AN OPTIMIZATION DETECTION ALGORITHM FOR COMPLEX INTRUSION INTERFERENCE SIGNAL IN MOBILE WIRELESS NETWORK

Li Gang*
Modern Educational Technology Center
Pingdingshan University, Pingdingshan, China

Abstract. At present, when detecting intrusive interference signals in classified form, the effect of channel denoising is very poor, and the characteristics of the extracted signals are not clear, which can not achieve effective detection of intrusion signals. An algorithm based on wavelet packet frequency hopping estimation for complex network intrusion detection is proposed in this paper. The soft and hard threshold method is used for wavelet coefficient decomposition, threshold processing, and signal reconstruction; according to probability statistics, a new sequence is composed of the spectral amplitude corresponding to the same frequency of each random variable in a random process and the spectrum matrix of intrusion interference signal is formed, so as to extract the characteristic spectrum of intrusion interference signal; by using the energy balance method, Gauss stochastic wavelet characteristics of intrusion signal can be simulated. The results of network intrusion detection are obtained by the Gauss additivity of the high-order cumulants of the network intrusion. The three edge centroid positioning method is applied to achieve the high-precision location of the intrusion point. Experiments show that the algorithm effectively improves the network channel denoising and the feature extraction effect of the intrusion signal, and it is also better than the current algorithm for the detection and location of the interference signals.

1. Introduction. In most non-commercial applications, such as environmental monitoring, forest fire prevention, wildlife tracking and monitoring applications, wireless sensor network security is not a very critical issue [17], while in other areas, such as wireless network security of residential quarters, monitoring the sensor network deployed by enemy military in the enemy occupied area, etc., the data collection and data transmission, even the node’s location distribution, should not let the unrelated personnel know nothing. How to ensure reliable data generation, secure transmission and efficient data aggregation is a problem to be solved in wireless sensor network security when making data acquisition, transmission, fusion and cooperative control perception in wireless sensor network [1,18].

With the continuous updating and enrichment of dynamic Web, the network has become a necessary platform for people to produce and live. A lot of the key information of finance, economy, and military must be transmitted and stored through the network [12,24]. In this regard, network security has become a very concerned topic. The root of network security is the active detection and interception. In

2010 Mathematics Subject Classification. 51A40.
Key words and phrases. Wireless network, intrusion interference signal, detection.
* Corresponding author: Li Gang.
large-scale integrated Internet, network intrusion signals show diversity and non-Gauss characterization. Therefore, anomaly detection and recognition of large-scale network intrusion signals in dynamic Web are needed. Through analyzing, filtering and detecting the characteristics of intrusion signals, and integrating them in the network security platform, it is necessary to achieve network intrusion interception and ensure network security [8, 20]. In the current detection algorithms, the network intrusion detection algorithms mainly adopt the nonlinear time series analysis algorithm. Because the network intrusion signal is non-stationary, the traditional time series analysis algorithm is difficult to effectively improve the detection probability, especially when the interference intensity is large, the detection accuracy will be limited.

In the network age, various types of network transmission data need to be fused and feature extraction processing. In this process, the network attack and the intrusion signal will be generated [5, 16]. Under the interference of complex network environment, the network attack and the characteristics of intrusion signal usually have high concealment, and have strong anti-interference ability. Therefore, it is difficult to identify and discover effectively by using the conventional signal detection algorithm [2, 14]. The purpose of this paper is to study the detection of network intrusion signals in complex and multi-interference conditions, which is of great significance to the field of network security.

2. An optimal detection algorithm for complex intrusion interference signals in mobile wireless network.

2.1. Removal of the interference in mobile wireless network. After wavelet decomposition of mobile network composite signals, the wavelet coefficient (signal energy) of the useful signal is greater than that (signal energy) of the noise. In this paper, we propose a suitable threshold value (reference value) to make thresholding the wavelet coefficients obtained by the decomposition. If the wavelet coefficient is less than the reference value, it is set to zero; if the wavelet coefficient is larger than the reference value, it is retained. In this way, the noise is removed, and the processed wavelet coefficients are used to reconstruct the wireless network signal.

Supposing the mixed signal of the mobile wireless network is \( f(t) \), then there is

\[
f(t) = x(t) + n(t)
\]  

(1)

Where, \( x(t) \) represents the original signal and \( n(t) \) represents the dual mode noise signal. According to the calculation of the formula (1), the process of restoring the useful signal in the mixed signals can be expressed as:

\[
Y = W(f) = D(Y, \lambda) = W(R)^{-1}
\]  

(2)

Where, \( W(f) \) represents the wavelet transform, \( W(R)^{-1} \) represents the inverse wavelet transformation, \( D(Y, \lambda) \) represents the thresholding of the wavelet coefficient, and \( \lambda \) represents the threshold.

In wavelet de-noising, threshold function is an indispensable part of wavelet de-noising. The soft and hard threshold functions in wavelet re defined as follows:

The hard threshold function is:

\[
\hat{w}_{j,k} = \begin{cases} w_{j,k} & |w_{j,k}| > \lambda \\ 0 & \text{others} \end{cases}
\]  

(3)
An Optimization Detection Algorithm

Figure 1. hard and soft threshold functions

\[ \hat{w}_{j,k} = \begin{cases} 
\text{sign}(w_{j,k}) & |w_{j,k}| > \lambda \\
0 & \text{others}
\end{cases} \]  

Where, \( \hat{w}_{j,k} \) represents the wavelet coefficient after processing, and \( w_{j,k} \) represents the wavelet coefficient. The hard and soft threshold functions are shown in Figure 1.

According to Figure 1, we can see that in range of \([-\lambda, \lambda]\), the hard threshold function and the soft threshold function set the noise’s wavelet coefficient to zero. In the range of \((\lambda, \infty)\) and \((-\infty, \lambda)\), the hard threshold function and the soft threshold function retain and construct the useful signal’s wavelet coefficient. The disadvantage of hard threshold function is that the function is discontinuous, and it is too sensitive to data changes [9]. It will generate oscillation when reconstructing the signal. Although the continuity of soft threshold function is good, shrinkage treatment will affect the approximation degree of reconstructed signal [15, 19]. In view of this, a new threshold function is designed on the basis of the hard and soft threshold functions above, and the control factor is introduced to control the shape of the function. The expression is:

\[ \hat{w}_{j,k} = \begin{cases} 
w_{j,k} - \lambda + w_{j,k} \cdot \lambda \cdot \mu & w_{j,k} > \lambda \\
w_{j,k} \cdot (1 + w_{j,k}) \cdot \mu & 0 < w_{j,k} < \lambda \\
-w_{j,k} \cdot \lambda \cdot \mu & -\lambda < w_{j,k} < 0 \\
w_{j,k} + \lambda - w_{j,k} \cdot \lambda \cdot \mu & w_{j,k} < -\lambda
\end{cases} \]  

Where, \( \mu \) represents the control factor. According to the formula (5), the value of \( \hat{w}_{j,k} \) is between \(|w_{j,k}| - \lambda\) and \(|w_{j,k}|\). The new threshold function curve is shown in Figure 2.

The analysis of Figure 2 shows that the control factor is used to control the shape of the control function, that is, the attenuation degree of the control function curve. The larger the \( \mu \) is, the slower the attenuation is. When \( \mu = 0 \), the new threshold function is equal to the soft threshold function [10]. The curve of the new threshold function is smooth and continuous, and the constant error is less than the soft threshold function. It has higher approximation ability, and its continuity
Figure 2. Improved threshold function

![Improved threshold function](image)

Figure 3. Selection rules of wavelet function and threshold

![Selection rules of wavelet function and threshold](image)

is the best. When the control factor $\mu$ increases or decreases, the curve of the new threshold function becomes steeper and smooth [3, 13].

To sum up, the wavelet function and threshold are selected and the rules selected are shown in Figure 3.

In the case of complex noise interference in mobile wireless network, the general formula $\lambda = \sqrt{2 \ln N}$ of threshold is used, and different thresholds $\lambda$ are applied in accordance with different decomposition scales.

$$\lambda_j = \frac{\sqrt{2 \ln N}}{\ln (j + 1)}$$  \hspace{1cm} (6)

Where, $j$ represents the decomposition scale and $N$ represents the number of decomposition layers.

The threshold is determined by using the formula (5), and the thresholding of the high frequency coefficient is realized. The reconstructed signal obtained by the
wavelet decomposition is as follows:

$$\tilde{f} (t) = \frac{\lambda_j \ln (j + 1)}{x (t)}$$ (7)

Where, $\tilde{f} (t)$ represents the reconfigurable signal of the mobile wireless network.

2.2. Feature extraction of complex interference signal in mobile wireless network. In order to improve the detection quality of intrusion interference signal in a mobile network, on the basis of Section 2.1, using probability statistics algorithm, a new sequence is composed of the spectral amplitude corresponding to the same frequency of each random variable in a random process and the spectrum matrix of intrusion interference signal is formed to obtain the spectrum distribution law of instantaneous interference of fixed frequency signal, so as to extract the characteristic spectrum of intrusion interference signal; The detailed steps are as follows:

It is assumed that, $X$ represents a random variable cluster consisting of $n'$ intrusion signals, $y'$ represents the frequency range of each cluster, and $n_{dj}'$ represents a constant threshold of a certain noise energy. A new sequence can be composed of the frequency spectrum values corresponding to the same frequency of random variables in a random process, and it is expressed as follows:

$$a' = \frac{n_{dj}' * y'}{n' + f g_{dj}' * X}$$ (8)

Where, $f g_{dj}'$ represents the spreading sequence.

It is assumed that $c_{f j}'$ represents the limited additivity of the probability of the network intrusion interference signal. In the random process $M'$ composed of the spectrum sequence of the network intrusion interference signal, with the increase of the random variable $M'_{wert}$, the probability of the corresponding spectrum amplitude will also increase. The formula (9) is used to construct the spectrum matrix of the network intrusion interference signal:

$$X (f) = \frac{M'_{wert} + M'_{f j} * f_0 + L * a'}{i (2\pi f_0)}$$ (9)

Where, $L$ represents the linear frequency modulation rate, $f_0$ represents the initial frequency, and $i$ represents the sampling period of the intrusion interference signal.

Assuming that $l'$ represents the amplitude corresponding to the same frequency, $g'$ represents the rate of the direct spreading pseudorandom code, and $b'$ represents the amplitude corresponding to the same frequency. $s'$ represents the total frequency of all the amplitudes at all frequencies, and $b_{em}'$ represents the spectrum distribution law of the instantaneous interference of the fixed frequency signal. Formula (10) is used to calculate $s'$.

$$s' = \frac{b_{em}' + b'}{g'} \otimes [l' \oplus i]$$ (10)

According to the formula (10), the statistical characteristics of the spectrum of the network intrusion interference signal at all time are calculated.

$$v' = \frac{a' + s' * X (f) b_{x_{npp}} * v}{s'}$$ (11)
Where, \( b'_{xnp} \) represents the changing state of the position of the signal, and \( v \) represents the extraction coefficient of the intrusion signal.

In summary, in the process of optimizing the detection of the intrusion interference signal in mobile network, the probability statistics algorithm is used to form a new sequence by the spectrum amplitude of the same frequency corresponding to the random variables in the random process, and the spectrum matrix of communication intrusion interference signal is established to obtain the spectrum distribution law of instantaneous interference fixed frequency signal, so as to extract the characteristics spectrum of communication intrusion interference signal, laying the foundation for realizing the optimal detection of the interference signal of the communication human in the mobile network.

2.3. Complex intrusion signal detection in the network based on wavelet packet frequency hopping estimation. Based on the extraction characteristics of the intrusion interference signal in Section 2.2, the wavelet packet frequency hopping estimation is used to detect the complex intrusion interference signal. The Fourier transform of a priori detected intrusion signal in large-scale integrated network is carried out, and the line spectrum of the intrusion interference signal is decomposed into:

\[
F(n) = \frac{1}{2\pi m} \otimes (\phi * m) \quad (12)
\]

Where, \( m \) represents the number of decomposition layers and \( \phi \) represents the decomposition coefficient.

The structure of the actual intrusion signal channel is judged by the calculation of the formula (12). Combined with the characteristics of the intrusion signal obtained in Section 2.2, the wavelet packet frequency hopping estimation method is used to detect the intrusion features. Based on the empirical mode decomposition of the network intrusion signals, it can get a set of two-dimensional functions of time scale \( A \) and time translation \( B \) that represent the internal detail features of the network intrusion signal.

\[
F(t) = \frac{|F(n)|}{A*B} \quad (13)
\]

Based on the formula (13), the wavelet packet frequency hopping is used to estimate the network intrusion signal by the wavelet function as the mother wavelet \( \psi(t) \). At the time frequency, the wavelet packet frequency hopping is estimated, and the sample estimation value of the network intrusion signal is obtained by rotating any phase angle.

\[
\tilde{r}(\tau) = \tilde{r}_s(\tau) + r_s(\tau) \quad (14)
\]

\[
\tilde{c}(\tau) = \tilde{c}_s(\tau) + c_s(\tau) \quad (15)
\]

Where, \( c_s(\tau) \) and \( r_s(\tau) \) represent the characteristic value of Gauss white noise and diagonal four-order relaxation cumulants, and \( \tilde{r}_s(\tau) \) and \( \tilde{c}_s(\tau) \) represent the characteristic value of weighted Gauss white noise and diagonal four-order cumulants.

According to the above, the \( K \)-order moment of complex intrusion interference signal is recorded as \( m_K(\tau_1, \tau_2, \ldots, \tau_{K-1}) \). The \( K \)-order joint moment of the random variable’s Gauss probability density characteristics of the complex intrusion signal is defined. Assuming that unilateral exponential random characteristic coefficient \( \eta \) is constant, the wavelet structure characteristics of network intrusion
signal is to obtain by using observation means. Using the state probability density transfer, the four-order cumulant slices of the output are as follows:

$$cum (\eta_1, \eta_2, \cdots , \eta_K) = \prod_K \eta_{mK}$$ (16)

The energy equilibrium algorithm is used to simulate the Gauss random wavelet characteristics of abnormal intrusion signals. Using the Gauss additivity of the high order cumulant of the abnormal intrusion signal, the amplitude frequency response of the network intrusion detection is obtained as follows:

$$cum (z_K) = cum (m_K (\tau_1, \tau_2, \cdots , \tau_{K-1})) \frac{\hat{c} (\tau)}{\hat{r} (\tau)} * \zeta$$ (17)

Where, $\zeta$ represents the control threshold of network intrusion detection. The threshold is between $[1,18]$, and the optimal detection effect can be obtained $[7,21]$. 

2.4. Location of complex intrusion interference signal in network. According to the detection results of network intrusion signals in Section 2.3, the three edge centroid positioning algorithm is used to locate the detection results. Firstly, TDOA distance measurement is carried out, and the principle of distance measurement is shown in Figure 4.

After receiving the information and ultrasonic signals of multiple mobile anchor nodes by the node to be located, the distance between each virtual coordinate point and the nodes to be located is calculated according to the principle of distance measurement in Figure 4 $[4,7]$. There are coordinates, the different points to be located and the unknown point $p$ in the plane. It is known that the coordinate location of the first $D_1$ points are $(\varsigma_1, \xi_1), (\varsigma_2, \xi_2), \ldots, (\varsigma_p, \xi_p)$ and the distance to the positioning point of $p$ is $d_1, d_2, \ldots, d_p$, then any two points can be obtained from a coordinate point to the first $p$ points. The distance between $(\varsigma_{J}, \xi_{J})$ is equal to $d_{I}$ and $d_{J}$. In the solved coordinates, the point $d_{I}$ of the distance closest to $(\varsigma_{I}, \xi_{I})$ is called the located near point of $(\varsigma_{J}, \xi_{J})$ $[6,22]$.

According to the above content, the calculated coordinates may have two points, a point or nothing. When the solution is two points, assuming that these two points are $(\varsigma, \xi)$ and $(\varsigma', \xi')$, the distance between $(\varsigma, \xi)$ and $(\varsigma_{I}, \xi_{I})$ is closer to $d_{I}$ than that of $(\varsigma', \xi')$ and $(\varsigma_{I}, \xi_{I})$, while point $(\varsigma, \xi)$ is the nearest point of point $D_1$ about $(\varsigma_{I}, \xi_{I})$.
and \((\varsigma_j, \xi_j)\). When the node does not exist, the near point of point D1 about \((\varsigma_1, \xi_1)\) and \((\varsigma_j, \xi_j)\) do not exist.

To sum up, the three point location algorithm of network intrusion interference signal is described by using Figure 5.

In Figure 5, the anchor nodes A1 and C1 are selected to solve the coordinate point \((\varsigma_3, \xi_3)\) and \((\varsigma_4, \xi_4)\). Anchor node B1 is used to determine which one of these two points is the positioning near point of node D1 about A1 and C1 [11, 23]. Node D1 stores the result of judgement. Anchor nodes B1 and C1 are selected to solve \((\varsigma_5, \xi_5)\) and \((\varsigma_6, \xi_6)\). The positioning near point of D1 about B1 and C1 are judged by using anchor node A1, and the judged results are stored by the node D1 to be located.

According to the location instructions in Figure 5, we can find out three location near points of the location point D1 to be located. Supposing that the location near point of D1 is \((\varsigma_2, \xi_2)\), \((\varsigma_3, \xi_3)\) and \((\varsigma_6, \xi_6)\), then point 2, 3 and 6 are the nearest points of D1, it can find out the line segment constituted by the three points (three points on the same line) or the centroid \((\varsigma', \xi')\) of the triangle, that is the location coordinate of the three edge centroid positioning algorithm used for the node D1 to be located.

\[
\varsigma = \frac{\varsigma_2 + \varsigma_3 + \varsigma_6}{3} \quad (18)
\]

\[
\xi = \frac{\xi_2 + \xi_3 + \xi_6}{3} \quad (19)
\]

Where, \(\varsigma\) and \(\xi\) represent the transverse ordinates of the location.

3. **Experimental results and analysis.** In order to test the performance of the intrusion signal detection under the interference of complex network, an experiment is carried out to test the algorithm designed in this paper. The experimental platform is built on MATLAB. The experimental data are based on the attack data of the KDD CUP99 intrusion detection system, which is established by the Massachusetts Institute of Technology and the Department of defense of the United
States. 30000 network access records are used for experiment, of which 20000 are normal access and 10000 are intrusion data. The experimental model is shown in Figure 6. The experiment will verify the proposed algorithm in the following aspects.

(1) The effect of the proposed algorithm on the denoising of mobile wireless network;
(2) The effect of the proposed algorithm on the feature extraction of intrusion interference signal.
(3) The effect of the proposed algorithm on the detection of intrusion interference signal.
(4) The effect of the proposed algorithm on the location of intrusion interference signal.

The results of the experiment are as follows:

The experimental results of Figure 7 show that the denoising effect of this algorithm is better than that of the traditional algorithm. In this paper, it is proposed that a suitable threshold can be selected to make thresholding for the wavelet coefficient obtained by the decomposition. If the wavelet coefficient is less than the reference value, it is set to zero; if the wavelet coefficient is larger than the reference value, it is retained. In this way, the noise in the wireless network is removed, and the processed wavelet coefficients are used to reconstruct the wireless network signal, so that the overall denoising effect of the proposed algorithm is better than that of the traditional algorithm.

As shown in Figure 8, the closer to 1 the coefficient of the extracted network intrusion features is, the better the extraction effect is. In the proposed algorithm, the probability statistics algorithm is used to form a new sequence by the spectrum amplitude of the same frequency corresponding to the random variables in the random process, and the spectrum matrix of communication intrusion interference signal is established to obtain the spectrum distribution law of instantaneous interference fixed frequency signal, so as to extract the characteristics spectrum of
The effect of the traditional algorithm on the denoising of wireless network communication intrusion interference signal. Thus, the feature extraction coefficient of intrusion signal is enhanced, and compared with the traditional algorithm, the proposed method has more advantages.

Figure 10 is a running wave of mobile wireless network. Using different location algorithms to locate the intrusion interference signal, the location effects of different algorithms are observed.

The analysis of the experimental results of Figure 9 and 10 shows that the proposed algorithm is superior to the traditional algorithm in intrusion signal detection and intrusion signal location. The algorithm in this paper takes the wireless network denoising as the premise, and uses the wavelet packet frequency hopping estimation method to detect the complex interference signal through the feature...
(a) The effect of the traditional algorithm on the feature extraction of wireless network intrusion signal

(b) The effect of the proposed algorithm on the feature extraction of wireless network intrusion signal

**Figure 8.** Comparison of the effect of different algorithms on the feature extraction of wireless network intrusion signal

extraction of the intrusion signal. The energy balance algorithm is used to simulate the Gauss random small change characteristics of abnormal intrusion signal. Using the Gauss additivity of the high-order cumulant of the network anomaly intrusion signal, the network intrusion detection output can be obtained, and the detection precision can be greatly improved. After the three edge centroid positioning algorithm to locate the intrusion signal, the reliability of the proposed algorithm is improved.

4. **Conclusions.** The wireless sensor network is developing intelligently, general-purpose and easy to use. The research on intrusion detection and location technology for wireless sensor network is a major direction in the intelligent development of
wireless sensor network. Through the denoising of the network channel, the feature extraction, detection and location of the network intrusion signal, the high-precision network intrusion detection is realized. But there are still the following contents, which need to be further improved in the future work:

(1) The performance of intrusion detection system needs to be improved, the detection ability of system to resist intrusion needs to be enhanced, and the resource consumption of intrusion detection system should be reduced.

(2) The response after the detection of the intrusion signals should be studied.
(a) The effect of the traditional algorithm on the location of the intrusion signal

(b) The effect of the proposed algorithm on the location of the intrusion signal

Figure 10. Comparison of the effect of different algorithms on the location of intrusion signal

REFERENCES

[1] M. A. Ambussaidi, X. He, P. Nanda and et al, Building an intrusion detection system using a filter-based feature selection algorithm, IEEE Trans. Comput., 65 (2016), 2986–2998.

[2] M. Andreolini, M. Colajanni and M. Marchetti, A Collaborative Framework for Intrusion Detection in Mobile Networks, Information Sciences, 2015.

[3] M. Arthur and K. Kannan, Cross-layer based multiclass intrusion detection system for secure multicast communication of manet in military networks, Wireless Networks, 1035–1059.

[4] G. Brinkmann, M. Preissmann and D. Sasaki, Snarks with total chromatic number 5. maloney, g.r. 2015. on substitution tilings of the plane with n-fold rotational symmetry, Discrete Mathematics and Theoretical Computer Science, 17 (2015), 369–382.

[5] K. A. P. Costa, L. A. M. Pereira, R. Y. M. Nakamura and C. R. Pereira, A nature-inspired approach to speed up optimum-path forest clustering and its application to intrusion detection in computer networks, Information Sciences, 294 (2015), 95–108.

[6] Y. H. Q., Network intrusion small signal detection model based on optimization particle swarm algorithm, Bulletin of Science and Technology, 193–195.

[7] L. I. Hui-Fang and X. G. Peng, Mobile intelligent terminal intrusion detection method based on cloud computing, Computer Simulation, 380–384.

[8] A. Khalili and A. Sami, Sysdetect: A systematic approach to critical state determination for industrial intrusion detection systems using apriori algorithm, Journal of Process Control, 32 (2015), 154–160.

[9] D. Kim, The development of ‘water strider’ inquiry learning program for improving scientific inquiry learning ability in the chapter ‘the little creatures world’ of the korea elementary school 5th grade science textbook, Eurasia Journal of Mathematics Science and Technology Education, 13 (2007), 3325–3348.
[10] Z. Lin and J. R. Wang, New riemann-liouville fractional hermite-hadamard inequalities via two kinds of convex functions, *Journal of Interdisciplinary Mathematics*, 20 (2017), 357–382.
[11] S. Masarat, S. Sharifian and H. Taheri, Modified parallel random forest for intrusion detection systems, *Journal of Supercomputing*, 2235–2258.
[12] A. Milenkoski, M. Vieira, S. Kounev, A. Avritzer and B. D. Payne, Evaluating computer intrusion detection systems: A survey of common practices, *Acm Computing Surveys*, 48 (2015), 1–41.
[13] D. Moon, S. B. Pan and I. Kim, Host-based intrusion detection system for secure human-centric computing, *Journal of Supercomputing*, 72 (2016), 2520–2536.
[14] M. N., D. R. and D. S. K., A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks, *IEEE Transactions on Vehicular Technology*, 120 (2017), 1684–1695.
[15] P. Nader, P. Honeine and P. Beauséjour, Online one-class classification for intrusion detection based on the mahalanobis distance, *Journal of Materials Science*, 23 (2015), 1260–1264.
[16] M. M. Rathore, A. Ahmad and A. Paul, Real time intrusion detection system for ultra-high-speed big data environments, *Journal of Supercomputing*, 72 (2016), 3489-3510.
[17] D. Samfat and R. Molva, Idamn: An intrusion detection architecture for mobile networks, *IEEE Journal on Selected Areas in Communications*, 15 (1997), 1373–1380.
[18] E. Vasilomanolakis, S. Karuppayah and M. Fischer, Taxonomy and survey of collaborative intrusion detection, *Acm Computing Surveys*, 47 (2015), 1–33.
[19] E. Viegas, A. O. Santin, A. Franca, R. Jasinski, V. A. Pedroni and L. S. Oliveira, Towards an energy-efficient anomaly-based intrusion detection engine for embedded systems, *IEEE Transactions on Computers*, 66 (2017), 163–177.
[20] B. W., J. A. and P. M., Improving network intrusion detection system performance through quality of service configuration and parallel technology, *Journal of Computer and System Sciences*, 48 (2015), 981–999.
[21] P. W., H. Q., M. X. J. and et al, A dynamic network threat assessment method based on multi-source information fusion, *Journal of China Academy of Electronics and Information Technology*, 17 (2010), 250–256.
[22] R. W. W., H. L. and Z. K., Intrusion alert correlation model based on data mining and ontology, *Journal of Jilin University (Engineering and Technology Edition)*, 899–906.
[23] X. Zhang and S. L. Yi, Green building evaluation methodology under ecological view, *Journal of Discrete Mathematical Sciences & Cryptography*, 20 (2017), 79–90.
[24] Q. Zhu, C. Fung, R. Boutaba and T. Basar, Guidex: A game-theoretic incentive-based mechanism for intrusion detection networks, *IEEE Journal on Selected Areas in Communications*, 30 (2012), 2220–2230.

Received July 2017; revised November 2017.

E-mail address: airleeg@163.com