






Research Article

A Blockchain-Enabled Trusted Protocol Based on Whole-Process User Behavior in 6G Network

Zhe Tu ^{1,2}, Huachun Zhou ^{1,2}, Kun Li ^{1,2}, Haoxiang Song ^{1,2} and Yuzheng Yang ^{1,2}

¹School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

²National Engineering Research Center of Advanced Network Technologies, Beijing 100044, China

Correspondence should be addressed to Huachun Zhou; hchzhou@bjtu.edu.cn

Received 7 July 2022; Revised 18 August 2022; Accepted 15 September 2022; Published 11 October 2022

Academic Editor: Hui Xia

Copyright © 2022 Zhe Tu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The access of massive users and devices in the 6G networks increases the risk of network attacks. Designing a trusted protocol to control user behavior can effectively improve the security capability of the network. However, most of the existing trusted protocols focus on unilateral user behavior and lack effective control over the whole process of user behavior. In this paper, we design a blockchain-enabled trusted protocol based on the whole-process user behavior. At first, we describe the Whole-Process User Behavior (WPUB) after the user accesses the network, and model the whole-process trusted control process. The proposed model establishes a trusted chain between user identity, access action, and communication traffic, and realizes the control of WPUB. Then, based on the proposed model, we design a whole-process trusted protocol with smart agents and smart contracts in combination with blockchain. Finally, we evaluate the designed protocol in the HyperLedger Fabric-based prototype system. Evaluations show that the proposed protocol can control the WPUB and reduce the risk of the network being attacked.

1. Introduction

The Sixth-Generation (6G) network realizes borderless connection under the global coverage, and enables the ubiquitous connectivity of massive users and devices by thoroughly integrating multiple heterogeneous networks, including satellite, air, ground, and sea networks [1–3]. The access of a large number of users and devices increases the potential risk of network attacks, bringing great challenges to network security [4–6]. The Trusted Protocol (TP) can effectively reduce the attacks launched by malicious users on the network by controlling and managing user behaviors, which is one of the important methods to improve network security [7–9]. How to construct a TP to detect malicious behaviors in 6G networks with massive connections is an urgent problem to be solved. However, traditional TPs (such as identity authentication, access control, and traffic detection) are mostly deployed in centralized networks and are difficult to be applied directly to 6G networks with dynamic changes in user behaviors and heterogeneous network structures. The 6G networks put forward new security requirements for TPs, which are mainly shown as follows.

- (i) Behavior traceability. For the dynamically changing user behavior in 6G heterogeneous networks, TPs need to be able to memorize the user's historical behavior and make an accurate and dynamic control based on the user behavior [10, 11]. Besides, the data for TPs should be shared among trusted distributed nodes.
- (ii) Privacy protection. User behavior data reflects the specific activities of users in the network [12, 13]. When analyzing user behavior, it should be ensured that user behavior data is not leaked and maliciously tampered with.

In recent years, as a key technology in the 6G network, blockchain has been widely used in various fields [14, 15]. The blockchain-based TPs can well meet the new security requirements of the 6G networks. On the one hand, storing user behaviors in the blockchain enables traceability of user historical behavior, making it possible to accurately control dynamically changing user behaviors. On the other hand, the decentralized and tamper-proof characteristics of blockchain ensure the security and reliability of the constructed blockchain-based TPs.

However, the existing blockchain-based TPs still have the following problems. Firstly, most of the existing methods manage user behavior under a single specific security requirement, and cannot comprehensively consider the whole-process user behavior after accessing the network. Secondly, the existing methods lack dynamic closed-loop feedback, and it is difficult to meet the needs of dynamic evaluation and closed-loop management. Therefore, it is urgent to construct a TP with dynamic closed-loop feedback that can comprehensively consider the whole-process user behavior.

In this paper, we design a Whole-Process User Behavior-based Blockchain-enabled Trusted Protocol (WPUB-BTP) that can control the whole-process user behavior after accessing the network. The proposed WPUB-BTP constructs a trusted control chain between user identity, access action, and communication traffic, and realizes the control of user behavior in the whole process. In addition, the protocol also builds dynamic closed-loop feedback based on user reputation, which realizes dynamic control of user behavior.

The contribution of this paper can be summarized as follows.

- (i) We design the trusted control model of the whole-process user behavior, which can comprehensively consider identity authentication behavior, access control behavior, and communication traffic behavior.
- (ii) We put forward a blockchain-enabled trusted protocol based on the proposed model to achieve dynamic control and closed-loop feedback on user behavior.
- (iii) We evaluate the trusted protocol in a HyperLedger Fabric prototype system. The evaluation shows that the proposed protocol can control the whole-process user behavior after the user accesses the network, and reduces the risk of the network being attacked.

The remainder of this paper is organized as follows. In Section 2, we review the secure control methods for user behavior based on blockchain. In Section 3, we design the trusted control model of the whole-process user behavior consisting of identity authentication behavior, access control behavior, and communication traffic behavior. Based on the proposed model, we put forward the blockchain-enabled trusted protocol in Section 4. The prototype system and evaluation analysis of the WPUB-BTP are represented in Section 5. In the end, conclusions are drawn in Section 7.

2. Related Work

In this section, we review the related work on blockchain-based security control methods in three aspects: identity authentication, access control, and malicious traffic detection.

2.1. Blockchain-Based Authentication Method. Identity authentication prevents malicious users from accessing the network by identifying user identities. Recently, many

researchers have designed many authentication methods based on blockchain technology to improve the security of the network.

In Vehicular Ad-hoc Networks (VANETs), Zheng et al. [16] proposed a blockchain-based authentication system, which can provide the trusted communication environment of the Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I). Similarly, Feng et al. [17] put forward a Blockchain-based Assisted Privacy-preserving authentication System (BAPS) for VANETs. The proposed system is efficient and scalable, and can efficiently achieve privacy-preserving authentication without any online registration center. In the Internet of drones, Feng et al. [18] presented a blockchain-based cross-domain authentication method to build an identity federation for collaborative domains. To ensure the privacy and security of the Intelligent Transportation Systems (ITS) networks, Qureshi et al. [19] proposed a Blockchain-based Privacy-Preserving Authentication model (BPPAU).

2.2. Blockchain-Based Access Control Method. The access control method can prevent malicious users from accessing network resources without authorization, and realize the management and control of user access behavior. With the development of blockchain, many blockchain-based access control methods have been proposed.

Tan et al. [20] suggested a blockchain-empowered general Green Smart Device (GSD) access control framework in the Green Internet of Things (GIoT). The proposed framework provides a fine-grained and extensible access control of GSDs and ensures the credibility and immutability of permission data and identity data during access. On the Internet of Things (IoT), Sun et al. [21] proposed a blockchain-based IoT access control system, which combines the permission blockchain, Attribute-Based Access Control (ABAC), and Identity-Based Signature (IBS) to achieve security, lightweight, and cross-domain access control. To provide decentralized Electrical Health Records (EHR) and service automation, a blockchain-based Internet of Medical Things (IoMT) architecture called Fortified-Chain is proposed by Egala et al. [22]. The proposed architecture can provide decentralized automation access control, security, and privacy. In the Industrial Internet of Things (IIoT), Feng et al. [23] put forward a novel access control framework based on blockchain, which consists of three types of chaincodes: PMC, ACC, and CEC. The proposed framework can achieve fast and reliable consensus based on historical behavior records stored in the ledger.

2.3. Blockchain-Based Traffic Detection Method. User traffic detection is another important way to improve network security. According to the way of traffic detection, it can be divided into methods-based statistical methods and methods based on machine learning methods [24]. In recent years, the development of blockchain has enabled more and more scholars to build detection models in blockchain networks based on existing traffic detection technologies.

In the Satellite Communication (SATCOM) systems, Cao et al. [25] proposed a blockchain-based access control and intrusion detection framework ACID, which can dynamically adjust the Access Control Rules (ACRs) and effectively detect attacks against smart contracts. Similarly, Guo et al. [26] proposed a blockchain-based Distributed Collaborative Entrance Defense (DCED) framework to protect the satellite networks from malicious attacks. Experiment shows that the proposed framework can effectively protect the bandwidth resources of satellite Internet from DDoS attacks. Ramanan et al. [27] put forward a blockchain-based decentralized replay attack detection mechanism for large-scale power systems. The proposed mechanism can detect coordinated replay attacks with full privacy. To prevent IoT devices and other computing resources from DDoS attacks, Hayat et al. [28] proposed a Multilevel DDoS mitigation approach (ML-DDoS) based on blockchain. The results show that the proposed framework can accurately detect DDoS attacks in IoT, and has good performance in throughput, latency, and CPU utilization.

In Table 1, we summarize the relevant work of blockchain-based TPs and analyze whether they meet the security requirements of TPs in 6G networks. The above methods put forward the blockchain-based TPs to improve network security in different aspects. However, most methods only focus on one aspect of user behavior and lack control of the whole-process user behavior after accessing the network. In addition, for dynamically changing user behavior in the 6G network, those methods lack closed-loop feedback, and cannot adjust control strategies in real time according to user behaviors. Therefore, based on blockchain, we build a trusted protocol with dynamic closed-loop feedback to realize the whole-process behavior control of users, so as to meet the security requirements of TPs in the 6G networks.

3. Trusted Control Model

In this section, we first present the whole-process user behavior description. Then, we describe the trusted control model of the whole-process user behavior.

3.1. Whole-Process User Behavior Description. Before introducing the trusted control model, the Whole-Process User Behavior (WPUB) in the 6G network needs to be defined. According to the different behaviors initiated by users after accessing the network, the WPUB can be divided into three sub-behaviors: Identity Authentication Behavior (IAB), Access Control Behavior (ACB), and Communication Traffic Behavior (CTB), as shown below.

$$WPUB \triangleq \{IAB, ACB, CTB\}. \quad (1)$$

IAB is the description of authentication behavior when a user accesses the network. The IAB can be represented as a set consisting of Authentication Protocol (AP), Environment Attributes (EA), Identity Attributes (IA), Device Attributes (DA), etc., as shown in the following equation:

$$IAB \triangleq \{AP, EA, IA, DA, \dots\}. \quad (2)$$

ACB describes the actions taken by the user to access the network resources, including Access Actions (AA), Resource Attributes (RA), User Privilege (UP), and Resource Privilege (RP). The ACB can be represented as

$$ACB \triangleq \{AA, RA, UP, RP, \dots\}. \quad (3)$$

CTB reflects the behavior of the traffic generated by the user's interaction with other network entities after accessing the network. According to the granularity level of the traffic, CTB can be divided into Packet Behavior (PB), Flow Behavior (FB), Host Behavior (HB), Session Behavior (SB), etc., as shown in the following equation:

$$CTB \triangleq \{PB, FB, HB, SB, \dots\}. \quad (4)$$

Therefore, according to the above equations (2-4), the WPUB can be expressed in detail as the follows:

$$WPUB \triangleq \begin{bmatrix} AP, EA, IA, DA, \dots \\ AA, RA, UP, RP, \dots \\ PB, FB, HB, SB, \dots \end{bmatrix}. \quad (5)$$

3.2. Whole-Process Trusted Control Model. To realize the trusted control of the WPUB, a Whole-Process Trusted Control model (WPTC) deployed in the access gateway is proposed. According to the division of WPUB, WPTC can be divided into three different modules: Identity Authentication Module (IAM), Access Control Module (ACM), and Traffic Detection Module (TDM). The proposed three modules can control and manage the user's sub-behavior to ensure the trust of each process. Besides, to achieve closed-loop feedback and dynamic control between three different control processes, a Dynamic Control Mechanism (DCM) based on the user's reputation is also proposed. The DCM constructs a dynamic control between user sub-behaviors in different modules and realizes the trusted control of whole-process behavior. The WPTC is shown in Figure 1.

3.2.1. Identity Authentication Module. The IAM authenticates the identity of users to ensure the trusted user identity, which is the first security protection barrier in the WPTC framework. To better model the IAM and reflect the control process of the module on IAB, we represent the Identity Authentication Result (IAR) as the mapping relationship of IAB, as shown in the following equation:

$$\begin{bmatrix} IAR_1^t \\ \dots \\ IAR_i^t \\ \dots \\ IAR_n^t \end{bmatrix} \triangleq f \left(\begin{bmatrix} IAB_1^t \\ \dots \\ IAB_i^t \\ \dots \\ IAB_n^t \end{bmatrix} \right). \quad (6)$$

TABLE 1: Analysis of related work.

Ref.	Year	Security requirement of trusted protocol in 6G networks						
		Trusted user identity	Trusted access actions	Trusted communication traffic	Closed-loop feedback	Privacy protection	Behavior traceability	
[16]	2019	✓	×	×	×	✓	✓	
[17]	2019	✓	×	×	×	✓	✓	
[18]	2021	✓	×	×	×	✓	✓	
[19]	2022	✓	✓	×	×	✓	✓	
[20]	2021	×	✓	×	×	✓	✓	
[21]	2021	×	✓	×	×	✓	✓	
[22]	2021	✓	✓	×	×	✓	✓	
[23]	2021	×	✓	×	×	✓	✓	
[25]	2021	×	✓	✓	×	✓	✓	
[26]	2022	×	×	✓	×	✓	✓	
[27]	2021	×	×	✓	×	✓	✓	
[28]	2022	×	×	✓	×	✓	✓	
Ours	2022	✓	✓	✓	✓	✓	✓	

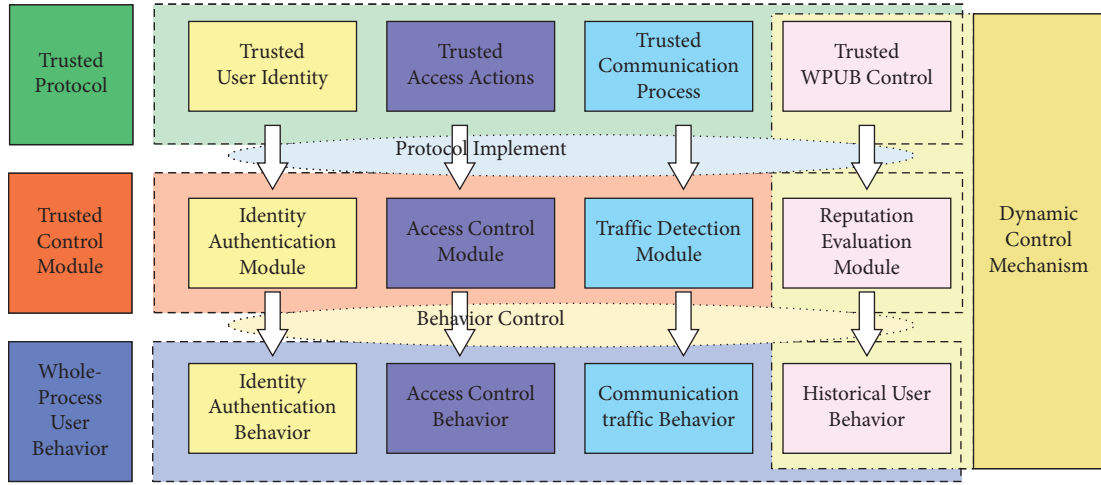


FIGURE 1: The framework of the whole-process trusted control model.

It is assumed that n users are accessing the network through the access gateway at time t . In (6), f is the trusted authentication protocol reflecting the relationship between IAR and IAB. IAB_i^t and IAR_i^t represent the IAB and IAR of user u_i at time t , respectively. If the identity of user u_i is trusted, the IAR_i^t is set to 1. Otherwise, IAR_i^t is set to 0. $1 \leq i \leq n$.

$$\begin{bmatrix} ACR_1^t \\ \dots \\ ACR_i^t \\ \dots \\ ACR_n^t \end{bmatrix} \triangleq g \left(\begin{bmatrix} ACB_1^t \\ \dots \\ ACB_i^t \\ \dots \\ ACB_n^t \end{bmatrix}, \begin{bmatrix} IAR_1^t \\ \dots \\ IAR_i^t \\ \dots \\ IAR_n^t \end{bmatrix} \right). \quad (7)$$

3.2.2. Access Control Module. The ACM is the key module to ensure the trust of access actions, which verifies whether the user can be authorized to access the Network Resources (NR) according to the access policy. The user needs to be authenticated before performing access control. A user with a trusted identity can access the network resources only after obtaining the legitimate access authorization. The ACM can be modeled as shown in (7). $g()$ is the trusted access control protocol. ACB_i^t and ACR_i^t represent the ACB and the Access Control Result (ACR) of user u_i at time t , respectively. If the access action of u_i is authorized, the access control result is 1. Otherwise, ACR_i^t is 0.

3.2.3. Traffic Detection Module. As an important component in WPTC, TDM detects the traffic in the network in real time and realizes the timely detection and blocking of malicious CTB. The TDM module provides a guarantee for the trust of the communication traffic. In the proposed WPTC, the user can only send traffic to the NR after obtaining access authorization. Therefore, we define the trusted traffic detection protocol in TDM as the mapping relationship between CTB, ACR, and Traffic Detection Results (TDR). $h()$ is the trusted traffic detection protocol. CTB_i^t and TDR_i^t , respectively, represent the CTB and the ACR of user u_i at time t . If the traffic initiated by u_i is detected as normal, then TDR_i^t is 1; if the CTB_i^t is detected as malicious traffic, TDR_i^t is 0.

$$\begin{bmatrix} TDR_1^t \\ \dots \\ TDR_i^t \\ \dots \\ TDR_n^t \end{bmatrix} \triangleq h \left(\begin{bmatrix} CTB_1^t \\ \dots \\ CTB_i^t \\ \dots \\ CTB_n^t \end{bmatrix}, \begin{bmatrix} ACR_1^t \\ \dots \\ ACR_i^t \\ \dots \\ ACR_n^t \end{bmatrix} \right). \quad (8)$$

3.2.4. Dynamic Control Mechanism. The above three modules control user sub-behaviors from three aspects: user identity, access action, and communication traffic. By constructing a trusted control chain of the “user identity-access action-communication traffic,” WPTC realizes the security control of user behavior in the whole process. In order to improve the security capability of closed-loop feedback and dynamic control, we introduce the DCM in WPTC.

DCM is the core control mechanism of WPTC, which can dynamically control the user’s behavior by evaluating the reputation of the user. In DCM, the user’s reputation is calculated by the Reputation Evaluation Module (REM), and the reputation is consisting of two kinds of subreputations: Sub-behavior Reputation (SR) and Global Reputation (GR). The SR is calculated by the historical behavior of each sub-behavior. Based on the division of the WPUB, the SR of user u_i at time t can be subdivided into user identity reputation UIR_i^t , access action reputation AAR_i^t , and communication traffic reputation CTR_i^t . The UIR_i^t , AAR_i^t , and CTR_i^t can be calculated by (9–11), respectively.

$$\begin{aligned} UIR_i^t &= \varphi_1(IAB_i^T) \\ &= \varphi_1(IAB_i^{t1}, \dots, IAB_i^{tm}), \end{aligned} \quad (9)$$

$$\begin{aligned} AAR_i^t &= \varphi_2(ACB_i^T) \\ &= \varphi_2(ACB_i^{t1}, \dots, ACB_i^{tm}), \end{aligned} \quad (10)$$

$$\begin{aligned} CTR_i^t &= \varphi_3(CTB_i^T) \\ &= \varphi_3(CTB_i^{t1}, \dots, CTB_i^{tm}). \end{aligned} \quad (11)$$

In (9)–(11), IAB_i^T , ACB_i^T , and CTB_i^T represent the historical sub-behaviors of IAB, ACB, and CTB in the time period T before time t , respectively. IAB_i^{t1} is the first historical sub-behavior IAB of u_i in the time period T . Likewise, the historical sub-behavior in the time period of ACB and CTB can be represented similarly to the IAB. φ_1 , φ_2 , and φ_3 are the reputation evaluation functions of IAB, ACB, and CTB, respectively.

The global reputation GR_i^t of user u_i can be calculated by the above three sub-behavior reputations, as shown in (12). θ is the global reputation calculation function.

$$GR_i^t = \theta(UIR_i^t, AAR_i^t, CTR_i^t). \quad (12)$$

When the user behavior is untrusted, based on proposed SR (UIR_i^t , AAR_i^t , CTR_i^t) and GR (GR_i^t), we put forward the

DCM in the above three models. The DCM can be divided into the following three stages.

In the identity authentication stage, the Dynamic Control Result (DCR) generated by DCM can be modeled as (13). When the identity of user u_i is untrusted ($IAR_i^t = 0$), the DCM can formulate different DCRs according to the different UIR_i^t . μ_1 is the security control judgment function of DCM in the IAM, and DCR_i^t is the DCR of user u_i at time t . If UIR_i^t is greater than the threshold value ω , the DCR_i^t of user u_i is set to “re-authenticate.” If $UIR_i^t < \omega$, the DCR_i^t is set to “access blocking,” and the user is not allowed to access the network.

$$DCR_i^t = \mu_1(UIR_i^t | IAR_i^t = 0). \quad (13)$$

In the access control stage, the dynamic control process can be represented as (14). The DCM in the ACM ensures that different control policies are implemented based on different UIR_i^t and AAR_i^t when user’s access behaviors are abnormal ($ACR_i^t = 0$). μ_2 is the security control judgment function of DCM in the ACM. If the access reputation value AR_i^t of user u_i is less than the threshold value λ_1 , DCR_i^t is “access blocking,” which means the access behavior of the user is blocked. If $\lambda_1 \leq AR_i^t < \lambda_2$, the user needs to be re-authenticated; If $AR_i^t \geq \lambda_2$, the DCR_i^t is “re-access control,” and the user needs to perform access control again. The AR_i^t can be calculated as follows. $AR_i^t = \psi(UIR_i^t, AAR_i^t)$. ψ is the evaluation function of the access behavior.

$$DCR_i^t = \mu_2(AR_i^t | ACR_i^t = 0). \quad (14)$$

In the traffic detection stage, DCM can be modeled as (15). When a user initiates abnormal traffic to the network ($CTB_i^t = 0$), DCM formulates different security control schemes based on the user’s global reputation GR_i^t to improve the security capability of the network. μ_3 indicates the security control judgment function of the DCM in the ACM. When the user traffic is detected as malicious traffic, the communication traffic is blocked. If the global reputation GR_i^t is less than ρ_1 , the user is recorded on the blacklist and is not allowed to access the network for a period of time. If $\rho_1 \leq GR_i^t < \rho_2$, the DCR_i^t is “re-authenticate”; If $GR_i^t \geq \rho_2$, the user should be “re-access control.” ρ_1 and ρ_2 are the threshold constants of global reputation in the traffic detection stage.

$$DCR_i^t = \mu_3(GR_i^t | CTB_i^t = 0). \quad (15)$$

In (13–15), the DCR_i^t is one of the elements in the set of Dynamic Control Policies (DCP). $DCR_i^t \in DCP$. DCP can be given as follows:

$$DCP = \{dcp_1, \dots, dcp_n\}. \quad (16)$$

In (16), dcp_n is the n th subcontrol policy in the DCP set. In the DCM, the subcontrol policy dcp_n can be set as “re-authentication,” “re-access control,” “access blocking,” “traffic blocking,” and so on according to the specific network scenario.

4. Blockchain-Enabled Trusted Protocol Based on WPUB

In this section, based on the proposed trusted control model, we design the Blockchain-enabled Trusted Protocol (WPUB-

BTP) including trusted user identity protocol, trusted access action protocol, and trusted communication traffic protocol.

In WPUB-BTP, the functions of the modules in the trusted control model are deployed in the access gateway and blockchain network in the form of Smart Agents (SA) and Smart Contracts (SC). The SA is mainly responsible for interacting with UEs, processing and forwarding the user requests, while the SC stores the user behaviors and generate trusted management policies in the blockchain.

The division of modules in the trusted control model can be shown as follows. The functions of the IAM are performed by the Identity Authentication Agent (IAA) and Identity Authentication Smart Contract (IASC), and the ACM is deployed as the Access Control Agent (ACA) and Access Control Smart Contract (ACSC). In addition, the TDM is deployed in WPUB-BTP as a Traffic Detection Agent (TDA) and Traffic Detection Smart Contract (TDSC). The Reputation Evaluation Smart Contract (RESC) in the blockchain network is deployed to perform the functions of the proposed REM. Besides, the user in the WPUB-BTP is represented as UE, and the network resources in the servers are abbreviated as NR.

In the following subsections, we will describe the three subprotocols in WPUB-BTP for security control of user sub-behaviors. The blockchain-enabled trusted protocol is shown in Figure 2.

4.1. Trusted User Identity Protocol. In the trusted user identity protocol, the IAA is used to forward and process the identity authentication requests of users, while the IASC stores the authentication credentials and generates the user authentication vector.

The trusted user identity protocol can be described as the following steps.

STEP 1: UE sends the authentication request to IAA;
STEP 2: IAA invokes the interface of IASC to generate authentication vector and authenticate user identity. If the user identity is authenticated successfully, go to STEP 4. Otherwise, go to STEP 3.

STEP 3: If the user identity is untrusted, IAA needs to query the User Identity Reputation (UIR) of the user, and generates the DCR according to the UIR;

STEP 4: Meanwhile, the IAA invokes IASC interfaces to record identity authentication behaviors.

STEP 5: RESC updates the user identity reputation based on the recorded IAB;

STEP 6: Finally, IAA returns the IAR or the DCR to UE.

4.2. Trusted Access Action Protocol. The trusted access action protocol in the WPUB-BTP is used to evaluate user access control behavior. In the trusted access action protocol, there are two components, ACA and ACSC, which perform the access control function. The ACA is used to forward the access control requests initiated by users, while the ACSC generates the access policy and stores the user access control behavior.

The trusted access action protocol consists of the following seven steps.

STEP 1: UE sends the access control request to the ACA.

STEP 2: After receiving the access control request, the ACA looks up the identity authentication result of the UE to verify whether the user identity is legal; If the user is illegal, the ACR is set to 0, and the next step is STEP 5. Otherwise, go to STEP 3.

STEP 3: If the identity of the user is trusted, the ACSC generates the access control policy for the UE. If the user access action is unauthorized, go to STEP 4. Otherwise, go to STEP 5.

STEP 4: ACA queries the user's Access Action Reputation (AAR), and generates the DCR based on the obtained AAR.

STEP 5: At the same time, the ACA invokes ACSC interfaces to record access control behaviors.

STEP 6: RESC updates the access action reputation based on the recorded ACB.

STEP 7: In the end, ACA returns the access control result or the dynamic control result to UE.

4.3. Trusted Communication Traffic Protocol. In the trusted communication traffic protocol, the TDA in the access gateway is the component that mainly performs the function of traffic detection. In TDA, different types of detection submodules can be deployed to detect the user traffic passing through the gateway in real time. The TDSC in the protocol periodically stores the communication traffic behavior of users.

The trusted communication traffic protocol is used to control the communication traffic behavior of users, which includes the following steps.

STEP 1: UE sends the communication traffic through the access gateway to the NR.

STEP 2: The TDA in the access gateway needs to ask the ACSC contract whether the user has permission to access NR when the user's traffic arrives for the first time.

STEP 3: If the UE is an authorized access user, the user is allowed to send traffic to network resources. At the same time, the TDA continuously detects the traffic between UE and NR in real time.

STEP 4: If the traffic initiated by the user is detected abnormal, the communication traffic needs to be blocked at the first time. Then, the TDA calls the interface of RESC to obtain the user's Communication Traffic Reputation (CTR), and generates the DCR based on the obtained CTR;

STEP 5: Meanwhile, the TDA periodically records the CTB in the TDSC contract based on the traffic detection results.

STEP 6: And the RESC updates the communication traffic reputation based on the recorded CTB.

STEP 7: At last, the TDA returns the dynamic control result to UE.

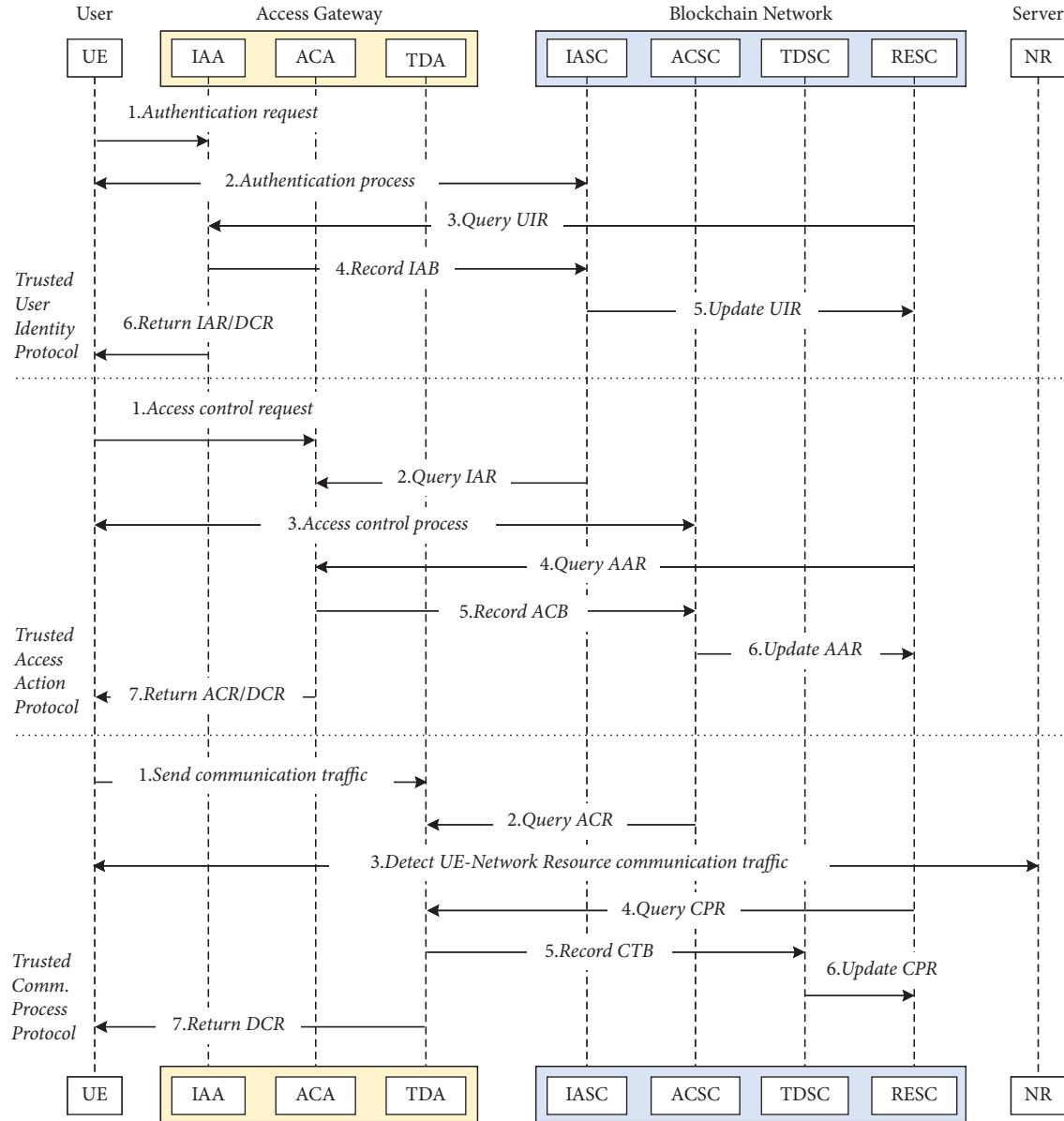


FIGURE 2: The blockchain-enabled trusted protocol.

5. Evaluation

In this section, we first introduce the prototype system based on the proposed WPUB-BCP protocol. Then, we evaluate the WPUB-BCP protocol in the HyperLedger Fabric prototype system.

5.1. Prototype System. As shown in Figure 3, based on the proposed WPUB-BTP protocol, a prototype system is deployed for evaluation. We deploy a server cluster based on VMware vSphere [29] virtualization platform. The server cluster consists of 12 servers, each configured with a 40G disk, 16G memory, and an 8-core processor. In the server cluster, 12 servers can be divided into satellite networks domain, cellular networks domain, and wireless local area

networks domain depending on the application scenario. And each domain contains one UE and three access gateways.

Compared with other blockchain platforms such as Ethereum (<https://ethereum.org/>), HyperLedger Fabric (<https://github.com/hyperledger/fabric/>) has the advantages of high modularity and scalability, and has been widely and maturely applied in various commercial scenarios. Therefore, in this article, we build the WPUB-BTP protocol prototype system based on Fabric. In the prototype system, the blockchain network is constructed on the nine access gateways.

In the prototype system, the HyperLedger Fabric blockchain network is divided into three organizations (3 Org), and each organization consists of one certificate authority (1 CA), three peer nodes (3 peers), and one

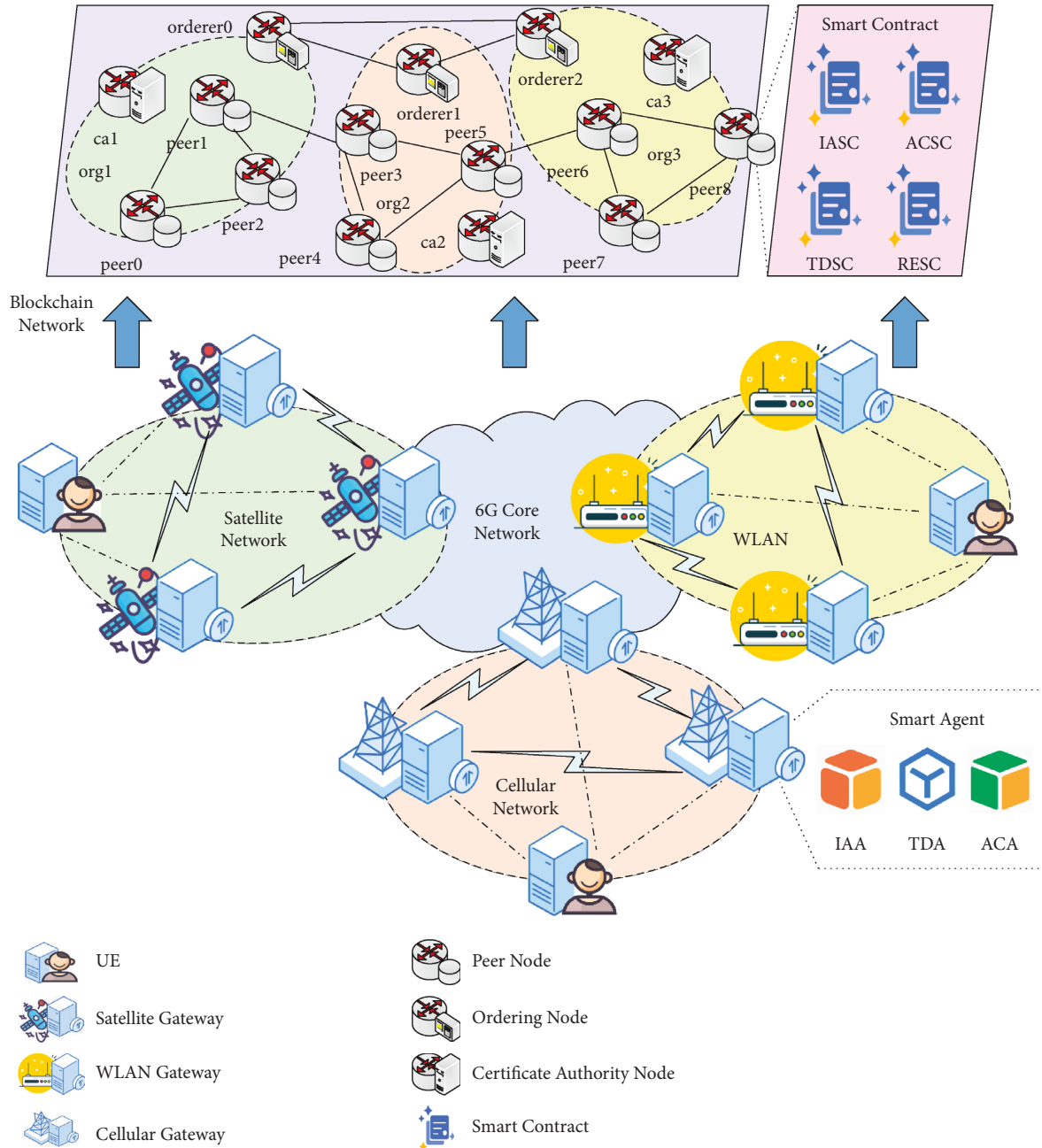


FIGURE 3: The prototype system of WPUB-BTP protocol.

ordering node (1 orderer). The access gateways initiate the transactions to the blockchain network through the SDK interface (`fabric-py-sdk` (<https://github.com/hyperledger/fabric-sdk-py/>)) for data storage, update, and query operations. Three smart agents (IAA, ACA, and TDA) written in Python (<https://docs.python.org/3.9/>) are deployed at each access gateways, performing identity authentication, access control, and traffic detection functions. In addition, we design four smart contracts (IASC, ACSC, TDSC, and RESC) based on the `go-lang` (<https://github.com/golang/go/>) language and deploy them in the blockchain network in the form of chaincodes. IASC and ACSC are used to control user authentication behavior and access control

behavior, respectively. TDSC is used to detect the traffic behavior sent by users, while RESC evaluates the reputation based on user authentication, access control, and traffic behavior to realize dynamic closed-loop control of user behavior.

To evaluate the performance of the proposed WPUB-BCP protocol, we deploy the specific control methods in each module (SA and SC). In our previous work [30], an authentication method based on EAP-MD5 is proposed for fast authenticate. Therefore, in the IAM module, we use the same authentication method to represent the trusted authentication protocol f , so as to ensure the trusted user identity. Besides, an access control method based on the

Attribute-Based Access Control (ABAC) model [31] is deployed in the ACM module to represent the trusted access control protocol g . In the TDM, we deploy the same traffic detection method based on the Deep Deterministic Policy Gradient (DDPG) algorithm as in [32] to represent the trusted communication traffic protocol h . In addition, the Beta Reputation System (BRS) [33] can give a comprehensive evaluation of users' positive and negative behaviors. Therefore, in this paper, we deploy the BRS in REM module to evaluate the reputation of user's sub-behavior ($UIR_i^t, AAR_i^t, CTR_i^t$) and to provide the feedback for dynamic control. φ_1, φ_2 , and φ_3 are the reputation value calculation formulas of beta reputation system. Specifically, the global reputation and the access reputation can be calculated as follows: $GR_i^t = 1/3 * (UIR_i^t + AAR_i^t + CPR_i^t)$, $AR_i^t = 1/2 * (UIR_i^t + AAR_i^t)$. In addition, the threshold constants in the DCM are set as follows: $\omega = 0.5, \lambda_1 = 0.35, \lambda_2 = 0.65, \rho_1 = 0.4, \rho_2 = 0.7$. μ_1, μ_2 , and μ_3 are set as described in Section 3.2.

5.2. Performance Evaluation. In this subsection, we first evaluate the performance of the three proposed trusted protocols: trusted user identity protocol, trusted access action protocol, and trusted communication traffic protocol. Subsequently, we functionally evaluated the designed dynamic control mechanism.

5.2.1. Trusted User Identity Protocol. Figure 4 shows the evaluation result of the trusted user identity protocol. We evaluate the control results of the trusted user identity protocol under 100, 500, 1000, 2000, 5000, and 10000 authentication requests, and the proportion of illegal users is 20%, 40%, 60%, and 80%, respectively. As can be seen from Figure 4, the proposed trusted user identity protocol can achieve accurate authentication of a large number of users. In addition, the proposed protocol can prevent illegal users from accessing the network, which improves the security of the network.

5.2.2. Trusted Access Action Protocol. Subsequently, we evaluate the trusted access action protocol with 100, 200, 500, and 1000 access control requests per second in, as shown in Figure 5. In the evaluation, it is assumed that 20% of the requests are sent by unauthenticated UEs and 80% by the trusted identity UEs. In addition, it is assumed that 60% of users with trusted identities can obtain access policies. As can be seen from Figure 5, the proposed trusted access action protocol can evaluate user access control behaviors and successfully generate the corresponding access policies. Furthermore, the evaluation results show that users without trusted identities cannot get access authorization, which ensures the security and credibility of the network from both user identity and access action.

5.2.3. Trusted Communication Traffic Protocol. In Figure 6, the management and control process of user traffic behavior by the proposed trusted communication traffic protocol is shown. We simulated the traffic sent by two types of

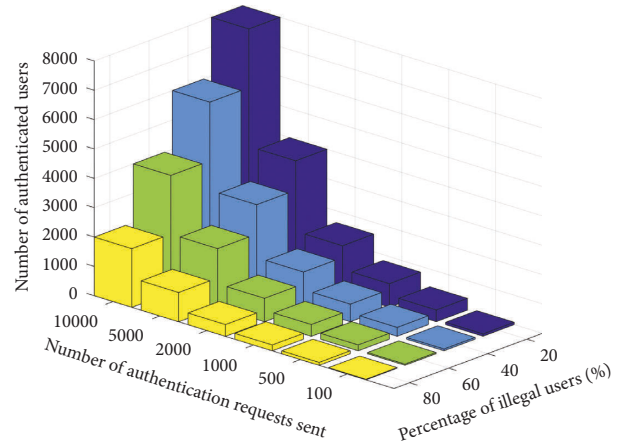


FIGURE 4: The evaluation of the trusted user identity protocol.

authorized users, namely normal user traffic and abnormal user traffic. Within 0–200 s, the normal users continuously send normal traffic to the network resource, while the abnormal users periodically launch attack traffic. Both the normal traffic and the abnormal traffic are generated according to traffic dataset collected in [20]. The traffic detection module is deployed in the access gateway at 50 s. As shown in the figure, the traffic detection module can distinguish the normal traffic and abnormal traffic according to the traffic characteristics. And the trusted communication traffic protocol can generate the real-time control policies to block the malicious traffic according to the detection results.

5.2.4. Dynamic Control Mechanism. In this subsection, we evaluate the continuous dynamic control results of the proposed dynamic control mechanism on user behavior when the user accesses the network and performs identity authentication, access control, and traffic detection in sequence.

As shown in Table 2, we simulate the user behavior of 200 users accessing the network. At the beginning of 200 users accessing the network, we set 50% of users to send correct authentication requests, 25% of high-reputation users (reputation greater than 0.5) to send incorrect authentication requests, and 25% of low-reputation users (low reputation greater than 0.5) to send a bad authentication request. The 100 users with trusted identities who send correct authentication requests need to perform access control when accessing network resources. Similarly, we set the following settings for users who send access control requests, among which 50% of users have successful access control, and 50% of users have failed access control; among the users whose access control fails, we set 50% of the users whose reputation is higher than 0.65, 30% of users have a reputation between 0.35 and 0.65, and 20% of users have a reputation below 0.35. Finally, among the 50 authorized users, we set 25 users send normal traffic, and the rest send abnormal traffic. In order to display the dynamic control results in the traffic detection stage, we divided the users sending abnormal traffic into three groups as follows: good reputation (reputation is greater than 0.7), moderate

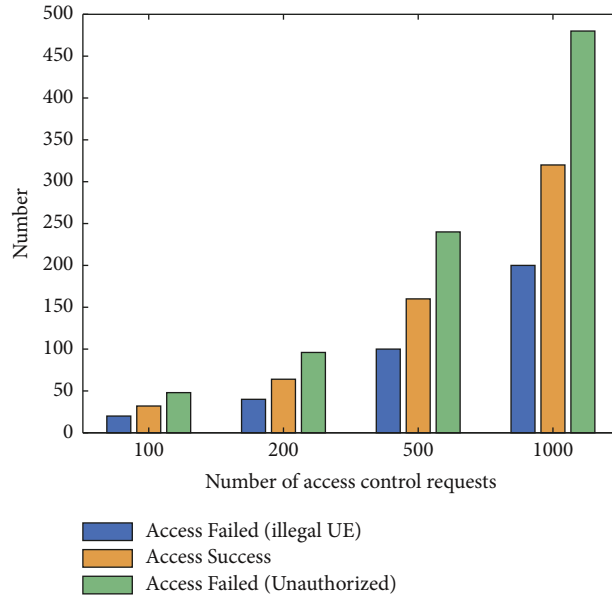


FIGURE 5: The evaluation of the trusted access action protocol.

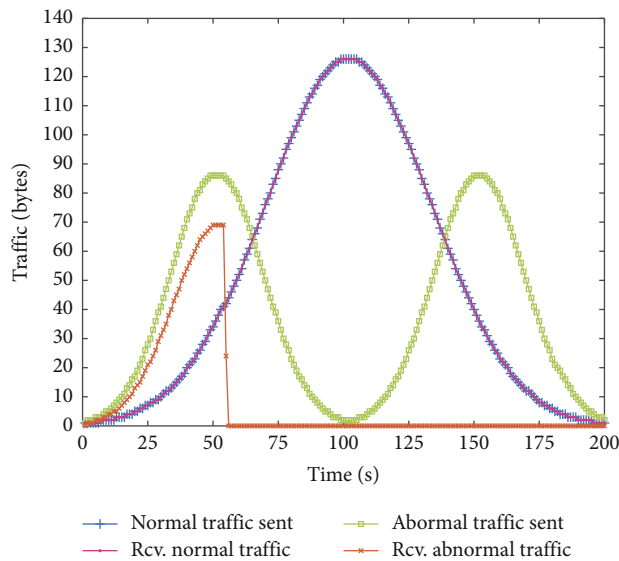


FIGURE 6: The evaluation of the trusted communication traffic protocol.

reputation (reputation is between 0.4 and 0.7), and low reputation (reputation is lower than 0.4). The three groups have 25, 15 and 10, users respectively.

Figure 7 shows the dynamic control results of the whole-process user behavior in three continuous stages. 0–200 s is the user identity authentication stage; 200–300 s is the user access control stage; and 300–350 s is the user traffic detection stage. It should be noted that, in order to visually display the results of dynamic control mechanism, Figure 7 only shows the number of users who successfully authenticated for the first time and access control for the first time, but does not show the number of users who successfully re-authenticated and re-access control.

In the identity authentication stage, we simulated a total of 200 users sending identity authentication requests to IAM. As can be seen from Figure 7, the designed IAM can accurately control user authentication behavior, and can generate different dynamic control results according to different reputation values of users.

Only users who are successfully authenticated in the identity authentication stage can perform access control. Therefore, in the access control stage, it can be seen from Figure 7 that the number of re-authentication (“re-auth”), re-access control (“re-acc. ctrl.”), and access blocking (“acc. block”) users changes with the time in the 200–300 s time period. The designed ACM module can generate

TABLE 2: User behavior grouping table.

Identity authentication stage			Access control stage			Traffic detection stage			
Number of users	Normal auth. request	100	Normal acc. ctrl. request	50	Abnormal traffic	Normal traffic	25		
						$GR_i^t < 0.4$	5		
						$0.4 \leq GR_i^t < 0.7$	10		
	Abnormal auth. request	$GR_i^t < 0.5$ $GR_i^t \geq 0.5$	50	Abnormal acc. ctrl. request	10 15 25	—	$AR_i^t < 0.35$	10	—
							$0.35 \leq AR_i^t < 0.6$	15	—
							$AR_i^t \geq 0.6$	25	—
						$GR_i^t \geq 0.7$	10	—	

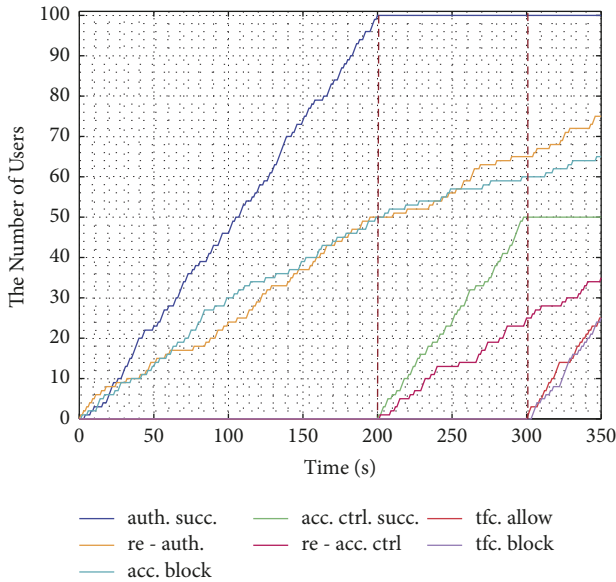


FIGURE 7: The evaluation of the dynamic control mechanism of the whole-process user behavior.

corresponding access control policies according to user’s access action.

In the traffic detection phase, as can be seen from Figure 7, the traffic detection module can allow users who send normal traffic (“tfc. allow”) to access network resources, and block the traffic sent by malicious users (“tfc. block”) in time. In addition, the designed dynamic feedback mechanism can generate accurate dynamic control results (“re-auth,” “re-acc. ctrl.,” and “acc. block”) according to the user’s reputation value when the traffic detection is abnormal. When the user’s reputation is lower than the threshold 0.4, the dynamic control mechanism will prevent users from accessing the network (“acc. block”). When the user reputation value is between 0.4 and 0.7, the proposed mechanism generates the dynamic control result of “re-auth.” When the user’s reputation is higher than 0.7, the user is asked to redo the access control process (“re-acc. ctrl.”).

6. Conclusion

In this paper, we have proposed a blockchain-enabled trusted protocol based on the whole-process user behavior. The proposed WPUB-BTP constructs a trusted control chain between user identity, access action, and communication

traffic, and realizes the control of user behavior in the whole process. In addition, the protocol also builds dynamic closed-loop feedback based on user reputation, which realizes dynamic control of user behavior. Eventually, we deployed the proposed protocol in the Hyperledger Fabric for evaluation. The results show that the proposed WPUB-BTP can control the whole-process user behavior and reduce the risk of network being attacked.

This paper focuses on demonstrating the dynamic trusted control mechanism based on whole-process user behavior. In future work, we will optimize the trusted subprotocol and parameter selection in each module, and conduct more in-depth research on authentication, access control, and malicious traffic detection.

Data Availability

The data that support the findings of this study can be obtained from the corresponding author upon reasonable request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Key R&D Program of China, under Grant no. 2018YFA0701604, and Fundamental Research Funds for the Central Universities, under Grant nos. 2021YJS012 and 2021YJS008.

References

- [1] H. Guo, J. Li, J. Liu, N. Tian, and N. Kato, “A survey on space-air-ground-sea integrated network security in 6G,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 53–87, 2022.
- [2] D. Je, J. Jung, and S. Choi, “Toward 6G security: technology trends, threats, and solutions,” *IEEE Communications Standards Magazine*, vol. 5, no. 3, pp. 64–71, 2021.
- [3] K. Wang, W. Quan, N. Cheng, M. Liu, Y. Liu, and H. A. Chan, “Betweenness centrality based software defined routing: observation from practical internet datasets,” *ACM Transactions on Internet Technology*, vol. 19, no. 4, pp. 1–19, 2019.

- [4] K. David and H. Berndt, "6G vision and requirements: is there any need for beyond 5G?" *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, pp. 72–80, 2018.
- [5] J. Dong, K. Wang, W. Quan, and H. Yin, "InterestFence: simple but efficient way to counter interest flooding attack," *Computers & Security*, vol. 88, Article ID 101628, 2021.
- [6] X. Zhang, Y. Zhao, and G. Min, "Intelligent video ingestion for real-time traffic monitoring," *ACM Transactions on Sensor Networks*, vol. 18, 2022.
- [7] A. G. Martín, A. Fernández-Isabel, I. Martín de Diego, and M. Beltran, "A survey for user behavior analysis based on machine learning techniques: current models and applications," *Applied Intelligence*, vol. 51, no. 8, pp. 6029–6055, 2021.
- [8] S. Ryu, Y. J. Kang, and H. Lee, "A study on detection of anomaly behavior in automation industry," in *Proceedings of the 2018 20th International Conference on Advanced Communication Technology (ICACT)*, Chuncheon, South Korea, February 2018.
- [9] X. Zhang, Z. Qi, G. Min, W. Miao, Q. Fan, and Z. Ma, "Cooperative edge caching based on temporal convolutional networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 9, pp. 2093–2105, 2022.
- [10] S. Zhang, J. Liu, H. Guo, M. Qi, and N. Kato, "Envisioning device-to-device communications in 6G," *IEEE Network*, vol. 34, no. 3, pp. 86–91, 2020.
- [11] Y. Siriwardhana, P. Porambage, and M. Liyanage, "AI and 6G security: opportunities and challenges," in *Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit*, Porto, Portugal, June 2021.
- [12] L. Jin, Y. Chen, T. Wang, P. Hui, and A. V. Vasilakos, "Understanding user behavior in online social networks: a survey," *IEEE Communications Magazine*, vol. 51, no. 9, pp. 144–150, 2013.
- [13] D. Jiang, Y. Wang, Z. Lv, S. Qi, and S. Singh, "Big data analysis based network behavior insight of cellular networks for industry 4.0 applications," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1310–1320, 2020.
- [14] S. Hu, Y. C. Liang, Z. Xiong, and D. Niyato, "Blockchain and artificial intelligence for dynamic resource sharing in 6G and beyond," *IEEE Wireless Communications*, vol. 28, no. 4, pp. 145–151, 2021.
- [15] A. H. Khan, N. Ul Hassan, C. Yuen et al., "Blockchain and 6G: the future of secure and ubiquitous communication," *IEEE Wireless Communications*, vol. 29, no. 1, pp. 194–201, 2022.
- [16] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, Article ID 117716, 2019.
- [17] Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: blockchain-assisted privacy-preserving authentication system for vehicular Ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146–4155, 2020.
- [18] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin, and K. K. R. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 6224–6238, 2022.
- [19] K. N. Qureshi, G. Jeon, M. M. Hassan, M. R. Hassan, and K. Kaur, "Blockchain-based privacy-preserving authentication model intelligent transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2022.
- [20] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green internet of Things," *ACM Transactions on Internet Technology*, vol. 21, no. 3, pp. 1–20, Article ID 80, 2021.
- [21] S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-based IoT access control system: towards security, lightweight, and cross-domain," *IEEE Access*, vol. 9, Article ID 36868, 2021.
- [22] B. S. Egala, A. K. Pradhan, V. Badarla, and S. P. Mohanty, "Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical Things with effective access control," *IEEE Internet of Things Journal*, vol. 8, no. 14, Article ID 11717, 2021.
- [23] Y. Feng, W. Zhang, X. Luo, and B. Zhang, "A consortium blockchain-based access control framework with dynamic orderer node selection for 5G-enabled industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2840–2848, 2022.
- [24] M. Li, H. Zhou, and Y. Qin, "Two-stage intelligent model for detecting malicious DDoS behavior," *Sensors*, vol. 22, no. 7, Article ID 2532, 2022.
- [25] S. Cao, S. Dang, Y. Zhang, W. Wang, and N. Cheng, "A blockchain-based access control and intrusion detection framework for satellite communication systems," *Computer Communications*, vol. 172, pp. 216–225, 2021.
- [26] W. Guo, J. Xu, and Y. Pei, "A distributed collaborative entrance Defense framework against DDoS attacks on satellite internet," *IEEE Internet of Things Journal*, vol. 9, no. 17, pp. 15497–15510, 2022.
- [27] P. Ramanan, D. Li, and N. Gebraeel, "Blockchain-based decentralized replay attack detection for large-scale power systems," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 52, no. 8, pp. 4727–4739, 2022.
- [28] R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C. W. Lin, "ML-DDoS: a blockchain-based Multilevel DDoS mitigation mechanism for IoT environments," *IEEE Transactions on Engineering Management*, pp. 1–14, 2022.
- [29] F. Guthrie, S. Lowe, and M. Saidel-Keesing, *VMware vSphere Design*, John Wiley & Sons, New York, NY, USA, 2011.
- [30] Z. Tu, H. Zhou, and K. Li, "A blockchain-based user identity authentication method for 5G," in *Proceedings of the 2021 5th International Symposium on Mobile Internet Security (MobiSec 2021)*, Jeju Island, Republic of Korea, October 2021.
- [31] V. C. Hu, D. R. Kuhn, and D. F. Ferraiolo, "Attribute-based access control," *Computer*, vol. 48, no. 2, pp. 85–88, 2015.
- [32] Z. Tu, H. Zhou, K. Li, M. Li, and A. Tian, "An energy-efficient topology design and DDoS attacks mitigation for green software-defined satellite network," *IEEE Access*, vol. 8, Article ID 211434, 2020.
- [33] A. Josang and R. Ismail, "The beta reputation system," in *Proceedings of the 15th bled electronic commerce conference*, Bled, Slovenia, June 2002.