Communications and Network, **2013, 5, 524-528**
http://dx.doi.org/10.4236/cn.2013.53B2096 Published Online September 2013 (http://www.scirp.org/journal/cn)

Research on Intrusion Detection Algorithm Based on Multi-Class SVM in Wireless Sensor Networks

Hangxia Zhou, Qian Liu, Chen Cui
Department of Computer Science and Technology, China Jiliang University, Hangzhou, China
Email: zhx@cjlu.edu.cn

Received June 2013

ABSTRACT

A multi-class method is proposed based on Error Correcting Output Codes algorithm in order to get better performance of attack recognition in Wireless Sensor Networks. Aiming to enhance the accuracy of attack detection, the multi-class method is constructed with Hadamard matrix and two-class Support Vector Machines. In order to minimize the complexity of the algorithm, sparse coding method is applied in this paper. The comprehensive experimental results show that this modified multi-class method has better attack detection rate compared with other three coding algorithms, and its time efficiency is higher than Hadamard coding algorithm.

Keywords: Wireless Sensor Network; Multi-Class; Network Security

1. Introduction

Wireless Sensor Network (WSN) consists of a large number of small sensor nodes in terms of self-organization and multiple hops. These sensor nodes have low cost, less energy, and limited processing ability. These nodes are applied to sense, collect and process the object within the network coverage area, and sent signals to the host user in the form of data. The sensor nodes are usually distributed in no security environment, and it is easy for them to be captured and manipulated by attackers. In recent years, WSN security has become the frontier research fields to scholars. The author in [1] summarized the types of attacks in WSN, such as blackhole attack, hello flooding attack, DoS attack, and selective forwarding attack and so on.

Support Vector Machine (SVM) is one of the most widely used classification methods in WSN. It has peculiar advantages in small sample, high dimension pattern recognition and nonlinear problems [2]. But the traditional support vector machine is designed for two-class classification so that it fails to handle multi-class problems. As a result, research on SVM multi-class classifier has become a necessity.

This paper proposed a modified Sparse-ECOC multi-class classification method. This method can be used to classify the traffic data collected by network nodes to determine whether the system is invaded by attackers. Experiments show that compared with the existing classification algorithm, this improved algorithm has higher attack detection rate and time efficiency.

2. Classical Algorithms

Compared with the traditional networks, wireless sensor network has the following two characteristics: the limitation of energy supply, processing speed and storage space. And the limitation of communication bandwidth, time delay, transmission packet size, etc.

Because of the limitations, safety prevention method which is commonly used in wired networks does not apply to wireless sensor networks. For this reason, this article chooses intrusion detection technology of SVM which conforms to the characteristics of WSN.

2.1. Support Vector Machine and Principle

Support vector machine is a new kind of machine learning method. It is based on statistical learning theory and structural risk minimization principle. In [3], the use of kernel function made the nonlinear flow data collected by sensor nodes to be mapped to a high-dimensional feature space, which greatly reduces the algorithm complexity, and effectively overcomes the "dimension disaster" problems which often appears in artificial neural networks. In [4], support vector machine has strong generalization ability in tackling small sample classification. The model proposed in [5] is suitable for low bandwidth and small packets situations in wireless sensor networks.

In SVM model, set input vector $x_i \in R^d$, category $y_i \in \{-1,1\}$, sample size $i, j = 1,2,...,n$, kernel function

$K(x_i, x_j)$, high dimensional feature space Z, nonlinear mapping $\varphi: R^d \to Z$. Nonlinear samples can be mapped to high-dimensional feature space Z by kernel function and mapping φ to construct an optimal separating hyperplane in Z. The points on the optimal separating hyperplane need to meet:

$$\omega \cdot \varphi(x) + b = 0, \quad (1)$$

and classification interval is equal to $2/\|\omega\|$. If we want the best effect of classifying, classification interval shall take the maximum, that is to say, $\|\omega\|$ shall take the minimum [6].

In practice, classic support vector machine cannot solve multi-class problems. So we need to take other ways to solve them. In [7], the author listed some common multi-class classification method, such as one-against-one method, one-against-all method, binary tree method, error correcting output codes (ECOC) method, directed acyclic graph SVM (DAGSVM) method, etc.

2.2. Hadamard Coding Algorithm

Hadamard error correcting output codes method is a typical algorithm which decomposes multi-class problem into several two-class problems. Hadamard matrix was proposed by James Joseph Sylvester on the basis of orthogonality in 1867 [8]. It is a square matrix which is made of "−1" and "+1", and any different two rows of it is mutually orthogonal. N dimensional Hadamard matrix can be obtained by $N/2$ dimensional matrix through the method of recursing.

$$H_2 = \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \quad H_N = \begin{pmatrix} H_{N/2} & H_{N/2} \\ H_{N/2} & -H_{N/2} \end{pmatrix} \quad (2)$$

For N dimensional matrix, any two rows or two columns are neither same nor complementary. The distance between any two rows or two columns is $N/2$. These features meet the needs of classifier training, but the first "−1" column in the matrix cannot be used for classifier coding. So the original N dimensional matrix needs to be cut in a certain degree.

3. Experimental Design and Implementation

Experimental design includes two aspects: coding matrix construction and the training of classifier. Coding matrix construction is conducted on the basis of Hadamard matrix. The realization of classifier is implemented on NS2 and LIBSVM platform.

3.1. Construct Modified Coding Matrix

According to the characteristics of the matrix and coding principles, the approach of Sparse-ECOC matrix structure can be shown as follows:

- Obtained a N dimensional Hadamard matrix according to Equation (2).
- Delete the first "−1" column, and obtained a $N \times (N-1)$ dimensional matrix.
- Take the first l lines of the matrix, and obtained a $l \times (N-1)$ dimensional matrix.
- Chose an element from each row and replace it with element "0". Ensure the minimum hamming distance as large as possible.

The sign l expresses sample class number. The modified coding matrix has simple coding scheme, less number of classifiers constructed, and convenient calculation. Any two rows or two columns are neither same nor complementary. The hamming distance between any two rows is equal to $N/2$.

The coding matrix constructed in this way is ternary code matrix. In ternary code encoding, element "1" expresses positive, element "−1" expresses negative, and element "0" expresses doing nothing with it [9]. The addition of zero elements made classifier more simplified, so we call this coding matrix Sparse-ECOC matrix.

The Sparse-ECOC matrix not only satisfies the training requirements of multi-class SVM classifier, but also reduces each single classifier's construction time because of the addition of zero elements. These properties effectively improve the training speed and comprehensive performance.

3.2. Classifier Implementation

The Sparse-ECOC multi-class algorithm proposed in this paper mainly detect for hello flooding attack, denial-of-service (DoS) attack, blackhole attack, selective forwarding attack and sybil attack in WSN. Detect and classify attacks by analyzing the energy of nodes and packets received and send situations in the networks. In order to reduce the complexity of calculation, we choose appropriate flow characteristics for each attack as less as possible.

For hello flooding attack, we select the energy of package sent as its feature. For DoS attack, we select the number of data packets received. For blackhole attack, we select the number of route request replies received, the number of route request replies sent, and the number of route request replies dropped. For selective forwarding attack, we select the number of route errors send and the number of route errors received. For sybil attack, we select the frequency of the node selected as cluster head [10].

Classifier realization mainly includes four processes: data acquisition, data preprocessing, kernel function selection and classifier training, algorithm verification (**Figure 1**).

1) Data acquision: Build a hierarchical and cluster structure model of WSN in NS2. We choose IEEE 802.15.4

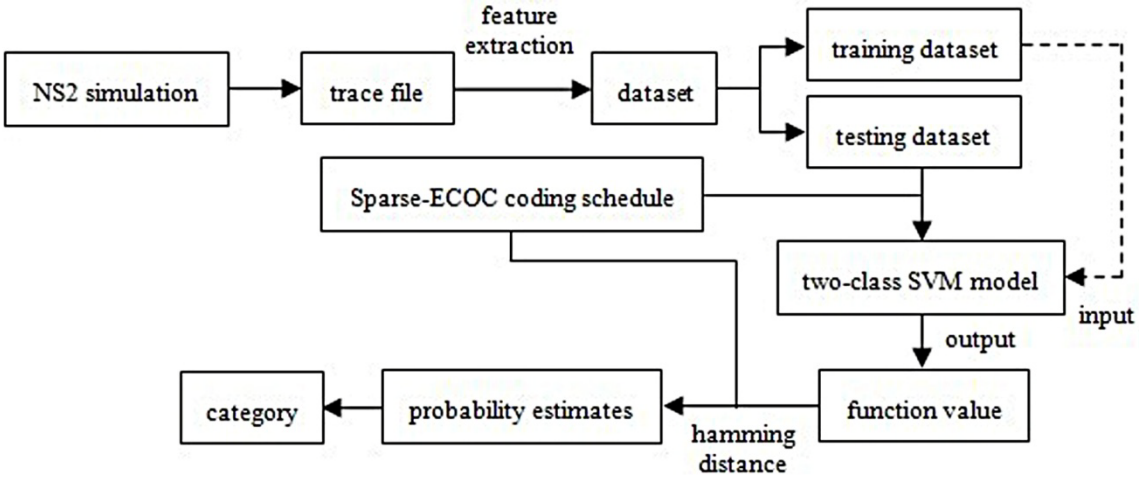

Figure 1. Classifier implementation process.

standard for media access control (MAC) layer and low energy adaptive clustering hierarchy (LEACH) protocal for network layer. Specific process can be implemented as follows.

a) Define the transmission channel, transmission model, the interface queue, topology, God object, the node's properties and actions in the node transmission process.

b) Add environmental parameters which would be needed in the operational process of LEACH protocol. Add malicious nodes of five attacks in a specific time one by one.

c) Monitor the network status, including node energy state, packet receiving and sending situation, cluster selected rules.

d) Extract trace files and construct datasets.

2) Data preprocessing

In order to avoid the singular sample data caused an increase of training time, normalize each column in the datasets. Then translate the normalized training dataset into seven two-type of datasets on the basis of **Table 1**. Element "1" expresses positive, element "−1" expresses negative, and element "0" expresses does nothing with it.

3) Kernel function selection and classifier training

In experiments, we select radial basis function (RBF) as the kernel function, and 250 rows of data as the training set. The optimal kernel parameters δ and penalty parameters C of seven two-class SVM classifier can be obtained in (2^{-10}, 2^{15}) through grid search and 5-fold cross validation method. With the optimal parameters the classifier can be trained.

4) Algorithm verification

Select six kinds of data from the normalized testing dataset. Input into seven classifier and got the output results. Calculate the hamming distance between outputs and Sparse-ECOC coding matrix. Take the category of the minimum hamming distance as its category of belonging.

Table 1. The Sparse-ECOC coding schedule.

Class	Codeword						
	SVM 1	SVM 2	SVM 3	SVM 4	SVM 5	SVM 6	SVM 7
1	−1	−1	−1	0	−1	−1	−1
2	+1	−1	+1	−1	0	−1	+1
3	−1	+1	0	−1	−1	+1	+1
4	+1	+1	−1	−1	+1	0	−1
5	0	−1	−1	+1	+1	+1	+1

$$D = \arg\min d\{A, M_i\} = \frac{1}{2}\sum_{j=1}^{l}\left|A_j - M_{i,j}\right| \quad (3)$$

Equation (3) is the minimum hamming distance formula. A_j is the code word of the jth column in the test sample output vector. $M_{i,j}$ is the code word of the ith row and the *j*th column in the Sparse-ECOC coding schedule.

4. Experimental Analysis

In the simulation, fifty sensor stationary nodes are distributed in the area of 100 × 100 meters. The initial energy of each node is two joules. Malicious nodes have enough energy. The total simulation time is 500 seconds.

In the experiments, the train data and test data are from NS2 wireless sensor network simulation. Datasets consists of five parts: node data in Hello flooding attack, DoS attack, blackhole attack, selective forwarding attack and sybil attack situations. This paper compares the performance of the modified algorithm with one-against-one method, one-against-all method and ECOC method (**Table 2**).

In **Figures 2** and **3**, we can see that Sparse-ECOC method has a distinct advantage in each attack detection when compares with one-against-one method and one-against-all method. The data in **Figure 4** shows the detection accuracy comparison between Sparse-ECOC method and Hadamard method. They have the similar accu-

Table 2. Detection accuracy and average training time of four ECOC encoding method.

Encoding Method	Detection Accuracy (%)					Average Training Time (s)
	hello flooding	blackhole	selective forwarding	DoS	sybil	
Sparse-ECOC	96.19	96.15	91.07	95.24	92.73	9.825189571
Hadamard	94.16	96.09	88.21	96.19	93.26	12.593525428
one-against-one	90.96	91.06	80.17	90.35	90.14	2.913055304
one-against-all	90.95	90.92	80.08	90.31	82.17	8.700531809

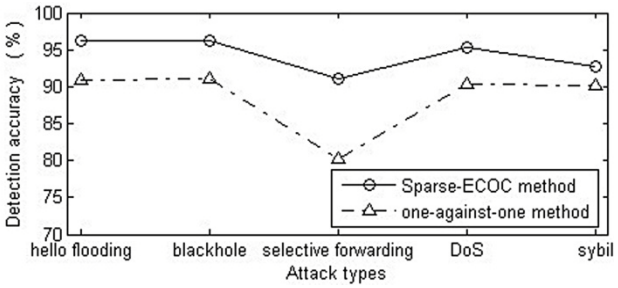

Figure 2. Accuracy comparison between Sparse-ECOC method and one-against-one method.

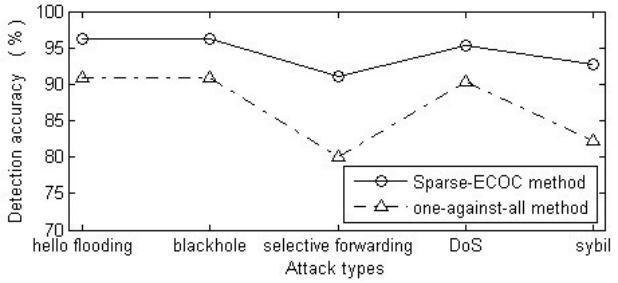

Figure 3. Accuracy comparison between Sparse-ECOC method and one-against-all method.

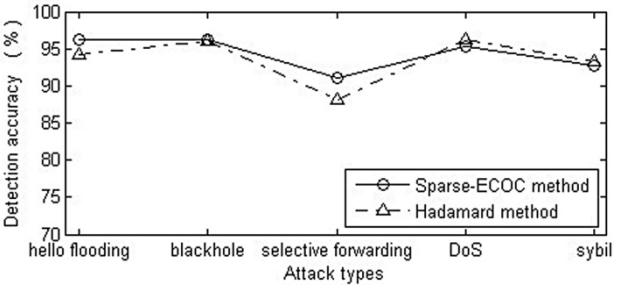

Figure 4. Accuracy comparison between Sparse-ECOC method and Hadamard method.

racy in blackhole attack, DoS attack and sybil attack, but Sparse-ECOC method is better in hello flooding attack and selective forwarding attack.

Figure 5 shows the number of sub-classifiers needed in four encoding methods and the training time cost of each sub-classifier. From the picture, we can see that one-against-one method spends the least amount of time, but it needs the most number of sub-classifiers. One-against-all method needs the least number of sub-classifiers, but it has low detection accuracy of attacks. Hadamard method has the same number of sub-classifiers as Sparse-ECOC method, but its time efficiency is far lower than the latter. These results demonstrate that Sparse-ECOC method provides a better approach for improving attack detection rate and time efficiency.

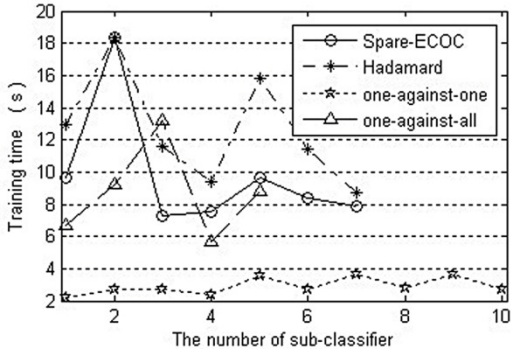

Figure 5. Training time of four encoding methods.

5. Conclusion

In this paper, a multi-class SVM algorithm is constructed based on Hadamard coding algorithm. Through the experiment, higher accuracy of attack detecting is obtained. By comparing the results with that of Hadamard method, one-against-one method and one-against-all method, it is found that the modified algorithm is a better approach for attack detection.

REFERENCES

[1] H. Ehsan and F. A. Khan, "Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs," *IEEE Trust, Security and Privacy in Computing and Communications Conference TRUSTCOM*, Liverpool, 25-27 June 2012, pp. 1181-1187.

[2] N. Shahid, I. H. Naqvi and S. B. Qaisar, "Quarter-Sphere SVM: Attribute and Spatio-Temporal Correlations Based Outlier & Event Detection in Wireless Sensor Networks," *IEEE Wireless Communications and Networking Conference WCNC*, Shanghai, 1-4 April 2012, pp. 2048-2053.

[3] S. Xu, C. Hu, L. Wang and G. Zhang, "Support Vector Machines Based on K Nearest Neighbor Algorithm for Outlier Detection in WSNs," *Proceedings of the 8th Wireless Communications, Networking and Mobile Computing International Conference WICOM*, Shanghai,

21-23 September 2012, pp. 1-4.

[4] D. Bi, X. Wang and S. Wang, "Particle Swarm Optimization Clustering for Target Classification in Wireless Sensor Networks," *Proceedings of the 4th Natural Computation International Conference*, Jinan, 18-20 October 2008, pp. 111-115.

[5] A. B. Raj, M. V. Ramesh, R. V. Kulkarni and T. Hemalatha, "Security Enhancement in Wireless Sensor Networks Using Machine Learning," *High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems HPCC-ICESS*, Liverpool, 25-27 June 2012, pp. 1264-1269.

[6] X. Liu, X. Zhang and J. Duan, "Speech Recognition Based on Support Vector Machine and Error Correcting Output Codes," *Pervasive Computing Signal Processing and Applications International Conference PCSPA*, Harbin, 17-19 September 2010, pp. 336-339.

[7] F. Masulli and G. Valentini, "An Experimental Analysis of the Dependence among Codeword Bit Errors in ECOC Learning Machines," *Neurocomputing*, Vol. 57, 2004, pp. 189-214. http://dx.doi.org/10.1016/j.neucom.2003.09.011

[8] J. Wales, "Hadamard matrix From Wikipedia," 2013. http://en.wikipedia.org/wiki/Hadamard_matrix.

[9] M. M. Khedkar and S. A. Ladhake, "Robust Human Iris Pattern Recognition System Using Neural Network Approach," *Information Communication and Embedded Systems International Conference ICICES*, Chennai, 21-22 February 2013, pp. 78-83.

[10] C. E. Loo, M. Y. Ng, C. Leckie and M. Palaniswami, "Intrusion Detection for Routing Attacks in Sensor Networks," *International Journal of Distributed Sensor Networks*, Vol. 2, No. 4, 2006, pp. 313-332. http://dx.doi.org/10.1080/15501320600692044

