1}, x_n$ they are periodic, but there are certain non-stationarity, in our detection scheme, we should find the interval rule of the time series and forecasting the next time data. Chaos time series prediction method no need to establish the subjective model in advance, it directly according to the calculated objective laws of the data sequence to predict, can avoid subjectivity and randomness of prediction and improve the prediction precision and reliability effectively[7].

3.3 Judgement of Chaotic System and Making Prediction

For the processed time series data, verifying its chaotic property, if the maximum Lyapunov exponent of a dynamic system is positive, we consider it is chaotic. In our paper, we judge whether the preprocessed data is chaotic by the largest Lyapunov exponent according to the following steps:

3.3.1.Computing the time delay: We choose the C-C method[8] to compute the embedding delay for it is easier to implement, useful for smaller data sets, and less demanding computationally. To a time series $x_1, x_2, x_3, \cdots x_{n-1}, x_n$, we reconstruct a phase space $X=\{X_i\}$ with the time delay τ and the embedding dimension m. For X_i is a point in the phase space, the correlation integral of the embedding time series is:

$$C(m,N,r,t)=\frac{2}{M(M-1)}\sum_{1\le i\le j\le M}\theta(r-\left\|X_i-X_j\right\|)r>0 \tag{3}$$

With the correlation integral, we can calculate:

$$S(m,r_j,t)=\frac{1}{t}\sum[C_s(m,\frac{N}{t},r_j,t)-C_s^m(1,\frac{N}{t},r_j,t)] \tag{4}$$

$$\Delta\bar{S}(t)=\frac{1}{4}\sum_{m=2}^{5}(\max[S(m,r_j,t)]-\min[S(m,r_j,t)] \tag{5}$$

The first minimum of $\Delta\bar{S}(t)$ is the optimal time delay τ.

3.3.2.Computing the embedding dimension: We use the Cao method[9] to determine the embedding dimension m . The relative length of a point in phase space is defined as:

$$L(i,d)=\frac{\left\|y_i(d+1)-y_{n(i,d)}(d+1)\right\|}{\left\|y_i(d)-y_{n(i,d)}(d)\right\|} i=1,2,\cdots,N-d\tau \tag{6}$$

At the same time

$$E(d)=\frac{1}{N-d\tau}\sum_{i=1}^{n-d\tau}L(i,d) \tag{7}$$

$$E1(d)=\frac{E(d)}{E(d+1)} \tag{8}$$

When $E1(d)$ tends to be stable, the corresponding d is the best embedding dimension m.

3.3.3.Phase space reconstruction: With the optimal time delay τ and the most suitable embedding dimension m , we can reconstruct a phase space :

$$X_i=\{x_i,x_{i+\tau},x_{i+2\tau},\cdots x_{i+(m-1)\tau}\} \quad i=1,2,3\cdots(n-(m-1)\tau) \tag{9}$$

3.3.4.Chaos validation: Calculating the maximum Lyapunov exponent $\lambda_{\max}$ by the small date set method[10] the nearest neighbors of each space point Y_j with limited short-term separation is computed as.

$$d_j(0)=\min_{j'}\left\|Y_j-Y_{j'}\right\|,\left|j-j'\right|>P \tag{10}$$

Estimating the value of $\lambda_{\max}$

$$\lambda_1(i,k)=\frac{1}{k\Delta t}\frac{1}{(M-k)}\sum_{j=1}^{M-k}\ln\frac{d_j(i+k)}{d_j(i)} \tag{11}$$

Combing equation (10) and (11)

$$d_j(i)=C_j e^{\lambda_1(\Delta t)},C_j=d_j(0) \tag{12}$$

Log on both sides

$$\ln d_j(i)=\ln C_j+\lambda_1(i\Delta t)(j=1,2,\cdots M) \tag{13}$$

$\lambda_{\max}$ can be approximated as the slop of the curve by the least square method. If $\lambda_{\max}>0$, the time series $x_1,x_2,x_3,\cdots x_{n-1},x_n$ is chaotic.

3.3.5.Prediction: When a time series is chaotic, it implies that the laws underlying the time series can be expressed as a deterministic dynamical system. Prediction then relies on the discovery of the empirical regularities from the experimental observations of the system. Neural networks are effective in this application because of their universal approximation capabilities. Fig. 3 present the RBF neural network prediction model.

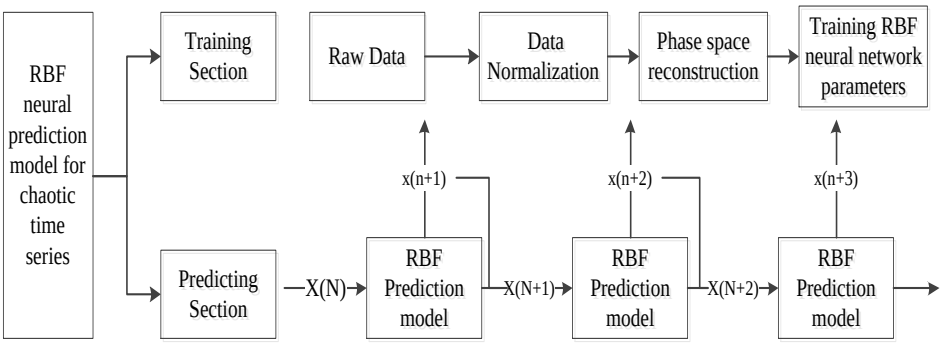


Figure 3. RBF neural network prediction model

3.4. Detection Algorithm

With the predicted and actual value, we can make detection for the false injected data attack.

Assuming the network transfer information is a steady periodic transmission, setting the cycle length is T and divide it into n time periods, extracting prediction samples $x_1, x_2, x_3, \cdots x_{n-1}, x_n$ respectively from each cycle, the average value and standard deviation of the receiving data in the base station of each cycle can be calculated:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{14}$$

$$S = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(\bar{x} - x_i)^2} \tag{15}$$

We set the $k * S$ as the threshold to determine whether the sensory data in the next cycle is normal or not, selecting the suitable k by experiment.

To record the number of abnormal occurrences per cycle, setting a counter (an initial value for 0 increasing function) in the BS, for each cycle the record will be saved and at the beginning of the cycle the counter cleared. Otherwise, we chose the embedding dimension m as the time window T_W, within T_W , we denote the number of abnormal for each cycle as : $y_1, y_2, y_3, \cdots y_m$, Then we compute μ and σ as follows:

$$\mu = \frac{\sum_{i=k-m}^{k-1} y_i}{m} \tag{16}$$

$$\sigma = \sqrt{\frac{1}{m-1}\sum_{i=k-m}^{k-1}(\mu - y_i)^2} \tag{17}$$

Setting the range of the next cycle anomalies as $[0, \mu + m * \sigma]$. Assuming that a cycle starts at t_0 time, the actual and predict value at time t are represented by x_t and x_t^+ , the number of abnormal occurrence denoted by y , thus the intrusion detection algorithm consists of the following steps:

Step 1: At the beginning of a cycles $y = 0$, for time t , BS compute x_t^+ based on RBF neural network;

Step 2: if ($t < t_0 + T$)

Step 3: if ($\left|x_t^+ - x_t\right| > k * S$) $y = y + 1$;

Step 4: else $y = y$;

Step 5: else if ($y > \mu + m * \sigma$) set an alarm, there is an attack within the cycle;

Step 6: else go to the next cycle

Step 7: end if

Step 8: end if

Step 9: end if

In this algorithm, we adopt dual judgment to detect anomalies and set threshold value by the embedding dimension m to improve the reliability of the test effectively.

4. Simulation Results

4.1 Experimental Environment

To evaluate the detection algorithm based on chaos theory, we make all x_i randomly distributed between one predefined range [min, max] to simulate WSN applications and select 5000 data items as the data set as in[3]. Simulation Platform is NS2 and MATLAB. For each link, we use different packet loss rates 0.1, 0.25, and 0.5 respectively.

We denote the following metrics to evaluate our scheme:

Detection rate r_d :

$$r_d = \frac{n'}{m'} \times 100\% \tag{18}$$

m' represent the number of measure abnormal data items and n' of them are detected.

4.2 Results and Analysis

Firstly, we judge whether the items has chaos characteristics or not. For the selected items, we compute the optimal embedding delay τ=2 (see Fig. 4) by the C-C method, then determine the minimum embedding dimension $m = 9$ (see Fig. 5) by the Cao method. We calculate the maximum Lyapunov exponent $\lambda_{\max}$ by the small data sets method, as shown in Fig. 6 the slope coefficient is the approximation of the $\lambda_{\max}$, we can estimate $\lambda_{\max} = 3.3028e-07 > 0$ which means the selected data has chaos characteristics.

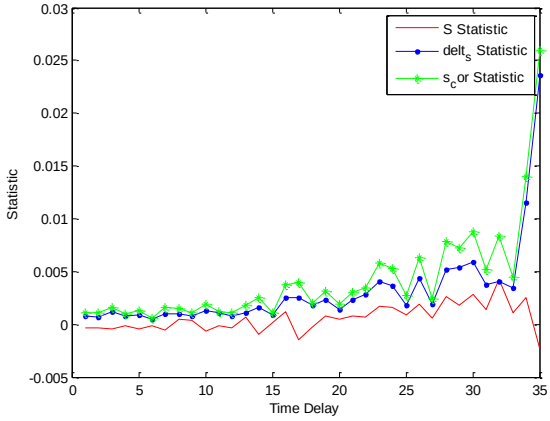


Figure 4. Phase Space Reconstruction of Random Data

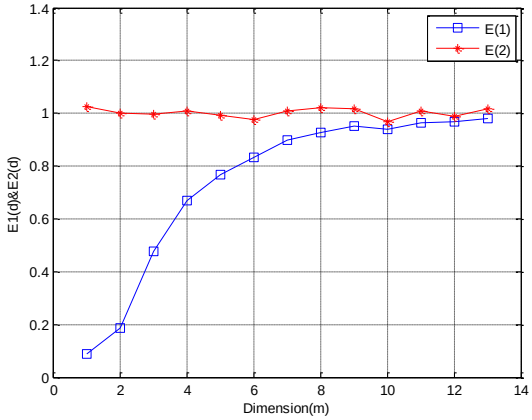


Fig. 5. The Optimal Minimum Embedding Dimension

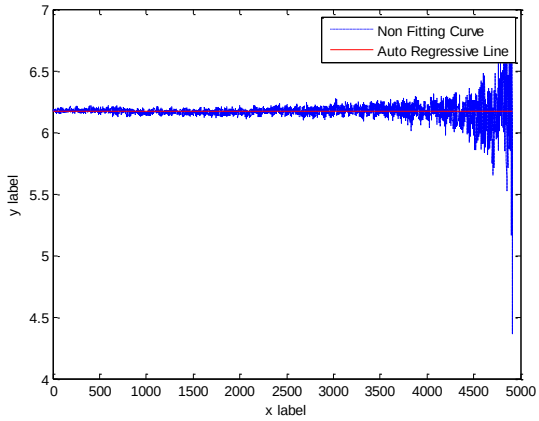


Figure 6. λ_{max} of Selected Items

Secondly, we predict the data directly by the EKF method, at the same time we reconstruct the phase space to the data then forecasting them by the RBF neural network.

As show in Fig. 7, the prediction error of our method is much lower than that of EKF method which imply using the RBF neural make prediction has a better prediction accuracy.

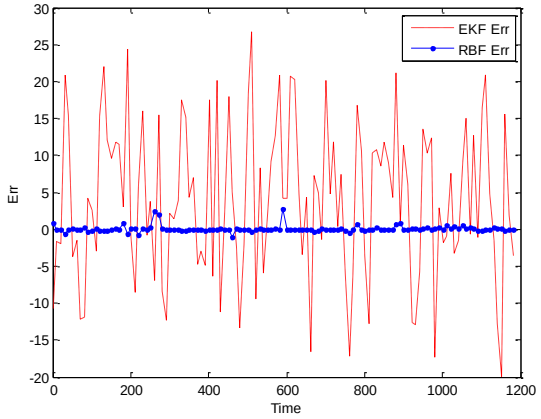
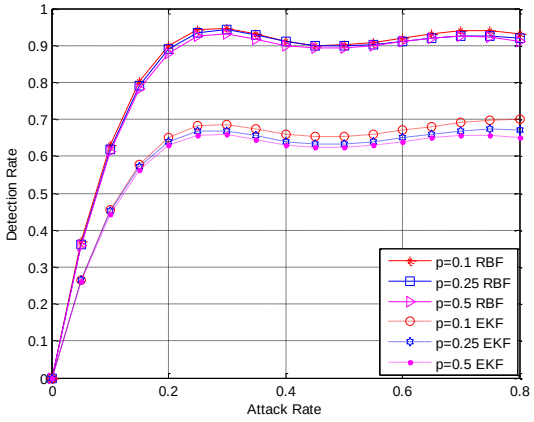
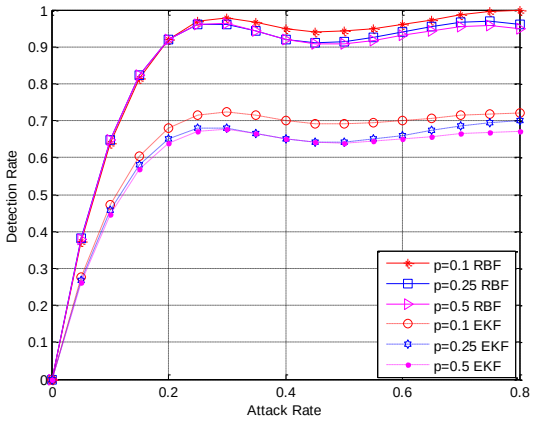


Figure 7. Prediction Error of RBF Neural Network and EKF

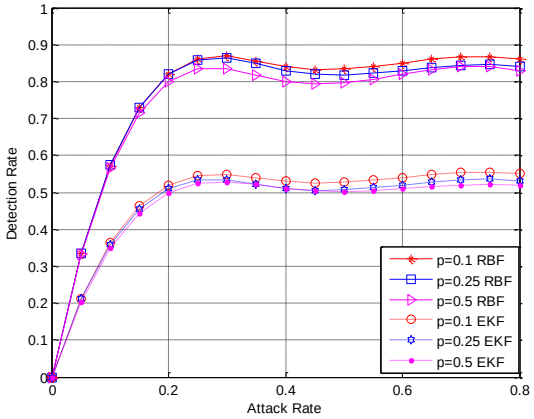
Finally we apply different threshold values by change the k and we random adding 20%,40%,60%,80% attack, get a set of detection rates.



(a) $k=1$



(b) $k=2$



(c) $k = 3$

Figure 8. Dectection Evaluation (a) k=1. (b)k=2. (c) k=3

In Fig. 8, it obvious that our method have a better performance. With the packet loss becomes larger, the detection rate decline, for the loss of more data packets will have a negative impact on the analysis of the internal law of the data. The experimental results also show when we set $k = 2$ our scheme has the best performance.

6. Conclude and Future Work

This paper proposed a novel and effective detection method of the data falsification attack in WSNs. Simulation results show that this method can improve the accuracy and reliability of the detection for false injected data attack, has a higher detection rate and less false positive rate. The deficiency is that the data processing process is complicated, and the detection module is running at the base station, reduce the system robust. In future work, we will find other more concise data processing method, reduce energy consumption of data processing and transplant detection module to the cluster head.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (NO.61370007, 61572206, U1405254), and the Program for New Century Excellent Talents in Fujian Province (2014FJ-NCET-ZR06) and by the Postgraduate Scientific Research Innovation Ability Training Plan Funding Projects of Huaqiao University (1511314005).

References

[1] O. Can and O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on, (2015), pp. 1-6.
[2] X. Cao, Z.-J. HAN, and G.-H. CHEN, "DoS Attack Detection Scheme for Sensor Networks Based on Traffic Prediction," CHINESE JOURNAL OF COMPUTERS-CHINESE EDITION-, vol. 30, (2007),pp. 1798.
[3] B. Sun, X. Shan, K. Wu, and Y. Xiao, "Anomaly detection based secure in-network aggregation for wireless sensor networks," IEEE Systems Journal, vol. 7, (2013), pp. 13-25.
[4] Q. Yu, L. Jibin, and L. Jiang, "An improved ARIMA-based traffic anomaly detection algorithm for wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 12, (2016), pp. 1-9.
[5] S. LIU, J.-j. ZHU, and Z.-y. MA, "Statistic Anomaly Intrusion Detection in Wireless Sensor Networks," Fire Control and Command Control, vol. 7, (2009),p. 037.
[6] H. Al-Hamadi and R. Chen, "Adaptive Network Defense Management for Countering Smart Attack and Selective Capture in Wireless Sensor Networks," IEEE Transactions on Network and Service

Management, vol. 12, (2015), pp. 451-466.
[7] H. Leung, T. Lo, and S. Wang, "Prediction of noisy chaotic time series using an optimal radial basis function neural network," IEEE Transactions on Neural Networks, vol. 12, (2001), pp. 1163-1172.
[8] H. S. Kim, R. Eykholt, and J. Salas, "Nonlinear dynamics, delay times, and embedding windows," Physica D: Nonlinear Phenomena, vol. 127, (1999), pp. 48-60.
[9] L. Cao, "Practical method for determining the minimum embedding dimension of a scalar time series," Physica D: Nonlinear Phenomena, vol. 110, (1997), pp. 43-50.
[10] M. T. Rosenstein, J. J. Collins, and C. J. De Luca, "A practical method for calculating largest Lyapunov exponents from small data sets," Physica D: Nonlinear Phenomena, vol. 65, (1993), pp. 117-134.