Multimed Tools Appl (2016) 75:14281–14305
DOI 10.1007/s11042-016-3402-6

A traffic anomaly detection approach in communication networks for applications of multimedia medical devices

Dingde Jiang[1] · Zhen Yuan[1] · Peng Zhang[1] · Lei Miao[2] · Ting Zhu[3]

Received: 23 November 2015 / Revised: 3 February 2016 / Accepted: 23 February 2016 /
Published online: 7 April 2016

Abstract Anomalous or unnormal multimedia medical devices are to yield anomaly network traffic and affect the diagnosis about medical issues. How to find anomaly network traffic is significantly important for normal applications of multimedia medical devices. This paper studies traffic anomaly detection problem in large-scale communication networks with multimedia medical devices. We employ empirical mode decomposition method and wavelet packet transform to propose an accurate detection method to capture it. Firstly, we use the wavelet packet transform to pre-treat network traffic. Network traffic is decomposed into multiple narrowband signals exhibiting more detailed features of network traffic. Secondly, the empirical mode decomposition method is utilized to divide these narrowband signals into the intrinsic mode function at different scales, in time and time-frequency domains. We calculate the spectral kurtosis value of the intrinsic mode function at these different scales to remove false components of the empirical mode decomposition. As a result, we can obtain new time and time-frequency signals which highlight the hidden nature of anomaly network traffic. Thirdly, we perform the reconstruction of empirical mode decompositions and wavelet packet transforms for the above time and time-frequency signals to attain a series of new time signals. Then we can find and diagnose abnormal network traffic. Simulation results show that our method is effective and promising.

Keywords Multimedia communication · Empirical mode decomposition · Spectral kurtosis · Anomaly detection · Network traffic

✉ Dingde Jiang
jiangdingde@ise.neu.edu.cn

[1] School of Computer Science and Engineering, Northeastern University, Shenyang 110819, China

[2] Department of Engineering Technology, Middle Tennessee State University, Murfreesboro, TN 37132, USA

[3] Department of Computer Science, State University of New York, Binghamton, NY 13905, USA

1 Introduction

With the development of wireless communications and wearable technologies, multimedia communication networks, which connect a variety of multimedia medical devices, are currently being used for clinic and medical issues, such as smart hospital, smart clinic, smart rehabilitation at home and so forth [1, 31, 33, 58, 64]. Extensive applications of multimedia medical devices have generated huge network traffic. Anomalous or unnormal multimedia medical devices are to yield anomaly network traffic and affect the diagnosis about medical issues. How to find anomaly network traffic is significantly important for normal applications of multimedia medical devices. Anomaly network traffic describes abnormal actions and behaviors existing in large-scale multimedia communication networks. These abnormal actions often have an important impact on multimedia communication networks, such as degrading network performance and even disrupting networks [8, 23, 38, 49, 60, 61]. This directly damages the clinic and medical process. Currently, firewall or anti-virus software is not sufficient to protect the security of network data when it suffered network attack such as Distributed Denial of Service (DDoS) attacks and network worms. False and false negative alarms of intrusion detection system directly impact its detection credibility [3, 12, 13, 29, 37, 39, 54], resulting in network disruptions and communication interruption when network attacks happen. Hence, fast detecting traffic anomalies in the networks, estimating the cause of abnormal flow, and quickly taking correct countermeasures are important prerequisites for network management and network operation [15, 21, 36, 44, 46, 59, 63, 65]. Therefore, traffic anomaly detection in large-scale multimedia communication networks used for medial issues has become a significant research topic. In this paper, we are to propose a new method to overcome this problem.

However, to carry out accurate detection of traffic anomaly is a challenge. It is significantly difficult to identify correctly network traffic because it contains many inherent properties [2, 14, 30]. Its larger change often results in the faults and congestions of networks. Traffic estimation can help to capture and extract network traffic nature [3, 44]. Network traffic anomalies reveal the anomalous or malicious behaviors that appear in communication networks. Discovering network traffic anomalies is to effectively detect and diagnose these anomalous or malicious behaviors that damage the network [7, 42, 50, 62]. Anomalous and abnormal traffic is often much smaller in volume than the normal background network traffic, and is immerged into the huge background traffic. Therefore, this makes it hidden and indiscoverable. Moreover, some of anomalous traffic also has burst characteristics and distributed properties. All of the above characteristics increase the difficulties in detecting anomalous network traffic [5, 7, 42, 50].

To overcome these problems, many methods have been proposed to detect anomalous traffic in communication networks. Lakhina et al. adopted the Principal Component Analysis (PCA) method to detect and diagnose network-wide traffic anomalies [29]. Federico et al. used a α-stable first-order model and a generalized likelihood ratio test to identify network traffic anomalies [12]. Thatte et al. used aggregate traffic statistics to find network anomalies [50]. The signal processing is also often exploited to identify network traffic anomalies. Akgül et al. studied the periodicity-based anomalies in network traffic [2]. Nawata et al. used time-periodical packet sampling to perform unsupervised ensemble anomaly detection [42]. Celenk et al. used the adaptive Wiener filtering process and auto-regressive moving average model to capture network feature changes [7]. Barford et al. proposed a Deviation Score Anomaly Detection (DSAD) approach to find the specious part in network-wide traffic [5]. Vishwanath et al. studied the TCP traffic abnormal problem in routers with the smaller buffer [51]. Chhabra et al. presented a SPatial Anomaly Detection (SPAD) method [10]. Alternatively, Yu et al. studied the modeling, analysis, and countermeasures for worm attacks on communication networks [62]. Qin et al. exploited the bind source separation method to find the abnormal traffic components in the network [44]. Guan et al. studied the detection and measurement method for the dynamic changes in critical traffic patterns [14]. However, due to the hidden nature of anomalous network traffic, these methods have many difficulties to detect accurately them.

In this paper, we propose a new detection method for anomaly traffic in large-scale multimedia communication networks for applications of multimedia medical devices for medical issues, called joint Wavelet packet transform and Empirical mode decomposition [17, 20] and spectral kurtosis [41] analysis-based Anomaly Detection (WESAD). Firstly, for the traditional empirical mode decomposition, we present a modified empirical mode decomposition process to extract the hidden nature of network traffic. Secondly, due to the mode aliasing of empirical mode decomposition, the wavelet packet transform is employed to divide the network traffic into a series of narrowband signals. By performing this pre-treatment process, we can easily obtain lots of continuous sub-signals (namely narrowband signals) which hold the obvious local features of the time-varying network traffic. Consequently, this is helpful to overcome the limitation of empirical model decomposition. Thirdly, the empirical mode decomposition method is utilized to divide these narrowband signals into the intrinsic mode functions at different scales, in time domain and time-frequency domain, respectively. And then we calculate the spectral kurtosis values of the intrinsic mode functions at these different scales to remove the false components of the empirical mode decomposition. As a result, in time-frequency domain, we can obtain lots of new time-frequency signals which highlight the hidden nature of the anomaly network traffic, while in time domain, a series of the time sub-signals are obtained. According to empirical mode decomposition and wavelet packet transform, we carry out the reconstruction for the above time and time-frequency signals to attain a series of new time signals. And then, based on the new time signals, we perform joint feature extractions, identify the suspicious network traffic, and make out the accurate anomaly detection. Finally, we conduct a series of tests to validate our method. Simulation results show that our method is effective and promising.

The rest of this paper is organized as follows. We state the related work in Section 2. Section 3 introduces problem statement and empirical mode decomposition. Section 4 derives our detection model and algorithm. Section 5 discusses simulation results and perform further analysis. Finally, we conclude our work in Section 6.

2 Related work

Network traffic anomaly detections are an significantly important research topic in the current networking community. PCA approach could effectively detect the anomaly component in network traffic [29]. The α-stable first-order model also could find the anomalous network traffic [12]. The statistics analysis could extract network anomalies [50]. The time-periodical packet sampling was used to find the traffic anomaly [42]. The Wiener filtering process and auto-regressive moving average model could capture the unnormal changes in network traffic [7]. These methods could effectively find out the anomalous parts in network traffic. Different from them, our method uses the empirical mode decomposition and wavelet packet transform to perform an accurate detection of network traffic anomalies. We use the wavelet packet transform to pre-treat the network traffic. Hence, we can accurately capture and exact the inherent characteristics of network traffic.

The deviation score was used to differentiate the difference between normal and anomalous parts in network traffic [5]. The spatial property was also exploited to refined and captured the anomalous changes of network traffic [10]. The bind source separation method to find the abnormal traffic components in the network [44]. These methods only analyzed the traffic properties in the time domain, while our method uses the time-frequency transform to attain the fine feature about network traffic. Our previous work also makes many researches for network traffic anomalies. The wavelet transform was used to capture the multi-scale characteristics in the time-frequency domain [28]. Compared to the normal network traffic, the anomaly traffic is much lower in volume. We analyzed the high-frequency property in the time-frequency by the wavelet transform [24]. The time-frequency analysis and deviation score approach were combined to capture the anomalous component of network traffic [22]. The network-wide perspective was exploited to the unnormal changes of network traffic in the transform domain [26]. We used the artificial neural network to estimate the end-to-end network traffic [25]. The time-frequency analysis was employed to attain the network traffic estimation [27]. Different from these previous work, in the paper, we first perform the pre-treating for network traffic. Then we can obtain the multiple narrowband signals which exhibit the more detailed features of network traffic. We use the empirical mode decomposition method to divide these narrowband signals into the intrinsic mode function at different scales, in time domain and time-frequency domain. In such a case, we can effectively attain the inherent nature of network traffic and perform the accurate detection.

Additionally, the distance, density, and the trend of density change of data were used to capture the inherent diversity property of network traffic [35]. The fuzzy c-means clustering (FCM) and Gaussian Mixture Model (GMM) were combined to reduce the computational complexity and guarantee clustering accuracy [34]. Roy et al. [45] surveyed current detection methods of network traffic anomaly. Xiong et al. [56] studied anomaly detection of cloud computing network traffic. Han et al. [16] used Empirical Mode Decomposition (EMD) to analyze network traffic. Huang et al. [18] used growing hierarchical self-organizing map to detect network traffic anomaly. Compared to these methods, we decompose the narrowband signals into the intrinsic mode function at different scales, in time domain and time-frequency domain, based on the empirical mode decomposition. The spectral kurtosis value of the intrinsic mode function at these different scales can be obtained to remove the false components of the empirical mode decomposition. In a result, our method has the more effective detection performance for network traffic anomalies.

Novakov et al. [43] exploited hybrid PCA-Haar Wavelet analysis to detect abnormal network traffic. Spognardi et al. [47] evaluated some main metrics proposed in the current literature using the real dataset. Won et al. [55] analyzed the longitudinal trendy of traffic anomalies for the trans-Pacific backbone network in 9 years from the long-term point of view, using the state-of-the-art anomaly detectors. Deng [11] proposed a modified instantaneous frequency algorithm and presented the corresponding traffic anomaly detection. Different from these methods, we use the empirical mode decomposition and reconstruction to extract the anomalous parts in the network traffic. We perform the more accurate analysis on the narrowband signals in terms of the intrinsic mode function at different scales.

Cheng et al. [9] used the wavelet analysis to detect and locate the network traffic anomaly. Sun et al. [48] used the Diffusion wavelets transform to analyze the traffic matrix and detect the traffic anomaly. Babaie et al. [4] used the unified manner to detect network anomalies. They exploited the spectral decomposition of a trajectory matrix to find the deviations from both between and within correlation present in the observed network traffic data. Wald et al. [52] used the Kyoto dataset to train and test the anomaly detection models proposed. They discussed several cases to validate their models and approaches. Marnerides et al. [40] surveyed the traffic anomaly detection approached in Internet backbone networks. Compared to these approaches, we combine the time-frequency transform and empirical mode decomposition to extract and diagnose the anomalous changes of network traffic. Our method makes the finer analysis in the multiple narrowband signals. Consequently, we can dig out the network traffic anomalies accurately.

3 Problem statement and empirical mode decomposition

Due to the time-varying and non-stationary characteristics of network traffic, it is difficult to describe accurately it [32, 53]. This is one of the main problems faced by network researchers and operators. To characterize and capture the anomaly network traffic, we are to take into account the empirical mode decomposition method [17] to decompose network traffic. By empirical mode decomposition, network traffic can be divided into different intrinsic mode function components. According to empirical mode decomposition theory [20], one can know that each intrinsic mode function component can truly reflect the true hidden information contained in network traffic. And each intrinsic mode function component is mutually orthogonal. Moreover, frequency and amplitude of each intrinsic mode function component can be modulated. After performing empirical mode decomposition, we can employ the different intrinsic mode function components to denote network traffic, where each intrinsic mode function component can be linear or nonlinear. In other words, we utilize empirical mode decomposition to decompose the network traffic into the orthogonal intrinsic mode function components.

As mentioned in [17], intrinsic mode function components are satisfied with the following constraints: The number of extreme points and zero-crossings must either equal or different at most by one; At each time point, the mean value of the upper envelope defined by the local maxima and the lower envelope defined by the local minima is zero. However, because of the complex properties of network traffic, it is significantly difficult to attain the intrinsic mode function components meeting the constraints above. Due to the characteristics of non-stationary and time-varying of network traffic, empirical mode decomposition method holds the problems of modal aliasing and false component when we directly extract characteristics of network traffic. Therefore, according to the traditional empirical mode decomposition [17, 19, 20], for network traffic $x(t)$, we propose the below empirical mode decomposition process:

Step 1: Set $r_0(t) = x(t)$, $i = 0$, and initialize the threshold a and the maximum iterative step K.
Step 2: Let $k = 0$, $h_{i+1,k}(t) = r_i(t)$, $s\_flag = 3$, $v = P$ (where $P \geq 0$), and let spline function $s(t)$ be a cubic spline.
Step 3: Find out local maxima and minima of the signal $h_{i+1,k}(t)$, and then use a $s(t)$ -based spline interpolation method to create two spline curve, namely the upper envelope $x_u(t)$ and lower envelope $x_l(t)$, where they go through all of the local maxima and minima of $h_{i+1,k}(t)$, respectively.

Step 4: Calculate the mean of the upper envelope and lower envelope by $m_{i+1,k} = (x_u(t) + x_l(t))/2$, and then set $h_{i+1,k+1}(t) = h_{i+1,k}(t) - m_{i+1,k}$.

Step 5: If $h_{i+1,k+1}(t)$ is satisfied with the conditions to be an intrinsic mode function component, go to Step 9.

Step 6: If $v > m_{i+1,k}$, then set $v = m_{i+1,k}$, $h(t) = h_{i+1,k+1}(t)$.

Step 7: if $s\_flag == 3$, then set the spline function $s(t)$ be a B-spline, $s\_flag = b$ and go back to Step 3.

Step 8: If $k \leq K$ and the following equation holds [46]:

$$\sum_{t=0}^{T} \frac{[h_{k-1}(t) - h_k(t)]^2}{{h_k}^2(t)} > a \tag{1}$$

set $k = k+1$, $s\_flag = 3$, and go back to Setp 3. or set $h_{i+1,k+1}(t) = h(t)$.

Step 9: Get the *ith* intrinsic mode function component $g_{i+1}(t) = h_{i+1,k+1}(t)$, and then set $r_{i+1}(t) = r_i(t) - g_{i+1}(t)$;

Step 10: If the residue $r_{i+1}(t)$ is not a monotonic function, then set $i = i+1$, and go back to Step 2. Or otherwise stop the empirical mode decomposition process and exit.

As mentioned in [17], after performing the above empirical mode decomposition process, we can decompose the network traffic $x(t)$ into a series of the orthogonal and independent intrinsic mode function component as follows:

$$x(t) = \sum_{i=1}^{m} g_i(t) + r_m(t) \tag{2}$$

where r_m is the residue component which represents the average trend of the signal $x(t)$, and m denotes the number of the functions.

According the modified empirical mode decomposition method proposed above, we use the multiple spline functions to overcome the limitation of using a single spline function. And we can get the optimal intrinsic mode function component according the above empirical mode decomposition process. Therefore, we can solve the problem that in fact the average of the envelopes separated from the actual signal components is not zero. By the above process, we can let the average value of the envelope be closer to zero. However, due to the characteristics of non-stationary and time-varying of network traffic, empirical mode decomposition method still has the problems of modal aliasing and false component. To overcome this problem, we combine the above proposed empirical mode decomposition process and wavelet packet transform to present our model and algorithm for the network traffic anomaly detection.

4 Detection model and algorithm

Here we use wavelet packet transform to pre-treat network traffic and decompose it into a series of narrowband signals with the same bandwidth at different scales. Different from [5], because of the low-, mid-, and high-frequency nature of anomaly network traffic, we use the smallest bandwidth at the small scales, large bandwidth at middle, and larger bandwidth at large. The ratio of the bandwidths at different scales is 1:2:4. The main cause doing so is that on the one hand, the abnormal network traffic is much smaller than the normal background traffic and is often submerged in the background traffic, and thus the abnormal network traffic hold the hidden nature and is significantly difficult to discover and extract. On the other hand, the normal background traffic is mainly gathered at the low frequency in contrast to middle and high frequencies. Figure 1 indicates the detection model used for the anomaly network traffic in this paper.

From Fig. 1, we can find that our detection model uses the wavelet packet transform to divide the network traffic into a series of narrowband signals. And then the above proposed empirical mode decomposition method is employed to decompose these narrowband signals into the intrinsic mode function components at different scales, in time domain and in time-frequency domain. As a result, we can correctly characterize the intrinsic characteristics of the network traffic so as to accurately descript and model it through this model. What follows is to discuss our detection algorithm.

4.1 Time-frequency analysis for network traffic

Here we exploit the wavelet packet transform to perform the time-frequency analysis. Different from other time-frequency analysis methods, wavelet packet transform can concurrently decompose the low- and high-frequency components of network traffic. Therefore, wavelet packet transform can obtain the more detailed feature components and thus can more accurately characterize the network traffic. The network traffic signal can be represented by a sequence of discrete time $x(t)$, where $t \in (1, N)$ and N is the length of the network traffic signal. Feature extraction based on wavelet packet transform exploits the principle of wavelet packet decomposition to realize orthogonal decomposition at different frequency bands; hereby signals with different frequency bands are obtained through decomposition at different scale j. As mentioned in [6, 57], let h_k and $g_k = (-1)^{k-1} h_{1-k}$ be a pair of conjugate mirror filters, and then wavelet packet transform can be defined as a family of functions determined by orthogonal scaling function $\phi(t)$, namely

$$\begin{cases} W_{2n}(t) = \sqrt{2} \sum\limits_{k \in Z} h_k W_n(2t-k) \\ W_{2n+1}(t) = \sqrt{2} \sum\limits_{k \in Z} g_k W_n(2t-k) \end{cases} \tag{3}$$

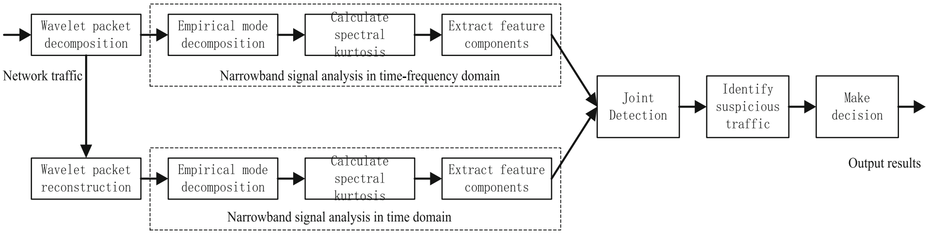

Wavelet packet decomposition
Empirical mode decomposition
Calculate spectral kurtosis
Extract feature components
Network traffic
Narrowband signal analysis in time-frequency domain
Joint Detection
Identify suspicious traffic
Make decision
Output results
Wavelet packet reconstruction
Empirical mode decomposition
Calculate spectral kurtosis
Extract feature components
Narrowband signal analysis in time domain

Fig. 1 Detection model for anomaly traffic in large-scale multimedia communication networks for medical issues

where $W_0(t) = \phi(t)$, $W_1(t) = \psi(t)$, and then,

$$\begin{cases} \phi(t) = \sqrt{2}\sum\limits_{k \in Z} h_k \phi(2t - k) \\ \psi(t) = \sqrt{2}\sum\limits_{k \in Z} g_k \phi(2t - k) \end{cases} \tag{4}$$

and n is the sampling number, k represents the spatial position information, $k = 1, 2, 3, \ldots n$. Function set $\{W_n(t)\}_{n \in Z}$ is determined by orthogonal scaling function $W_0(t) = \phi(t)$. Through wavelet packet decomposition, the coefficient of network traffic signal $x(t)$ in the subspace is $\{c_j^{n,k}\}$, namely

$$c_j^{n,k} = \int_R x(t) 2^{j/2} \overline{W_n(2^j t - k)} dt \tag{5}$$

therefore, in subspace Ω_{2n}^{j-1} and Ω_{2n+1}^{j-1}, there exists the follow equation [21]:

$$\begin{cases} c_{j-1}^{2n}[k] = \sum\limits_{l \in Z} \overline{h_{l-2k}} c_l^{n,j}[l] \\ c_{j-1}^{2n+1}[k] = \sum\limits_{l \in Z} \overline{g_{l-2k}} c_l^{n,j}[l] \end{cases} \tag{6}$$

Equations (3)–(6) denote the wavelet packet transform for the network traffic $x(t)$, where $c_{j-1}^{2n}[k]$ and $c_{j-1}^{2n+1}[k]$ indicate wavelet packet coefficients. In the wavelet packet transform, the scaling coefficient obtained by low-frequency filter shows profile information of network traffic signals, while wavelet coefficient obtained by high-frequency filter describes the details of network traffic signals.

Now we discuss the network traffic reconstruction from the wavelet packet transform. Without loss of generalization, for the given network traffic signal $x(t)$, $\{c_j^{n,k} : k \in Z\}$ is the wavelet packet coefficients of $x(t)$, which indicate the n wavelet packet on scale j. According to $\{c_{j-1}^{2n,k}, c_{j-1}^{2n+1,k} : k \in Z\}$ and time-frequency analysis theory, we can infer $\{c_j^{n,k} : k \in Z\}$ as follows:

$$c_j^{n,k} = \sum_{l \in Z} \left[h_{k-2l} c_{j-1}^{2n,k} + g_{l-2k} c_{j-1}^{2n+!,k} \right] \tag{7}$$

where $\{\mathrm{h}_k\}_{k \in Z} \in l^2(Z)$ are the coefficients of the low-pass filter and $\{\mathrm{g}_k\}_{k \in Z} \in l^2(Z)$ are the coefficients of the high-pass filter. According to Eq. (7), we can reconstruct the network traffic $x(t)$.

4.2 Feature extraction for narrowband signals

The Wavelet packet decomposition possesses the characteristic that when the decomposition scale increases, the widen spectrum window can further split the more detailed properties. More importantly, the wavelet packet decomposition can divide the higher frequency band. It can divide the given complex non-stationary network traffic signal into arbitrary band through a set of orthogonal low-pass filters h_k and high-pass filter g_k. In this paper, the purpose of introducing a pretreatment based on wavelet packet decomposition is to preferably portray the high-frequency information by decomposing wavelet space W_j.

To facilitate the following formulation, set

$$U_j^n = span\left\{2^{\frac{j}{2}} W_n\left(2^j t - k\right)\right\} \tag{8}$$

where $\{2^{-j/2} W_n(2^j t - k)\}$ denotes a wavelet library generated by scaling function $\phi(t)$ [6], and $span\{\cdot\}$ denotes all wavelet library in $\{2^{-j/2} W_n(2^j t - k)\}$ for $\forall\, k$. And then we hold the below equation:

$$\begin{cases} U_j^0 = v_j & j \in Z \\ U_j^1 = \mathrm{w}_j & j \in Z \end{cases} \tag{9}$$

where v_j and w_j denote the scaling and wavelet coefficients of wavelet transforms. Subspace $\{v_j\}_{j \in Z}$ and $\{w_j\}_{j \in Z}$ are constituted by scaling and wavelet functions, respectively. According to the multi-resolution analysis theory, we can get the formula $V_{j-1} = V_j \oplus W_j$. And then Eq. (8) can be denoted as [14]:

$$U_j^0 = U_{j+1}^0 \oplus U_{j+1}^1 \tag{10}$$

As mentioned in [6], the spatial decomposition of the wavelet packet transform can be expressed as:

$$U_j^k = U_{j+1}^{2k} \oplus U_{j+1}^{2k+1} \quad j \in Z, \;\; k \in Z^+ \tag{11}$$

where U_{j+1}^{2k} and U_{j+1}^{2k+1} are subspaces of U_j^k. In the theory of multi-resolution analysis, there is:

$$L^2(R) = \overset{+\infty}{\underset{j=-\infty}{\oplus}} \mathrm{W}_j$$

where U_j^k is expressed by W_j^k, then the below equation is obtained [6]:

$$W_j^k = U_j^k = U_{j+1}^{2k} \oplus U_{j+1}^{2k+1} \quad j \in Z, \;\; k \in Z^+ \tag{12}$$

In wavelet packet decomposition process, decomposing subspaces $\{V_j\}_{j \in Z}$ and $\{W_j\}_{j \in Z}$ obtained in multi-resolution analysis by binary format. The general expression of spatial decomposition of the wavelet packet can be expressed as:

$$W_j = U_{j+k}^{2^k} \oplus U_{j+k}^{2^k+1} \oplus \ldots \oplus U_{j+k}^{2^k+p} \tag{13}$$

where $k \neq 0, j \in Z, p = 2^k - 1$, and Z denotes the integer.

According to Eqs. (9)–(13), we find that by performing wavelet packet decompositions, network traffic signal is divided into a series of the continuous narrowband signals. As discussed in Section 2, although the modified empirical mode decomposition method proposed in this paper can better capture the network traffic characteristics, it still takes on the mode aliasing problem. To further overcome this problem, as denoted in our detection model in Fig. 1 here we use the modified empirical mode decomposition in Section 2 to decompose the narrowband signal generated by the wavelet packet transform.

Without loss of generality, assume that the network traffic $x(t)$ is decomposed with the M layers of wavelet packet transform and the sampling frequency is f_s. And then the bandwidth of each narrowband signal sequence generated by the wavelet packet decomposition on layer J is $f_s/2^{J+1}$, where $1 \leq J \leq M$. As a result, the original network traffic signal $x(t)$ is decomposed into

2^M narrowband signals $z_i(t)$ through wavelet packet decomposition, where $i = 0, 1, 2, \ldots, 2^M - 1$, namely

$$x(t) = \bigcup_{i=0}^{i=2^M-1} z_i(t), \quad i = 0, 1, 2, \ldots, 2^M-1 \tag{14}$$

where $z_i(t)$ corresponds to the $c_i[k]$ which is the wavelet packet transform coefficients.

According to Eq. (2) and the empirical mode decomposition method proposed in Section 2, we can obtain the following equation:

$$\begin{cases} c_0[k] & = & \sum_{i=1}^{m_0} g_{0i}[k] + r_{m_0}[k] \\ c_1[k] & = & \sum_{i=1}^{m_1} g_{1i}[k] + r_{m_1}[k] \\ \cdots & & \\ c_{2^M-1}[k] = \sum_{i=1}^{m_{2^M-1}} & g_{\left(2^M-1\right)i}[k] + r_{m_{2^M-1}}[k] \end{cases} \tag{15}$$

where r_{m_s} is the residue component denoting the average trend of signal $c_s[k]$, $g_{0s}[k]$ represents the intrinsic mode function component of signal $c_s[k]$, and $s = 0, 1, 2, \ldots, 2^M - 1$.

4.3 Spectral kurtosis analysis for intrinsic mode functions

The spectral kurtosis is defined as fourth-order spectrum accumulation of the normalized energy [41]. It can be used to measure the peak values of the probability density function of a process at a certain frequency. From the signal processing point of view, the spectral kurtosis can be interpreted as the kurtosis value calculated for the output of the ideal filter group at frequency f. Thus, the spectral kurtosis is sensitive to the transient components in a signal, and also can more accurately indicate which frequencies they are to occur at. In this paper, we use the spectral kurtosis method to calculate kurtosis values of the intrinsic mode function components denoted in Eq. (15). As a result, we can precisely position the anomaly network traffic.

For a signal $y(t)$, its Wold-Cramer decomposition [41] in frequency domain can be expressed as follows

$$y(t) = \int_{-\infty}^{+\infty} e^{j2\pi f t} H\left(t, f, \overline{w}\right) dX(f) \tag{16}$$

where $H\ (t, f, \overline{w})$ is the time-varying transfer function which represents the complex envelope of a signal $y(t)$ in time t and frequency f, $dX(f)$ is a spectral process of signal $x(t)$. As $H\ (t, f, \overline{w})$ is a random function, the shape of the envelope depends on the time-varying random variable $\overline{w}$. And then we can obtain the following equation:

$$S_{2nY}(t,f) = \frac{\left|H(t,f)dX(f)\right|^{2n}}{df} = \left|H(t,f)\right|^{2n} * S_{2nX}(t,f) \tag{17}$$

where $S_{2nY}(t,f)$ is the 2n-order instantaneous moments of signal $y(t)$ that indicates the energy contained in the complex envelope at time t and frequency f, $S_{2nX}(t,f)$ is the

2n-order instantaneous moment of signal $x(t)$. Equation (17) provides a theoretical basis for studying the time-frequency characteristics of a non-stationary process, which aggregate the average value of multiple outputs. And the 2n-order instantaneous moments $S_{2nY}(f)$ can be denoted as:

$$\begin{aligned} S_{2nY}(f) &= E\{S_{2nY}(t,f)\} \\ &= E\left\{\left|\mathrm{H}\left(t,f\right)\right|^{2n}\right\} * S_{2nX}(f) \end{aligned} \tag{18}$$

where E is expectation operator.

The network traffic can be regarded as a non-stationary process, and thus $c_s[k]$ in Eq. (15) generally hold this property. An important characteristic of the non-stationary process is non-Gaussian and the best statistics of this feature is the spectral accumulation. When spectrum cumulative amount is higher than or equal to the even-order moment of fourth-order, it has a non-zero value for non-Gaussian process. Fourth-order spectral cumulative amount $C_{4Y}(f)$ is defined as [41]:

$$C_{4Y}(f) = S_{4Y}(f) – 2S_{2Y}^2(f), \quad f \neq 0 \tag{19}$$

And then the spectral kurtosis $K_Y(f)$ defined as [41]:

$$\begin{aligned} K_Y(f) &= \frac{C_{4Y}(f)}{S_{2Y}^2(f)} = \frac{S_{4Y}(f)}{S_{2Y}^2(f)} -2 \\ &= \frac{E\{S_{4Y}(t,f)\}}{E\{S_{2Y}(t,f)\}^2} \text{ -2 }, \quad f \neq 0 \end{aligned} \tag{20}$$

From Eqs. (19)–(20), we can find that the stronger non-Gaussian the signal is, the larger the signal fourth-order spectral accumulation $C_{4Y}(f)$ is, and the higher spectral kurtosis $K_Y(f)$ is. Therefore, the transient abnormalities can be better detected from the signal through the spectral kurtosis value. This motivates us to detect the anomaly network traffic by calculate its spectral kurtosis value.

To accurately detect the anomaly network traffic, according to our detection model, we calculate the spectral kurtosis value of each intrinsic mode function component. And thus the transient information hidden in the intrinsic mode function components can be identified. Therefore, the more obvious the feature of the transient information contained in the frequency band is, the greater the spectral kurtosis $K_Y(f)$ of corresponding intrinsic mode function component is. And the spectral kurtosis is used to measure the energy spectrum amplitude and thus can easily describe the anomaly components in Eq. (15). Assume that $H(g_{sv}[k])$ represents the energy spectrum of the intrinsic mode function components $g_{sv}[k]$ in Eq. (15). According to Eq. (20), the spectral kurtosis value $J(g_{sv}[k])$ of each intrinsic mode function component $g_{sv}[k]$ can be attained as follows:

$$J(g_{sv}[k]) = \frac{mean\left((H(g_{sv}[k]))^2\right)}{\left(\left(mean(H(g_{sv}[k]))^2\right)\right)^2} - 2 \tag{21}$$

where $mean(.)$ denotes the average operator and $s = 0, 1, 2, \ldots, 2^M - 1$.

4.4 Detection algorithm

Now we are to derive our detection algorithm for the anomaly network traffic. Given a threshold α, if $J(g_{sv}[k])>\alpha$, then the corresponding intrinsic mode function component $g_{sv}[k]$ is chosen out according to Eq. (21). Repeating in such a way, we can obtain the j intrinsic mode function components within the given frequency band as follows:

$$I_{sj}=\left\{g'_{s1}[k],g'_{s2}[k],\ldots,g'_{sj}[k]\right\}\subset I_{sm} \tag{22}$$

where $I_{sm}=\{g_{s1}[k],\ldots,g_{sm}[k]\}$, $m=m_0,m_1,\ldots,m_{2^M-1}$, and notation ' is used to label a new variable value in set I_{sm}.

By Eq. (22), we can get the below equation:

$$c_s^j[k]=\sum_{q=1}^{j}g'_{sq}[k] \tag{23}$$

where $s\subset\{0,1,\ldots,2^M-1\}$. According Eq. (23), we can acquire the wavelet packet coefficients in the different frequency with the suspicious anomaly features. By Eq. (7), the following equation can be obtained:

$$\begin{cases} c_{j-M+1}^{n,k} = \sum\limits_{l\in Z}\left[h_{k-2l}c_{j-M}^{2n,k}+g_{l-2k}c_{j-M}^{2n+1,k}\right] \\ c_{j-M+2}^{n,k} = \sum\limits_{l\in Z}\left[h_{k-2l}c_{j-M+1}^{2n,k}+g_{l-2k}c_{j-M+1}^{2n+1,k}\right] \\ \ldots \\ c_j^{0,k} = \sum\limits_{l\in Z}\left[h_{k-2l}c_{j-1}^{0,k}+g_{l-2k}c_{j-1}^{1,k}\right] \end{cases} \tag{24}$$

As a result, we get the reconstructed time signal as follows:

$$\hat{x}_s(t)=c_j^{0,k} \tag{25}$$

where $\hat{x}_s(t)$ denotes the suspicious network traffic signal in the time domain corresponding to Eqs. (23)–(24).

Now we are to further decide whether $\hat{x}_s(t)$ has the anomaly components. As discussed in [29], we employ the 3δ method to make sure the detection threshold β. If the below equation holds:

$$\hat{x}_s(t)>\beta \tag{26}$$

then we the corresponding parts in $\hat{x}_s(t)$ is abnormal.

So far, we have discussed our whole algorithm. What follows is the detailed algorithm steps:

Step 1: Initialize the thresholds a and β, and give the network traffic signal $x(t)$.

Step 2: According to Eqs. (3)–(6), perform the wavelet packet transform, and get the sequences $c_s[k]$ where $s=0,1,2,\ldots,2^M-1$.

Step 3: For each $c_s[k]$, carry out the decomposition according to Eqs. (8)–(15) and the modified empirical mode decomposition algorithm proposed in Section 2. And then obtain the intrinsic mode function components $g_{sv}[k]$ for $c_s[k]$ where $s = 0, 1, 2, \ldots, 2^M - 1$ and $v = 1, 2, \ldots, m$, and $m \in \{m_0, m_1, \ldots, m_{2^M-1}\}$.

Step 4: Calculate the spectral kurtosis values of each intrinsic mode function component $g_{sv}[k]$ according to Eqs. (16)–(21). And get its spectral kurtosis value $J(g_{sv}[k])$.

Step 5: If $J(g_{sv}[k]) > \alpha$, the corresponding intrinsic mode function component is chosen. And get the selected intrinsic mode function component set $I_{sj} = \{g'_{s1}[k], g'_{s2}[k], \ldots, g'_{sj}[k]\}$.

Step 6: According to Eqs. (23)–(24), calculate out the time domain signal $\hat{x}_s(t)$.

Step 7: If Eq. (26) holds, the corresponding parts in $\hat{x}_s(t)$ is labeled as the abnormal network traffic.

Step 8: If all the wavelet packet components are performed according to the above steps, then save the results to the file and exit. Or otherwise go back to Step 2.

5 Simulation results and analysis

In this section, we are to discuss our algorithm performance and perform lots of numerical experiments to validate our method. To verify the effectiveness and feasibility of our detection algorithm WESAD, we exploit the traffic data from the real backbone network, namely the Internet2 network (http://www.internet2.edu/), as background traffic. Then three attacks are injected into the ground traffic to check and analyze the WESAD's detection performance. The Internet2 network mainly serves for education and research in America, which contains 12 router nodes, and thus has 144 origin–destination flows. According to the above discussion, we conduct a series of tests to validate WESAD algorithm. Moreover, we compare it with PCA [29], DSAD [5], SPAD [10] algorithms to analyze their detection performance.

5.1 Anomaly detection

Figure 2 plots out the network traffic with and without anomaly. We can find from Fig. 2 that the network traffic with anomaly is nearly same as the one without anomaly. And thus it is significantly difficult to directly detect and diagnose the abnormal network traffic. Moreover, the hidden nature of the anomaly network traffic further enhances the difficulty. Figures 3 and 4 indicate the wavelet packet coefficients of anomaly network traffic at different nodes. Although wavelet packet decompositions can characterize effectively the detailed parts in network traffic, Figs. 3 and 4 tell us that the wavelet packet coefficients are very time-varying. And at the different decomposition nodes, the wavelet packet coefficients of the abnormal network traffic describe the joint time-frequency properties. This is helpful to carry out the further analysis for network traffic in order to extract and capture abnormal components.

Figure 5 denotes the intrinsic mode function components of the anomaly network traffic after performing the empirical mode decomposition process according to our algorithm. We can easily see that the intrinsic mode function components illuminate the hidden nature and detailed parts. This demonstrates that our detection model and algorithm are feasible. Figure 6 plots out the detection results for the network traffic with and without anomaly, where the red dot line denotes the detection threshold and the cyan dot rectangle represents the abnormal network traffic parts. For the network traffic without anomaly, we can find that our method does not check out the abnormal

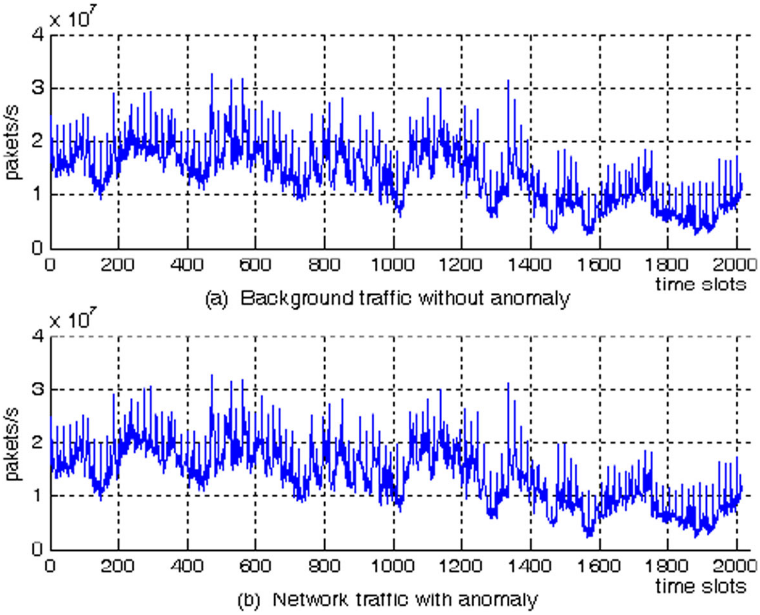


Fig. 2 Network traffic with and without anomaly

parts. This is reasonable and same as our expectation. For the network traffic with anomaly, Fig. 6 shows that our algorithm can accurately detect them. As shown in Fig. 6, our algorithm can correctly check and find out where the abnormal network traffic exists. More importantly, from Fig. 6, we also find that for the abnormal

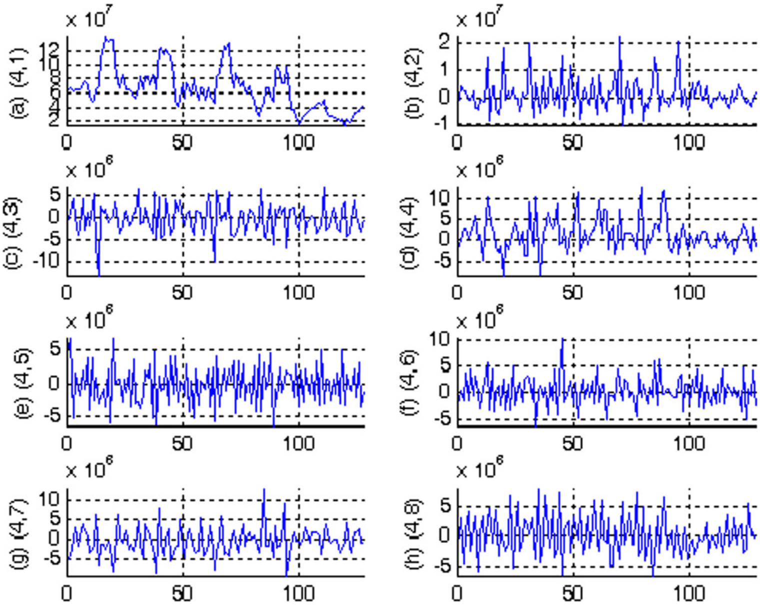


Fig. 3 Wavelet packet coefficients at different nodes, from (4,1) to (4,8)

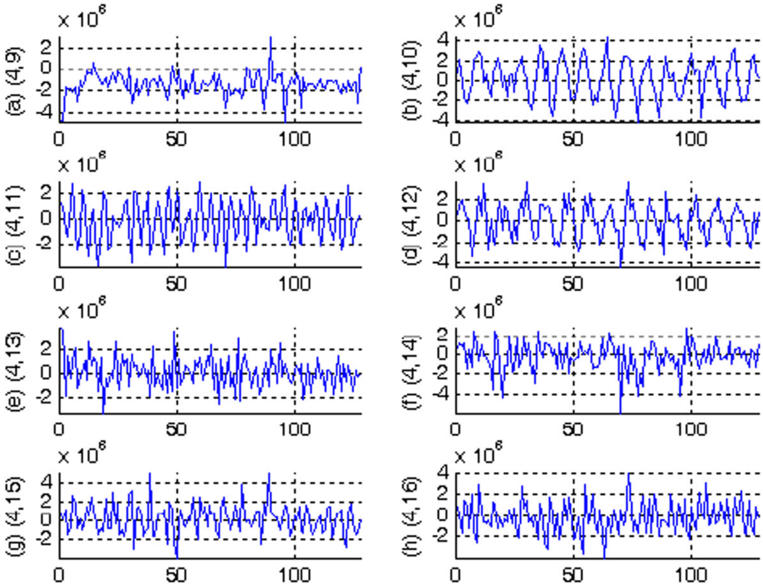


Fig. 4 Wavelet packet coefficients at different nodes, from (4,9) to (4,16)

network traffic, in contrast to the normal network traffic, the hidden abnormal features are highlighted by our method. And for the normal network traffic, we difficultly determine the appropriate threshold, while for the abnormal network traffic our algorithm can find the effective and feasible threshold to separate the anomalies. This

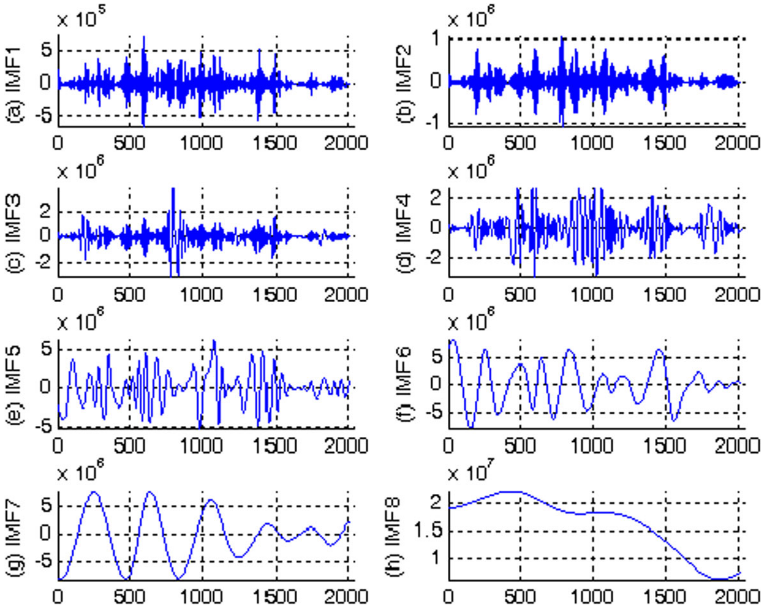


Fig. 5 intrinsic mode function components

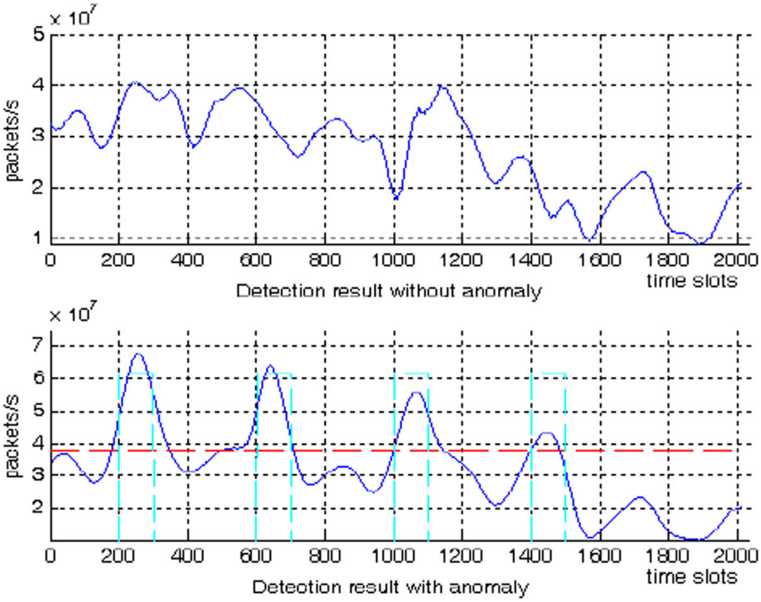


Fig. 6 Detection results for network traffic with and without anomaly

further illuminates that our model and algorithm can effectively detect and find the abnormal components in the network traffic.

5.2 Detection performance

To further validate our detection method, we now discuss and analyze its detection performance. What follows is to discuss the impact of the different anomaly windows and time slots on the detection accuracy of our algorithm. Figures 7 and 8 illustrate the detection results for the network traffic with the different anomaly windows and time slots, respectively, where the red dot line denotes the detection threshold and the cyan dot rectangle indicates the place where the abnormal network traffic exists. From Fig. 7, we can observe that although the time windows where the anomaly network traffic takes place are significantly different, our algorithm can accurately detect all anomaly parts in the network traffic. This demonstrates that our algorithm can diagnose the abnormal parts in the different anomaly time windows of network traffic. Figure 8 tells us that although the time points that the anomaly network traffic appears are very different, our algorithm can still find out the anomaly components in the network traffic. This further indicates that our algorithm can effectively and accurately check and detect the abnormal network traffic.

5.3 Comparative analysis

Now we discuss and analyze our algorithm WESAD and other three algorithms, namely PCA, DSAD, and PSAD. To show detection performance of four algorithms, we evaluate them with three attacks, where Attack 1, Attack 2, and Attack 3, denote low-frequency, medium-frequency, high-frequency, and mixed-frequency attacks, respectively, using the 7-week background traffic in the Internet2 network.

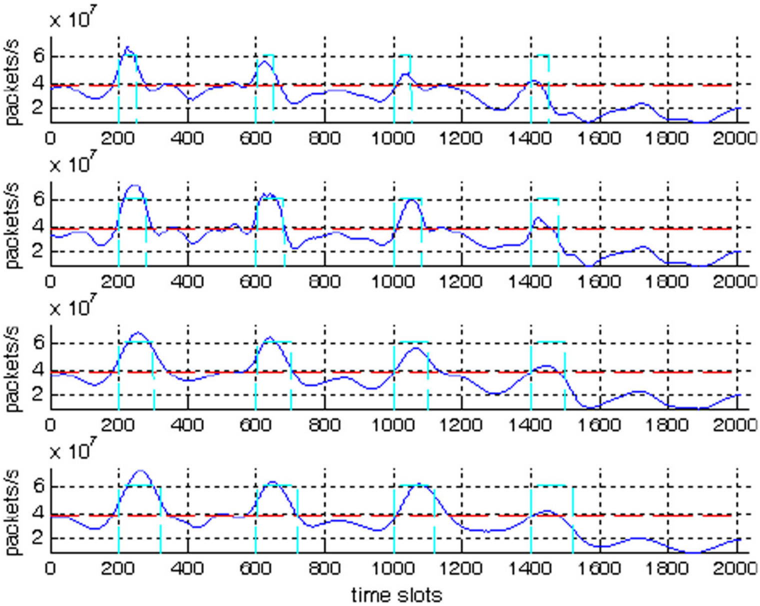


Fig. 7 Detection results with different anomaly windows

Figures 9, 10, and 11 describe the Receiver Operating Characteristic (ROC) curve of four detection algorithms for Attacks 1, 2, and 3, respectively. From Fig. 9, we can find that WESAD holds the best detection performance for Attack 1, SPAD is better, DSAD is worse, and PCA is the worst of all. Moreover, Fig. 9 indicates that the ROC curve of WESAD is far superior to that of the other three algorithms. When the false positive rate is 0.2, the true positive rates of WESAD, DSAD, SPAD, and PCA are about 0.97, 0.60, 0.50, and 0.46,

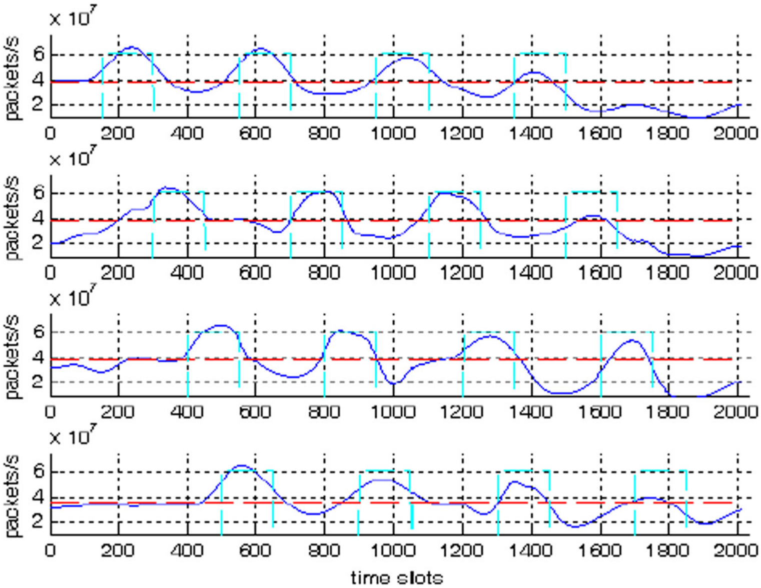


Fig. 8 Detection results with different anomaly time slots

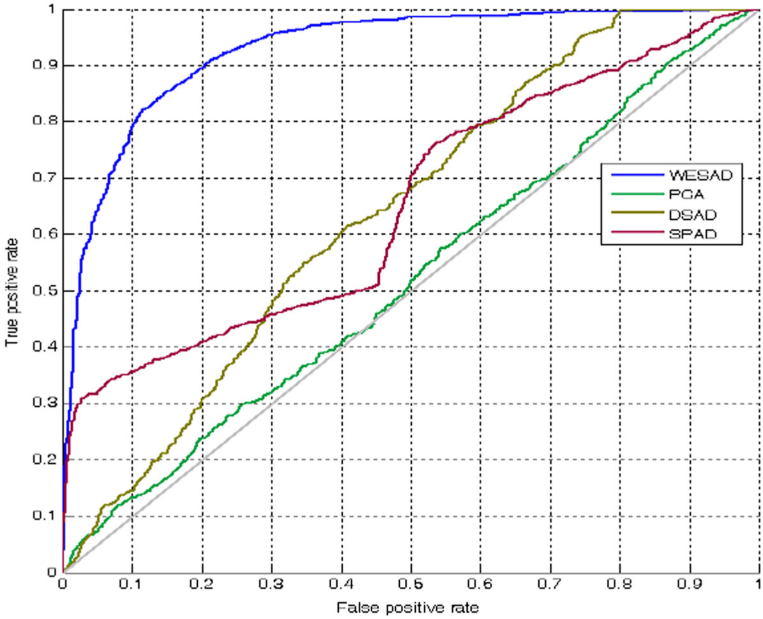


Fig. 9 ROC curve of detection algorithms for Attack 1

respectively. Figure 10 reveals that WESAD can make the most accurate detection for Attack 2 than the other three algorithms. When the false positive rate is 0.2, the true positive rates of WESAD, PCA, SPAD, and DSAD are approximately 0.96, 0.62, 0.58, and 0.29, respectively. Figure 11 expounds the different ROC curves of four detection algorithms for Attack 3. From

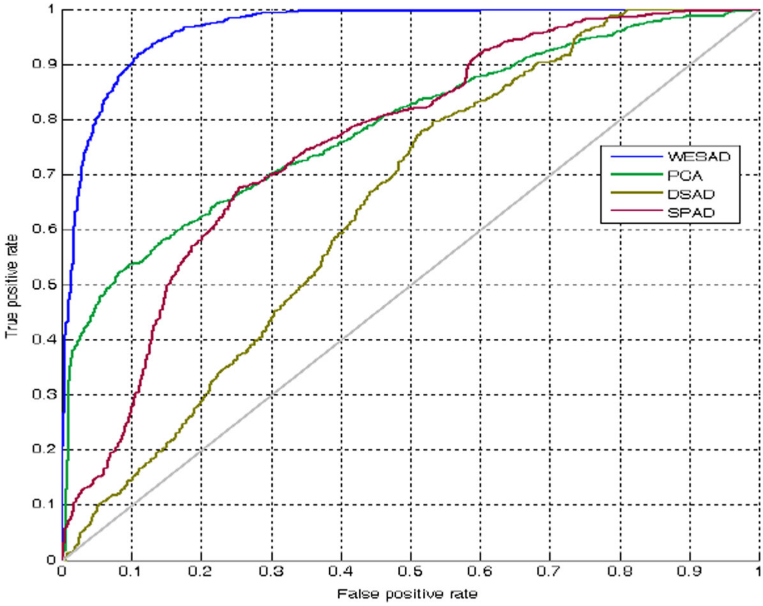


Fig. 10 ROC curve of detection algorithms for Attack 2

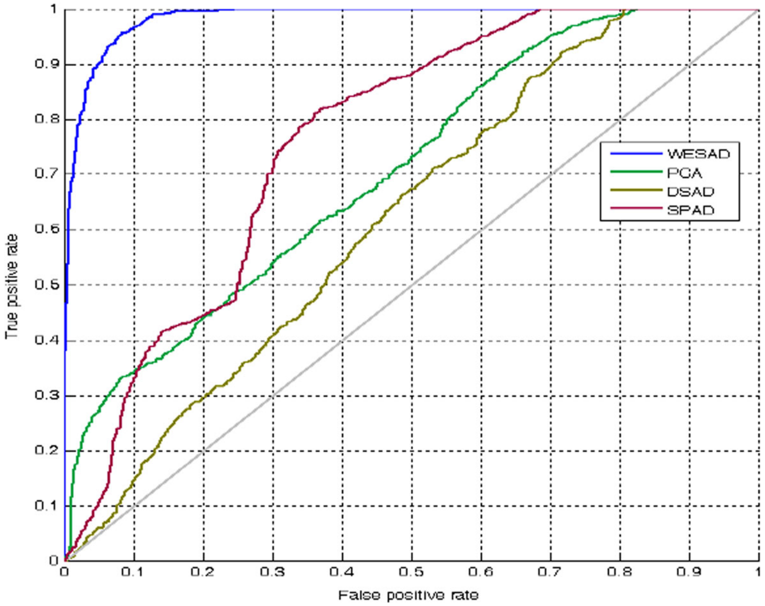


Fig. 11 ROC curve of detection algorithms for Attack 3

Fig. 11, we can find that when the false positive rate is 0.1, the true positive rates of WESAD, PCA, SPAD, and DSAD are 0.96, 0.35, 0.34, and 0.15 or so, separately. Therefore, Figures 10, 11, and 12 show that in contrast to other three algorithms, WESAD holds the best detection accuracy and ability.

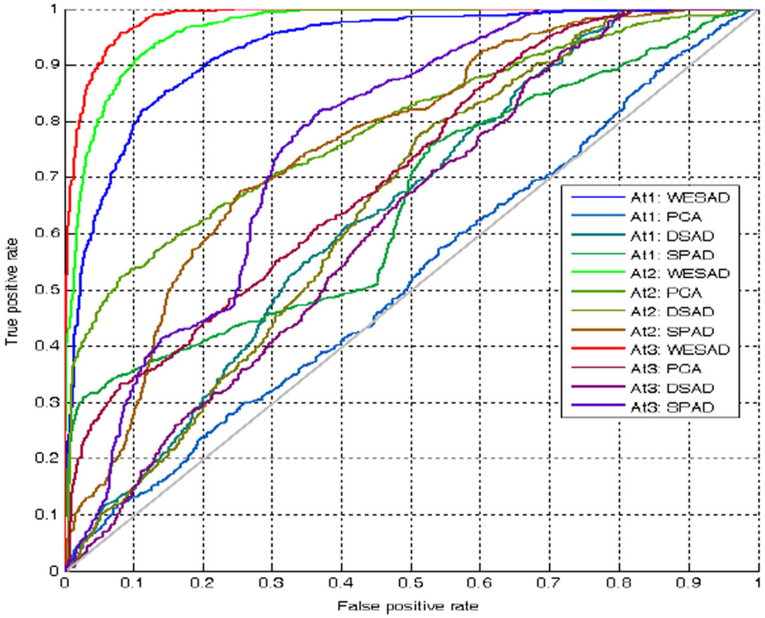


Fig. 12 ROC curve of detection algorithms for three Attacks

To elaborate detection performance of four algorithms more clearly, we plot out ROC curves of their detections for different attacks in Fig. 12, where $Ati-$ denotes network traffic with Attack i. Figure 12 states that for three attacks, WESAD always contains the largest true positive rate for the given false positive rate than other three algorithms. More importantly, as shown in Fig. 12, the ROC curve of WESAD for any attack is by far on top of those of other three algorithms. This further explains that WESAD exhibits accurate detection ability for anomaly network traffic.

6 Conclusions

This paper investigated traffic anomaly detection in large-scale multimedia communication networks connecting a variety of multimedia medical device for clinic and medical issues. By taking into account time-frequency analysis theory, we use the wavelet packet transform and empirical mode decomposition and spectral kurtosis method to propose a new anomaly detection method for network traffic. Due to the restriction of modal aliasing of traditional empirical mode decomposition, we present a modified empirical mode decomposition process to overcome this limitation. At the same time, we also consider to use the wavelet packet decomposition to solve further this shortcoming of empirical mode decomposition process. And then an anomaly detection model is proposed to identify the abnormal components in the network traffic. After carrying out the wavelet packet decomposition, we divide the network traffic into a series of narrowband signals. These narrowband signals are used to perform the modified empirical mode decomposition process, and the corresponding intrinsic mode function components are extracted. Then we calculate the spectral kurtosis values of all intrinsic mode function components and find out the main intrinsic mode function parts by our method to characterize the abnormal network traffic. By our method, the hidden abnormal traffic buried into the large background network traffic is to extract correctly and accurately. And then according the corresponding the detection threshold, the anomaly parts in network traffic is captured. Finally, we conduct a series of test to validate our method via the real background traffic in a real backbone network. Simulation results show that our approach is more effective and promising than previous methods.

To obtain the real traffic with known anomaly is significantly difficult. We only use simulation method to validate and verify our detection approach. To further demonstrate the detection performance of our method, we will perform a few tests in the real commercial networks in the near future.

Acknowledgments This work was supported in part by the National Natural Science Foundation of China (Nos. 61571104, 61071124), the General Project of Scientific Research of the Education Department of Liaoning Province (No. L20150174), the Program for New Century Excellent Talents in University (No. NCET-11-0075), the Fundamental Research Funds for the Central Universities (Nos. N150402003, N120804004, N130504003), and the State Scholarship Fund (201208210013). The authors wish to thank the reviewers for their helpful comments.

References

1. Ahmad A, Abdur Rahman M, Sadiq B et al (2015) Visualization of a scale free network in a smartphone-based multimedia big data environment. In Proc. BigMM'15, pp 286–287
2. Akgül T, Baykut S, Kantarci ME et al (2011) Periodicity-based anomalies in self-similar network traffic flow measurements. IEEE Trans Instrum Meas 60(4):1358–1366

3. Anand A, Muthukrishnan C, Akella A et al (2009) Redundancy in network traffic: findings and implications. In Proc. SIGMETRICS, pp 37–48
4. Babaie T, Chawla S, Ardon S (2014) Network traffic decomposition for anomaly detection. arXiv preprint arXiv:1403.0157, pp 1–22
5. Barford P, Kline J, Plonka D et al (2002) A signal analysis of network traffic anomalies. In Proc. IMW, pp 71–82
6. Bayram I, Selesnick I (2008) On the dual-tree complex wavelet packet and m-band transforms. IEEE Trans Signal Process 56(6):2298–2310
7. Celenk M, Conley T, Willis J et al (2010) Predictive network anomaly detection and visualization. IEEE Trans Inf Forensics Secur 5(2):288–299
8. Chandola V, Banerjee A, Kumar V (2012) Anomaly detection for discrete sequences: a survey. IEEE Trans Knowl Data Eng 24(5):823–839
9. Cheng J, Qian J, Qian K (2013) The effectively method of detecting network traffic anomaly. Adv Mater Res 2013:411–414
10. Chhabra P, Scott C, Kolaczyk E et al (2008) Distributed spatial anomaly detection. In Proc. INFOCOM'08, Phoenix, AZ, pp 2378–2386
11. Deng F (2013) Fast algorithm network traffic anomaly detection based on instantaneous frequency. Bull Sci Technol 29(7):170–172
12. Federico S, Juan IA, Pablo C et al (2011) Anomaly detection in network traffic based on statistical inference and α-stable modeling. IEEE Trans Dependable Secure Comput 8(4):494–509
13. Fu C, Zhang P, Jiang J et al A (2015) Bayesian approach for sleep and wake classification based on dynamic time warping method. Multimed Tools Appl : 1–20
14. Guan X, Qin T, Li W et al (2010) Dynamic feature analysis and measurement for large-scale network traffic monitoring. IEEE Trans Inf Forensics Secur 5(4):905–919
15. Guo C, Guo Q, Jin M et al (2015) Dynamic systems based on preference graph and distance. Discrete Contin Dyn Syst Ser S 8(6):1139–1154
16. Han J, Zhang J (2013) Network traffic anomaly detection using weighted self-similarity based on EMD. In Proc. Southeastcon'13, pp 1–5
17. Hu X, Peng S, Hwang W (2012) EMD revisited: a new understanding of the envelope and resolving the mode-mixing problem in AM-FM signals. IEEE Trans Signal Process 60(3):1075–1086
18. Huang S, Huang Y (2013) Network traffic anomaly detection based on growing hierarchical SOM. In Proc. DSN'13, pp 1–2
19. Huang NE, Shen Z, Long SR et al (1998) The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis. Proc R Soc Lond A 454(1971):903–995
20. Ji H, Long J, Fu Y et al (2011) Flow pattern identification based on EMD and LS-SVM for gas–liquid two-phase flow in a minichannel. IEEE Trans Instrum Meas 60(5):1917–1924
21. Jiang D, Hu G (2009) GARCH model-based large-scale IP traffic matrix estimation. IEEE Commun Lett 13(1):52–54
22. Jiang D, Han Y, Xu Z et al (2010) A time-frequency detecting method for network traffic anomalies. In Proc. ICCP'10, pp 94–97
23. Jiang D, Xu Z, Chen Z et al (2011) Joint time-frequency sparse estimation of large-scale network traffic. Comput Netw 55(10):3533–3547
24. Jiang D, Zhang P, Xu Z et al (2011) A wavelet-based detection approach to traffic anomalies. In Proc. CIS'11, pp 993–997
25. Jiang D, Xu Z, Nie L et al (2012) An approximate approach to end-to-end traffic in communication networks. Chin J Electron 21(4):705–710
26. Jiang D, Xu Z, Zhang P et al (2014) A transform domain-based anomaly detection approach to network-wide traffic. J Netw Comput Appl 40(2):292–306
27. Jiang D, Zhao Z, Xu Z et al (2014) How to reconstruct end-to-end traffic based on time-frequency analysis and artificial neural network. AEU Int J Electron Commun 68(10):915–925
28. Jiang D, Yao C, Xu Z et al (2015) Multi-scale anomaly detection for high-speed network traffic. Trans Emerg Telecommun Technol 26(3):308–317
29. Lakhina A, Crovella M, Diot C (2004) Diagnosing network-wide traffic anomalies. In Proc. SIGCOMM, pp 219–230
30. Lazarou GY, Baca J, Frost VS et al (2009) Describing network traffic using the index of variability. IEEE Trans Netw 17(5):1672–1683
31. Lian S, Gritzalis S (2015) Innovations in emerging multimedia communication systems. Telecommun Syst 59(3):289–290
32. Lin PJ, Dow CR, Hsuan P, Hwang SF (2011) An efficient traffic control system using dynamic thresholding techniques in wireless mesh networks. Int J Commun Syst 24(3):325–346
33. Lin Y, Yang J, Lv Z et al (2015) A self-assessment stereo capture model applicable to the internet of things. Sensors 15(8):20925–20944

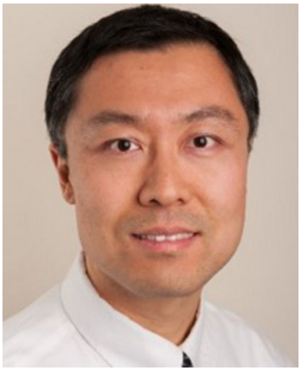
34. Liu D, Lung C, Lambadans I et al (2013) Network traffic anomaly detection using clustering techniques and performance comparison. In Proc. CCECE'13, pp 1–4
35. Liu D, Lung C, Seddigh N et al (2014) Network traffic anomaly detection using adaptive density-based fuzzy clustering. In Proc. TrustCom'14, pp 823–830
36. Lv Z, Yin T, Han Y et al (2011) WebVR——web virtual reality engine based on P2P network. J Netw 6(7): 990–998
37. Lv Z, Tek A, Silva FD et al (2013) Game on science-how video game technology may help biologists tackle visualization challenges. PLoS One 8(3):57990
38. Lv Z, Halawani A, Fen S et al (2015) Touch-less interactive augmented reality Game on vision based wearable device. Pers Ubiquit Comput 19(3):551–567
39. Ma R, Yao L, Jin M et al (2015) Robust environmental closed-loop supply chain design under uncertainty. Chaos Soliton Fract
40. Marnerides AK, Schaeffer-Filho A, Mauthe A (2014) Traffic anomaly diagnosis in Internet backbone networks: a survey. Comput Netw 2014(73):224–243
41. Millioz F, Martin N (2011) Circularity of the STFT and spectral kurtosis for time-frequency segmentation in Gaussian environment. IEEE Trans Signal Process 59(2):515–524
42. Nawata S, Uchida M, Gu Y et al (2010) Unsupervised ensemble anomaly detection through time-periodical packet sampling. In Proc. INFOCOM, pp 1–9
43. Novakov S, Lung C, Lambadaris I et al (2013) Studies in applying PCA and wavelet algorithms for network traffic anomaly detection. In Proc. HPSR'13, pp 185–190
44. Qin T, Guan X, Li W et al (2011) Monitoring abnormal network traffic based on blind source separation approach. J Netw Comput Appl 2011(34):1732–1742
45. Roy DB, Chaki R (2014) State of the art analysis of network traffic anomaly detection. In Proc. AIMoC'14, pp 186–192
46. Sheng SD, Hossain N et al (2015) Modeling of mobile communication systems by electromagnetic theory in the direct and single reflected propagation scenario. Applications and Techniques in Information Security. Springer Berlin Heidelberg :280–290
47. Spognardi A, Villani A, Vitali D et al (2014) Large-scale traffic anomaly detection: analysis of real netflow datasets. E-Business and Telecommunications: International Joint Conference, ICETE 2012, Rome, Italy, July 24–27, 2012. Revised Selected Papers, 2014, 455:192–208
48. Sun T, Tian H (2014) Anomaly detection by diffusion wavelet-based analysis on traffic matrix. In Proc. PAAP'14, pp 148–151
49. Tavallaee M, Stakhanova N, Ghorbani A (2010) Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Trans Syst Man Cybern Part C Appl Rev 40(5):516–524
50. Thatte G, Mitra U, Heidemann J (2011) Parametric methods for anomaly detection in aggregate traffic. IEEE Trans Netw 19(2):512–525
51. Vishwanath A, Sivaraman V, Rouskas GN (2011) Anomalous loss performance for mixed real-time and TCP traffic in routers with very small buffers. IEEE Trans Netw 19(4):933–946
52. Wald R, Khoshgoftaar T, Zuech R et al (2014) Network traffic prediction models for near-and long-term predictions. In Proc. BIBE'14, pp 362–268
53. Wang X, Qian H (2012) Hierarchical and low-power IPv6 address configuration for wireless sensor networks. Int J Commun Syst 25(12):1513–1529
54. Wang Y, Su Y, Agrawal G (2015) A novel approach for approximate aggregations over arrays. In Proc. the 27th International Conference on Scientific and Statistical Database Management :1–4
55. Won Y, Fontugne R, Cho K et al (2013) Nine years of observing traffic anomalies: trending analysis in backbone networks. In Proc. IM'13, pp 636–642
56. Xiong W, Hu H, Xiong N et al (2014) Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. Inf Sci 258(2014):403–415
57. Xu L (2005) Cancellation of harmonic interference by baseline shifting of wavelet packet decomposition coefficients. IEEE Trans Signal Process 53(1):222–230
58. Yan Y, Yang Y, Meng D et al (2015) Event oriented dictionary learning for complex event detection. IEEE Trans Image Process 24(6):1867–1878
59. Yang J, Chen B, Zhou J et al (2015) A low-power and portable biomedical device for respiratory monitoring with a stable power source. Sensors 15(8):19618–19632
60. Yang J, He S, Lin Y et al (2015) Multimedia cloud transmission and storage system based on internet of things. Multimed Tools Appl :1–16
61. Yang T, Yu B, Wang H et al (2015) Cryptanalysis and improvement of Panda-public auditing for shared data in cloud and internet of things. Multimed Tools Appl :1–18

62. Yu W, Zhang N, Fu X et al (2010) Self-disciplinary worms and countermeasures: modeling and analysis. IEEE Trans Parallel Distrib Syst 21(10):1501–1514
63. Zhang X, Han Y, Hao D et al (2015) ARPPS: augmented reality pipeline prospect system. Neural Information Processing. Springer International Publishing, pp 647–656
64. Zhang S, Zhang X, Ou X et al (2015) Assessing attack surface with component-based package dependency. Network and System Security. Springer International Publishing 405–417
65. Zhou H, Liu B, Luan T et al (2014) Chaincluster: engineering a cooperative content distribution framework for highway vehicular communications. IEEE Trans Intell Transp Syst 15(6):2644–2657

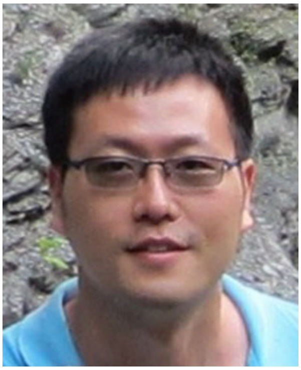
Dingde Jiang is an Professor in the College of Information Science and Engineering at Northeastern Southern University, Shenyang, China. He received the Ph.D. in Communication and Information Systems from University of Electronic Science and Technology of China, Chengdu, China, in 2009. From 2013 to 2014, he was a Visiting Scholar with the Department of Computer Science and Engineering at University of Minnesota, Minneapolis, MN, USA. His research focuses on network measurement, modeling and optimization, performance analysis, network management, network security in communication networks, particularly in software defined networks, information-centric networking, energy-efficient networks, and cognitive networks. His research is supported by the National Science Foundation of China, the Program for New Century Excellent Talents in University of Ministry of Education of China, and so on. He has been serving as an Editor for 1 international journals. He served as a technical program committee (TPC) member for several international conferences. He has received the Best Paper Awards at the International Conferences.

Zhen Yuan received BSc in College of Information Science and Engineering, Northeastern University, Shenyang, China, in 2012. She received MS in Communication and Information System, Northeastern University, Shenyang, China, 2014. Her research interests include modeling and optimization, performance analysis, network management.

Peng Zhang in College of Electronic and Information Engineering, Northeastern University at Qinhuangdao, China, in 2011. He received MS in Communication and Information System, Northeastern University, China, in 2013. His research interests include energy-efficient networks, traffic modeling, and network management.



Lei Miao is currently an assistant professor at Mechatronics Engineering, Dept. of Engineering Technology Middle Tennessee State University, Murfreesboro, USA. I received my Ph.D. degree from Boston University, Master's and Bachelor's degrees from Northeastern University of China, in 2006, 2001, and 1998, respectively. I was with Nortel Networks in Billerica, MA, from 2006 to 2009. I taught at the University of Cincinnati from 2009 to 2011 as a visiting professor. Most recently, I was with NuVo Technologies/Legrand North America from 2011 to 2014. His research interests include Discrete Event Dynamic Systems, Computer Networks, Systems Control and Optimizations, Wireless Communications and its applications, Embedded Systems, Intelligent Transportation Systems.



Ting Zhu is an assistant professor in the Department of Computer Science and Electrical Engineering at the University of Maryland Baltimore County, USA. He received his Ph.D. from the Department of Computer Science and Engineering at the University of Minnesota in 2010. He received his B.S. and M.E. degree from the Department of Information Science and Electronic Engineering at the Zhejiang University in 2001 and 2004, respectively. His research interests include wireless networks, renewable energy, embedded systems, distributed systems, and security.