Journal of Information Hiding and Privacy Protection
DOI:10.32604/jihpp.2021.016690
Article

Tech Science Press

A Broadcast Storm Detection and Treatment Method Based on Situational Awareness

Zhe Zhu[1], Mingjian Zhang[2], Yong Liu[1], Lan Ma[1] and Xin Liu[1,*]

[1]School of Computer Science & School of Cyberspace Security, Xiangtan University, Xiangtan, China
[2]Key Laboratory of Network Crime Investigation of Hunan Provincial Colleges, Hunan Police Academy, Changsha, China
[*]Corresponding Author: Xin Liu. Email: liuxin@xtu.edu.cn

Received: 08 January 2021; Accepted: 27 March 2021

Abstract: At present, the research of blockchain is very popular, but the practical application of blockchain is very few. The main reason is that the concurrency of blockchain is not enough to support application scenarios. After that, applications such as Intervalue increase the concurrency of blockchain transactions. However, due to the problems of network bandwidth and algorithm performance, there is always a broadcast storm, which affects the normal use of nodes in the whole network. However, the emergence of broadcast storms needs to rely on the node itself, which may be very slow. Even if developers debug the corresponding code, they cannot conduct an effective test in the whole network. Broadcast storm problem mainly occurs in scenarios with large transaction volume, such as the financial industry. Due to its characteristics, the concurrency of transactions in the financial industry will increase at a certain time. If there is no effective algorithm to deal with it, the broadcast storm will be triggered and the whole network will be paralyzed. To solve the problem of the broadcast storm, this paper combines blockchain, peer-to-peer network, artificial intelligence, and other technologies, and proposes a broadcast storm detection and processing method based on situation awareness. The purpose is to cut off the further spread of broadcast storms from the node itself and maintain the normal operation of the whole network nodes.

Keywords: Blockchain; broadcast storms; situational awareness

1 Introduction

Blockchain is a decentralized protocol [1]. It is a distributed database system involving nodes that can securely store data, and the information is transparent and non-tamper. It can automatically execute intelligent contracts without any central organization audit.

The current technology architecture of blockchain 2.0 USES a five-layer architecture [2,3], as shown in Fig. 1. From bottom to top, it is respectively the data layer, the network layer, the consensus layer, the incentive layer, and the intelligent contract layer.

The data layer is the lowest level of technology, mainly storing block data to ensure the security of accounts and transactions. Data storage is mainly based on the Merkle tree, which is realized by block and chain structure. The security of accounts and transactions is based on digital signatures, hash functions, and asymmetric encryption techniques.

The network layer mainly realizes the connection and communication of nodes through P2P network. There is no central server and users exchange information with each other. Each user node has the function of the server.

The consensus layer mainly realizes that all nodes in the whole network reach agreement on transactions and data to prevent various consensus attacks, so the algorithm used in this layer is called consensus algorithm.

The incentive layer mainly realizes the issuance of blockchain tokens through the issuance mechanism and the distribution mechanism of blockchain tokens [3].

An intelligent contract is an executable computer program that automatically executes when conditions are met. Intelligent contracts based on blockchain include transaction processing and saving mechanism, and a complete state machine for accepting and processing various intelligent contracts. And transaction saving and state processing are done on the blockchain.

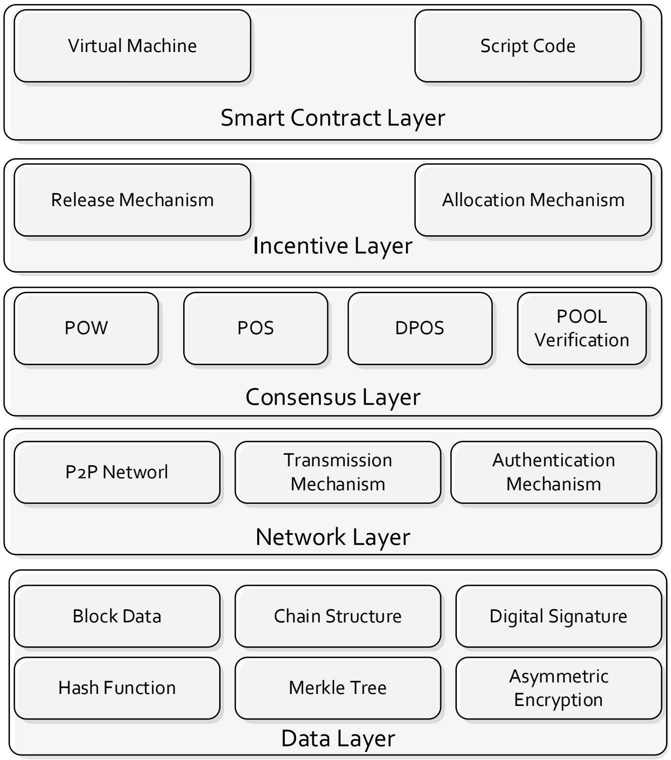

Figure 1: Blockchain five-tier architecture

Security situational awareness can be understood as the customer's safety brain, which is a big data security analysis platform integrating detection, early warning, and response disposal. It takes full traffic analysis as the core and combines threat reporting, behavior analysis modeling, UEBA, fall host detection, graph association analysis, machine learning, big data association analysis, visualization, and other technologies to realize threat visualization, attack, and suspicious traffic visualization and other functions [4]. Can effectively help customers in the advanced threat intrusion before the loss of timely detection of threats.

At present, blockchain is mainly used in the financial industry, which has a demand for large-scale consensus and a large number of participants. It is easy to generate a broadcast storm when the transaction concurrency is very large.

To solve the above technical problems, this paper proposes a broadcast storm detection and processing method based on situational awareness with a simple algorithm and high detection accuracy.

2 Model Design

The framework of the prediction system in this paper is shown in Fig. 1. As can be seen from Fig. 1, the overall design idea of the prediction system is as follows:

(1) The network situation from normal network to broadcast storm is simulated by the Huawei

ENSP platform as datasets.

(2) The datasets adopt WPD decomposition to smooth the high-frequency components of network situation and improve the resolution of network situation components.

(3) When a broadcast storm occurs, variables such as packet rate, transmission rate, throughput, packet loss rate, jitter rate, and delay will all change, so they are all used as input vectors.

(4) The LSTM network model is established to predict broadcast storms.

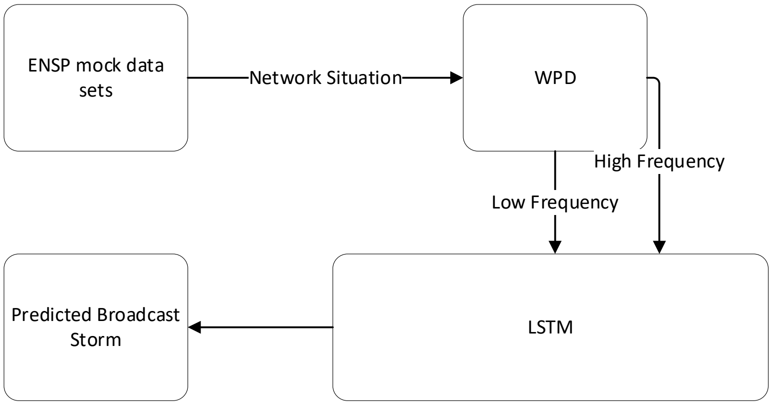

Figure 2: The model design process

2.1 Wavelet Packet Decomposition

WPD is generated and developed based on wavelet decomposition (WD). WD is suitable for processing non-stationary signals, while WPD has great application value for gradual signals [6]. WPD is more complicated than WD [5]. Based on WD, the high-frequency part of the signal is further decomposed by WPD. This gives you more details about the characteristics of the signal. The result of decomposition is to map the original signal to 2j (j is the number of decomposition layers) wavelet bun space. The decomposition algorithm is shown in Eq. (1):

$$\begin{cases} d_l^{j,2n} = \sum_k h_{k-2l} d_k^{j-l,n} \\ d_l^{j,2n+1} = \sum_k g_{k-2l} d_k^{j-l,n} \end{cases} \tag{1}$$

where $d_l^{j,2n}$, $d_l^{j,2n+1}$are coefficients of WPD,h_{k-2l}, $g_{k-2l}$are low-pass and high-pass filter of WPD.

WPD is used to get the component of packet rate of different frequencies. In the decomposition experiment, it was found that the three-layer decomposition had the best effect, namely, j = 3. The package rate component consists of 8 sets of components, including 4 sets of low-frequency components and 4 sets of high-frequency components. Fig. 3 and Fig. 4 show the low-frequency and high-frequency components. The high-frequency component fluctuates greatly and the resolution is low, which is clearly shown in the figure. The high-frequency component has no advantage in the direct prediction of the package rate. It is necessary to further decompose the high-frequency components to improve their resolution.

2.2 LSTM Model Design

LSTM neural network includes forgetting gate between input gate, output gate and hidden layer, which makes LSTM have stronger coordination memory ability than RNN network [7]. It is mainly used to solve the gradient problem of RNN.

The main structure of LSTM is shown in Fig. 3. LSTM contains the chain-like structure developed by each repeating module [8]. And each repeating module has four layers of the neural network, which is the σ layer and tanh layer in Fig. 5. Each round rectangle in Fig. 5 is called a cell. The neurons in the first layer are the sigmoid control layer of the forget gate [9], which is represented by Eq. (2).

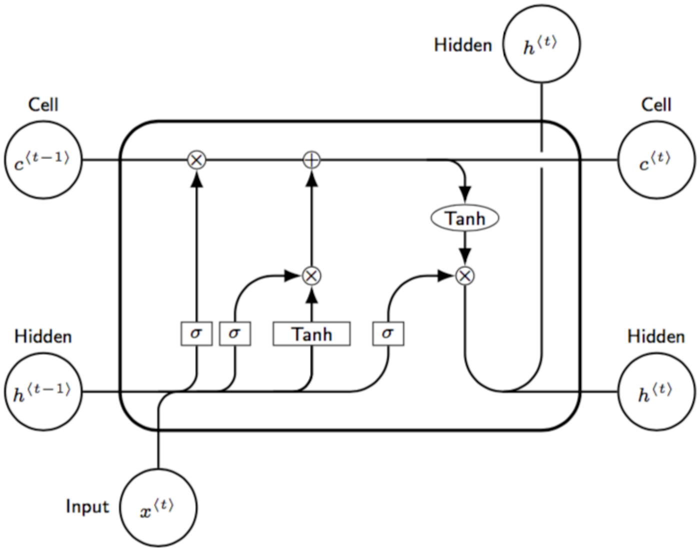

Figure 3: LSTM structure

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (2)$$

f_t represents the output of the oblivion gate, σ is the sigmoid activation function, W_f is the weight of the oblivion gate, $[h_{t-1}, x_t]$represents the matrix or vector with the same number of combined rows of columns, where h_{t-1} represents the state vector of the last hidden layer, $x_t$represents the input vector of LSTM.

The second layer is the sigmoid control layer for the input gate.

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (3)$$

i_t represents the output of the input gate, W_i is the weight of the input gate, and B_i is the deviation of the input gate.

The third layer is the tanh layer.

$$\tilde{C}_t = tanh(W_c[h_{t-1}, x_t] + b_c) \quad (4)$$

$\tilde{C}_t$ represents the output of tanh layer, tanh is hyperbolic tangent activation function,W_c is the weight of the upgrade value, and b_c is the deviation of the upgrade value.

According to formula (5), the old state of unit $C_{t-1}$is updated to $\tilde{C}_t$.

$$C_t = f_t * C_{t-1} + i_t * \tilde{C}_t \quad (5)$$

Finally, after formula (6) passes through the tanh layer, the output gate of sigmoid is shown in formula (7). The output gate of tanh layer is multiplied by the output gate, so that forgetting and memory parameters reach the final output position.

$$O_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (6)$$

$$h_t = O_t \tanh{(C_t)} \quad (7)$$

O_t is the output of the output gate, $W_0$is the weight of the output gate, and b_0 is the bias of the output gate.

3 Node Health Value

This section describes the node health value strategy and the corresponding calculation methods.

3.1 Node Anomaly Determination

Whether abnormal node connection next broadcast storm process as follows: when the node within the set time interval to send 20 times more than the same broadcast packets, decide the node state as the abnormal state, in the abnormal state of the node, situational awareness system based on node calculation packets destined for an hour before departure package rate, transmission rate, throughput, jitter rate, time delay network characteristics, connection time is less than 1 h to send packets to calculate in one hour, use these network characteristics LSTM model matching calculation, predicted that the next node network state.

Due to its memory characteristics, LSTM has a strong ability to learn time series. Therefore, LSTM neural network has a great advantage in time series prediction. Besides, the LSTM can automatically encode and select important information. This advantage avoids the problem of large prediction errors caused by the low resolution of the original network situation. In this experiment, the LSTM network is adopted as the main structure of the prediction network model.

3.2 Node Health Value Evaluation Model

Under normal condition:

$$R_n = R_{n-1} + T \times W_R, R_n \in \{0,100\}, W_R \in \{0,10\} \tag{8}$$

$$R_1 = P_0 + T \times W_R \tag{9}$$

$$T = \begin{cases} 1 & t = 360 \\ 0 & t < 360 \end{cases} \tag{10}$$

Under abnormal condition:

$$R_n = R_{n-1} - t_i, t_i \in \{0,100\} \tag{11}$$

P_0 represents the preset health value, R_n and R_{n-1} represent the node health value established at the n and n-1 time, W_R represents the weight of health value, T represents the weight of time, if less than 1 h, it is 0, if more than 1 h, it is 1. Is the accumulated value of time, adding 1 every 10 seconds; When a node has been connected for more than one hour, when the node is disconnected and connected again, W_R will add 1.

When node P is in normal state, increase the health value of node P. The upper limit of the health value of node P is 100, and the health value will not increase after reaching the upper limit.

When node P is in abnormal state, reduce the health value of node P. If abnormal node P returns to normal within the specified time interval, the deducted health value will be returned. When node P continues to be in an abnormal state, the health value of node P will continuously decrease to the set danger threshold. At this time, node P is in a dangerous state.

3.3 *Behavioral Strategies Based on Health Values*

When the node is in a normal state, the node health value continues to increase with the increase of time, and the next local node L gives priority to connecting nodes with higher health value.

If nodes are in a state of abnormal, judge whether the health value of the abnormal node to satisfy local node L connection by setting threshold, if met, L to continue with this exception, local node connection, if not satisfied, will temporarily disconnect with the abnormal node connections, based on the abnormal nodes of the upper limit of the current health value and health value of the difference, judge the next set up the connection interval.

The specific formula is as follows:

$$T_{n+1} = (100 - R_n) \times 3600 \tag{12}$$

T_{n+1} is the time interval for the next connection establishment, in seconds.

When the node is in a dangerous state, that is, the node's health value drops to the danger threshold; The local node L is marked as "unconnectable" in the database for this dangerous node; The next time a dangerous node tries to establish a connection with local node L, the local node L rejects the connection.

3.4 The Detailed Steps

3.4.1 The situational awareness system calculates the number of “unconnected” nodes of local nodes in a certain period in real-time, and carries out threat assessment of the network environment according to the number of “unconnected” nodes. When the number of “unconnected” nodes reaches one-third of the total number of nodes, the threat level is Level 1, then Step 3.4.2 is entered. When the number of “unconnected” nodes reaches half of the total number of nodes, the threat level is Level 2, and then Step 3.4.3 is entered. When the number of "unconnected" nodes reaches two-thirds of the total number of nodes, Step 3.4.4 is entered.

3.4.2 The situation awareness system conducts network early warning to local nodes, and the entry step is 3.4.5.

3.4.3 The situational awareness system sends warning information to local nodes for processing. When the local node is not processed, the situational awareness system automatically disconnects the abnormal node, entering Step 3.4.5.

3.4.4 The situational awareness system automatically disconnects the abnormal nodes directly to prevent the spread of the broadcast storm. Step 3.4.5.

3.4.5 The situational awareness system feeds the processing results back to the local node and maintains them in the form of logs.

4 Conclusion

In order to evaluate the error of power prediction, three error indexes were analyzed and compared. They are MAE (mean absolute error), MAPE (mean absolute percentage error), as shown in Eqs. (13) and (14).

$$MAE = \frac{1}{N}\sum_{i=1}^{N}|x_i - \hat{x}_i| \tag{13}$$

$$MAPE = \frac{1}{N}\sum_{i=1}^{N}|\frac{x_t - \hat{x}_t}{x_t}| \tag{14}$$

where x_t(t = 1,2,...,N) is the original network situation dataset. $\hat{x}_t$(t = 1,2,...,N) is the predicted datasets of the prediction model.

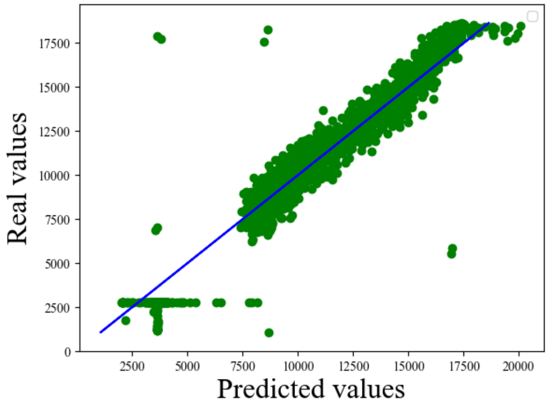

Figure 4: SVR model effects

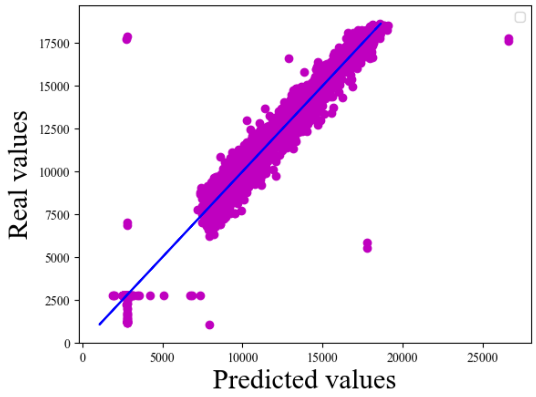

Figure 5: LSTM model effects

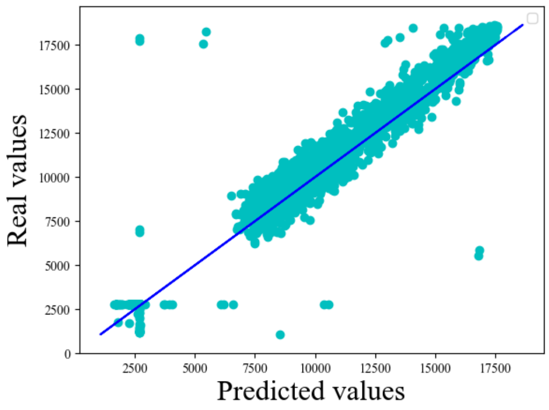

Figure 6: GBRT model effects

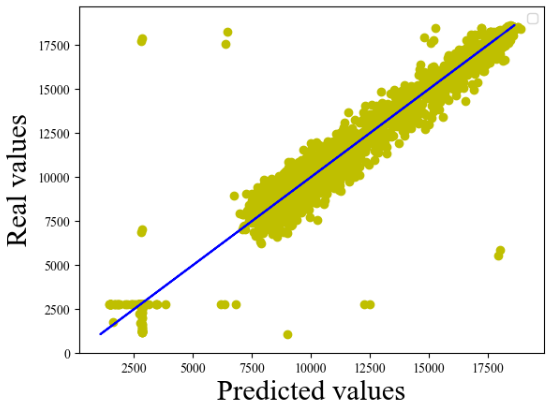

Figure 7: GRU model effects

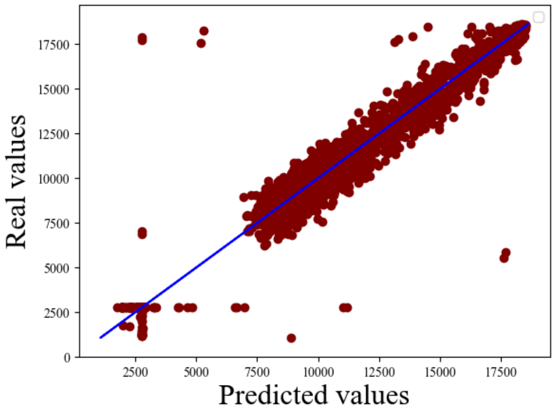

Figure 8: OUR model effects

Table 1: OURS model effects

Model	**MAE**(KW)	**MAPE**(%)
SVR	**0.028**	**17.037**
LSTM	**0.017**	**5.868**
GBRT	**0.009**	**3.603**
OURS	**0.008**	**1.946**

It can be seen from the above results that the model in this paper has a good effect. Compared with LSTM, the error value is reduced by 67%.

Supported by the Open Research Fund of Key Laboratory of Network Crime Investigation of Hunan Provincial Colleges, Grant No. 2018WLFZZC003.

Funding Statement: Supported by the Open Research Fund of Key Laboratory of Network Crime Investigation of Hunan Provincial Colleges, Grant No. 2018WLFZZC003.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Jiang, M. Liu, C. Yang, Y. Liu and R. Wang, "A Blockchain-based authentication protocol for WLAN mesh security access," *Computers, Materials & Continua,* vol. 58, no. 1 pp. 45–59, 2019.

[2] C. Rahalkar and D. Gujar, “Content addressed P2P file system for the web with Blockchain-Based Meta-Data integrity,” in *2019 Int. Conf. on Advances in Computing, Communication and Control (ICAC3)*, Mumbai, India, 2019, pp. 1–4, 2019.

[3] L. Bahri and S. Girdzijauskas, “Blockchain technology: practical P2P computing (tutorial),” in *2019 IEEE 4th Int. Workshops on Foundations and Applications of Self* Systems (FAS*W)*, Umea, Sweden, 2019, pp. 249–250, 2019.

[4] B. F. Ibrahim, M. Toycan and H. A. Mawlood, “A comprehensive survey on VANET broadcast protocols,” in *2020 Int. Conf. on Computation, Automation and Knowledge Management (ICCAKM)*, Dubai, United Arab Emirates, 2020, pp. 298–302, 2020.

[5] J. Zhao, J. Lou, J. Sun, Z. Feng, P. Li *et al.,* “A new method for faulty line selection in distribution systems based on wavelet packet decomposition and signal distance,” in *2019 IEEE 8th Int. Conf. on Advanced Power System Automation and Protection (APAP)*, Xi’an, China, 2019, pp. 596–600, 2019.

[6] P. Li and W. Niu, “Applications of LSTM model for aeroengine forecasting,” in *2020 7th Int. Conf. on Dependable Systems and Their Applications (DSA)*, Xi’an, China, 2020, pp. 168–172, 2020.

[7] Y. Su, J. Yu, M. Tan, Z. Wu, Z. Xiao *et al.,* “A LSTM based wind power forecasting method considering wind frequency components and the wind turbine states,” in *22nd Int. Conf. on Electrical Machines and Systems (ICEMS)*, Harbin, China, 2019, pp. 1–6, 2019.

[8] K. Peng, W. Bai and L. Wu, “Passenger flow forecast of railway station based on improved LSTM,” in *2nd Int. Conf. on Advances in Computer Technology, Information Science and Communications (CTISC)*, Suzhou, China, 2020, pp. 166–170, 2020.

[9] K. Li, H. Li, H. Hou, K. Li and Y. Chen, “Proof of vote: a high-performance consensus protocol based on vote mechanism & consortium blockchain,” in *Proc. 2017 IEEE 19th Int. Conf. on High Performance Computing and Communications,* Bangkok, Thailand, pp. 466–473, 2017.