Research on Attack Signal Feature Extraction Method of Multipath TCP Transmission System Based on Wavelet Energy Entropy

Lejun Ji, Gang Lei(✉), Ruiwen Ji, Junyi Wu, and Keyang Gu

School of Software, Jiangxi Normal University, Nanchang 330022, China
leigang@jxnu.edu.cn

Abstract. Multipath transmission technology provides a strong theoretical support for the realization of parallel multi-channel data transmission for multi-host mobile terminal devices, and is an ideal scheme for high performance and high quality data transmission in wireless network environment. MPTCP is one of the representative achievements, and its security and robustness have aroused wide concern and discussion among researchers at home and abroad. In view of the characteristics of non-stationary signals transmitted by MPTCP, this paper combines wavelet transform analysis method and information entropy theory, and uses wavelet energy entropy to achieve the method of feature extraction of attack signals. Finally, the simulation analysis is carried out and good experimental results are obtained. The following conclusions are drawn: according to the law of wavelet energy entropy changing with wavelet decomposition scale, the attack signal is different from the normal signal. Based on this feature, attack signals in MPTCP transmission system can be well detected, which provides a new thinking and new means for anomaly detection and online monitoring of MPTCP transmission system.

Keywords: Multipath TCP · Wavelet transform · Wavelet energy entropy · Feature extraction · Robustness

1 Introduction

With the booming development of mobile Internet technology and the increasing popularity of multi-host mobile smart terminal devices, multipath transmission

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant No. 61962026, and by the Postgraduate Innovation Fund of Jiangxi Provincial Department of Education under Grant YC2021-S258.

Y. Cao and X. Shao (Eds.): MONAMI 2022, LNICST 474, pp. 398–412, 2023.
https://doi.org/10.1007/978-3-031-32443-7_29

technology has been widely studied and discussed, and its application fields and practical values are being constantly broadened and explored. Compared with the traditional single-path transmission mode, multipath transmission technology can organically integrate various wireless access technologies (WiFi, 4G, Bluetooth, etc.) and better aggregate a variety of heterogeneous wireless network resources, thus effectively improving the performance of application data transmission and transmission quality of service [1]. Among them, the most representative MPTCP (Multipath TCP) can meet the requirements of network application data transmission with high bandwidth, high rate, and low delay, and maximize the utilization of network resources. Therefore, MPTCP will become the core transmission protocol of the Internet in the future [2]. However, facing the increasingly complex and critical cyber security situation, the security and robustness of MPTCP transmission system has become a hot topic for national and international research scholars.

In the real network environment, the robustness of multipath transmission system mainly includes structural robustness and performance robustness. However, the complex and changeable intentional network attack will have a serious impact on the structural and performance robustness of MPTCP transmission system, and then affect the transmission performance of the transmission system and user service quality [3]. However, the research of multipath transmission theory and algorithm based on MPTCP is mainly focused on path management and data scheduling, while the research of network security and robustness is relatively lacking [4–6]. Among the only relevant studies, the research on security-related issues can be roughly divided into abnormal attack traffic detection and robustness modeling and optimization. Therefore, the characteristics of abnormal attack traffic signals can be extracted timely and effectively to accurately distinguish normal signals from attack signals, which will play a decisive role in the rapid detection of attack signals in MPTCP transmission system.

Among the existing signal analysis methods, the wavelet analysis method is a time-frequency multi-resolution analysis method proposed by the French scientist J. Morlet in the early 1980s [7]. This method overcomes the disadvantage that the STFT (Short-Time Fourier Transform) window size does not vary with frequency, and evolves on this basis, which provides a possibility for studying time series better [8]. It is an ideal tool for time-frequency analysis and processing of non-stationary signals because it can intuitively reveal the various cycles of variation hidden in the time series, fully reflect the trend of the system on different time scales, and further estimate the future development trend of the system. Wavelet analysis theory has been widely used in signal analysis and detection, image recognition, computer classification and processing, medical imaging and diagnosis [9], numerical analysis [10] and other scientific fields [11].

In this paper, the wavelet transform analysis method is applied in MPTCP transmission system to realize multi-resolution analysis and time-division and frequency localization fine expression of MPTCP non-stationary signals, so as to extract component sequences of different frequency ranges. Meanwhile, this paper uses wavelet energy entropy to design and implement attack feature extraction method suitable for MPTCP transmission system, and studies the numerical characteristics of attack signal different from normal signal. Finally, this paper conducts simulation experiment analysis based on NS2 (Network Simulator version 2) platform [12] to verify the rationality and effectiveness of the design method. The experimental results show that wavelet energy entropy can be used as the classification feature of normal signals and attack signals in MPTCP transmission system, which lays a theoretical foundation for anomaly detection in multipath transmission system, and further improves the robustness and security of MPTCP multipath transmission system.

The organization of the remaining chapters is as follows. In Sect. 2, we mainly introduce the wavelet transform analysis method, information entropy and wavelet energy entropy related theoretical knowledge, including the basic concept and working principle. In Sect. 3, we introduce in detail the research thinking and design process of attack signal feature extraction method of MPTCP transmission system. In Sect. 4, we elaborate on the construction of MPTCP transmission system simulation environment and the results of experimental operation, and finally draw experimental conclusions. In Sect. 5, we give a brief summary of the paper and look into the future work and challenges to be faced.

2 Wavelet Transform and Wavelet Energy Entropy

2.1 Wavelet Transform

Wavelet transform is a time-frequency domain multi-resolution function analysis method based on FT (Fourier Transform), which attracts more and more attention. At first, the wavelet transform analysis method was used to analyze the local characteristics of seismic signals, but now it has been gradually applied in nonlinear scientific research fields such as data compression, speech analysis and processing, fault detection and signal analysis [13]. In this method, the infinite trig function basis of FT is replaced by the attenuation wavelet basis of finite length, which overcomes and breaks through the limitation of FT, and has good localization properties in both time domain and frequency domain, and solves the problem of resolution contradiction between time domain and frequency domain [14].

The basic principle of wavelet transform is a process of multi-scale decomposition (transformation) or reconstruction (inverse transformation) of time-varying signals through the expansion and translation operation of wavelet to form wavelet basis (wavelet function), analyze the general picture or details of signals, and realize the analysis of local characteristics of different time scales and space of signals [15]. Its main feature is that certain aspects of the problem are sufficiently highlighted through transformations, culminating in temporal segmentation at high frequencies and frequency segmentation at low frequencies, so that any detail of the signal can be attended to and the time-frequency variation characteristics of the time series can be analysed through wavelet coefficients.

The selection of wavelet function is the premise of wavelet analysis. It refers to a class of functions that are oscillatory and can rapidly decay to zero, namely, the wavelet function $\psi(t) \in L^2(R)$ and satisfy:

$$\int_{-\infty}^{+\infty} \psi(t)\, dt = 0 \tag{1}$$

After a series of scaling and translation operations, it can form the general form of the wavelet function [16],

$$\psi_{a,b}(t) = |a|^{-\frac{1}{2}} \psi\left(\frac{t-b}{a}\right), a, b \in R, a \neq 0 \tag{2}$$

where, $\psi_{a,b}(t)$ is basic wavelet; a is the scaling scale, reflecting the period length of wavelet; b is the translation parameter, the translation in reaction time. For the same signal or time series, if different wavelet functions are selected, the results will often be different, sometimes even very different. The most common wavelet transform forms are CWT (Continuous Wavelet Transform) and DWT (Discrete Wavelet Transform) [17].

For any given finite signal $f(t) \in L^2(R)$, its continuous wavelet transform form is

$$W_f(a,b) = |a|^{-\frac{1}{2}} \int_R f(t)\, \overline{\psi}\left(\frac{t-b}{a}\right) dt \tag{3}$$

where, $W_f(a,b)$ is the CWT coefficient, $\overline{\psi}\left(\frac{x-b}{a}\right)$ and is the complex conjugate function of $\psi\left(\frac{x-b}{a}\right)$. For discrete time series signals, suppose the function $f(k\Delta t)$ ($k = 1, 2, \cdots N$; Δt is the sampling interval), then the discrete wavelet transform form is [18]

$$W_f(a,b) = |a|^{-\frac{1}{2}} \Delta t \sum_{k=1}^{N} f(k\Delta t)\, \overline{\psi}\left(\frac{k\Delta t - b}{a}\right) \tag{4}$$

At this point, $W_f(a,b)$ is the DWT coefficient.

2.2 Information Entropy

In the 1940s, C. E. Shannon proposed the basic concept of information entropy by referring to the concept of thermodynamics, and gave the mathematical expression of information entropy. In information theory, information entropy describes the uncertainty of each possible event of information source, and represents the average amount of information provided by each symbol and the average uncertainty of information source [19,20]. Information entropy can generally be used as a quantitative statistical indicator of the information content of a system, and can also be used to estimate the complexity of random signals.

For a system with an uncertain state, if a random variable X is used to characterize the state of the system, the probability of x_j is $p_j = p\{X = x_j\}, j =$

$1, \cdots, L$, and $\sum_{j=1}^{L} p_j = 1$, the information obtained from a certain result of X can be represented by $I_j = \log(1/p_j)$, so the information entropy of X is [21]

$$H(X) = -\sum_{j=1}^{L} p_j \log(p_j) \tag{5}$$

where, when $p_j = 0$, $p_j \log(p_j) = 0$. It is easy to see from the form of expression that information entropy has the basic properties of monotonicity, non-negativity and accumulation.

2.3 Wavelet Energy Entropy

Wavelet transform has good ability of time-frequency localization analysis. Multi-scale analysis brings the construction and implementation of wavelet function into a unified framework and has corresponding practical fast algorithm. Therefore, wavelet energy entropy of signal can be obtained by combining wavelet transform analysis method with information entropy theory.

Let $E = E_1, E_2, \cdots, E_m$ be the wavelet energy entropy of the signal $x(t)$ at the m scale. In a given time window, the power E_j of each component is added up to equal the total power of the signal. Suppose $p_j = E_j/E$, then the corresponding wavelet energy entropy is defined as [22]

$$WEE = -\sum_{j=1} p_j \log(p_j) \tag{6}$$

3 Attack Signal Feature Extraction Method of MPTCP Transmission System

Based on previous theoretical research, according to the characteristics of MPTCP transmission system multipath parallel transmission, wavelet transform analysis method, information entropy theory knowledge, in MPTCP transmission system, wavelet entropy correlation technology is used to design feature extraction method suitable for multipath transmission system attack signal. This method can realize online monitoring and anomaly detection of transmission system and provide a new solution to anomaly detection in multipath transmission system. The general steps of the attack signal feature extraction method are shown in Fig. 1.

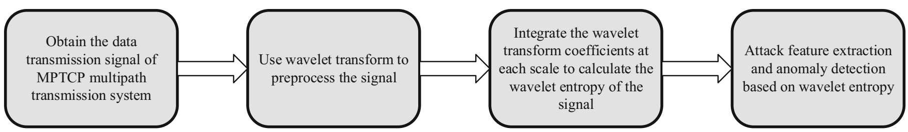

Fig. 1. Schematic diagram of MPTCP attack signal feature extraction method.

According to the schematic diagram of the above operation process, this feature extraction method can roughly include signal preprocessing, wavelet energy entropy calculation, attack signal feature extraction and anomaly detection.

3.1 Signal Preprocessing

From a macroscopic point of view, the large-scale network traffic in MPTCP transmission system almost shows all the characteristics of signals [23]. Therefore, we can regard MPTCP network transmission data flow as signal, and further analyze the characteristics of MPTCP transmission data flow, such as change trend, change amplitude and change period, by using signal processing method. Under normal circumstances, the collected signals can not be directly extracted from the features, often need to be preprocessed. Therefore, this paper uses wavelet transform analysis method to denoise and scale decompose the original signal.

The wavelet denoising method in this paper uses threshold denoising method [24]. Its basic principle is to set a threshold value for the wavelet coefficients on the decomposition scale, and it is considered that the wavelet coefficients smaller than the threshold value are caused by noise, and the wavelet coefficients larger than the threshold value are caused by signals. Then, the wavelet coefficients corresponding to the noises on these decomposition scales are thresholding to zero, and the wavelet coefficients corresponding to the signals on these decomposition scales are retained [25]. Finally, the thresholding signal is reconstructed, so the reconstructed signal is denoising signal based on wavelet transform, and the next step of feature extraction can be carried out.

In general, two problems need to be considered to extract signal features by wavelet decomposition: the selection of wavelet basis function and the determination of decomposition layers. If there are too few layers, it is difficult to extract fault details of signals, while if there are too many layers, the calculation is complicated, feature extraction dimension is high, and transmission and storage costs are high [26]. At present, we use different wavelet functions and decomposition layers to decompose and reconstruct the transmitted signal, and determine the best wavelet basis function and decomposition scale by comparing with the original signal.

3.2 Calculation of Wavelet Energy Entropy

After wavelet transform, the original signal is mapped to the time-scale plane, and the signal changes can be observed at multiple scales (different resolutions) at any time interval. Because a large number of wavelet decomposition coefficients reflect the results of wavelet transform multi-resolution analysis, these coefficients contain a large amount of characteristic information about the transmission system or the signal itself [27]. Assuming that each scale is a signal source, the wavelet coefficients at each scale are equivalent to the information sent by a signal source. Therefore, in this paper, these wavelet transform coefficients are fused and processed effectively, and the universal characteristics of signals in MPTCP multipath transmission system are characterized by calculating the wavelet energy entropy of signals.

3.3 Attack Feature Extraction and Anomaly Detection

For non-stationary signals, a good time-frequency analysis method can detect the unstable change of signal frequency with time, and then extract the important features of the signal. In this paper, according to the calculated wavelet energy entropy, through the comparison of experimental results to achieve the accurate differentiation of normal signals and attack signals, more intuitive, effective and convenient to carry out information extraction, signal detection and feature recognition of various transmission signals in the MPTCP transmission system.

4 Experimental Simulation Analysis

In order to verify the rationality and effectiveness of the attack signal feature extraction method of the MPTCP transmission system, this paper simulates the MPTCP multipath transmission system based on NS2 experimental platform. In addition, this document uses LDDoS (Lowrate Distributed Denial Service) attacks [28] as an example to simulate a network attack on a multipathing transmission system. Finally, the reliability of wavelet energy entropy as attack feature classification is verified by comparing the results of wavelet energy entropy without attack and with attack, so as to realize feature extraction and anomaly detection of network attack signals in MPTCP multipath transmission system.

4.1 Simulation Environment Construction

In this paper, the MPTCP multipath transmission system is built on the NS2 simulation experimental platform based on TCL (Tool Command Language) programming, and the end-to-end multipath parallel transmission communication between communication devices is simulated. At the same time, in order to simulate the network attack of MPTCP multipath transmission system, this paper deploys ten dummy computers to send LDDoS attack data stream to a router at the same time, and ensures the best attack effect.

As shown in Fig. 2, in the simulated MPTCP multipath transmission system, the Sender (server) and the Receiver (multi-host mobile terminal device) are realizing parallel multipath data transmission through three different communication modes (Path A, Path B and Path C), and ten puppet machines ($Attack_0, Attack_1, \cdots, Attack_9$) are simultaneously attacking the router R_0. In this case, the MPTCP multipath transmission system includes normal data flow and LDDoS attack data flow. Table 1 shows the settings of basic parameters such as the bandwidth, transmission delay, and path management algorithm of each transmission path in the MPTCP multipath transmission system. The total data transmission time is 300 s. Except that the network parameters of LDDoS

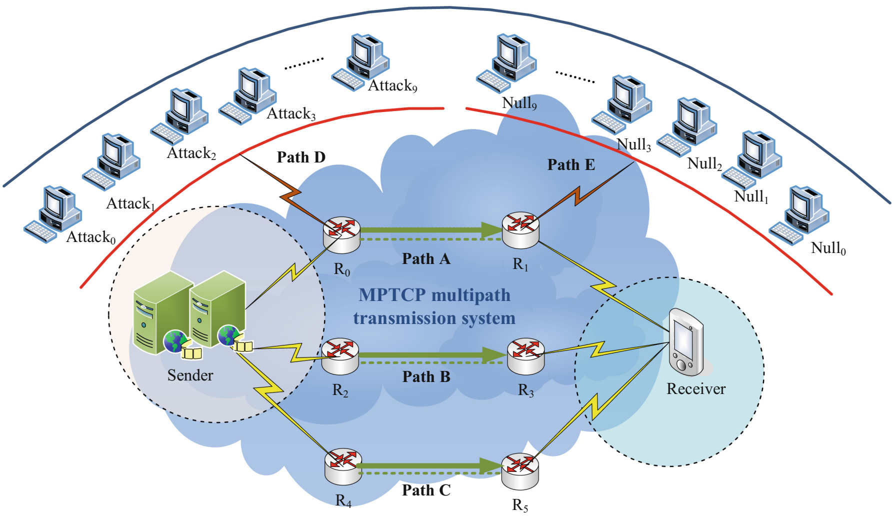

Fig. 2. MPTCP multipath transmission system network topology.

Table 1. MPTCP multipath transmission system network parameter settings.

Path	Bandwidth	Transfer delay	Path management algorithm
Path A	10 Mb	50 ms	DropTail
Path B	10 Mb	50 ms	DropTail
Path C	10 Mb	50 ms	DropTail
Path D	1 Mb	50 ms	DropTail
Path E	1 Mb	50 ms	DropTail

attack are different, the network topology parameters in the case of no attack are the same as those in the case of attack.

As for the simulation implementation of LDDoS attack in MPTCP multipath transmission system, this experiment realizes constant bit rate data transmission based on CBR type data packets, and each packet size is 200 bytes. We set the attack period of LDDoS attack as 200 ms, the attack duration as 600 ms and the attack rate as 1 Mbps. The specific parameter settings can be represented by the following expression [29]. P indicates the attack period, T indicates the attack duration, and V indicates the attack rate. In order to achieve better attack effect, this paper sets up ten dummy computers to launch network attacks of different durations on the transmission system on the nodes whose operation time is 50 s, 120 s and 200 s respectively.

$$LDDoS\,(P,T,V) = (200\,\text{ms}, 600\,\text{ms}, 1\,\text{Mbps}) \tag{7}$$

4.2 Simulation Results Analysis

Signal Preprocessing Results Analysis. In the signal preprocessing part, the experiment takes the throughput data obtained by the MPTCP multipath transmission system as the original signal, and applies the discrete wavelet transform technology to carry out threshold denoising and multi-scale decomposition. The wavelet basis function adopts db6 wavelet basis, and the number of decomposition layers is determined to be 6.

Discrete wavelet transform method mainly includes DWT decomposition method and DWT reconstruction method. The basic principle of DWT decomposition method is similar to that of signal filtering by using a pair of high-pass filter and low-pass filter. The basic principle of reconstruction method is roughly the same as that of decomposition method, but the operation direction is completely opposite [30]. In the signal decomposition part, the original signal is decomposed into level 1 approximate component signal and level 1 detail component signal after the first layer wavelet decomposition. The second layer wavelet decomposition is to decompose the approximate component signals obtained from the first layer, and so on. After the original signal is decomposed by six-layer multi-scale discrete wavelet transform, the specific decomposition results are shown in Fig. 3 and 4.

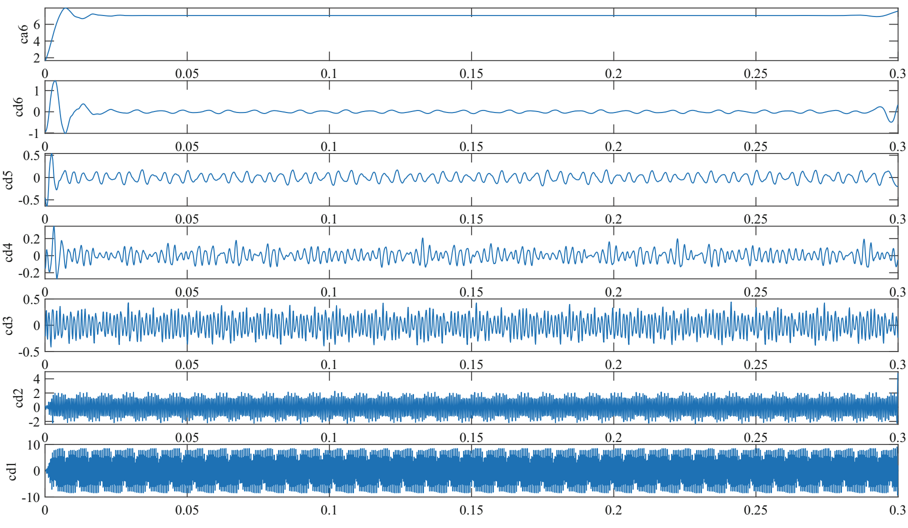

Fig. 3. Multi-scale detail component signal and level 6 approximate component signal without attack.

As shown in the Fig. 3 and 4, $cd1, cd2, \cdots, cd6$ respectively represent the detail component signals obtained by discrete wavelet multi-scale decomposition, and $ca6$ represent the level 6 approximate component signals obtained by discrete wavelet multi-scale decomposition. The multi-scale detail component

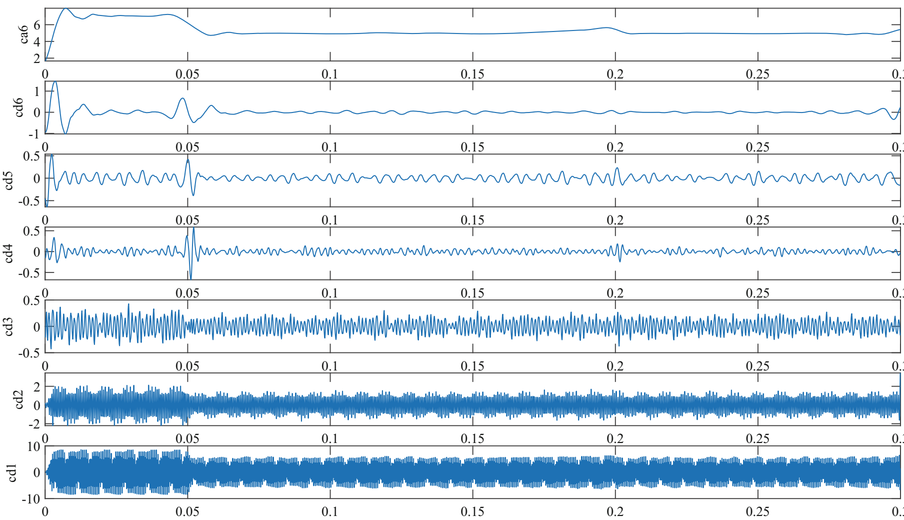

Fig. 4. Multi-scale detail component signal and level 6 approximate component signal under attack.

signal represents the high frequency information of the original signal, which is assumed to be the "noise" information of the original signal and continuously filtered out in the decomposition process. The multi-scale approximate component signal represents the low-frequency information of the original signal, and the level 6 approximate component signal is the decomposed signal obtained by the final wavelet decomposition. Figure 5 and 6 show the comparison of original signal and decomposed signal without attack and with attack.

As shown in the Fig. 5 and 6, whether in the case of no attack or with attack, the original signal with complex changes and frequent jitter is constantly removed from the influence of high-frequency noise during the decomposition process of discrete wavelet transform, and finally the decomposed signal with obvious change trend and easy for intuitive analysis is obtained. Thus, the characteristics of the original signal can be observed on a broad time scale, which really embodies the advantages of multi-scale time-frequency analysis of wavelet transform.

Wavelet Energy Entropy Comparative Analysis. The wavelet coefficients at each scale obtained from the above discrete wavelet multi-scale decomposition include various characteristic analyses of the transmission system or the signal itself. Based on Shannon information entropy theory, the wavelet energy entropy of the multi-scale signal is calculated and its change curve is drawn. Figure 7 shows the comparison of multi-scale wavelet energy entropy changes under the two conditions. As shown in the Fig. 7, the blue curve represents the change of wavelet energy entropy with the increase of scale in the case of no attack, and

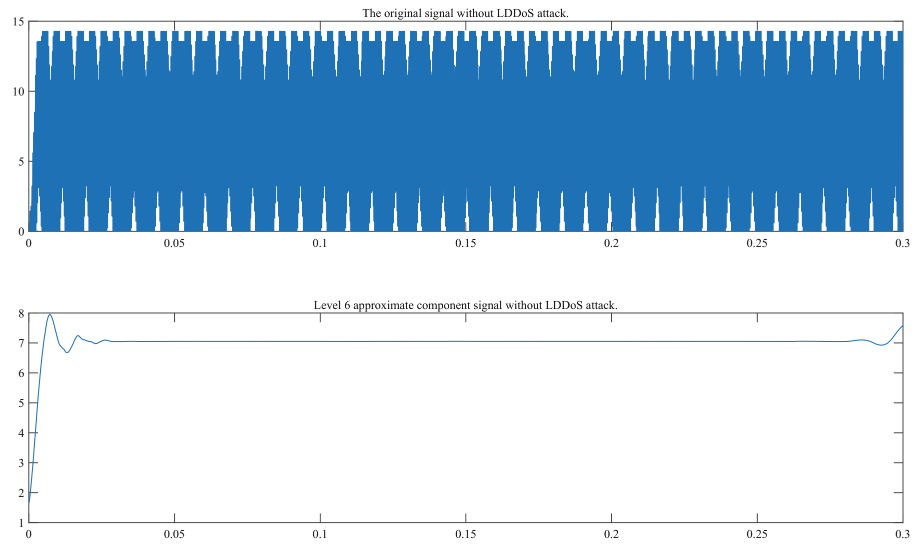

Fig. 5. Original signal and decomposition signal without attack.

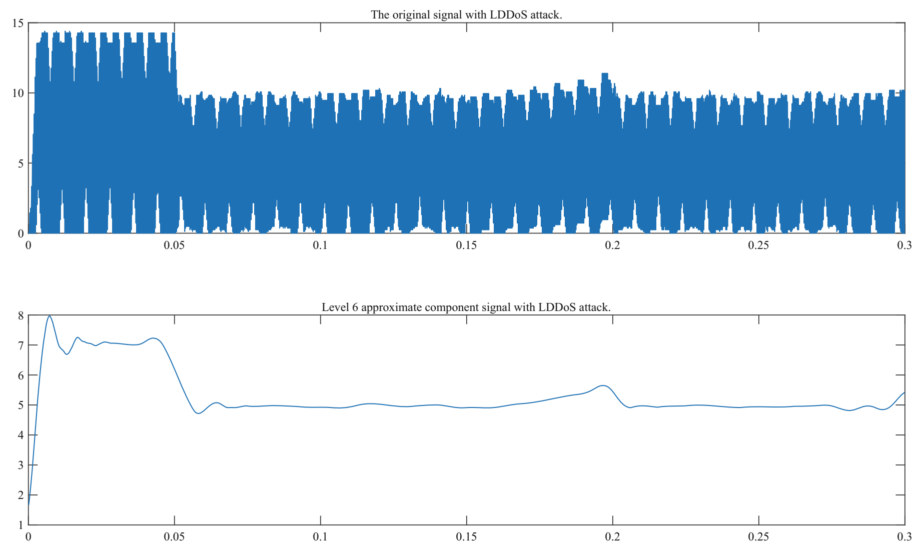

Fig. 6. Original signal and decomposition signal under attack.

the red curve represents the change of wavelet energy entropy with the increase of scale in the case of attack.

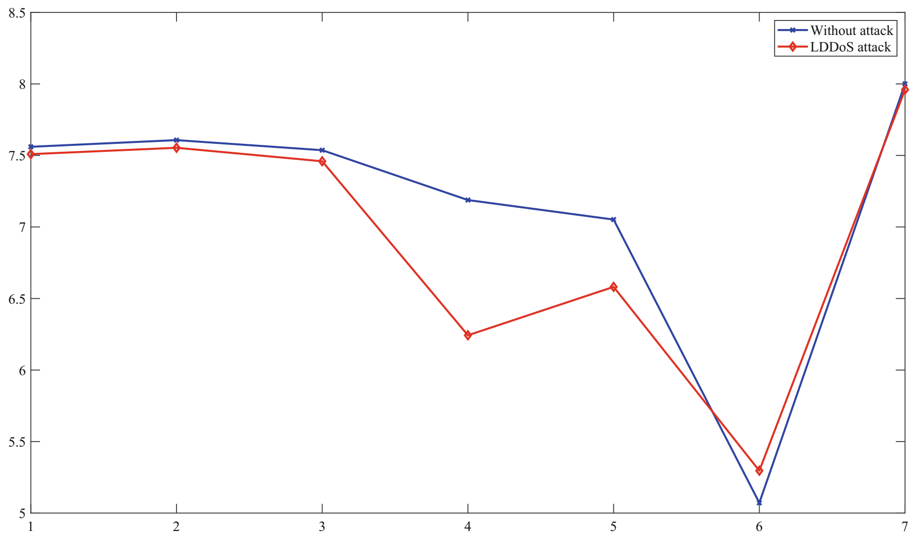

Fig. 7. Comparison diagram of multi-scale wavelet energy entropy change.

According to the working principle of wavelet energy entropy, the wavelet energy entropy value of multi-scale signal without attack is 7.5605, 7.6072, 7.5368, 7.1882, 7.0518, 5.0716, 8.0005 respectively. The wavelet energy entropy of multi-scale signal with attack is 7.5092, 7.5536, 7.4593, 6.2430, 6.5813, 5.2960 and 7.9596, respectively. In this paper, the mean value and variance of wavelet energy entropy are calculated to observe the overall trend of wavelet energy entropy under the two conditions. By calculation, the mean value of wavelet energy entropy without attack is 7.1452, and the variance is 0.9302. In the case of attack, the mean value of wavelet energy entropy is 6.9431 and the variance is 0.8878.

Through comparative analysis, it is found that the mean value of wavelet energy entropy in the case of attack is smaller than that in the case of no attack, and the variation range of wavelet energy entropy in the case of attack is smaller than that in the case of no attack. It can be found that attack abnormal signals can reduce the mean and amplitude of wavelet energy entropy of MPTCP multipath transmission signals, indicating that MPTCP transmission signals have worse similarity and higher complexity in the case of attack. Therefore, wavelet energy entropy can be used as the classification feature of normal signals and attack signals in the MPTCP multipath transmission system, and can be used as the indicator basis for abnormal detection of attack signals.

5 Conclusions and Future Works

In this paper, on the basis of the research status at home and abroad and the research dynamic, combined with the present trend of the development of the Internet, this paper proposes a MPTCP multipath transmission system to attack the signal feature extraction method, in order to achieve the anomaly recognition and detection of MPTCP transmission system to lay the theoretical foundation, thus improve the MPTCP multipath transmission network security and robustness of the system. This method combines the wavelet transform analysis method with the information entropy theory, and uses the wavelet energy entropy to distinguish the normal signal from the attack signal, so as to achieve the purpose of feature extraction of the attack signal. The simulation results show that wavelet energy entropy can be used as the classification feature of normal signal and attack signal in the MPTCP transmission system, and the feature extraction method is reasonable and effective. However, the change trend of the wavelet energy entropy index used in the feature extraction method depends on the decomposition scale of the wavelet transform, which may lead to the stability of the experimental results need to be further strengthened. In the future research work, on the basis of the wavelet transform analysis method, we can study the wavelet variance based on the wavelet transform coefficients, compare and analyze the wavelet variance and the wavelet energy entropy, compare the advantages and disadvantages of the two methods, and further improve research on feature extraction method of attack signal in the MPTCP multipath transmission system.

References

1. Cao, Y., Liu, Q., Zuo, Y., Ke, F., Wang, H., Huang, M.: Receiver-centric buffer blocking-aware multipath data distribution in MPTCP-based heterogeneous wireless networks. KSII Trans. Internet Inf. Syst. **10**(10), 4642–4660 (2017)
2. Nguyen, K., Kibria, M., Ishizu, K., Kojima, F., Sekiya, H.: An approach to reinforce multipath TCP with path-aware information. Sensors **19**(3), 476 (2019)
3. Cao, Y., Ji, R., Ji, L., Shao, X., Lei, G., Wang, H.: MPTCP-meLearning: a multi-expert learning-based MPTCP extension to enhance multipathing robustness against network attacks. IEICE Trans. Inf. Syst. **E104D**(11), 1795–1804 (2021)
4. Zhu, M., et al.: BELIA: bandwidth estimate-based link increase algorithm for MPTCP. IET Netw. **6**(5), 94–101 (2017)
5. Cao, Y., Ji, R., Ji, L., Lei, G., Wang, H., Shao, X.: l^2-MPTCP: a learning-driven latency-aware multipath transport scheme for industrial internet applications. IEEE Trans. Industr. Inform. **18**, 8456–8466 (2022)
6. Cao, Y., Ji, R., Huang, X., Lei, G., Shao, X., You, I.: Empirical mode decomposition-empowered network traffic anomaly detection for secure multipath TCP communications. Mob. Netw. Appl. (2022)
7. Li, B., Chen, X.: Wavelet-based numerical analysis: a review and classification. Finite Elem. Anal. Des. **81**, 14–31 (2014)
8. Ling, T., Liu, H., Gong, S., Huang, F.: Construction and application of a new biorthogonal wavelet basis for a quantitative analysis of GPR signals. J. Appl. Geophys. **170**, 103837 (2019)

9. Hu, R., Monebhurrun, V., Himeno, R., Yokota, H., Costen, F.: An adaptive least angle regression method for uncertainty quantification in FDTD computation. IEEE Trans. Antennas Propag. **66**(12), 7188–7197 (2018)
10. Hu, R., Monebhurrun, V., Himeno, R., Yokota, H., Costen, F.: A general framework for building surrogate models for uncertainty quantification in computational electromagnetics. IEEE Trans. Antennas Propag. **70**(2), 1402–1414 (2021)
11. Li, Q., Tong, X.: Application of wavelet analysis method in radar echo signal detection. In: Han, S., Ye, L., Meng, W. (eds.) AICON 2019. LNICST, vol. 286, pp. 327–333. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-22968-9_28
12. Wu, M., Shanmugam, S., Welsch, C., Yi, M.: Palmitoylation of hepatitis C Virus NS2 regulates its subcellular localization and NS2-NS3 autocleavage. J. Virol. **94**(1) (2020)
13. Hu, R., Liu, Y., Gu, K., Min, X., Zhai, G.: Toward a no-reference quality metric for camera-captured images. IEEE Trans. Cybern. (2021)
14. Kumar, T., Mandal, U.: Wavelet transform associated with linear canonical Hankel transform. Math. Methods Appl. Sci. **42**(9), 3167–3178 (2019)
15. Abuhamdia, T., Taheri, S., Burns, J.: Laplace wavelet transform theory and applications. J. Vib. Control **24**(9), 1600–1620 (2018)
16. Ramya laxmi, K., Pallavi, S., Ramya, N.: A hybrid approach of wavelet transform using lifting scheme and discrete wavelet transform technique for image processing. In: Satapathy, S.C., Raju, K.S., Shyamala, K., Krishna, D.R., Favorskaya, M.N. (eds.) Advances in Decision Sciences, Image Processing, Security and Computer Vision. LAIS, vol. 3, pp. 643–651. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-24322-7_76
17. Pandey, C., Phukan, P.: Continuous and discrete wavelet transforms associated with Hermite transform. Int. J. Anal. Appl. **18**(4), 531–549 (2020)
18. Shin, D.K., Moon, Y.S.: Super-resolution image reconstruction using wavelet based patch and discrete wavelet transform. J. Signal Process. Syst. **81**, 71–81 (2015)
19. Li, Z., Qu, L., Zhang, G., Xie, N.: Attribute selection for heterogeneous data based on information entropy. Int. J. Gen. Syst. **50**(5), 548–566 (2021)
20. Gao, J., Liu, F., Zhang, J., Hu, J., Cao, Y.: Information entropy as a basic building block of complexity theory. Entropy **15**(9), 3396–3418 (2014)
21. Salazar, S.J.C., Laguna, H.G., Dahiya, B., Sagar, R.P.: Correction to: Shannon information entropy sum of the confined hydrogenic atom under the influence of an electric field. Eur. Phys. J. D **75**(255), 127 (2021)
22. Chen, Y., Zhang, Y., Lu, H.M., Chen, X., Li, J., Wang, S.: Wavelet energy entropy and linear regression classifier for detecting abnormal breasts. Multimed. Tools Appl. **77**, 3813–3832 (2018)
23. Tychkov, A.Y., Alimuradov, A.K., Churakov, P.P.: Erratum to: adaptive signal processing method for speech organ diagnostics. Meas. Tech. **59**, 684 (2016)
24. Wu, G., He, Y.: Application of wavelet threshold denoising model to infrared spectral signal processing. Spectrosc. Spectr. Anal. **29**(12), 3246–3249 (2009)
25. Zhang, X., Zou, Z., Guo, H., Yin, J.: Wavelet denoising Method with a novel wavelet threshold function applied in enoising ship maneuvering test data. Indian J. Geo-Marine Sci. **46**(9), 1780–1787 (2017)
26. Khatter, A., Reddy, N., Thakur, A.: Wavelet decomposition based authentication scheme for dental CBCT images. In: Kolhe, M.L., Tiwari, S., Trivedi, M.C., Mishra, K.K. (eds.) Advances in Data and Information Sciences. LNNS, vol. 94, pp. 567–576. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-0694-9_53

27. Patil, D.D., Singh, R.P.: ECG classification using wavelet transform and wavelet network classifier. In: Dash, S.S., Naidu, P.C.B., Bayindir, R., Das, S. (eds.) Artificial Intelligence and Evolutionary Computations in Engineering Systems. AISC, vol. 668, pp. 289–303. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-7868-2_29
28. Lei, G., Ji, L., Ji, R., Cao, Y., Yang, W., Wang, H.: Can wavelet transform detect LDDoS abnormal traffic in multipath TCP transmission system? Secur. Commun. Netw. **2021**, 1–8 (2021)
29. Lei, G., Ji, L., Ji, R., Cao, Y., Shao, X., Huang, X.: Extracting low-rate DDoS attack characteristics: the case of multipath TCP-based communication networks. Wireless Commun. Mob. Comput. **2021**, 1–10 (2021)
30. Dutt, R., Balouria, A., Acharyya, A.: Discrete wavelet transform based methodology for radar pulse deinterleaving. CSI Trans. ICT **7**, 141–147 (2019)