Wavelet and Kalman Filter-Empowered Traffic Detection for Secure QUIC Network Communication

Liang Shan[1,2(✉)], Junyi Wu[1,2], Keyang Gu[1,2], Jinquan Nie[1,2], and Riqing Xu[1,2]

[1] School of Software, Jiangxi Normal University, Nanchang 330022, China
{shanliang1981,wujunyi,gukeyang,jqnie,yhfan,richard}@jxnu.edu.cn
[2] Jiangxi Provincial Engineering Research Center of Blockchain Data Security and Governance, Nanchang 330022, China

Abstract. HTTP/3.0 is an application layer protocol built on top of QUIC, which utilizes its characteristics to provide faster and more reliable data transmission. The combi-nation of HTTP/3.0 and QUIC is considered an important development direction for the next generation of internet transmission protocols. QUIC (Quick UDP In-ternet Connection), as an efficient data transmission protocol, can provide better data transmission quality and user experience with its low latency and high data transmission speed characteristics. However, various new network attacks such as LDDoS attacks constantly threaten the transmission capability and robustness of QUIC transmission systems. To solve this problem, based on the Self-similarity and randomness of QUIC network traffic, a traffic detection model of QUIC network communication based on wavelet and Kalman filter is proposed. First, simulate LDDoS attack through NS3, then use wavelet transform to pre-process the jitter signal after the attack, and then use Kalman filter to denoise. At last, it is compared with the jitter signal which is processed only by Kalman filter. The experiment proves that this method can be used for attack detection and pre-vention of network nodes.

Keywords: QUIC · LDDoS attack · Wavelet transform · Wavelet transform

1 Introduction

1.1 A Subsection Sample

HTTP/3.0 is a new generation HTTP protocol based on the QUIC protocol, with lower latency, better congestion control mechanism, and better security. The combination of HTTP/3.0 and QUIC points the way for the development of next-generation inter-net transmission protocols. The development of HTTP/3.0 has solved some perfor-mance issues of HTTP/2.0 under high latency and high packet loss rates. QUIC, as the underlying transport protocol of HTTP/3.0, has new features such as fast connec-tion establishment, multiplexing, and fast

Y. Cao and X. Shao (Eds.): DIONE 2023, LNICST 515, pp. 137–149, 2025.
https://doi.org/10.1007/978-3-031-80713-8_10

retransmission. In order to quickly establish a connection and reduce the low latency of the connection, QUIC directly sends data when establishing the connection, which is a 0-RTT method that improves the con-nection speed compared to the network latency of TCP triple handshake. In addition, QUIC uses the Connection ID as a unique identifier, so when the network link state changes, no additional handshake reconnection time will be added. The QUIC proto-col also supports multiplexing technology, which means that multiple data streams can be transmitted simultaneously in a connection without waiting for the previous data stream to complete. This can improve the load capacity of the connection while ensuring network transmission efficiency and speed. In order to quickly retransmit data packets and reduce transmission delays caused by network packet loss, QUIC has established a fast retransmission mechanism. If a packet with a smaller than expected sequence number is received, QUIC can use a timestamp to determine whether the packet has timed out and quickly decide whether to retransmit.

However, the fast connection establishment, multiplexing, and fast retransmis-sion features of the QUIC protocol are also easily exploited by some malicious at-tackers for launching DoS, DDoS, and LDDoS (Low and Slow Distributed Denial of Service) attacks, mainly manifested in the following aspects:

- The quick connection mechanism of the QUIC protocol allows attackers to estab-lish a large number of connection requests in a short period of time, occupying server resources, and causing a denial of service attack (DoS).
- QUIC protocol multiplexing technology, which transfers multiple application streams in parallel on the same QUIC connection, allows attackers to launch LDDoS attacks on a single connection that are difficult to accurately detect and filter.
- The rapid retransmission mechanism of the QUIC protocol allows attackers to occupy network bandwidth and cause a denial of service (DoS) attack in case of network congestion through rapid retransmissions.
- The timestamp mechanism of the QUIC protocol allows attackers to forge the source IP address and send a large number of low-speed and long-lasting LDDoS attacks to avoid being detected by some security devices.

The large-scale deployment and application of emerging information technolo-gies have led to an increasing number of various network attacks. An increasing number of network security studies have pointed out that many network attacks have the ability to adapt to targets and can be hidden in massive network backend traffic, causing a loss of normal user traffic and posing a serious threat to network services [1,2]. Therefore, there is an urgent need to study solutions to improve the defense capability and robustness of QUIC networks, such as adding firewall rules, traffic filtering, and other measures. This paper proposes a QUIC network traffic anomaly detection model based on wavelet transform and Kalman filter. First, simu-late LDDoS attack through NS3, then use wavelet transform to preprocess the jitter signal after the attack, and then use Kalman

filter to further denoise. Experiments show that this method has better denoising effect than the method using only Kal-man filter, and can effectively detect LDDoS attacks.

2 Related Work

2.1 A Subsection Sample

At present, the research on the security of QUIC is still in its infancy, especially the research on network traffic anomaly detection based on QUIC is still relatively lack-ing. A large number of studies have shown that the analysis and detection of network traffic is the focus of research on discovering abnormal network traffic. For different network application scenarios, researchers have proposed a variety of abnormal network traffic detection methods. t. Although there are more and more studies, there is still a lack of research on the security of the QUIC protocol. Numerous studies have shown that the analysis and detection of network traffic are the focus of research to find abnormal network traffic. Researchers have recently proposed various abnormal network traffic detection methods for different network application scenarios. Leland et al. [3] first discovered the self-similarity of network traffic. This feature has also been proved to be the basis for judging normal flow in subsequent studies [4,5]. Sheluhin et al. [6] used a multi-scale analysis method combined with wavelet analysis to study the multi-fractal characteristics of network traffic and realized the genera-tion of abnormal traffic by monitoring fractal dimension jumps. Pei et al. [7] proposed a user-customizable personalized anomaly detection framework to detect the generation of abnormal traffic in the network and also presented an anomaly detec-tion method with long short-term memory. The method has the characteristics of network self-encoding. A. Minh Tuan Nguyen, and K. K. B et al. [8] proposed a new network intrusion detection system (NIDS) algorithm that directly selects improved feature subsets for network intrusion detection by utilizing exhaustive search based on genetic algorithm (GA) and fuzzy C-means clustering (FCM).

Among all network attack detection, the detection of LDDoS (Low and Slow Dis-tributed Denial of Service) attacks has received much attention. The reason is that LDDoS attacks are different from previous flooding attacks, as they send requests or connections at very low rates, typically much slower than normal traffic. Due to the low rate of LDDoS attacks, which mix attack traffic with normal traffic, traditional IDS cannot effectively detect them [9], thereby effectively interfering with the nor-mal operation of the target system. Therefore, there is an urgent need to implement effective detection and defense against LDDoS attacks. YU CHEN, KAI HWANG et al. proposed a detection method based on digital signal processing, with the main idea of extracting the frequency domain characteristics of traffic for detection [10–12]. However, this detection method has a high rate of missed detection, and the different values of frequency points result in unstable detection results. With the promotion of Kalman filter algorithm in the fields of geology, navigation and signal, ZJ Wu, M Yue proposed

a LDDoS attack detection method based on Kalman filter, and used the error between the one-step prediction value and the optimal estimation as the standard of LDDoS attack detection [13]. This paper proposes an anomaly detection method for QUIC network based on wavelet transform and Kalman filter, which is used to detect LDDoS attacks in QUIC network. The experimental results show that it has better detection effect than the traditional anomaly detection method using only Kalman filter.

3 Principle of Wavelet Transform

3.1 A Subsection Sample

Wavelet transform is a signal analysis method that can decompose signals into sub signals of different frequencies and provide local information in terms of time and frequency. Wavelet transform is based on a set of functions (wavelet functions) that exhibit time and frequency localization characteristics. The principle of wavelet transform can be summarized as the following steps:

(1) Choose a wavelet basis function: First, you need to choose a wavelet basis function that is suitable for the signal characteristics. Commonly used wavelet basis functions include Haar, Daubechies, Morlet, etc.
(2) Continuous wavelet transform: for Continuous signal x (t), wavelet transform calculates the wavelet coefficient by inner product of signal and wavelet basis function. The formula for continuous wavelet transform is as follows:

$$w(a,b) = \int x(t)\psi(a,b)dt \tag{1}$$

Among them, a and b are scaling factors (controlling the scaling of wavelet functions) and smoothing factors (controlling the movement of wavelet functions), $\psi(a,b)$ are wavelet basis functions.
(3) Discrete wavelet transform: for the discrete signal x [n], the wavelet transform can be calculated by Discretization. Discrete wavelet transform uses discrete wavelet basis function, which is realized by cascade filtering and down sampling of signals. Usually, iterative methods are used for multi-level wavelet decomposition.
(4) Wavelet decomposition: through continuous or Discrete wavelet transform, the signal can be decomposed into sub signals of different scales (frequencies). Each scale corresponds to a low-frequency part (approximate coefficient) and a high-frequency part (detail coefficient). Wavelet decomposition provides local information of signals in terms of time and frequency, and higher scale detail coefficients represent higher frequency signal features.
(5) Wavelet reconstruction: By performing inverse wavelet transform on approximation coefficients and detail coefficients, the decomposed signal can be reconstructed back to the original signal. The wavelet basis function used in the reconstruction process is the inverse transformation of the original wavelet basis function.

Wavelet transform has many advantages, such as time-frequency locality, multi-resolution analysis ability and good compression performance. It is widely used in many fields, such as signal processing, image processing, data compression, pattern recognition, etc. By analyzing wavelet coefficients at different scales, more comprehensive signal feature information can be obtained, thereby achieving more accurate signal analysis and processing.

4 Kalman Filter Theory

4.1 A Subsection Sample

Kalman filter is the best and most efficient algorithm [14]. The main idea of Kalman filter algorithm is based on a state space model, which describes the system state, observation value and state transition law. At each time, the Kalman filter updates the state estimation at the current time through the state transition equation and ob-servation equation according to the state estimation and observation values at the previous time. By iterating this process, the Kalman filter can continuously revise and update the state estimation to obtain the optimal estimation of the system state. The recursive filtering process of Kalman filter is mainly divided into two steps: prediction step and update step.

a. Prediction steps: The prediction step of Kalman filter algorithm gives a series of time updating equations, which realizes the prediction function of current time state variables. The algorithm implementation of the prediction step is as follows [15].

$$\hat{x}_{k|k-1} = F_k \hat{x}_{k-1|k-1} + B_k u_k \tag{2}$$

$$\hat{P}_{k|k-1} = F_k P_{k-1|k-1} F_k^T + Q_k \tag{3}$$

Among them, xk—k-1 is the prior predictive value of the state variable at the current time, Fk is the State-transition matrix, xk-1—k-1 is the posterior estimate of the state variable at the previous time, Bk is the input control matrix, uk is the control varia-ble of the current state, Pk—k-1 is the prior predicted value of the covariance of the current state variable, and Qk is the covariance of the process noise. With the prior predicted values at the current moment, it is possible to prepare for the next step of updating the posterior estimate of the current state based on the measured val-ues.

b. Update steps: The update step of Kalman filter algorithm gives a series of measurement update equations, which realizes the correction function of the current state variable's predicted value.

$$K_k = \hat{P}_{k|k-1} H_k^T (H_k \hat{P}_{k|k-1} H_k^T + R_k)^{-1} \tag{4}$$

$$\hat{x}_{k|k} = \hat{x}_{k-1|k-1} + K_k y_k - H_k \hat{x}_{k|k-1} \tag{5}$$

$$\hat{P}_{k|k} = \hat{P}_{k-1|k-1} + H_k y_k - H_k \hat{x}_{k|k-1} \tag{6}$$

Among them, yk is the measurement value at time k, Hk is the observation matrix, Rk is the measurement noise covariance, Kk is the Kalman gain, and xk—k is the pos-terior estimate of the state variable at the k-th moment, Pk—k is the posterior esti-mate of the state covariance at the k-th moment. By iterating the prediction step and the update step, the Kalman filter can provide the optimal estimation of the system state and has good anti noise performance. To sum up, the workflow of the Kalman filter algorithm is shown in Fig. 1

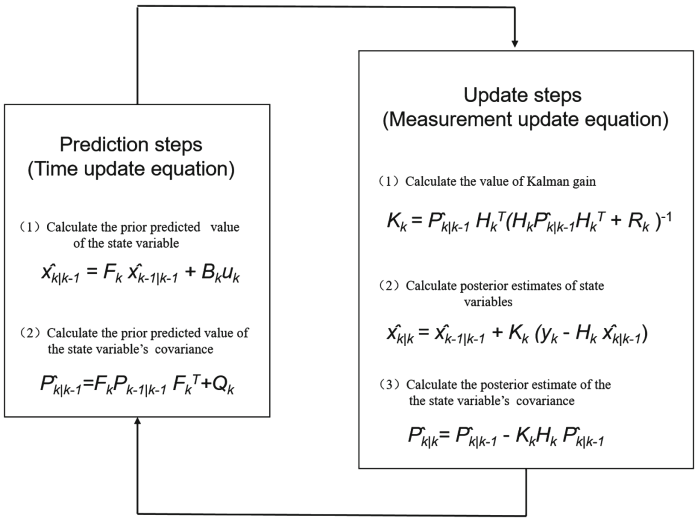

Fig. 1. Data Processed by Wavelet Transform and Kalman filter

5 Data Processing for Wavelet Denoising

5.1 A Subsection Sample

In the QUIC network, once subjected to LDDoS attacks, the transmission of data packets will experience significant fluctuations due to increased delay jitter. According to this fact, this paper proposes an anomaly detection method of QUIC network based on wavelet transform and Kalman filter. LDDoS (Low and Slow Distributed Denial of Service) attack is a variant of distributed denial of service (DDoS) attack. Unlike traditional DDoS attacks, LDDoS attacks employ a low and slow approach to evade detection and prevention by conventional DDoS mitigation mechanisms. The basic principle of LDDoS attacks is to utilize a large number of distributed attack nodes to send requests or occupy service resources at extremely low rates and frequencies. Attackers can initiate a large number of QUIC connection requests, occupying the connection resources of the target server, greatly affecting the quick establishment of QUIC connections. Attackers

can also take advantage of QUIC's support for multiple parallel data streams, maliciously sending large amounts of data streams, occupying server resources, and leading to a decrease in service performance. To detect LDDoS attacks, we must first study the characteristics of network traffic when attacks occur. This article uses the NS3 network simulator to simulate the transmission signal of the QUIC network, and combines it with the DCE (Direct Code Execution) plugin to simulate LDDoS attacks in NS3. The time series Line chart of the original data with LDDoS jitter obtained through NS3 simulation drawn by MATLAB software is shown in Fig. 2 The original signal is extracted as the observation value of the Kalman filter combination model based on wavelet analysis. The jitter delay of QUIC signal with a duration of 40 s and an attack time of 20 s is extracted as a data acquisition Index set for comparison and analysis of the algorithms proposed in this paper.

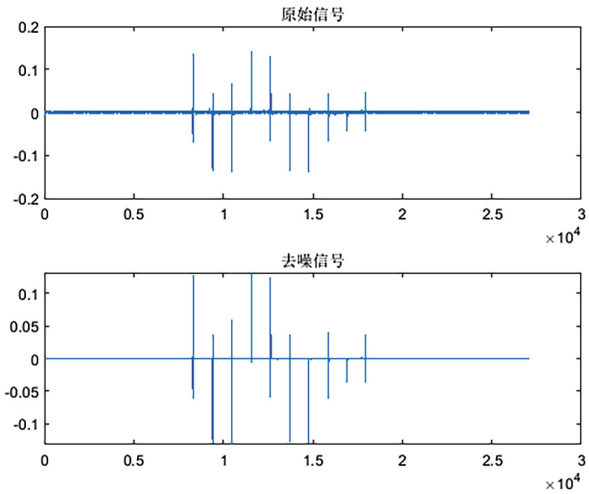

Fig. 2. Jitter amplitude after LDDoS attack

From Fig. 2, it can be seen that during the attack period (10 s to 30 s), the traffic at the victim end decreased and the traffic jitter became stronger. In order to provide smoother detection data for subsequent Kalman filter, it is necessary to carry out wavelet transform on the sampled signal to extract the change trend of waveform. This article uses Haar wavelet to perform the first stage of smoothing and denoising on the above data using three-level decomposition. Haar wavelet is the simplest orthogonal wavelet function, and its formula is as follow.

$$\Psi(\mathbf{t}) = \begin{cases} 1 & 0 \leq t < 1/2 \\ -1 & 1/2 \leq t < 1 \\ 0 & others \end{cases} \tag{7}$$

Among them, (t) Represents the Haar wavelet function, and t represents the time variable. Haar wavelet function appears in the form of Step function and has block structure. It is a compact wavelet basis function commonly used in fields such as signal analysis, data compression, and image processing. The comparison between the original signal and the denoised signal processed using Haar wavelet is shown in Fig. 3. After this transformation, the original waveform becomes relatively smooth. Only before and after the attack, there is no sudden change in the short interval. At the same time, the amount of data to be processed is reduced, which is more conducive to the denoising effect of the Kalman filter in the next stage.

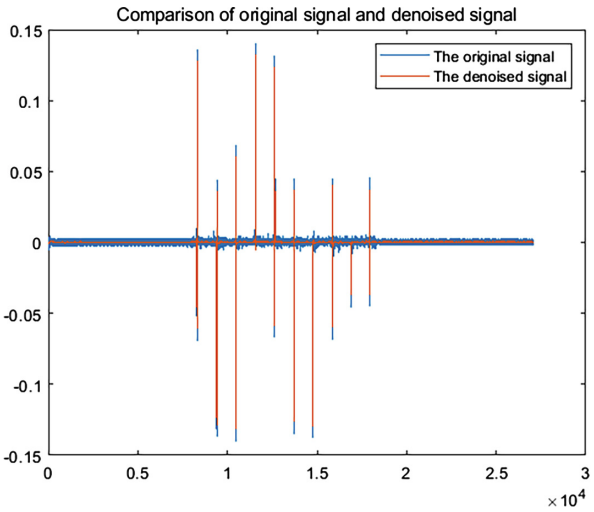

Fig. 3. Haar wavelet smoothing denoising effect diagram

6 Kalman Filtering Algorithm

On the basis of the above wavelet analysis, continue to use the Kalman filter algo-rithm to further predict and estimate the data after the wavelet transform. Set the covariance Q of process noise to 0.1 and the covariance R of observation noise to 0.5. Algorithm 1 is a pseudocode description of the Kalman filtering algorithm.

Continue to use Kalman filter algorithm to further predict and estimate the data after wavelet transform. The results are shown in Fig. 4.

As shown in the Fig. 4, the effect of further processing the data processed by the wavelet transform with Kalman filter shows that the wavelet transform can pro-vide good anti noise performance in the signal decomposition process,

Algorithm 1 algorithm caption

Input: input Z(k) % Observational values
Output: output **Xkf(k)** % Prior estimate

```
initialization
for k=2:N do
    fprintf('X(%d)=%f n', k, X(k)):
    X_pre=F*Xkf(k-1);                % Update predicted values
    P_pre=F*P(k-1)*F'+Q;             % Predict the covariance of time k
    Kg=P_pre*inv(H*P_pre*H'+R); % Calculate again Kalman
    e=Z(k)-H*X_pre:
    Xkf(k)=X_pre+Kg*e;               % Optimal estimation value of time k
    Err_Messure(k)=abs(Xkf(k)-X_pre); % The error between a prior and
  %a poste-rior
    P(k)=(I-Kg*H)*P_pre;             % Update the covariance at time k
    return result
```

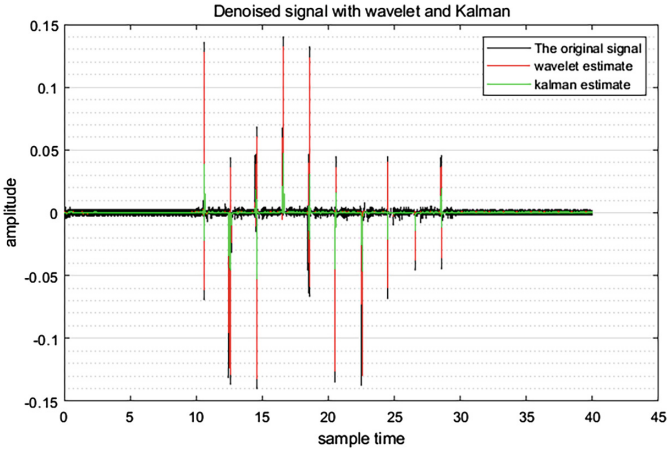

Fig. 4. Haar wavelet smoothing denoising effect diagram

but there may still be some residual noise. The use of Kalman filter can further reduce the impact of noise and improve signal quality. Wavelet transform usually decomposes signals into approximate coefficients and detail coefficients, where the detail coefficients contain the high-frequency components of the signal. Kalman filter is used to process the detail coefficient, which can smooth the signal and reduce the sharp transition. Wavelet transform has the characteristic of time-frequency localization, which can provide local information of signals at different times and frequencies. Combin-ing the state update and prediction steps of Kalman filter, we can better track the dynamic changes of signals and improve the accuracy and effect of signal analysis and processing.

7 Comparison with Traditional Kalman Filtering Algorithms

In order to verify the superiority of the detection method of wavelet transform combined with Kalman filter compared with the traditional detection method of only using Kalman filter, comparative experiments are carried out in this paper. Using the NS3 network simulator to simulate the transmission signal of QUIC network, and combining with the DCE (Direct Code Execution) plugin to simulate LDDoS attacks in NS3. The original data of LDDoS jitter amplitude obtained through NS3 simulation in Fig. 2 is directly processed by Kalman filter, as shown in Fig. 5.

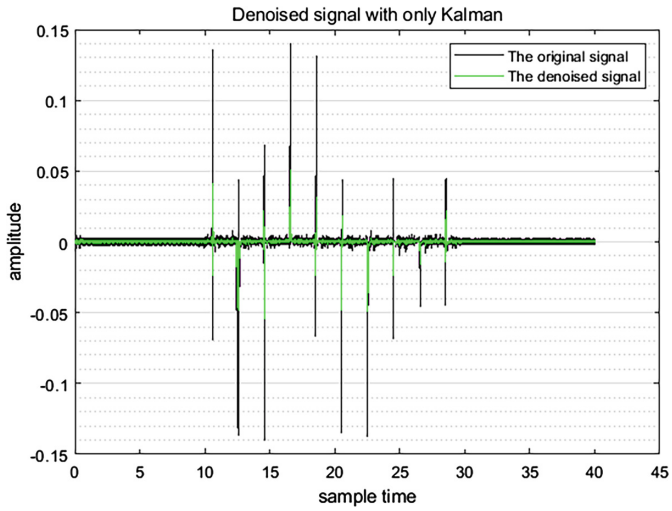

Fig. 5. Traditional Kalman filter processing results

Comparing Fig. 4 with Fig. 5, it is not difficult to find that the processing method of wavelet transform combined with Kalman filter can better remove noise, separate features, adapt to nonlinear signals, realize time-frequency localization and compress data than the processing method of single Kalman filter. This joint method combines the advantages of wavelet transform and Kalman filter, and has higher effect and accuracy for signal processing and analysis tasks. To quantify the advantages and disadvantages of the two detection methods, the mean error of prior and posterior is introduced As a measurement standard. The calculation formula is as follow.

$$\varepsilon = \frac{1}{n}\sum_{i=1}^{n}\left|\hat{x}_{k|k-1} - \hat{x}_{k|k}\right| \tag{8}$$

Among them, x(k—k-1) and x(k—k) represents a priori predictor and a posterior Estimator, respectively. In the filtering process, a prior represents the predicted state based on the system model, and a posterior represents the estimated state corrected based on observation data. Calculating the mean error of prior and posterior can be used to evaluate the noise suppression effect of filters. If the mean error of the prior and posterior is reduced, it means that the filter has successfully reduced the impact of noise on the signal and improved the accuracy of the signal. A smaller mean error indicates that the filter has a better suppression effect on noise. The value of in the two detection methods are shown in Fig. 6 and Fig. 7. The calculation results are shown in Table 1.

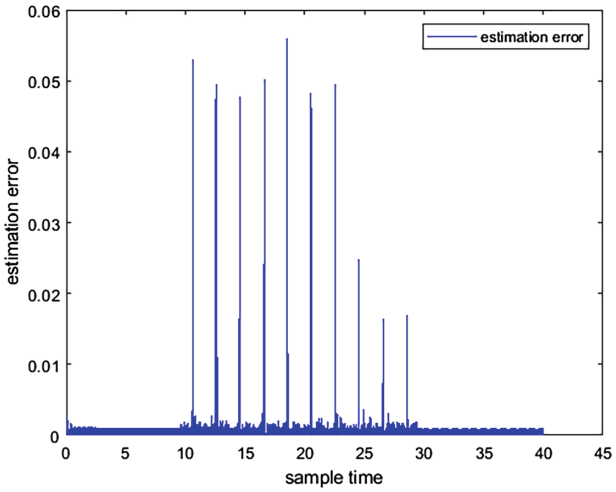

Fig. 6. Prior and posterior errors of single Kalman filter

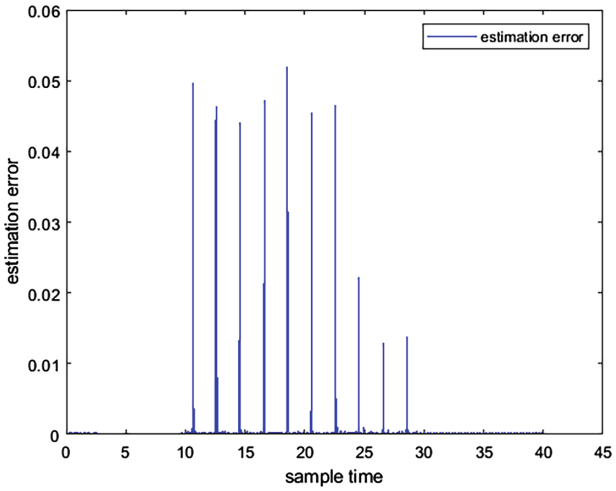

Fig. 7. A priori and a posteriori error of wavelet transform combined with Kalman filter

Table 1. .

Mean error	Wavelet transform combined with Kalman filter method	Single Kalman filter method
ε	0.000081	0.000417

8 Conclusion

Based on the Self-similarity and randomness of QUIC network traffic, this paper proposes a detection method of wavelet transform combined with Kalman filter for LDDoS attacks in QUIC network. First, simulate LDDoS attack through NS3, then use wavelet transform to preprocess the jitter signal after the attack, and then use Kalman filter to further smooth denoising. At last, the method is compared with the dithering signal which is processed only by Kalman filter without wavelet transform, and the effectiveness of the method is proved. It can be used for attack detection and prevention of network nodes.

References

1. Cao, Y., Ji, R., Ji, L., Bao, M., Yang, W.: Can multipath TCP be robust to cyber attacks? a measuring study of MPTCP with active queue management algorithms. Secur. Commun. Netw., 1–11 (2021)
2. Wang, A., Chang, W., Chen, S., Mohaisen, A.: Delving into internet DDos attacks by botnets: characterization and analysis. IEEE ACM Trans. Netw. **26**(6), 2843–2855 (2018)
3. Leland, W.E., Taqqu, M.S., Willinger, W., Wilson, D.V.: On the self-similar nature of Ethernet traffic (extended version). IEEE/ACM Trans. Network. **2**(1), 1–15 (1994)
4. Giorgi, G., Narduzzi, C.: A study of measurement-based traffic models for network di-agnostics. IEEE Trans. Instr. Meas. **57**(8), 1642–1650 (2008)
5. Lemeshko, O., Mersni, A., Nevzorova, O.: Analysis of Influence of network architecture nonuniformity and traffic self-similarity properties to load balancing and average end-to-end delay. In: Radivilova, T., Ageyev, D., Kryvinska, N. (eds.) Data-Centric Business and Applications. LNDECT, vol. 48, pp. 767–787. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-43070-2_33
6. Sheluhin, O.I., Lukin, I.Y.: Network traffic anomalies detection using a fixing method of multifractal dimension jumps in a real-time mode. Autom. Control. Comput. Sci. **52**(5), 421–430 (2018)
7. Pei, J., Zhong, K., Jan, M.A., Li, J.: Personalized federated learning framework for network traffic anomaly detection. Comput. Netw. **209**, 108906 (2022)
8. Nguyen, M.T., Kim, K.: Genetic convolutional neural network for intrusion detection systems. Future Gener. Comput. Syst. **113**, 418–427 (2020)
9. Kuzmanovic, A., Knightly, E.W.: Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In: ACM Sigcomm Conference on Applications. ACM (2003)
10. Cheng, C.M., Kung, H.T., Tan, K.S.: Use of spectral analysis in defense against DoS attacks. In: Global Telecommunications Conference, GLOBECOM'02, vol. 3, pp. 2143–2148. IEEE (2002)

11. Networking and Mobile Computing (2005). https://doi.org/10.1007/11534310
12. Chen, Y., Hwang, K., Kwok, Y.K.: Filtering of shrew DDoS attacks in frequency domain. In: The IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05), Sydney, NSW, Australia, pp. 8–793 (2005). https://doi.org/10.1109/LCN.2005.70.
13. Wu, Z.J., Yue, M.: Detection of LDDoS attack based on Kalman filtering. Acta Electronica Sinica (2008)
14. Mohinder, S.: Kalman filtering theory and practice using matlab (2001)
15. Welch, G., Bishop, G.: An Introduction to the Kalman Filter. University of North Carolina at Chapel Hill (1995)