IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 15, 2019, accepted March 5, 2019, date of publication March 8, 2019, date of current version March 26, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2903816

A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation

HONGSONG CHEN[1], CAIXIA MENG[2], ZHIGUANG SHAN[3], ZHONGCHUAN FU[4], AND BHARAT K. BHARGAVA[5], (Fellow, IEEE)

[1]School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
[2]Public Security Technology Department, Railway Police College, Zhengzhou 450053, China
[3]State Information Center of China, Beijing 100045, China
[4]Department of Computer Science, Harbin Institute of Technology, Harbin 150001, China
[5]Department of Computer Science, Purdue University,West Lafayette, IN 47907, USA

Corresponding author: Hongsong Chen (chenhs@ustb.edu.cn)

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFB0803403, Grant 2018YFB0803400, and Grant 2018YFB0505302, in part by the National Natural Science Foundation of China under Grant 61832012, in part by the National Social Science Fund of China under Grant 18BGJ071, and in part by the Fundamental Research Funds for the Central Universities under Grant TW201706.

ABSTRACT Low-rate Denial of Service (LDoS) attack is a special DoS attack. The routing protocol is vulnerable to many types of attacks in a wireless sensor network (WSN), which is an important network type of the Internet of Things (IoT). The novel LDoS attack to the routing protocol is proposed to evaluate the security and trust mechanism in the WSN. In fact, the LDoS attack is difficult to be detected due to its small-signal characteristics, so it is a serious threat to the security and trust of the WSN. A Hilbert–Huang transform (HHT) time–frequency joint analysis approach is utilized to analyze the non-stationary small signal that is produced by the LDoS attack. However, false intrinsic mode function (IMF) components are the challenge problems to precisely detect the LDoS attack. Correlation coefficient and Kolmogorov–Smirnov (KS) test approaches are united to evaluate the trustworthy of IMF components and exclude the false IMF components. Hilbert–Huang transformation and trust evaluation approaches are combined to detect the novel LDoS attack in Zigbee WSN. CC2530 system-on-chip integrated with ZigBee protocol is utilized to build a wireless sensor node. Random routing REQuest (RREQ) flooding attack is used to implement the routing layer LDoS attack in Zigbee WSN. If the correlation coefficient value of IMF component relative to original traffic is more than 0.3 and the KS similarity probability value of the IMF component relative to the original traffic is more than 0.4, the IMF component is identified as high trust IMF components that will be used to detect LDoS attack. If the IMF component only satisfies one of the trust evaluation conditions, the IMF component is identified as low trust IMF component. Otherwise, the IMF component is the false IMF component. We have proposed a scalable LDoS attack detection architecture for both WSN and IoT. The experimental results demonstrate that the novel approach is highly effective to detect the LDoS attack in the ZigBee WSN.

INDEX TERMS LDoS attack, HHT, trust evaluation, ZigBee WSN, IoT, intrusion detection.

I. INTRODUCTION

With the rapid development and application of Internet of Things (IoT), many smart devices are connected to Internet. With the convenience brought by the IoT and services, potential security problems and threats exist in the IoT applications. For example, In 2016 Mirai Botnet caused a Distributed Denial of Service (DDoS) to Dyn DNS servers by massively distributed flooding attack, that was produced by massive IoT devices, such as routers and cameras. So DoS attack traffics from IoT devices have been a serious threat to current Internet infrastructure. Although the total DDoS

The associate editor coordinating the review of this manuscript and approving it for publication was Ennan Zhai.

attack traffic is huge in Mirai Botnet massive attack, the attack traffic from single IoT device is small. It is difficult to detect the small signal from single IoT attack device according to the traditional method.

In IoT device and network, wireless sensor network is an important part of IoT network. Wireless Sensor Network (WSN) can be used to many application aspects, such as smart home, industry automatic control, intelligent traffic monitoring system, and smart city system. However, the security challenges are hindering the widespread application and development of WSN.

WSN is expected to provide secure and trust network communication and service to the users. Most security research works in WSN pay attention to the data confidentiality and integrity, however, routing protocol and network security are also important to WSN. Denial of Service attack is a serious threat to network security in WSN. All kinds of DoS attack are being main security challenges to the security and trust of WSN. There are many types of DoS attacks in the WSN, such as Denial of sleep, Distributed Denial of Service, Low-rate Denial of Service, Routing flood, SYN flood [1].

Nithya [2] review the security research of the wireless sensor networks, and discuss on the current state of the security attacks and countermeasures and in WSNs, DoS attacks may exist in any layer, such as physical layer, network layer, transport layer and application layer. Network security of WSN is still an open problem in current research domain.

Low rate Pulsating DoS (LPDoS) attack is researched by Kaur and Agrawa [3]. The research aim is to detect the LDoS attacks dynamically. The Shiryaev-Roberts's algorithm has been shown effectively. Active Queue Management (AQM) techniques were used by them to detect and mitigate these attacks. However, routing layer LDoS attack should be considered to provide secure and dependable network services in WSN.

The Low-rate DoS (L-DoS) attack is difficult to be detected [4]. The Active Queue Management schemes have been compared to search the decrease in network performance, that is due to L-DoS attack. The attackers exploit the vulnerability of TCP congestion control mechanism. While the routing layer LDoS attack maybe impact the network performance, the attack should be researched in WSN.

Yang *et al.* [5] proposed a Polynomial-based Compromise-Resilient En-route Filtering scheme, which can filter false injected data and achieve well recovery capability. The scheme used polynomials instead of Message Authentication Codes to provide security protection. However, the scheme needs some additional verification computing cost.

Singh *et al.* [6] proposed that explicit query based distributed denial of service (DDoS) attack detection and prevention method in Mobile Ad-hoc NETworks (MANET).How to implement the attack and security scheme in a real test-bed is a great challenge.

Yin *et al.* [7] present a framework for software-defined Internet of Things (SD-IoT). The framework includes a controller pool containing SD-IoT controllers. They propose an algorithm to detect and mitigate DDoS attacks using the SD-IoT framework. How to propose a scalable detection architecture to be suitable both WSN and IoT is a challenge.

Nain *et al.* [8] proposed a secure IEEE 802.15.4 transceiver design scheme that mitigated multiple attacks by using a physical layer encryption method that reduced the computation costs at the upper layers.

Fog/edge computing has been proposed to be integrated with Internet of Things (IoT) to enable computing services deployed at network edge, aiming to improve the resilience of the services in case of failures and attacks [9].

Cao *et al.* [10] propose that industrial distributed denial of service (DDoS) prevention solutions are important to keep business online. However, these solutions suffer from the challenge: although they do well in defending against extremely large scale DDoS attacks, they are not effective to the sophisticated DDoS attacks which are produced by massive unauthorized IoT devices, such as LDoS attack by IoT devices.

Tan *et al.* [11] propose a computer vision method to detect the DoS attack, which treats the traffic records as images. A multivariate correlation analysis approach is proposed to convert the traffic records to the respective images. The images are used as the observed objects in the DoS attack detection system, which is based on a dissimilarity measure, namely Earth Mover's Distance. KDD Cup 99 dataset and ISCX 2012 IDS Evaluation dataset are used to evaluate the intrusion detection system, experimental results show that the computer vision method is effective. How to use a novel measure to detect DoS attack in WSN is a great challenge problem.

Jeong *et al.* [12] propose a hybrid approach to integrate computational analysis with visual analytic to detect network intrusions. Multi-Resolution Analysis (MRA) and Principal Component Analysis (PCA) are combined to analyze network traffic data. Discrete Wavelet Transform (DWT) is used as MRA method to extract features. PCA is applied to transform the extracted features to identify principal components. However, the analysis result of DWT depends on the selection of Wavelet base function.

Jiang *et al.* [13] propose a traffic anomaly detection method that combines Empirical Mode Decomposition(EMD) and wavelet packet transform. Network traffic is decomposed into multiple narrow-band signals by the wavelet packet transform, which exhibiting more detailed features of network traffic. Then, the empirical mode decomposition method is used to divide the narrow-band signals into the intrinsic mode function, in different time and frequency domains. They calculate the spectral kurtosis value of the intrinsic mode function at different scales to remove the false components. Anomaly detection results show that the approach is effective. How to use the Empirical Mode Decomposition method to detect the abnormal traffic in wireless sensor network is a meaningful work.

Chistokhodova and Sidorov [14] propose a method to detect low-rate denial-of-service attacks, which uses

additional timestamps. The classifier with memory stores the state of the system, that is not limited by the sliding window. In their attack model, the target of victim is the web-server, how to detect low-rate denial-of-service in WSN is a great problem.

Zhang *et al.* [15] propose an intrusion detection based on dynamic state context and hierarchical trust in WSNs, which is flexible for constantly changing WSNs. The environment, states of nodes, and variations in trust value are always changing. The intrusion detection method based on a self-adaptive dynamic trust threshold is described, which is suitable for cluster-based WSNs. Tampering attack or a black hole attack are simulated in NS2 simulator. However. LDoS attack is also a serious threat to the WSN.

Cao *et al.* [16] propose a severe attack on ZigBee networks named as ghost attack, which used the underlying vulnerabilities of the IEEE 802.15.4 security suites to exhaust the energy of the target nodes. However, how to detect the ghost and improve the security of Zigbee networks are great challenges to current researchers.

Internet of Things is a concept which leverages on the power of networks to create ubiquitous sensor-actuator networks [17]. With the advance of cloud computing, the concept of IoT can be integrated with the basic elements having limited resource. PRITEE PARWEKAR evaluates the possibilities by integrating the IoT and Cloud Computing.

Distributed denial of service attack is the primary threat for the security in the collaborative wireless Mobile Ad hoc networks. Poongodi and Bose [18] have designed an intrusion detection system using the trust evaluation metrics. The probability of the overall trust evaluation is calculated by Trust Hypothesis Statistics, Frequency value, Cluster Separation value, Dominant Cluster value and Trust Network Security Policy. The trust evaluation probability is used to detect the flooding DDOS attacks in the Mobile Ad hoc networks. NS2 simulation experiments were used to validate the intrusion detection system. However, how to validate the intrusion detection approach in a real wireless network environment is a great challenge.

Pang and Liu [19] present a secure networked predictive control system architecture for the data security and control of networked systems, which provides the data confidentiality service, detection and compensation of deception attacks.

An active detection-based security and trust routing

scheme named ActiveTrust is proposed for WSNs [20]. The innovation of ActiveTrust is that it avoids black holes through the active creation of a number of detection routes to quickly detect and obtain nodal trust and improve the data route security.

To counter the threat of malicious spoofing attacks, Zhang *et al.* [21] develop the Secure Location of Things (SLOT) framework which extended current approaches and was able to deal with such threats.

Keerthi and Venkatarm [22] propose a Wormhole Attack Confirmation System that used a honeypot to mitigate false alarms in Mobile Ad hoc Networks and protect its resources.

A puzzle-based co-authentication scheme is proposed [23]. In the scheme, the Hash puzzle is designed to mitigate DoS attacks against the pseudonymous authentication process, that is facilitated through collaborative verification.

A novel multi-agent-based dynamic lifetime intrusion detection and response scheme are proposed to combat the two types of attacks [24]. Agent can periodically update itself by the trustworthiness of the neighbor nodes.

Han *et al.* [25] develop a new context-based pairing mechanism called Perceptio that uses time as the common factor across different sensor types. Perceptio creates event fingerprints that can be matched across a variety of IoT devices.

Rezvani *et al.* [26] demonstrate that several existing iterative filtering algorithms, while more robust against collusion attacks, they propose an improvement for iterative filtering techniques by providing an initial approximation which makes them not only collusion robust, but also more accurate and faster converging.

Rullo and Bertino [27] present Protocol-Adaptable Security Tool (PAST), a security tool for the IoT, which allow for the design and the management of detection techniques tailored to specific attacks and specific IoT instances.

As analysis from the above research works, LDoS attack is a great challenge to the security of WSN, however, there is not an efficient experimental approach to detect the routing layer LDoS attack in WSN.

The traditional LDoS attack utilizes the vulnerability of TCP congest control mechanism, the average value of LDoS attack traffic is close to that of normal network traffic. In WSN, as the routing protocols are simple, and the network topology can be controlled by the routing protocol, the routing protocol of WSN is vulnerable to some DoS attacks, such as the Low-rate Denial of Service(LDoS) attack. Network topology and performance can be impacted by the LDoS attack. To realize the two goals–both impacting the network performance and avoiding to be detected, routing-layer LDoS attack in WSN is proposed and implemented in this paper. In the routing layer LDoS attack, the average routing traffic from the attacker is close to normal routing traffic, at the same time, the network performance is affected by the attack.

HHT is an efficient method to analyze non-linear and non-stable signal, as the limited resource of the sensor nodes and the problem of HHT method, how to use the HHT method to detect the LDoS attack in WSN is a great challenge. The organization of the paper is described as the followings: Problem statement is described in section II. The novel solution combining HHT and trust evaluation is proposed in section III. Experiment workflow and network scenario are described in section IV. Routing layer LDoS attack experiment in Zigbee WSN is given in section V. Intrusion detection experiments by the novel solution are described in section VI. Scalable LDoS attack detection architecture in IoT network environment is proposed in section VII. Comparison analysis to other methods is described in section VIII. The conclusion is drawn in section VIIII.

II. PROBLEM STATEMENT

In WSN, the routing protocols are simple, however, the topology structure and network performance can be affected by the routing protocol if it is attacked. So the routing protocol of WSN is easily vulnerable to DoS attacks, such as the LDoS attack. The traditional LDoS attack utilizes the vulnerability of TCP congest control mechanism, the novel routing-layer LDoS attack is proposed to promote the security and trust research in WSN. The routing layer LDoS attack attempts to disrupt the network topology control mechanism in WSN and decrease the network performance, at the same time, the average number of routing traffic is similar to that of normal routing traffic to evade intrusion detection. So routing layer LDoS attack and detection in WSN are a great challenge to current researchers.

Because of the limited resource of wireless sensor node, the complex and online intrusion detection techniques cannot be directly used on the WSN node. As the traffic of LDoS attack is similar to that of normal routing protocol traffic, traditional threshold-based abnormal detection method cannot be directly used to detect the routing layer LDoS attack in WSN. At the same time, there is no congestion control mechanism in routing protocol of WSN, the routing protocol is vulnerable to LDoS attack. So how to detect the routing layer LDoS attack in WSN is a great challenge problem.

When the time-frequency analysis HHT method is utilized to analyze the LDoS traffic data offline, the small signal produced by LDoS attack is difficult to be detected because of the interfere of false IMF components. Trust computing is quantitative information system security approach. The concept and method of trust computing are utilized to improve the dependability of intrusion detection analysis. How to evaluate the trustworthy of Intrinsic Mode Function (IMF) components and identify the trust IMF components is also a great challenge. Based on the analysis above, there are two main problems in the LDoS attack detection in WSN.

(1) Traditional DoS detection method is difficult to detect the LDoS attack, as the traffic of LDoS attack is similar to that of normal traffic in WSN. Routing layer LDoS attack detection in resource-limited WSN is a problem.

(2) HHT time-frequency analysis method may be interfered as the small signal characteristic of LDoS attack, because the false IMF components are mixed in the normal IMF components. Trust evaluation of the IMF components is also a problem.

III. THE NOVEL SOLUTION COMBINATION HHT AND TRUST EVALUATION

To solve the problems described above, an architecture of LDoS attack detection in WSN is proposed. The proposed architecture is shown in figure 1.

Consider the constraints of energy in Wireless Senor Networks, there are two parts in the LDoS attack detection architecture in figure 1,the first part is WSN routing traffic capture module, which runs in the WSN sniffer node; the second part is security analysis module, which runs in the security analysis server.

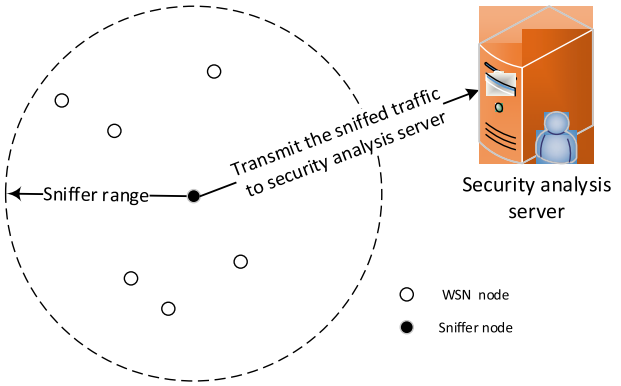

FIGURE 1. Architecture of LDoS attack detection in WSN.

The security researchers can use the sniffer node and packet sniffer software to capture and record the routing traffic in the sniffer range. In ZigBee WSN, the sniffer range is equal to ZigBee communication scope, that is 50 meters indoor or 200 meters outdoor according **IEEE** 802.15.4 standard.

Consider the proposed approach will be used for both WSN and IoT (Internet of Things), the sniffered network traffic can be transferred to security analysis server by the different communication protocol, such as WiFi, Bluetooch, LoRa (LongRange), NB-IoT

(Narrow Band-Internet of Things), USB (Universal Serial Bus), 5G, and so on. That depends on the application scenarios and design requirements.

In this paper, to validate the LDoS attack detection algorithm in the experiment, the ZigBee sniffer node is connected to security analysis server by USB protocol interface, which is installed the Smart Packer Sniffer software. The routing traffic data in the sniffer range is captured by the sniffer node, then the traffic is transmitted to security analysis server by the USB interface. So the security researchers can analyze the captured traffic according to HHT time-frequency signal analysis approach in offline mode.

The security analysis server implements the detection of the attacks by analyzing the sniffed routing traffic from the sniffer node. According to the monitor interval set by the security administrator, the WSN sniffer node transmits the sniffed routing traffic to the security analysis server periodically. If there is no routing traffic in this period, the sniffer node will not transmit any data to the security analysis server, so the energy consumption in detection system is controlled in the minimum level.

The routing traffic is converted and preprocessed to time series dataset in the security analysis server.

A novel solution which combines HHT and trust evaluation approach is proposed to precisely detect the small signal of LDoS attack. HHT time-frequency signal analysis approach is used to decompose and analyze the network

traffic time-serial dataset to IMF components, then the IMF components are evaluated by trust evaluation approach to obtain the trust IMF components. So the trust IMF components will be used to analyze and detect LDoS attack in WSN.

To improve the detection precision of LDoS attack, two types of trust evaluation approaches are united to evaluate the trustworthy of the IMF components, they are correlation coefficient approach and Kolmogorov-Smirnov test approach. Correlation coefficient is a numerical measure of correlation, which means a statistical relationship between two random variables. The Kolmogorov-Smirnov statistic test quantifies a distance between the empirical distribution function of the sample and the cumulative distribution function of the reference distribution, or between the empirical distribution functions of two samples. The two statistic approaches are united to evaluate the trustworthy of IMF components. The novel LDoS attack detection algorithm combining HHT and trust evaluation, that is shown in table 1.

TABLE 1. The novel LDoS attack detection algorithm combining HHT and trust evaluation.

Algorithm 1 The novel LDoS attack detection algorithm
Input:Normal traffic ***N*** and LDoS attack traffic ***A***
Output:LDoS attack time range, LDoS attack node
(1) Load the Normal traffic ***N*** and LDoS attack traffic ***A***
(2) Execute HHT on ***N*** and ***A*** to obtain IMF components set *Nc*, *Ac*
(3) Correlation coefficient calculation on *Ac* to their original traffic *A*
(4) Similarity probability calculation by KS test on *Ac* to their original traffic *A*
(5) **For** every IMF components in *Ac*
(6) **If** (Correlation coefficient value<0.3&&Similarity probability value <0.4)
(7) The IMF component is identified as false IMF component
(8) **If** (Correlation coefficient value>=0.3&&Similarity probability value >=0.4)
(9) The IMF component is identified as high trust IMF component
(10) **Else**
(11) The IMF component is identified as low trust IMF component
(12) **End For**
(13) Analyze the trust IMF components based on LDoS detection rule
(13) **For** every trust IMF component in *Ac*
(14) **If** the difference between the trust *Ac* IMF components and the related *Nc* IMF component is more than *30%* in HHT time-frequency analysis
(14) The time range of suspicious LDoS attack can be detected
(15) Comprehensive analysis on all trust *Ac* IMF components and related *Nc* IMF component
(16) The time range and attack node of LDoS attack can be detected
(17) End For
(18) **Return** LDoS attack time range and LDoS attack node

A. HILBERT-HUANG TRANSFORM TIME-FREQUENCY SIGNAL ANALYSIS APPROACH

As Hilbert-Huang Transform (HHT) is widely used to analyze the non-stationary signal, such as biomedical applications, financial applications, image processing, ocean engineering, health monitoring, speech recognition and network abnormal traffic detection [28]. It is proposed to detect the small signal produced by routing layer LDoS attack in WSN. Huang et al. proposed an adaptive data analysis approach named Empirical Mode Decomposition (EMD) to decompose the data signal into a set of intrinsic mode functions (IMFs) components, that extracted meaningful instantaneous amplitude and frequency information with the Hilbert transform.

EMD is an adaptive process that depends on two basic requirements:

1) the number of extreme and zero-crossings must be equal or differ by one;

2) the mean value of the envelope defined by local maxima and minima must be equal to zero at any point.

IMF component can be expressed by a simple harmonic function, an IMF component may have variable amplitude and frequency. The procedure of extracting an IMF component is described as the following steps:

1) Identify all the local extreme in the data signal.

2) Connecting all the local maxima by a cubic spline line as the upper envelope.

3) Connecting all the local minima by a cubic spline line as the lower envelope.

4) Obtain the mean curve value between the upper envelope and the lower envelope.

The upper and lower envelopes should cover all the data between them. The average value of the envelopes is m_1. The difference between the original data $X(t)$ and m_1 is the first component h_1, which is shown in formula (1):

$$h_1 - m_{11} = h_{11} \tag{1}$$

After the first round of calculation, a peak maybe become a local maximum. In the subsequent calculation process, h_1 can only be treated as a proto-IMF,As h_1 is generally not stationary data series, the new average value m_{11} is calculated on the h_1 as the same method. In the next step, h_1 is calculated as formula (2):

$$h_1 - m_{11} = h_{11} \tag{2}$$

After repeated calculation for k times, h_{1k} becomes an IMF, that is shown in formula (3):

$$h_{1(k-1)} - m_{1k} = h_{1k} \tag{3}$$

Then, h_{1k} is been as the first IMF component, it stands for the highest frequency component. Standard deviation (SD) is a stoppage criterion of the calculation process. In this paper, the *SD* value of stoppage criteria is between 0.2 and 0.3. It is shown in formula (4):

$$SD = \sum_{t=0}^{T} \left[\frac{\left| h_{1(k-1)}(t) - h_{1k}(t) \right|^2}{h^2_{1(k-1)}(t)} \right] \tag{4}$$

When the stopping criterion is satisfied the data range-[0.2,0.3], the first IMF component can be obtained. The other IMF components can be calculated as the similar approach.

Theoretically, an analytic signal $z(t)$ can be calculated from a real signal $x(t)$ and its Hilbert transform $y(t)$ [28], which are

shown in formula (5), (6):

$$y(t) = \frac{1}{\pi} P \int_{t-\tau}^{\infty} \frac{x(\tau)}{t-\tau} d\tau \tag{5}$$

$$z(t) = x(t) + jy(t) \tag{6}$$

where P stands for the principal value of the singular integral, the imaginary part $y(t)$ is the Hilbert transform of the real part $x(t)$.

B. TRUST EVALUATION OF THE IMF COMPONENTS

As the routing traffic in LDoS attack is random and complex, the maximum value of LDoS attack traffic is close to the value of normal routing traffic. When the LDoS attack traffic is decomposed by EMD algorithm, the false IMF components will appear, that will impact the precision of LDoS attack detection. We need an effective approach to evaluate the trustworthy of IMF components and choose trust IMF components.

In this paper, there are two approaches to be used to evaluate the trustworthy of the IMF components and identify the trust IMF components, which can be used to identify and detect LDoS attack in WSN. The trust IMF components are selected to improve the detection precision of LDoS attacks. If the IMF component is evaluated as trust component by the two statistical approaches at the same time, the IMF component will be identified as high trust component; if the IMF component is evaluated as trust component only by one statistical approach, the IMF component will be identified as low trust component; if the IMF component is not evaluated as trust component by any statistical approach, the IMF component will be identified as false component. The high trust IMF components will be used to analyze and detect the LDoS attack in WSN; the low trust IMF components will be used to assistant analysis in LDoS attack detection, the false IMF component will not be used to detect the LDoS attack. So our approach can solve the problem of trust IMFs identification and improve the precision of LDoS attack detection.

C. IMF COMPONENT TRUST EVALUATION BY CORRELATION COEFFICIENT APPROACH

As the small signal of LDoS attack is random and complex, false IMF components can be introduced in HHT analysis process, the detection precision of LDoS attacks will be impacted by the false IMF components. To solve the problem, the correlation coefficient approach is proposed to identify the trust IMF components to improve the LDoS detection precision.

Correlation coefficient calculation [29] between two time series is expressed as the following formula (7):

$$\rho_{\mathrm{xy}} = \frac{\sum_{n=0}^{\infty} x(n)y(n)}{\sqrt{\sum_{n=0}^{\infty} x^2(n) \sum_{n=0}^{\infty} y^2(n)}} \tag{7}$$

In this paper, $x(n)$ is the time series of IMF component, $y(n)$ is the time series of the original traffic signal, n is the number of time series. The ρ_{xy} stands for the correlation coefficient between the IMF component and original traffic signal, the value range of correlation coefficient is between 0 and 1.When the value is closer to 1, the more correlative between them, the higher trust degree of the IMF component; when the value is closer to 0, the more irrelevant between them, the lower trust degree of the IMF component. So the correlation coefficient calculation method can be used to evaluate the trustworthy of IMF components in LDoS attack detection of WSN.

D. IMF COMPONENT TRUST EVALUATION BY KOLMOGOROV-SMIRNOV TEST

If only the correlation coefficient approach is used to evaluate the trustworthy of the IMF component, error detection or missing detection maybe occur in HHT time-frequency joint analysis. So Kolmogorov-Smirnov test approach is used as the second approach to evaluate the trustworthy of IMF components. The Kolmogorov-Smirnov test is a non-parametric test approach to measure the given data is generated from a known distribution (one-sample test), or the two sets of data are generated from the same distribution (two-sample test) [30]. The two-sample KS test is one of the most general non-parametric approaches to compare the similarity of two samples distribution, as it is sensitive to the differences in location and shape of the empirical cumulative distribution functions of two samples. The two-sample KS test is used to calculate the similarity of the IMF component and its original traffic data, so the similarity is used as important evidence of IMF component trust evaluation.

Support the CDF (cumulative distribution function) of two time-series are $f(x)$ and $r(x)$,the largest absolute difference between the two CDF is expressed by D,it is shown in formula(10).

$$D = \max_{-\infty \le x \le +\infty} |f(x) - r(x)| \tag{8}$$

The similarity probability of the two data samples is given in formula (11).

$$prob(D) = Q_{KS}\left[\left(\sqrt{N_e} + 0.12 + \frac{0.11}{\sqrt{N_e}}\right) D\right] \tag{9}$$

With

$$N_e = \frac{N_1 N_2}{N_1 + N_2} \tag{10}$$

In the formula (12), N_1 and N_2 stand for the sample number of the two time-series. In the formula (13), Q_{KS} stands for KS probability distribution function.

$$Q_{KS}(\lambda) = 2\sum_{j=1}^{\infty} (-1)^{j-1} e^{-2j^2\lambda^2} \tag{11}$$

Seen from (13), when the $\lambda \to 0, Q_{KS}(\lambda) \to 1$; while $\lambda \to \infty, Q_{KS}(\lambda) \to 0$.

So when the cumulative distribution function of two time-series is similar, their similarity probability is close to 1, the more similarity between them, the higher trust degree of the IMF component; otherwise their similarity probability is close to 0,the more irrelevant between them, the lower trustworthy of the IMF component. So the KS similarity probability calculation method can be used to evaluate the trustworthy of IMF components.

So correlation coefficient calculation and Kolmogorov-Smirnov test can be united to solve the problems of trustworthy IMF component evaluation.

IV. EXPERIMENT WORKFLOW AND NETWORK SCENARIO

To verify our LDoS attack detection approach, experiment workflow and ZigBee WSN scenario are designed. Zigbee protocol stack is widely used in wireless sensor network, Zigbee wireless sensor nodes with CC2530 SoC (System on a Chip) is used to build the Zigbee wireless network and topology. The Zigbee node is built by CC2530 SoC with standard IEEE 802.15 Zigbee protocol stack. Zigbee network monitor tool is used to monitor the network topology, which is shown in figure 3, the attack node and sniffer node are set to obtain the LDoS attack traffic and normal traffic. Network traffic is collected by the sniffer node, which runs Zigbee Packet Sniffer software and is connected to the security analysis Server by USB interface, so the sniffed traffic file is analyzed by the security administrator. Consider the proposed approach will be used for both WSN and IoT, the sniffered network traffic can be transferred to a security analysis server by WiFi,LoRa,NB-IoT,USB,5G,and so on. The number of routing request packets in one second is counted to build the time series statistic file. At least two types of experiments were executed on the network topology, normal network traffic file was achieved in the first experiment; hybrid traffic file which combing normal traffic and LDoS attack traffic was achieved in the second experiment. HHT and EMD signal analysis methods were used to decompose and analyze the two types of traffics. In the EMD signal process of small LDoS attack traffic, false IMF components may be produced. Correlation coefficient and KS test approaches are united to evaluate the trustworthy of the IMF components. The trust IMF components will be selected to analyze and detect LDoS attack. Routing layer LDoS attack simulation experiment and HHT-based attack detection experiment workflow is shown in figure 2.

Seen from figure 2, WSN network topology and routing protocol are designed and configured, a LDoS attack model is designed to build the routing layer LDoS attack, security detection model is designed and configured according to the security requirement. The normal network traffic and LDoS attack traffic are generated according to the network configuration, then the routing traffics are captured by TI SmartRF Protocol Packet Sniffer software. Then the captured routing traffic is transferred to the security analysis server by USB protocol interface periodically. The captured packet file format is Packet Sniffer Format (PSD), we use

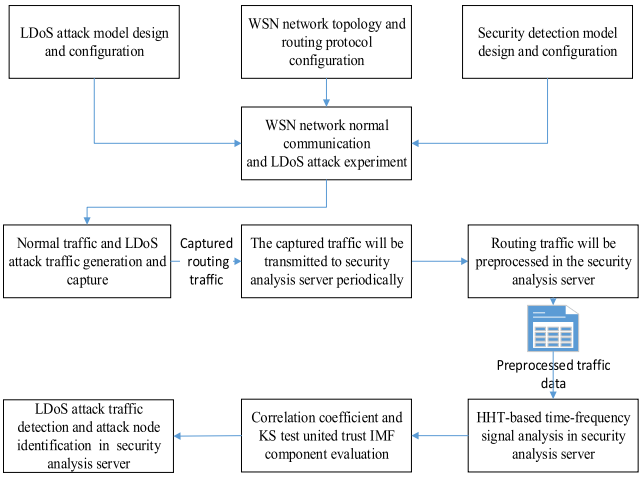

FIGURE 2. Workflow of LDoS attack and HHT-based detection experiment.

PSD_2_PCAP_Convert software tool to convert the captured PDS-format traffic file to PCAP-format traffic file in the security analysis server, then the routing message number in every second is summarized at the traffic preprocessing stage. Then the preprocessed traffic statistic data will be analyzed by HHT approach.

HHT time-frequency analysis approach is utilized to analyze the preprocessed statistic data and detect the LDoS attack offline. To solve the interference problem of false IMF components, correlation coefficient and KS-test approaches are united to evaluate and recognize the trust IMF components to improve the precision of LDoS attack detection. When the LDoS attack traffic is detected, the node that generated the LDoS attack traffic is identified as LDoS attack node. The configuration of Zigbee network attack experiment is shown in the table 2.

TABLE 2. Zigbee network attack experiment configuration.

Parameter type	Value
Experiment time	200s
Wireless Node type	CC2530 SoC
Number of nodes	6
Number of Attack node	1
Number of Sniffer node	1
Attack node ID	3
Communication protocol	Zigbee
Routing protocol	AODV
MAC layer protocol	IEEE 802.15.4
Attack type	Random LDoS attack
Attack duration	20-30s 65-90s 115-125s 150-170s

In the experiment configuration, Ad hoc On-demand Distance Vector(AODV) is a popular routing protocol in WSN, that is widely used in WSN and wireless Ad hoc network.

A random low-rate Route REQuest (RREQ) flooding attack mode is proposed to generate routing layer LDoS attack traffic in WSN.

The network topology of the LDoS attack experiment is gotten by Zigbee Sensor Monitor software, which is shown in figure 3.

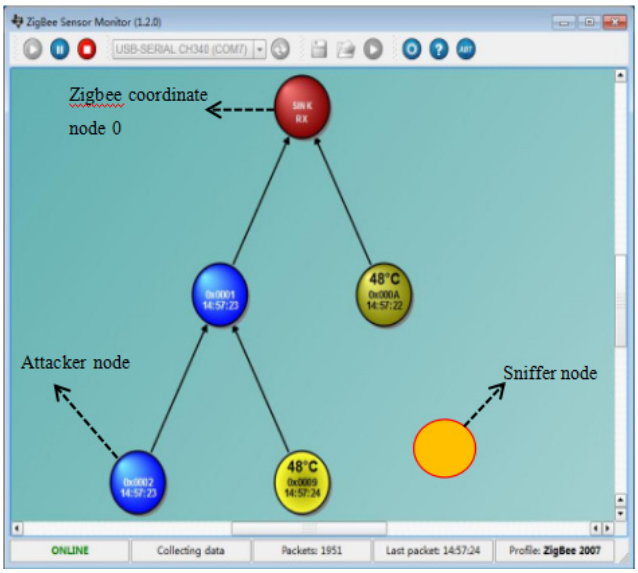

FIGURE 3. LDoS attack network topology in WSN.

Seen from the figure 3, there are six nodes in WSN experiment scenario. Node 0 is Zigbee coordinate node, there are one LDoS attack node and one Zigbee sniffer node in the network topology.

The sniffer node is shown in figure 4.

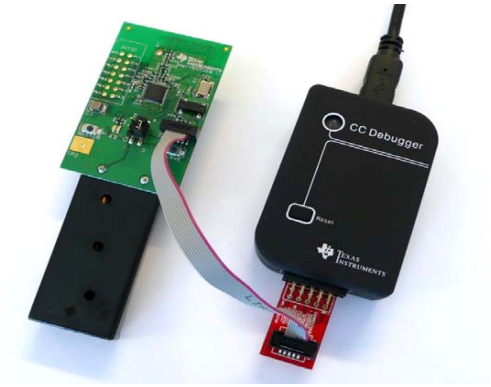

FIGURE 4. Sniffer node.

The sniffer node can capture the routing traffic and transfer the traffic data to data analysis server by USB protocol interface. TI Zigbee Packet Sniffer software is installed in the sniffer node to capture the network traffic.

The normal WSN nodes are shown in figure 5.

Seen from figure 5, the normal nodes can be plugged the sensors and build the Zigbee network by AODV routing protocol and Zigbee protocol stack.

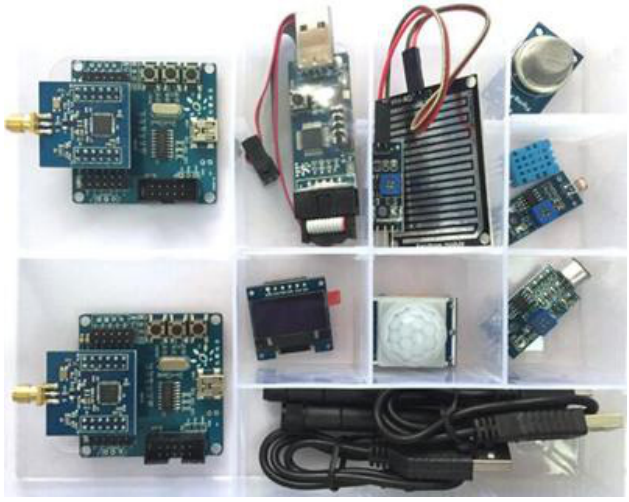

FIGURE 5. Normal nodes in WSN.

V. ROUTING LAYER LDoS ATTACK EXPERIMENT

In Zigbee WSN, the Network Coordinator node is built firstly, then the router node and endpoint node joint to the WSN according to the Zigbee protocol. If the source node needs transfer data to the other node, AODV routing protocol will be used to build the route path from the source node to the destination node. Because the AODV routing protocol is a passive routing protocol, only when the route path is needed to be built, the Routing request message and Routing reply message will be sent and transferred. When the attack sends data to a node which does not exist in the WSN, the Routing request broadcast will be triggered, if the frequency and duration of the RREQ messages are more than a threshold value, the network performance will be impacted. In this paper, the forged RREQ messages generated by the LDoS attack node is injected to the WSN at low rate, so the network performance is impacted potentially, at the same time, the LDoS attack small signal is similar to the normal traffic signal, the maximum routing message number of the LDoS attack in one second is no more than that of the number of routing message in normal network traffic. The characteristics of LDoS attack improve the difficulty of attack detection.

In the Zigbee LDoS attack experiment, when the attack node sends data to the unreachable destination node in a low duration time, the LDoS attack will be triggered. The interval time of LDoS attack is set to 0.25 second, the starting time and finish time of RREQ flood attack are random to evade detection. AODV routing protocol is used to build a route path in the Zigbee WSN. Routing Request function is called by the LDoS attack software in AODV protocol stack, the LDoS attack software is developed by C programming language and compiled by IAR Embedded Workbench IDE, then the LDoS software is programmed to the attack node by Zigbee Flash Programmer. The attack variables and parameters are set in the attack program. In the first experiment, the network traffic is normal; in the second experiment, the duration time of RREQ flood attacks are 20-30 second, 65-90 second,

115-125 second and 150-170 second. All network events and data in sniffer communication scope are captured by the TI Packet Sniffer. The Zigbee Sniffer node is connected to a security analysis server by a standard USB interface, which is about 50 meters indoor or 200 meters outdoor. Then the network routing traffic data is analyzed by HHT method in the security analysis server. The time-series traffic under normal traffic mode and LDoS attack mode are shown in figure 6.

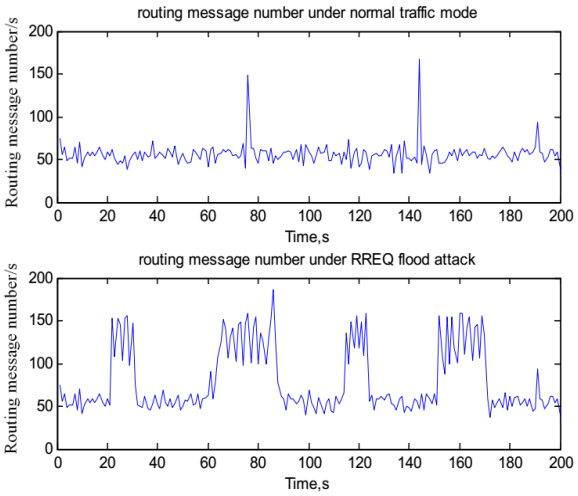

FIGURE 6. Routing message statistic under different conditions in the experiment.

Seen from figure 6, the maximum number of the routing message in LDoS attack traffic is close to that of normal traffic. It is difficult to detect LDoS attack traffic only by traditional threshold detection approach. However, the network performance has been impacted, the packet loss ratio has increased from 0.1% to 0.35% under the LDoS attack. If the LDoS attack does not be detected efficiently, the network performance will be affected by the routing layer LDoS attack continuously.

VI. LDoS ATTACK DETECTION EXPERIMENTS BY THE NOVEL SOLUTION

A. LDoS ATTACK DETECTION BY HHT ANALYSIS APPROACH

Because the LDoS attack is random, the routing message number of LDoS attack is similar to that of normal routing traffic, the traditional approach is difficult to detect the random LDoS traffic attack. HHT methods can extract and analyze the LDoS features in time domain and frequency domain by signal analysis method. Then intrinsic mode functions (IMFs) components are decomposed by Empirical Mode Decomposition (EMD) method. Matlab program are designed and implemented the HHT approach. The IMF components decomposition results of normal traffic and attack traffic by HHT algorithm are shown from figure 7 to figure 11.

Seen from figure 7 to figure 11, the instantaneous amplitude and the frequency signal of the IMF components are extracted and calculated according to the HHT algorithm. From the first IMF component to the fifth IMF component, the frequency values of IMF components are sorted in descending order.

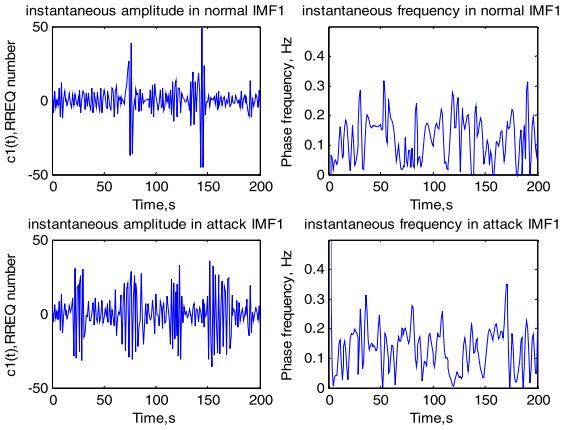

FIGURE 7. Instantaneous amplitude-frequency in the first IMF component.

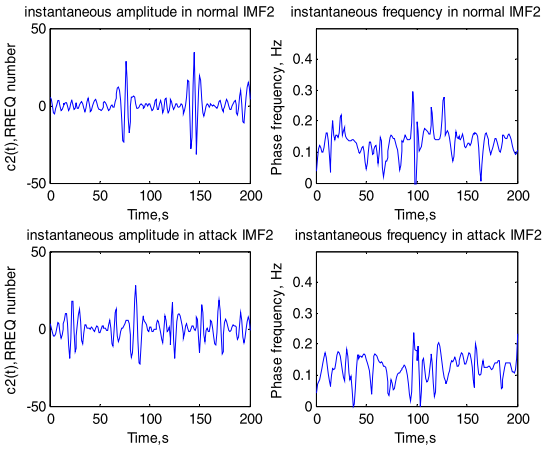

FIGURE 8. Instantaneous amplitude-frequency in the second IMF component.

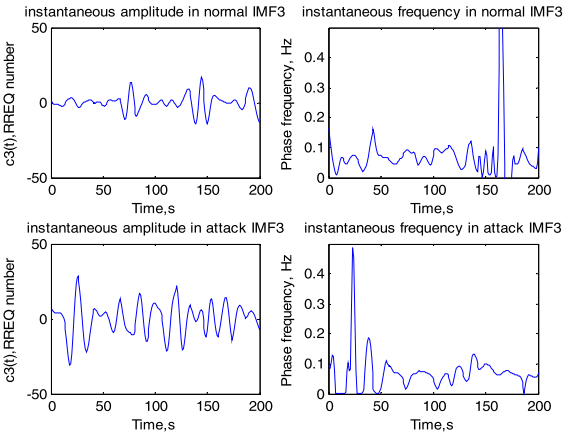

FIGURE 9. Instantaneous amplitude-frequency in the third IMF component.

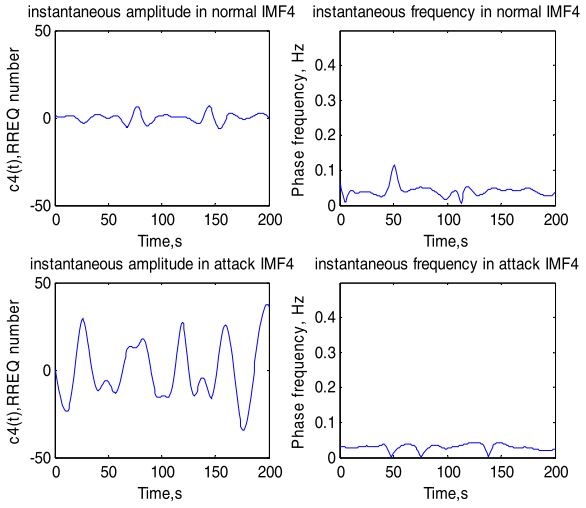

FIGURE 10. Instantaneous amplitude-frequency in the fourth IMF component.

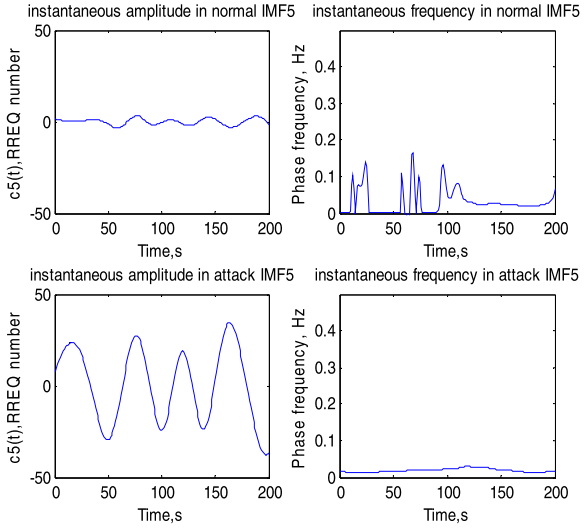

FIGURE 11. Instantaneous amplitude-frequency in the fifth IMF component.

Zigbee network traffic packets are captured by the TI Packet Sniffer software in the Zigbee sniffer node under its communication scope, the captured traffic is converted to PCAP format, so it can be preprocessed to the time-serial data, which is fed to HHT time-frequency analysis algorithm.

Comparison analysis between normal IMF components and attack IMF components are utilized to detect the routing layer LDoS attack in WSN. However, there are some contradictory and false detection results when analyzing the different IMF components. By analyzing the difference between the first normal IMF component and the first attack IMF component in figure 6, there is no significant difference between them on the maximum instantaneous amplitude value, however, there is a significant difference between them on a signal period, the differences are more than 30% in 20-30s,60-90s,110-125s and 150-170s, which can be inferred that potential LDoS attacks maybe occur in these period. Similarly, as shown in figure 7,there are no significant differences on the instantaneous amplitude and signal period in the second IMF component. Seen from figure 8,there is a significant difference in the maximum instantaneous amplitude in 20-30s, it is inferred that the LDoS attack occurred in this period in the third IMF component. As shown in figure 9,there are significant differences in the fourth IMF component on the maximum instantaneous amplitude in 20-30s, 65-90s,115-125s and 150-175s, the differences are more than 30%, so potential LDoS attacks can be inferred in these period. Seen from figure 10,there are significant differences in the fifth IMF component on the maximum instantaneous amplitude in 20-30s,40-50s,60-90s,110-125s,130-140s and 150-175s, the differences are more than 30%,so potential LDoS attacks can be inferred in these period.

By analyzing and comparing the difference between the normal IMF components and attack IMF components, potential LDoS attack can be inferred. However, the analysis results are not consistent, some results are contradictory. To solve the problem of contradictory and false LDoS attack detection in different IMF components, the IMF component should be evaluated by trust IMF evaluation approach to improve the precision of LDoS attack.

Correlated coefficient and KS test approaches are statistical approaches to calculate the similarity between the IMF component and the original traffic signal, the more similarity value of the IMF component relative to original traffic, the more trustworthy of the IMF component. In this paper, the correlated coefficient and KS test approach are united to evaluate the trustworthy of IMF components. So the precision of LDoS attack detection will be improved.

B. TRUST IMF COMPONENT EVALUATION BY CORRELATION COEFFICIENT AND KS TEST

As the low-rate and random characteristics of LDoS attack in this paper, the detection precision was impacted by the false IMF components in the HHT time-frequency analysis process. Correlation coefficient and KS test approaches are utilized to evaluate trust IMF components to improve the precision of LDoS detection.

According to formula (9), correlation coefficient method is used to evaluate the trustworthy of IMF components according to the correlation coefficient values between the IMF component and original routing traffic. The correlation coefficient values of IMF components relative to original LDoS routing traffic in the experiment are listed in table 3.

According to formula (11), KS test method is used to evaluate the trustworthy of IMF components according to the similarity probability values between the IMF component to original LDoS routing traffic. The similarity probability values of IMF components to original LDoS routing traffic are listed in table 4.

Seen from the table 3, the correlation coefficient values of the five IMF components relative to original LDoS routing traffic are different. If sorting the five IMF components

TABLE 3. Correlation coefficient values of the IMF components to LDoS traffic.

IMF component	Correlation coefficient value
IMF1	0.4558
IMF2	0.2027
IMF3	0.1386
IMF4	0.3476
IMF5	0.2825

TABLE 4. Similarity probability values of the IMF components to LDoS traffic.

IMF component	Similarity probability value
IMF1	0.649
IMF2	0.289
IMF3	0.368
IMF4	0.728
IMF5	0.486

according to the correlation coefficient values, the descending order should be IMF1,IMF4,IMF5,IMF2,IMF3. According to algorithm1 in table 1, the correlation coefficient values of IMF1,IMF4 are more than 0.3,that of IMF5,IMF2,IMF3 are less than 0.3. So IMF1,IMF4 may be trust IMF components, while IMF5,IMF2,IMF3 may be false IMF components. The trust evaluation results depend on the similarity probability value of the IMF components relative to original LDoS traffic.

Seen from the table 4, the similarity probability of the five IMF components to original LDoS traffic are different. If sort the five IMF components according to the similarity probability to original LDoS traffic, the descending order should be IMF4,IMF1,IMF5,IMF3,IMF2. According to algorithm1 in table 1, the similarity probability of IMF4,IMF1,IMF5 are more than 0.4, that of IMF3,IMF2 are less than 0.4. So IMF4,IMF1,IMF5 may be trust IMF components, while IMF3 and IMF2 may be false IMF components. Combining the analysis results from both correlation coefficient and similarity probability method,IMF1 and IMF4 are identified as high trust IMF components, IMF5 is identified as low trust IMF component,IMF3 and IMF2 are identified as false IMF components.

To demonstrate the trust evaluation condition, trust evaluation value, result and usage, the trust evaluation relationships are shown in table 5.

Thus we should pay attention to analyze the high trust IMF4,IMF1, the low trust IMF5 will be as assistant analysis usage. While IMF3,IMF2 are excluded to be analyzed, as they are identified as false IMF components.

As analyzed in the IMF1 component, potential LDoS attack can be inferred in 20-30s,60-90s,110-125s, and 150-170s,at the same time, as analyzed in IMF4 component, potential LDoS attack can be inferred in 20-30s,65-90s,115-125s and 150-175s. We can combine the comprehensive analysis results to obtain the final LDoS attack detection results,

TABLE 5. Trust evaluation relationships.

Trust evaluation conditions	Trust evaluation value	Trust evaluation degree	Trust evaluation result	Trust evaluation usage
Satisfy the two conditions	2	High trust IMF component	IMF4,IMF1	Be used to detect LDoS attack
Satisfy only one condition	1	Low trust IMF component	IMF5	Be used as LDoS assistant analysis
Does not satisfy any condition	0	false IMF component	IMF3,IMF2	Can not be used to detect LDoS attack

we deduce that LDoS attack can occur in 20-30s 65-90s 115-125s 150-170s.

As analyzed in IMF5 component, potential LDoS attack can be inferred in 20-30s,40-50s,60-90s,110-125s,130-140s and 150-175s. As the LDoS attack analysis results are included in the analysis results by IMF5, so LDoS attack analysis results deduced by high trust IMF4 and IMF1 are confirmed again. However, the traffic in 40-50s will not be treated as LDoS attack, because it is only deduced by the low trust IMF5 component.

Based on the above analysis, the LDoS attack traffic detection results are in 20-30s 65-90s 115-125s 150-170s,which are deduced by the high trust IMF components and confirmed by low trust IMF component. As the LDoS attack traffic is generated from node 3, so node 3 is recognized as the malicious LDoS attack node. The detection results match the LDoS attack configuration experiment well. The detection precision is higher than that from false or low trust IMF components.

VII. SCALABLE LDoS ATTACK DETECTION ARCHITECTURE IN IOT NETWORK ENVIRONMENT

IoT needs constant monitoring of the objects and the attacks, WSN is a key portion of IoT, We propose a scalable LDoS attack detection architecture in Cloud-based IoT network environment, which is suitable for both WSN and IoT, that is shown in figure 12.

As shown in figure 12, the scalable LDoS attack detection architecture is hierarchical and collaborative, it combines the advantages of cloud computing and edge computing. There are three key parts in the architecture, they are sniffer node, Edge computing security analysis server and cloud computing security analysis server. The sniffer nodes are used to capture and transmit the network traffics to the Edge computing security analysis server, the communication

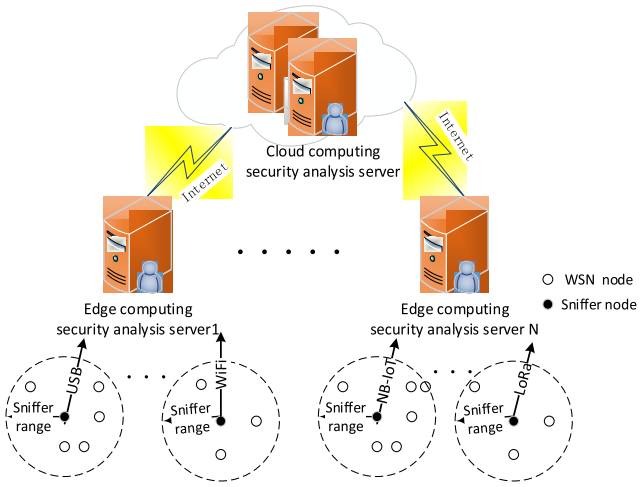

FIGURE 12. Scalable LDoS attack detection architecture in cloud-based IoT network environment.

protocols between the sniffer nodes and Edge computing security server can be USB,WiFi,BlueTooch,NB-IoT,LoRa and 5G, which depend on the real network scenarios and security requirements. The Edge computing security analysis server implements the detection of the attacks by preprocessing and analyzing the sniffed routing traffic. Then the Edge computing security analysis server transmits the preprocessed and structured traffic data to the Cloud computing security analysis server periodically. The collaborative analysis results can be deduced from the results both in Edge computing security analysis server and Cloud computing security analysis server. The structured traffic data includes the ID of the WSN node, and the number of the network traffic per second from the WSN node. The IoT global traffic monitor matrix M in cloud server represents the routing traffic distribution of the IoT nodes in current time, M is updated for one second, the matrix M is defined in formula (12).

$$M = \begin{bmatrix} & SA_1 & \dots & SA_i & \dots & SA_n \\ ID_1 & N_{SA_1-ID_1} & \dots & N_{SA_i-ID_1} & \dots & N_{SA_n-ID_1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ ID_j & N_{SA_1-ID_j} & \dots & N_{SA_i-ID_j} & \dots & N_{SA_n-ID_j} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ ID_m & N_{SA_1-ID_m} & \dots & N_{SA_i-ID_m} & \dots & N_{SA_n-ID_m} \end{bmatrix} \tag{12}$$

where the row represents the traffic/second from one WSN node, the column represents traffic/second from one Edge computing security analysis server. The ID_j stands for the j-th WSN node,SA_i stands for the i-th Edge computing security analysis server, $N_{SAi\text{-}IDj}$ stands for the traffic/second from j-th WSN node observed by the i-th Edge computing security analysis server. From the IoT global traffic monitor matrix in cloud server, the LDoS attack can be detected by the attack detection algorithm both on the Edge computing security analysis server and Cloud computing security analysis server, so it is cooperative attack detection approach. The security administrator can ensure which domain and which WSN node the LDoS attacks occurred will be detected.

VIII. COMPARISON TO OTHER APPROACHES

To show the advantages of our approach, different methods are selected to compare our approach to existing methods, the comparison is shown in table 6:

TABLE 6. Comparison our approach with existing methods.

Different detection approaches	Time-frequency analysis	Attack detection experiment	Trust evaluation	WSN attack detection	Scalable to IoT network
D. H. Jeong, B. Jeong [12]	support	abnormal traffic detection	none	none	difficult
Zhihua Zhang[15]	none	DoS detection	none	support	middle
Poongodi M , Bose S [18]	none	DDoS detection	support	support	middle
Our approach	support	LDoS detection	support	support	easy

As shown in table 6, there are 5 items to be used to compare different attack detection approaches in WSN, the items are time-frequency analysis, attack detection experiment, trust evaluation, WSN attack detection, scalable to IoT network. All the items are supported in our approach, only some of the items are supported in other existing methods. Moreover, the difficulty of the LDoS attack detection in WSN is more than other attack detection. The trust evaluation approach which combining correlation coefficient and KS test is firstly proposed to select trust IMF components. Our LDoS detection architecture is easy to be scalable to IoT network environment. Overall our approach performs better than other existing methods.

IX. CONCLUSION

Routing protocol is a critical component of the WSN in current IoT (Internet of Things) network technique. The routing protocol is vulnerable to LDoS attack, which is difficult to be detected by the traditional method. LDoS attack detection is a great challenge to current intrusion detection techniques in WSN.

A novel LDoS attack detection approach combining Hilbert-Huang Transformation and Trust evaluation is proposed in Zigbee WSN. There are three main contributions in our research work:

(1) Scalable LDoS attack detection architecture in Cloud-based IoT network environment

The scalable LDoS attack detection architecture is hierarchical and collaborative, it combines the advantages of cloud computing and edge computing. A novel data structure-IoT global traffic monitor matrix is proposed to record the time-serial traffic data in cloud server.

(2) A novel HHT-based LDoS attack detection algorithm in Zigbee WSN

As LDoS attack traffic is small signal compared to original traffic, HHT time-frequency joint analysis approach is proposed to analyze and detect the routing layer LDoS attack. EMD method is utilized to decompose the original traffic signal to a set of IMF components as their intrinsic characteristic. Only trust IMF components can be utilized to detect the LDoS attack based on LDoS detection rules in Zigbee WSN.

(3)IMF components trust evaluation approach combining correlation coefficient and KS test

As the signal of LDoS attack is the random small signal, the false components are mixed in the IMFs components, which results in the contradictory LDoS detection results. Correlation coefficient and KS test approaches are united to evaluate the trustworthy of IMF components, so the detection precision of LDoS attack is improved by the novel approach. The false IMF component will be excluded. Only trust IMF components can be used to detect the LDoS attack in ZigBee WSN.

Experimental results demonstrate that the novel LDoS attack detection approach is effective to detect the LDoS attack in WSN. Correlation coefficient united KS test method is highly efficient to evaluate and select high trust IMF components. Aiming to the future research, we have proposed a scalable LDoS attack detection architecture for both WSN and IoT network environment, which combines Edge computing and Cloud computing efficiently. To the best of our knowledge, the work is the first quantitative LDoS attack and detection experimental research on Zigbee WSN. The novel detection architecture and approach will promote HHT and trust evaluation application for WSN and IoT security research.

REFERENCES

[1] A. M. Abdullah, M. B. Alsolami, and M. H. Alyahya "Intrusio, detection of DoS attacks in WSNs using classification techniuqes," *J. Fundam. Appl. Sciences.*, vol. 10, no. 4, pp. 298–303, 2018.

[2] N. Savarimuthu, "An investigation on security attacks in wireless sensor network," *J. Pure Appl. Math.*, vol. 119, no. 15, pp. 925–927, 2018.

[3] G. Kaur and P. Agrawal, "Detection of LDoS attacks using variant of CUSUM and Shiryaev—Roberts's algorithm," in *Proc. 4th Int. Conf. Parallel, Distrib. Grid Comput.*, Dec. 2017, pp. 363–369.

[4] S. Patel and A. Sharma, "The low-rate denial of service attack based comparative study of active queue management scheme," in *Proc. 10th Int. Conf. Contemp. Comput. IEEE Comput. Soc.*, Aug. 2017, pp. 1–3.

[5] X. Yang *et al.*, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[6] N. Singh *et al.*, "Explicit query based detection and prevention techniques for DDOS in MANET," *Int. J. Comput. Appl.*, vol. 53, no. 2, pp. 19–24, 2013.

[7] D. Yin, L. Zhang, and K. Yang, "A DDoS attack detection and mitigation with software-defined Internet of Things framework," *IEEE Access*, vol. 6, pp. 24694–24705, 2018.

[8] A. K. Nain *et al.*, "A secure phase-encrypted IEEE 802.15.4 transceiver design," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1421–1427, Aug. 2017.

[9] J. Lin *et al.*, "A survey on Internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[10] Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, "Understanding Internet DDoS mitigation from academic and industrial perspectives," *IEEE Access*. vol. 6, pp. 66641–66648, 2018.

[11] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu, and J. Hu, "Detection of denial-of-service attacks based on computer vision techniques," *IEEE Trans. Comput.*, vol. 64, no. 9, pp. 2519–2533, 2015.

[12] D. H. Jeong, B. Jeong, and S. Ji, "Designing a hybrid approach with computational analysis and visual analytics to detect network intrusions," in *Proc. IEEE 7th Annu. Comput. Commun. Workshop Conf. (CCWC)*. Las Vegas, NV, USA, Jan. 2017, pp. 1–7.

[13] D. Jiang *et al.*, "A traffic anomaly detection approach in communication networks for applications of multimedia medical devices," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14281–14305, Nov. 2016.

[14] A. A. Chistokhodova and I. D. Sidorov, "Novel method for low-rate ddos attack detection," *J. Phys., Conf. Ser.*, vol. 1015, 2018, pp. 032024-1–032024-5. doi: 10.1088/1742-6596/1015/3/032024.

[15] Z. Zhang, H. Zhu, S. Luo, Y. Xin, and X. Liu, "Intrusion detection based on state context and hierarchical trust in wireless sensor networks," *IEEE Access*, vol. 5, pp. 12088–12102, 2017.

[16] X. Cao *et al.*, "Ghost-in-ZigBee: Energy depletion attack on ZigBee-based wireless networks," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 816–829, Oct. 2016.

[17] P. Parwekar, "From Internet of Things towards cloud of things," in *Proc. 2nd Int. Conf. Comput. Commun. Technol.*, Sep. 2011, pp. 329–333.

[18] M. Poongodi and S. Bose, "A novel intrusion detection system based on trust evaluation to defend against DDoS attack in MANET," *Arabian J. Sci. Eng.*, vol. 40, no. 12, pp. 3583–3594, 2015.

[19] Z. H. Pang and G. P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, nos. 1334–1342, pp. 1334–1342, Sep. 2012.

[20] Y. Liu *et al.*, "ActiveTrust: Secure and trustable routing in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 2013–2027, Sep. 2017.

[21] P. Zhang, S. G. Nagarajan, and I. Nevat, "Secure location of things (SLOT): Mitigating localization spoofing attacks in the Internet of things," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 2199–2206, Dec. 2017.

[22] T. D. S. Keerthi and P. Venkatarm, "Confirmation of wormhole attack in MANETs using honeypot," *Comput. Secur.*, no. 76, pp. 32–49, Jul. 2018.

[23] P. Liu *et al.*, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.

[24] H. Chen *et al.*, "Design and performance evaluation of a multi-agent-based dynamic lifetime security scheme for AODV routing protocol," *J. Netw. Comput. Appl.*, vol. 30, no. 1, pp. 145–166, 2007.

[25] J. Han *et al.*, "Do you feel what i hear-enabling autonomous IoT device pairing using different sensor types," in *Proc. IEEE Symp. Secur. Privacy (SP)*. San Francisco, CA, USA, Sep. 2018, pp. 836–852.

[26] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 98–110, Feb. 2015.

[27] A. Rullo and E. Ertino, "PAST: Protocol-adaptable security tool for heterogeneous IoT ecosystems," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Jun. 2016, pp. 1–8.

[28] N. E. Huang and S. S. Shen, *Hilbert-Huang Transform and Its Applications*. Singapore: World Scientific, 2005, pp. 298–306.

[29] H. Jahanirad, "CC-SPRA: Correlation coefficients approach for signal probability-based reliability analysis," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, to be published. doi: 10.1109/TVLSI.2018.2886027.

[30] G. Ferraioli, B. Kanoun, V. Pascazio, and G. Schimzi, "SAR image restoration via a NL approach based on the KS Test," *Proc. IEEE Int. Geosci. Remote Sens. Symp.*, Jun. 2018, pp. 5820–5822.

HONGSONG CHEN received the Ph.D. degree in computer science from the Harbin Institute of Technology, in 2006. He has been an Associate Professor with the University of Science and Technology Beijing (USTB), China, since 2008. He was a Visiting Research Scholar with the Department of Computer Science, Purdue University, from 2013 to 2014. He is a High-Level Member of the China Computer Federation. He has published more than 50 academic papers and five books. His research interests include cloud computing and cloud security, wireless network security, and trust computing. He received the Excellent Young Academic Paper Award from USTB, in 2009, and the Beijing Science and Technology Achievement Award, in 2018.

CAIXIA MENG received the master's degree in computer science from Zhengzhou University, in 2008. She has been an Associate Professor with the Public Security Technology Department, Railway Police College, China, since 2008. She has published more than 20 academic papers. Her research interests include network and information security, data analysis, and information forensics.

ZHIGUANG SHAN was born in 1974. He received the B.A. degree in automation engineering and the Ph.D. degree in computer science from the University of Science and Technology Beijing, Beijing, China, in 1997 and 2002, respectively. He is a Professor and the Director of the Informatization and Industry Development Department, State Information Center of China. He also serves as the Director of the China Smarter City Development and Research Center. His main research interests include computer networks, performance evaluation, strategic planning and top design of smarter city, macro planning, and developing policies of informatization. He has co-authored more than 70 papers in research journals and conference proceedings and nine books in these areas.

ZHONGCHUAN FU received the Ph.D. degree from the Department of Computer Science, Harbin Institute of Technology, China, in 2006, where he is currently an Associate Professor with the Department of Computer Science. His research interests include computer system security, fault-tolerant computing, and trust computing.

BHARAT K. BHARGAVA received the B.E. degree from the Indian Institute of Science and the M.S. and Ph.D. degrees in electrical engineering from Purdue University, West Lafayette, IN, USA, where he is currently a Professor of computer science. His research interests include mobile wireless networks, secure routing and dealing with malicious hosts, providing security in service-oriented architectures (SOA), adapting to attacks, and experimental studies. He is a Fellow of the IEEE Computer Society. His name has been included in the *Book of Great Teachers* at Purdue University. Moreover, he was selected by the Student Chapter of the ACM at Purdue University for the Best Teacher Award.