Journal of Software Engineering

ISSN 1819-4311

Academic Journals Inc.

www.academicjournals.com

Journal of Software Engineering 8 (4): 225-238, 2014
ISSN 1819-4311 / DOI: 10.3923/jse.2014.225.238

Intrusion Detection System Based on Integration of Neural Network for Wireless Sensor Network

Fan Lu and Liejun Wang
Information Science and Engineering, Xinjiang University, Urumqi, China

Corresponding Author: Wang Liejun, Information Science and Engineering, Xinjiang University, Urumqi, China

ABSTRACT

According to the energy constrained, low-storage space and limited computing ability of wireless sensor network nodes, an intrusion detection model based on GA-LMBP was proposed. Compared with traditional methods, the program takes advantage of offline learning neural network algorithm to build detection model without storing large amounts of intrusion features, saving storage resources. Compared with the use of promiscuous mode capturing data, multi-detection cooperative mechanism reduces energy consumption. Simulation results show that GA-LMBP intrusion detection model in terms of performance, energy consumption, storage costs, the detection rate and false detection rate is better than those of traditional methods.

Key words: Wireless sensor networks, intrusion detection, fusion algorithm, cooperative detection mechanism

INTRODUCTION

As the wireless sensor networks deployed in unattended environments, nodes data vulnerable to eavesdropping, tampering or falsification and cause serious consequences, so that intrusion detection of wireless sensor networks faces enormous challenges (Ponomarchuk and Seo, 2010). In the traditional internet networks (Sun *et al*., 2007) and *ad hoc* network (Mostarda and Navarra, 2008), intrusion detection technologies (He *et al*., 2013) can be divided into feature detection and misuse detection, but restrictions by the node energy, storage space and computing power and other aspects of wireless sensor network (Hortos, 2010; Islam and AshiqurRahman, 2011), so that the sensor nodes can't store large amounts of intrusion featuresand make a real-time intrusion detection (Livani and Abadi, 2011), therefore traditional, intrusion detection technology being used in wireless sensor networks is difficult.

There are many methods for intrusion detection of wireless sensor network. Doumit and Agrawal (2003) proposed an intrusion detection solution based on the security level and stochastic learning process, they use the location information associated with the level of security and the hidden Markov model to detect abnormal behavior of unknown. Su *et al*. (2007) proposed eHIP solution to improve the security of clustered sensor network which is energy efficient hybrid intrusion prevention systems. This system including intrusion prevention subsystem AIP based on the authentication and intrusion detection subsystem CID based on the cooperation, to support different levels of security needs and reduce the consumption of energy in clustering of sensor networks. Agah and others by using game theory based on the fight to find the most vulnerable nodes in sensor networks and protect them (Agah *et al*., 2004). Da Silva *et al*. (2005) defines the

multiple rules to detect intrusion occursand automatic alarm when trigger more than threshold. But they did not take into account the wireless sensor network's own limitations, so these are difficult to apply in actual environment.

Neural network has the self-learning, associative memory and fuzzy computing power, this makes the neural network can not only identify the existing attack mode, but also detect the unknown attack, it is very meaningful for intrusion detection (Yu and Li, 2006; Yi *et al*., 2011; Salmon *et al*., 2013). On the one hand, as long as providing the training data, the neural network can be used offline learning to extract the characteristic patterns of sensor activity, to establish a simple feature set without the need to compare the huge intrusion feature library. These behavioral characteristics sets obtained from study stored in the neural network weights, save a lot of storage space. Neural network, on the other hand, can make use of a large number of invasive instances training to learn the knowledge, obtain the prediction ability and this process can be completely abstract calculation. Neural networks can be automatic control system of the internal relation between each measure, make its maximum close to real system working model or network attack model, thus the monitoring data input to it can make quite a correct judgment (Wang *et al*., 2011). In view of the wireless sensor network node itself limits, the use of the advantage of neural network, this study proposes an intrusion detection system based on integration of neural network for wireless sensor networks which is GA-LMBP intrusion detection system.

GA-LMBP ALGORITHM

Levenberg-Marquardt Algorithm (LMBP): Levenberg-Marquardt algorithm (Lourakis, 2005) is an optimization algorithm of standard BP algorithm. It is the combination of the gradient descent method and gauss Newton method and it is a fast algorithm of using standard numerical optimization techniques. It has both the local convergence of gauss Newton methodand the global features of gradient descent method. On the local search ability, LMBP algorithm is better than the standard BP algorithm. Due to the use of approximate second order derivative information, LMBP algorithm is much faster than the gradient method, especially when the input is low dimension, LMBP algorithm show the high performance. Therefore, LMBP algorithm is better than the standard BP algorithm for intrusion detection. w_k represents network weights vector k-th iteration; the new weight vector can be calculated according to the following rules:

$$W^{k+1} = W^k + \Delta W \tag{1}$$

$$MSE(w) = \frac{1}{2}\sum_{i=1}^{N} e_i^2(w) = \frac{1}{2}\sum_{i=1}^{N}(o_i - d_i)^2 \tag{2}$$

In the Eq. 2, o_i and d_i are the output of network output layer and the desired output respectively, MSE (w) is error energy function. The Eq. 1 and 2 are single output network, if it is a multi-output network, simply accumulating the square-error of the output layer which is the accumulative item from m to m×n:

$$\Delta w = -[J^T(w)J(w) + \mu I]^{-1}J^T(w)e(w) \tag{3}$$

In the Eq. 3, $e(w)=[e_1(w), e_2(w),\cdots, e_N(w)]^T$, N is the number of output layer neurons, I is a unit matrix, J(w) is the Jacobian matrix.

Genetic Algorithm (GA): Genetic algorithm (Deb *et al.*, 2002) is a kind of probabilistic adaptive and iterative optimization process. It has good global search and difficult to fall into local minimum. Even if the fitness function is not continuous and irregular, it also can find the overall optimal solution with great probability. It has the characteristics of parallel processing and not relies on the gradient information, which can be used to optimize the BP neural network.

In the genetic algorithm, selection, crossover and mutation operations are the key process to survival of the fittest. So, we need to choose appropriate methods for genetic operation. In this scheme, selecting operation use the roulette wheel selection method, probability of being selected for each individual is:

$$P_i = \frac{F_i}{\sum_{i=1}^{N} F_i} \tag{4}$$

In the Eq. 4, F_i is the fitness function of individual i, N is the number of individuals for the population. Using the selected probability P_i, we select individuals to crossover operation from the population.

Crossover operation use arithmetic crossover, the purpose is to generate new individuals. Assume that the x_1 and x_2 in the population is selected for crossover operation parent, produced by the parent generations $x_1^{'}$ and $x_2^{'}$ is Eq. 5:

$$\begin{cases} x_1^{'} = ax_1 + (1-a)x_2 \\ x_2^{'} = ax_2 (1-a)x_1 \end{cases} \tag{5}$$

Mutation operation use non-uniform mutation, the purpose is to produce new individuals. The non-uniform mutation is making a random disturbance on the value of the original gene, the results as a new gene values after disturbance. First of all, we should obtain the variance of chromosomes d (x_i):

$$d(x_i) = \begin{cases} (b_i - x_i)[r(1-t)]^h & \text{sign} = 0 \\ (x_i - a_i)[r(1-t)]^h & \text{sign} = 1 \end{cases} \tag{6}$$

In the Eq. 6, a_i and b_i are the values of the left and right confine, r is a random number produced on (0, 1), $t = g_c/g_m$, g_c is the current evolution algebra, g_m is the maximum evolution generation, then we can obtain the new chromosome (Eq. 7):

$$x_i^* = \begin{cases} x_i + d(x_i) & \text{sign} = 0 \\ x_i - d(x_i) & \text{sign} = 1 \end{cases} \tag{7}$$

Introducing the benefits of this function is that x_i is available in a wide range of changes, that is, the search space islarge. As for evolution (t becomes large), the conversion range of x_i becomes small, this will help improve the accuracy of genetic algorithms.

The combined use of genetic algorithms and LMBP algorithm called GA-LMBP algorithm. The algorithm can not onlymeet the global properties of Genetic Algorithm (GA), also can have LMBP

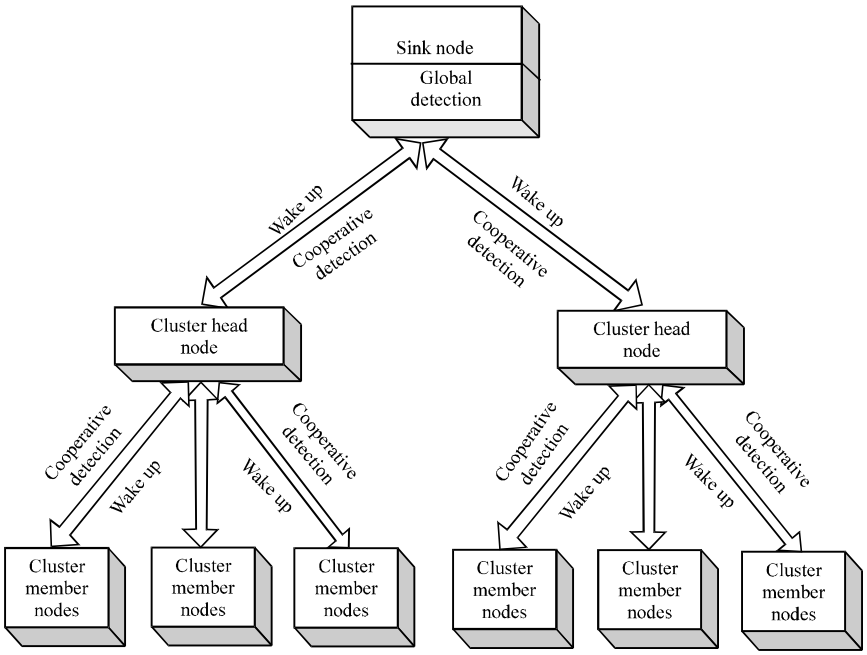

Fig. 1: Network architecture and multi-level cooperation mechanism

algorithm in the local fast convergenceproperties. The genetic algorithm is used for searching in a larger range and optimizing the initial weights of neural network. LMBP algorithm is used for the local fast convergence and optimization of network structure and parameters. The algorithm overcomes the shortcoming of BP neural network which is easy to fall into local minimum point. And the algorithm is easier to get the global optimal solution. GA-LMBP algorithm have been applied in some scenes, this study first applied the algorithm in wireless sensor network intrusion detection.

INTRUSION DETECTION SYSTEM

Network structure and system model: This study uses the clustering of the wireless sensor network. The network consists of three layers: Sink nodes, cluster head nodes and cluster member nodes. The clustering network structure can control the most of nodes communication in a small range. The most important thing is reduced the communication between the nodes. This greatly reduces the communication overhead of the network, which is beneficial to prolong the network life cycle. Network architecture is Fig. 1.

In the stage of establishing an intrusion detection model, let GA-LMBP model offline learning. We use a lot of experimental data in the computer for the training to get intrusion detection mechanism and we install the detection mechanism which we get in the sink node, cluster head nodes and cluster member nodes.

In network intrusion detection phase, we use the multi-layer cooperative detection mechanism. The first layer is when the sink node perceived danger, considered it is a potential invasion, the sink node according to its own global detection mechanism to detect the invasion. The second layer is awakening of cooperative detection of cluster nodes in the region. The cluster head nodes use their own detection mechanism to judge if it was a invasion. If they are still unable to determine the invasion behavior, then they will wake up cluster member nodes in the region for cooperative detection and judgment. The third layer is the cluster head nodes

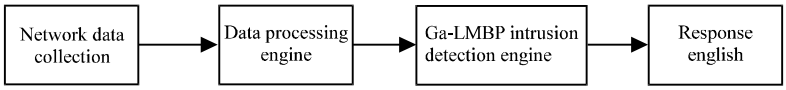

Fig. 2: Wireless sensor network intrusion detection model

Table 1: Type sizes for camera-ready papers

Information collected	Intrusion behavior
Node data	Data forgery attack
Packet transmission rate	Energy depletion attack
Packet reception rate	Sink node forgery attack
Packet loss rate	Black hole attack, Select forward attack
Packet matching rate	Tampering attack
Packet return rate	Blocking attack
Packet transmission energy	Hello attack, Wormhole attack
Node energy decline rate	DOS attack

summary the characteristics of the abnormal information and report to the sink node. At this point, the sink node has the most detailed data information. It will make the most accurate intrusion detection judgment. So, multilayer cooperative detection mechanism not only reduces the energy consumption of sensor nodes but also improving the detection rate of the intrusion detection, reducing the error detection rate.

This scheme uses fusion algorithm of genetic algorithm and the LMBP neural network in intrusion detection. As shown in Fig. 2, the intrusion detection model is put forward. The model consists of three processing engine: Data processing engine, GA-LMBP intrusion detection engine and response engine.

Data processing engine: The engine includes data feature extraction and data preprocessing. After the collected useful data features, the engine will reduce the dimension of input data. And then the engine will be data normalization, standardization and put the data into GA-LMBP intrusion detection engine. Data collection features as shown in Table 1.

Data feature extraction: Using PCA method to feature extraction of collected data and eliminating noise data and redundant features. The specific approach as follows:

Step 1: Zero mean normalization: The value of the attribute based on the mean and standard deviation of standardization.v is the value of A, v is normalized to v', calculated by the following Eq. 8:

$$v' = \frac{v - A}{\delta_A} \tag{8}$$

In the Eq. 4, A and δ_A are the mean and standard deviation of attribute A.

Step 2: Calculate the eigenvalues of the covariance matrix Σ

Step 3: Calculate the eigenvectors and eigenvalues of the covariance matrix, the eigenvectors is a unit vector

Step 4: Choose the main composition and form feature vector matrix (Eq. 9):

$$\text{Feature} = (\text{eig}_1, \text{eig}_2, \text{eig}_3, \cdots, \text{eig}_n), d < D \tag{9}$$

In the Eq. 4, the eigenvector matrix is composed of main feature vector matrix by selected. We extract the feature items to be combined, so that we can describe a typical attack in the form of vector. As the GA-LMBP network training sample, we can set up the characteristics of different attacks.

Data preprocessing: After the dimension reduction of original data and the data cannot be directly as the input of the network. These data must be converted to the identified data of GA-LMBP network. In order to make the output value between 0~1, we need to normalize the eigenvalue. The normalization process is as follows:

Step 1: Use Eq. 10 to calculate the mean μ of all the eigenvalues.

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{10}$$

Step 2: After getting the mean of the characteristic value, we can calculate the standard deviation σ of all the eigenvalues (Eq. 11):

$$\sigma = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n} (x_i - \mu)^2} \tag{11}$$

Step 3: Through the characteristic value of standard deviation, we can get standardized attribute values y_i (Eq. 12):

$$y_i = \frac{x_i - \mu}{\sigma} \tag{12}$$

The resulting values y_i can be used by the GA-LMBP intrusion detection engine.

GA-LMBP intrusion detection engine: We put the processed data input GA-LMBP intrusion detection engine and the intrusion detection engine process the data to determine whether it is an intrusion. If the engine finds it is a kind of attack, the response engine will receive a warning message and recorded in the log file for a rainy day. If the alarm information for an attacker sample library has great value in improving and updating, such as discovering new attacks. We can send the alarm information to the sink node to join the attack sample library, let the GA- LMBP network learning, thus improving the processing capacity of the network.

The GA-LMBP algorithm is applied to intrusion detection, we need to redesign the chromosome encoding and fitnessfunction of genetic algorithms.

Chromosomal gene coding design: We adopt high precision floating-point encoding instead of the ordinary binary encoding, to avoid mapping error in the process of encoding and decoding. Chromosome code string arrange to form by weight vector and the threshold value of each layer. Each code string represent a particular form of neural network, which is shown in chromose gene encoding scheme as below:

$$[w_{ij}][v_{ki}][\theta_j][\theta_k]$$

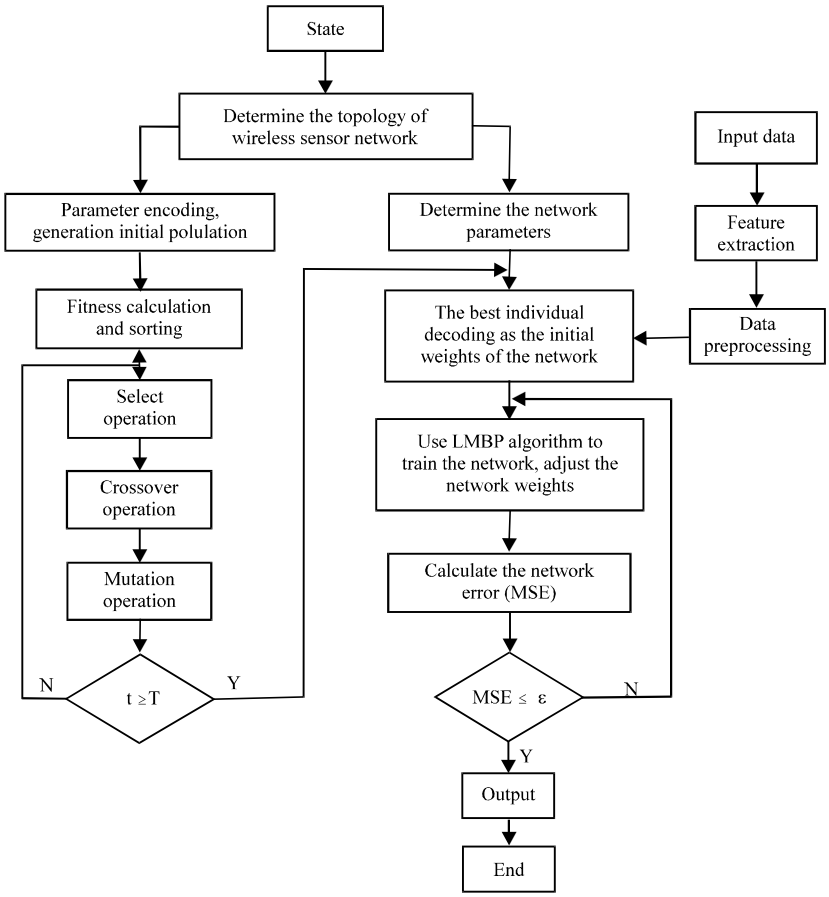

Fig. 3: GA-LMBP algorithm implementation process

In encoding scheme $[w_{ij}]$ is the connection weights between the input layer and hidden layer; $[w_{ki}]$ is the connection weights between the hidden layer and output layer; $[\theta_j]$ is the j-th neuron threshold of the hidden layer; $[\theta_k]$ is the k-th neuron threshold of the output layer.

Design of fitness function: Fitness function is to guide the search of evaluation function in genetic algorithm, it is not subject to constraints such as function of continuity or derivative. An important feature of feedforward neural network is that the energy value of the error function smaller, the better performance of the network. So, the fitness function of the scheme is defined as Eq. 13:

$$F(x)=\frac{1}{E(w)} \tag{13}$$

The required function designs are completed. Then the GA-LMBP intrusion detection system can use programs to realize. GA-LMBP algorithm implementation process shows in Fig. 3.

Application process is as follows:

Step 1: Determine the topology of wireless sensor networks

Step 2: Given the initial population Pop (N, L) and evolutionary algebra t, set the chromosome gene encoding and thefitness function F (x)

Step 3: Calculate the fitness values of individuals and the value in accordance with the smallest, reserve the best individual of maximum fitness value

Step 4: Selection operation, use roulette selection method, the individuals selected for crossover operation

Step 5: Crossover operation, use arithmetic crossover to generate new individuals

Step 6: Mutation operation, use non-uniform mutation to generate new individuals.

Step 7: Retained the optimal individual and new individuals and make them form the next generation of the population

Step 8: Determine whether the evolution algebra t to the evolution of the set algebra T, if the target is reached, the genetic algorithm (GA) ends and the next step. Otherwise, return to step 3

Step 9: The best individual decoding, after decoding the value use for the LMBP network optimal initial weights and thresholds and gives the error allowed values of ε and μ

Step 10: Put the pretreatment of data into LMBP neural network for training

Step 11: Calculate the output value o_k and the error energy function E(w) of neural network

Step 12: Calculate the weight of the amount of change $\triangle w$ and calculate the new weight vector

Step 13: If $E(w) < \varepsilon$, show that the algorithm is convergent, output the result and go to the next step. Otherwise go to step 10

Step 14: Output the result, end

GA-LMBP algorithm program implementation process as shown in Fig. 3.

If the intrusion detection engine found intrusion behavior, analysis of the intrusion behavior and it will report theresult to the response engine.

Response engine: In view of the invasion have been detected, the sink node using response can be divided into local response and global response. The local response is that sink node broadcast the intrusion node location information in the whole network and sink node remind the other nodes to reduce contact with the node. The global response is that isolate suspicious nodes by updating the routing or updating communication keys.

SIMULATION AND PERFORMANCE ANALYSIS

Simulation: Through the simulation experiment to validate the advantages of GA-LMBP algorithm is applied to wireless sensor network. The performance of the detection model was analyzed by the detection rate and false detection rate, power consumption and storage overhead. This study uses the MATLAB R2009a and OMNET++ 4.1 emulator as experimental platform. The 200 nodes deployed evenly to the area of 500×500 m. Use clustering algorithm to form 20 clusters, members of the cluster node communication radius is 50 m, the communication area of cluster head nodes can basically cover the entire deployment area. The communication range of sink node can cover the entire area. It has a very large processing power and storage space. In the process of nodes communication, we will simulate the invasion of the network.

Training data and testing data using the wireless sensor network dataset of naval research laboratory, this data setcontains the normal flow set {NS1, NS2} and attack data sets {AS1, AS2, AS3, AS4}.The attack dataset simulation realized Passive Sinkhole Attacks (PSA), Periodic Route Error Attacks (PREA), Active Sinkhole Attacks (ASA) and DOS four attack scenarios, which also

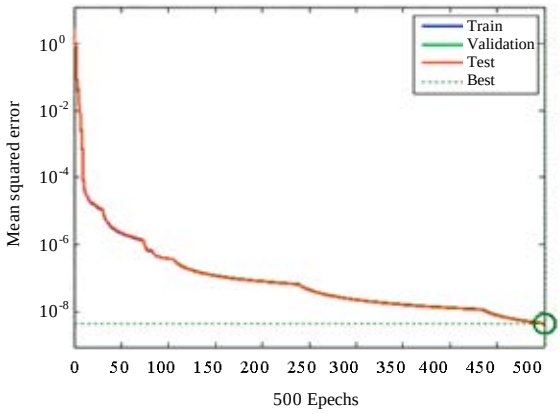

Fig. 4: BP model training performance curve, Best Validation performance is 4.4604e-000 at epoch 500

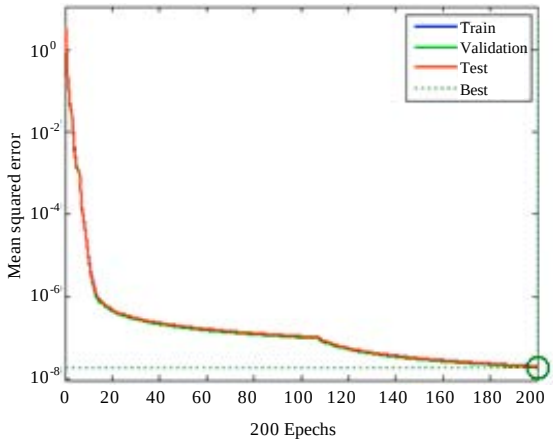

Fig. 5: GA-LMBP model training performance curve, Best Validation performance is 1.8154e-008 at epoch 200

includes a large number of normal data. The four categories of attack is currently way of wireless sensor network intrusion. Therefore, we can use these four categories of data to experiment. We randomly selected training and testing samples of each 1000, which accounted for normal data 60%, DOS attack samples representing 15%, PSA attack sample accounted for 10%, PREA attack samples representing 10%, ASA attack samples accounted for 5%.

Detection performance analysis: Population size in the Gnetic Agorithm (GA) is set to 50, the coefficient of variationis set to 0.068, the cross coefficient is set to 0.75, the evolution algebra is set to 500. Set the number of input layer neurons in the LMBP algorithm for 8, the number of hidden layer neurons for 6, the number of output layer neurons for 4. In terms of algorithm performance, the standard BP model is compared with GA-LMBP model. Figure 4 shows the error value (MSE) of standard BP model reaches the set value is best when computing iteration number up to 500

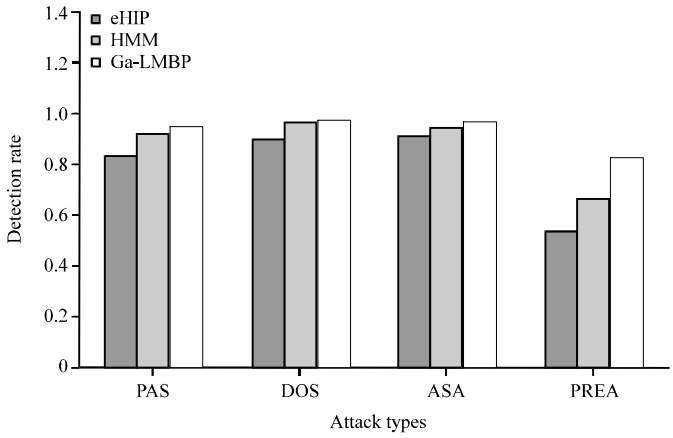

Fig. 6: Contrast detection rate

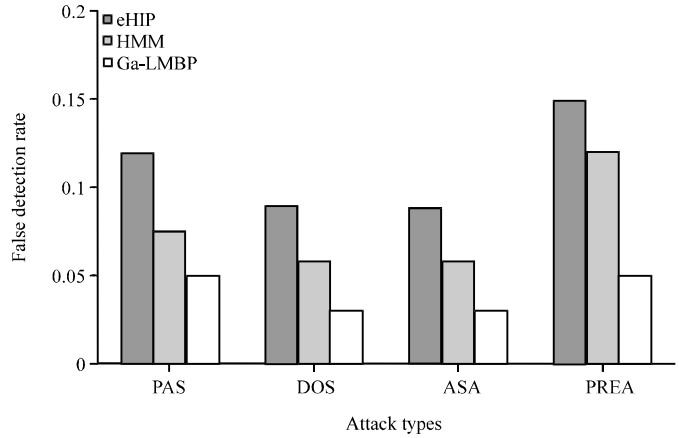

Fig. 7: Error detection rate

times. Figure 5 shows the error value (MSE) of GA-LMBP model reaches the set value is Best when computing iteration number up to 200 times. This shows that during the training period, learning time, fast convergence speed and accuracy, etc., GA-LMBP model is superior to BP standard model.

In the intrusion detection performance, the model of this study compared with eHIP model and the HMM model. eHIPmodel use the detection method which Su *et al.* (2007) proposed, this model adopts the hybrid intrusion prevention system of energy efficient to improve the security of sensor networks. HMM model use the detection method which Doumit and Agrawal (2003) proposed, this model adopts a intrusion detection scheme which is based on a level of security and random learning process. It uses the location information related security level and the hidden Markov model to detect abnormal behavior of the unknown. Figure 6 and 7 shows the four kinds of attacks on eHIP model, the HMM model and GA-LMBP model after processing, the contrast of detection rate and false detection rate.

By comparing the experimental results, GA-LMBP intrusion detection model in the detection rate and false detection rate were better than on eHIP model and the HMM model. In terms of detection rate, as we can see in Fig. 6, the scheme is effective detection for PAS, DOS, ASA, PREA four types of attack. Because the model uses the fusion algorithm of Genetic Algorithm (GA) and

the LMBP neural network, combining the global search capability of genetic algorithm and local convergence of the LMBP neural network, to make the detection system can quickly and accurately detect the various attacks.

In the aspect of error detection rate, Fig. 7 shows that this scheme for four types of attacks has lower error detection rate, especially in the aspect of PREA type of attack detection. In eHIP model and HMM model, nodes compare abnormal flow with normal flow, each abnormal behavior is considered an intrusionand it is prone to false positives. The model of multi-layer cooperative detection mechanism exist multilayer confirm invasion behavior, reducing false positives. Using the neural network fault tolerance effectively reduces the error detection rate of detection system.

Energy analysis: Because the sensor's energy consumption of communication greater than the energy consumption of calculation. So the main energy consumption is receiving and transmitting data consumption. Energy model used in this study based on Xiangning and Yulin (2007). Communication model use the multipath effect model, scilicet a message of length l (bits), the transmission distance is d, the energy consumption of transmitting data shows in Eq. 14:

$$E_{Tx}(l,d) = E_{Tx}(l) + E_{Tx}(l,d) = lE_{elec} + l\varepsilon_{mp}d^4 \quad (14)$$

Energy consumption of receiving data shows in Eq. 15:

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \quad (15)$$

So, the total energy consumption to complete a communication shows in Eq. 16:

$$E(l,d) = l(2E_{elec} + \varepsilon_{mp}d^4) \quad (16)$$

In Eq. 16, ε_{mp} is the signal amplification factor of the amplifier, E_{elec} is the energy consumption of the circuitwhich sent or received every bits of data.

Through simulation experiment, we got the energy consumption of three models. In Fig. 8, we can see the scheme's overall energy consumption is less than the other two models. Because the HMM model's nodes has been in mixed mode collecting flow information and keeping communication, so it has maintained a high energy consumption. eHIP model using periodic communication also consumes large energy. This scheme uses multilayer cooperative mechanisms, ordinary nodes just waking up by sink node for cooperative detection, it dormant in other time and consuming less energy. So, this scheme has obvious advantage in energy consumption and the scheme can be applied to actual circumstances.

Storage performance analysis: Nodes storage resources of wireless sensor network are very limited. In this study, the proposed scheme can save storage costs very well. We use the calculation method of Brea *et al.* (2013) to calculate the storage capacity of each model. In a random access memory RAM, there are M-bit addresses. An address can store 2^M bits of information. Its storage capacity is (Eq. 17):

$$C = 2^M \text{ (bit)} \quad (17)$$

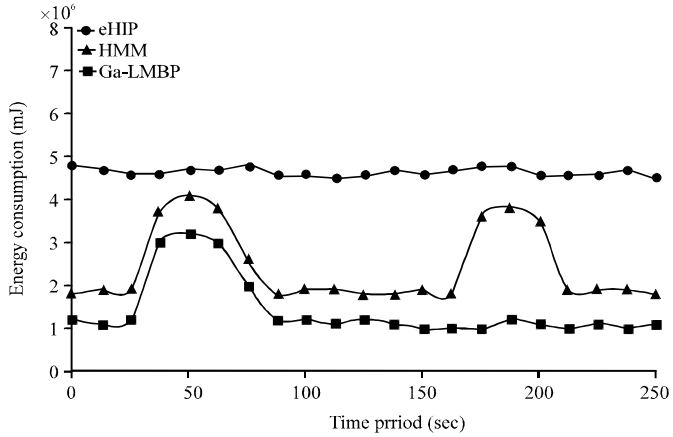

Fig. 8: Comparison of energy consumption

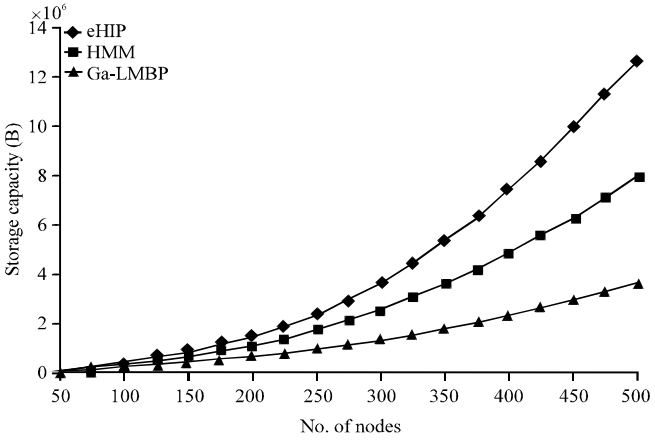

Fig. 9: Comparison of storage

According to the definition of neural network model, each neuron connects with other maximum of N-1 neurons. The threshold function argument up to N-1 and most have numbers of 2^{N-1} networks which can be divided into different network. The storage capacity of N-1 numbers of neurons is (Eq. 18):

$$a(\frac{N}{2})^3 \le C \le N(N-1)2^N \text{ (bit)} \tag{18}$$

In Eq. 18, a is 0.33. Figure 9 is a comparison of the three models' storages, visibly in this study, storage capacity of the model is much better than the other models. Because of the neural network approach for distributed storage, the parameter values store in the weight matrix. Through the associative memory ability of neural network, it can identify normal behavior and intrusion behavior, without the need of carrying a lot of intrusion detection signatures to compare and detect. So, it can save lots storage space. When the nodes number is greater, the more obvious it can save storage space.

CONCLUSION

This study proposes an intrusion detection model of wireless sensor network based on GA-LMBP algorithm. Compared with the traditional intrusion detection model based on BP, the proposed model has the following features: (1) Adopting multilayer cooperative detection mechanism, don't need to always wake nodes to collect information, reducing the energy consumption of sensor nodes, (2) For the first time, GA-LMBP algorithm is introduced into intrusion detection system, making this model has the self-learning, associative memory and fuzzy computing ability. The algorithm not only makes the network detection rate improved, also makes the network error detection rate reduced and (3) The experimental results show that the model not only has high detection rate and false detection rate is low and it has lower energy consumption. However, the response engine of the detection model is not perfect, we don't have a complete response mechanism and this will be the next focus of research study.

ACKNOWLEDGMENT

Thanks for this study is supported by the Natural Science Foundation of Xinjiang Province with grant No. 2014211B008. The author would like to thank the anonymous reviewers for their constructive comments that helped the quality of this study.

REFERENCES

Agah, A., S.K. Das, K. Basu, M. Asadi, 2004. Intrusion detection in sensor networks: A non-cooperative game approach. Proceedings of the 3rd IEEE International Symposium on Network Computing and Applications, August 30-September 1, 2004, Cambridge, MA., USA., pp: 343-346.

Brea, J., W. Senn and J.P. Pfister, 2013. Matching recall and storage in sequence learning with spiking neural networks. J. Neurosci., 33: 9565-9575.

Da Silva, A.P.R., M.T.H. Martins, B.P.S. Rocha, A.A.F. Loureiro and L.B. Ruiz *et al.*, 2005. Decentralized intrusion detection in wireless sensor networks. Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, October 13, 2005, ACM Press, Montreal, Quebec, Canada, pp: 16-23.

Deb, K., A. Pratap, S. Agarwal and T. Meyarivan, 2002. A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Trans. Evol. Comput., 6: 182-197.

Doumit, S.S. and D.P. Agrawal, 2003. Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks. Proceedings of the IEEE Military Communications Conference, Volume 1, October 13-16, 2003, Boston, MA., USA., pp: 609-614.

He, D.J., C. Chen, S. Chan, J.J. Bu and L.T. Yang, 2013. Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks. IEEE Trans. Ind. Electron., 60: 5348-5354.

Hortos, W.S., 2010. Neural methods based on modified reputation rules for detection and identification of intrusion attacks in wireless ad hoc sensor networks. Proceedings of the Evolutionary and Bio-Inspired Computation: Theory and Applications, April 22, 2010, Orlando, FL., USA.

Islam, M. and S. AshiqurRahman, 2011. Anomaly intrusion detection system in wireless sensor networks: Security threats and existing approaches. Int. J. Adv. Sci. Technol., 36: 1-8.

Livani, M.A. and M. Abadi, 2011. A pca-based distributed approach for intrusion detection in wireless sensor networks. Proceedings of the International Symposium on Computer Networks and Distributed Systems, February 23-24, 2011, Tehran, Iran, pp: 55-60.

Lourakis, M.I.A., 2005. A brief description of the levenberg-Marquardt algorithm implemented by levmar. http://www.ics.forth.gr/~lourakis/levmar/levmar.pdf.

Mostarda, L. and A. Navarra, 2008. Distributed intrusion detection systems for enhancing security in mobile wireless sensor networks. Int. J. Distrib. Sens. Networks, 4: 83-109.

Ponomarchuk, Y. and D.W. Seo, 2010. Intrusion detection based on traffic analysis and fuzzy inference system in wireless sensor networks. J. Convergence, 1: 35-42.

Salmon, H.M., C.M. de Farias, P. Loureiro, L. Pirmez and S. Rossetto *et al.*, 2013. Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques. Int. J. Wireless Inform. Networks, 20: 39-66.

Su, W.T., K.M. Chang and Y.H. Kuo, 2007. eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks. Comput. Networks, 51: 1151-1168.

Sun, B., L. Osborne, Y. Xiao and S. Guizani, 2007. Intrusion detection techniques in mobile *ad hoc* and wireless sensor networks. IEEE Wireless Commun., 14: 56-63.

Wang, S.S., K.Q. Yan, S.C. Wang and C.W. Liu, 2011. An integrated intrusion detection system for cluster-based wireless sensor networks. Expert Syst. Appl., 38: 15234-15243.

Xiangning, F. and S. Yulin, 2007. Improvement on LEACH protocol of wireless sensor network. Proceedings of the International Conference on Sensor Technologies and Applications, October 14-20, 2007, IEEE, Valencia, Spain, pp: 260-264.

Yi, X.M., P. Wu, L.J. Liu and D. Dai, 2011. Research on WSNs intrusion detection technology based on PSO-RBF. Transducer Microsyst. Technol., 30: 9-11.

Yu, H. and Q.Y. Li, 2006. The information fusion algorithm based on the neural network and its use in the network intrusion detection. J. Naval Univ. Eng., 18: 103-107.