Network Management Research Group J. Yan
Internet-Draft H. Zhou
Intended status: Informational Y. Yang
Expires: October 13, 2024 H. Song
Z. Tu
Beijing Jiaotong University
April 8, 2024
Document: draft-tu-nmrg-blockchain-trusted-protocol-03.txt

A Blockchain Trusted Protocol for Intelligent Communication Network

Abstract

This document defines a blockchain-based trusted protocol for sixth-generation (6G) intelligent communication network.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 13, 2024.

Copyright Notice

Table of Contents

1. Introduction

The sixth-generation (6G) network promotes the interconnection of everything and put forward higher requirements for network security. The existing network architecture mainly focuses on the end-to-end communication process and lacks the dynamic feedback to the user behavior. Based on the current network architecture, 6G intelligent communication network introduces collaborative processing unit and intelligent agent unit at the access gateway, and uses environment, media, and security knowledge base to realize dynamic control and closed-loop feedback of user behavior [ICN20]. Based on the 6G intelligent communication network architecture, this document proposes a blockchain-based trusted protocol for user behavior control. By constructing the trust link of "user identity-communication behavior-user reputation-security control", the designed trusted protocol forms the dynamic feedback and global control ability of the whole-process user behavior after users access the network.

This document designs a blockchain trusted protocol in 6G intelligent communication network, including trusted authentication protocol, trusted access control protocol, trusted locator/identifier separation protocol and trusted feedback control protocol [BTP22].

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Blockchain Trusted Protocol Architecture

The blockchain trusted protocol is deployed at the access gateways in the form of smart contracts. The smart contract in the blockchain is used to store the user's identity, access behavior, identification and other information, and security control the user's behavior together with the collaborative processing unit.

Figure 1 shows the architecture of the blockchain trusted protocol, and the components in the architecture will be introduced separately next.

- User Equipment (UE): We use UE to represent all users and devices in the 6G intelligent communication network, such as users, intelligent devices, IoT devices, etc. When a UE accesses the network or want to obtain the network resources, it needs to send a corresponding request to the access gateway. Only when the initiated request is approved, the UE can obtain the corresponding permission to access the network and resources.

- Access Gateway (AG): The AG is responsible for receiving and forwarding requests sent by UE. Multiple different AGs run the same consensus algorithm to form a blockchain network. Besides, the collaborative processing module is deployed in the AG to response and control the user behavior.

- Collaborative Processing Module (CPM): The CPM responds, forwards, and processes the requests initiated by UE. In the process of user behavior control, CPM is the executor of security control of UE, which is responsible for executing and forwarding the control results generated by smart contracts.

- Smart Contract (SC): The SC is deployed in the blockchain network built by the AGs running the same consensus algorithm. In the blockchain trusted protocol architecture, the designed trusted protocol consists of four sub-protocols. And each sub-protocol is deployed in the blockchain network in the form of smart contract (identity authentication contract, access control contract,

locator/identifier separation contract, and feedback control contract) to security manage and control the user behavior.

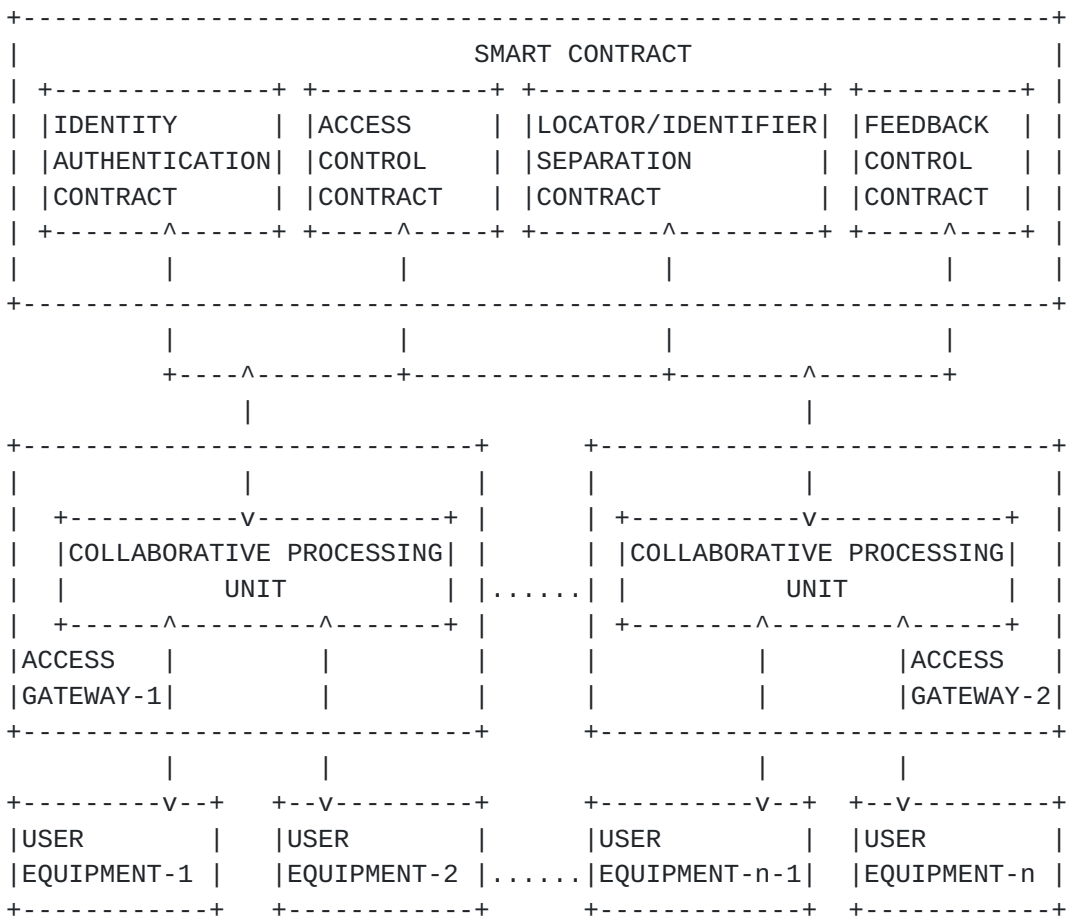

Figure 1 The architecture of blockchain trusted protocol

o Identity Authentication Contract (IAC): The IAC is used to authenticate the UE identity and ensure that the identity is trusted. In the process of identity authentication, IAC not only respond to the authentication request initiated by UE and generate the corresponding authentication vectors, but also stores the authentication behavior in the blockchain to ensure the traceability of the user's authentication behavior.

o Access Control Contract (ACC): The ACC generates the corresponding access control policy according to the access request initiated by the UE to ensure the action of UE is trusted. Similarly, the ACC records the access behavior of UE. On the one hand, it is used to evaluate the user reputation of the feedback control module, and on the other hand, it guarantees the traceability of access behavior of UE.

- Locator/Identifier Separation Contract (LISC): The LISP protocol is used in the 6G intelligent communication network to isolate the access network form the backbone network, which can improve the security capabilities of the network by separating the identity and location [RFC6830]. Therefore, in the trusted protocol architecture, we use the LISC to store the mapping relationship between the end-identifier (EID) and the routing-locator (RLOC).

- Feedback Control Contract (FCC): The FCC is used to evaluate the reputation value of the UE. This contract evaluates the UE by obtaining various historical behavior data (such as authentication behavior, access control behavior, etc.), and develops different levels of security control policies based on the calculated reputation value.

In the following section, we describe the four trusted sub-protocols in detail.

4. Blockchain Trusted Authentication Protocol

In the blockchain trusted authentication protocol, the CPM forwards and processes the identity authentication requests of UE, while the IAC stores the authentication credentials and generates the user authentication vector.

Figure 2 shows the blockchain trusted authentication protocol, and the trusted authentication protocol can be described as the following steps.

STEP 1: UE sends the UE Authentication Request (UAR) to the CPM, the UAR contains the identity of UE U_id and UE identification information I_ua.

STEP 2: CPM invokes the interface of IAC UEAuth() to generate authentication vector. The input of UEAuth() contains U_id and I_ua.

STEP 3: IAC returns the generated authentication vector (AV) to CPM.

STEP 4: UE, CPM, and IAC interact with each other to authenticate UE according to the generated authentication vector.

STEP 5: IAC stores the Identity Authentication Behavior B_ia of UE in the blockchain, the B_ia includes the UE identity U_id, identity authentication result R_ia, authentication time T_ia.

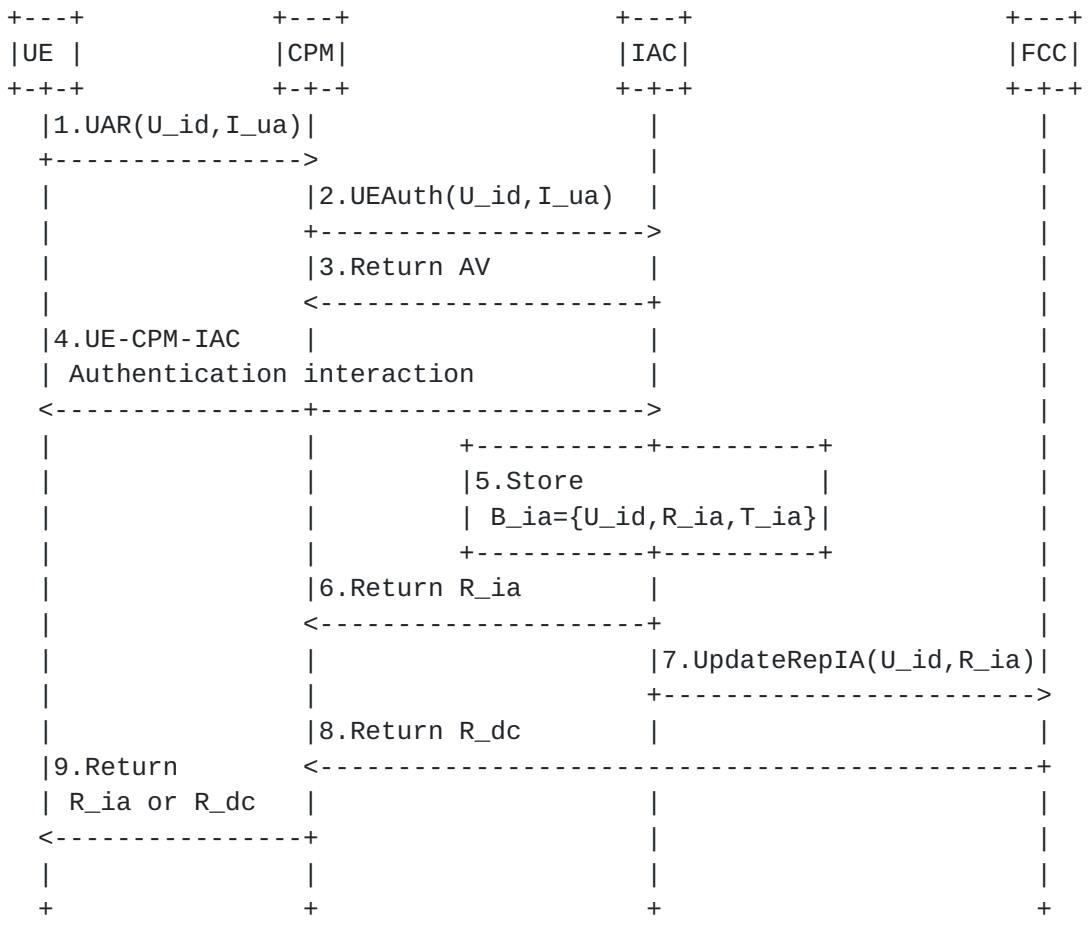

Figure 2 The blockchain trusted authentication protocol

STEP 6: IAC returns the authentication result R_ia to CPM.

STEP 7: The IAC invokes the UpdateRepIA() function of FCC to update the identity authentication reputation value of UE. The UpdateRepIA() contains U_id and R_ia of UE.

STEP 8: If the UE is authenticated successfully, go to STEP 9. Otherwise, the FCC calculated the authentication reputation, generates and rerturns the Dynamic Control Result R_dc to CPM based on the evaluated reputation value.

STEP 9: CPM forwards the R_ia or the R_dc to the UE.

5. Blockchain Trusted Access Control Protocol

The trusted access control protocol is used to evaluate UE access control behavior. In the trusted access control protocol, the CPM is used to forward the access control requests initiated by UE, while

the ACC generates the access policy and stores the user access control behavior.

Figure 3 represents the blockchain trusted access control protocol.

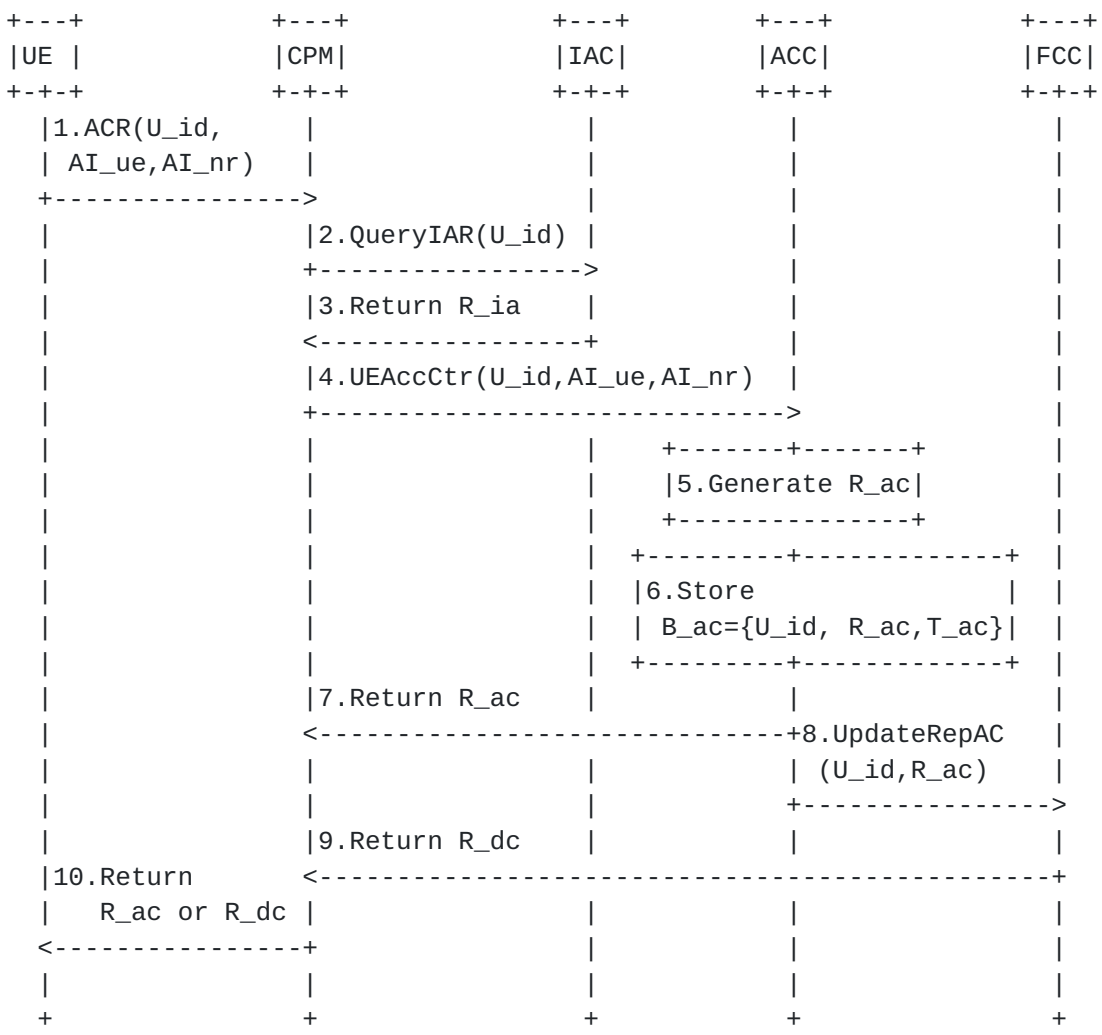

Figure 3 The blockchain trusted access control protocol

STEP 1: UE sends the Access Control Request (ACR) to CPM, ACR contains the UE identity U_id, access control information of UE AI_ue, and the access control information of the network resource AI_nr.

STEP 2: The CPM calls the QueryIAR() function of IAC to query the authentication result of UE, the input of function QueryIAR() contains U_id.

STEP 3: The IAC queries the authentication result of UE stored in the blockchain and returns the identity authentication result R_ia to the

CPM. If the UE is illegal, the access control result R_ac is set to 0, and the next step is STEP 6. Otherwise, go to STEP 4.

STEP 4: If the identity of UE is trusted, the CPM invokes the UEAccCtr() function of ACC to generate the access control policy of UE. The input of UEAccCtr() contains U_id, AI_ue, and AI_nr.

STEP 5: The ACC generates the access control result R_ac according to the AI_ue and AI_nr.

STEP 6: Based on the generated R_ac, the ACC stores the access control behavior B_ac of UE in the blockchain. B_ac contains the U_id, R_ac, and access control time T_ac.

STEP 7: AAC returns the access control result R_ac to CPM.

STEP 8: The ACC invokes the UpdateRepAC() function of FCC to update the access control reputation value of UE. The UpdateRepAC() contains U_id and R_ac of UE.

STEP 9: If the access action of UE is authorized, go to STEP 10. Otherwise, the FCC calculated the access control reputation, generates and rerturns the Dynamic Control Result R_dc to CPM based on the evaluated access control reputation.

STEP 10: CPM forwards the R_ac or the R_dc to the UE.

6. Blockchain Trusted Locator/Identifier Separation Protocol

After the UE completes the authentication and access control process, the EID and RLOC mapping transformation process also needs to be performed to improve the network security.

The blockchain trusted locator/identifier separation protocol implements the mapping and conversion of EID and RLOC. In the blockchain trusted locator/identifier separation protocol, the CPM invokes the interface of the LISC to query the mapping relationship between EID and RLOC, and the LISC stores and records the pairing information of EID and RLOC to realize the separation mapping between user identity and the network location.

Figure 4 shows the blockchain trusted locator/identifier separation protocol, and it can be described as the follows.

STEP 1: UE-1 obtains the EID address (EID2) of the UE-n through the domain name systems or other methods, fills in each header and payload information, and constructs the data packet.

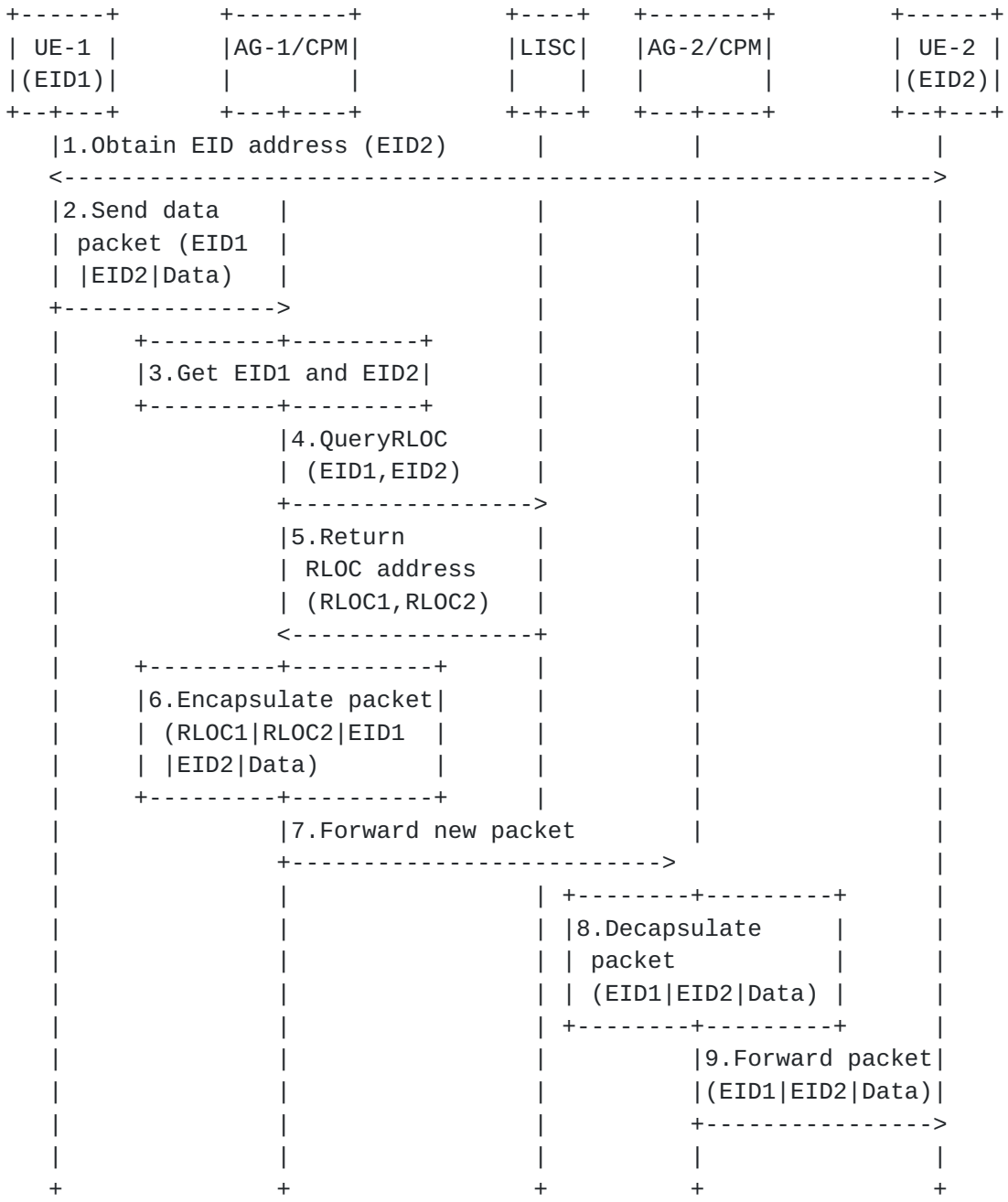

Figure 4 The blockchain trusted locator/identifier separation protocol

STEP 2: UE-1 sends the data packet, the data packets that need to pass through the core network will be directly forwarded to the AG-1. The source and destination address in the packets are set to EID1 and EID2, respectively.

STEP 3: After receiving the packet, AG-1 obtains the IP address information in the packets, including the source address (EID1) and destination address (EID2).

STEP 4: The CPM invokes the QueryRLOC() function of LISC to query the RLOC address of EID1 and EID2. The input of QueryRLOC() contains EID1 and EID2.

STEP 5: The LISC queries the mapping relationship between EID and RLOC registered in the blockchain, and returns the RLOC addresses (RLOC1 and RLOC2) corresponding to EID1 and EID2 to CPM respectively.

STEP 6: After successfully obtaining the RLOC addresses corresponding to the two EIDs, AG-1 encapsulates the new IP header before the original packet. In the new IP header, the source address is set to RLOC1 and the destination address is set to RLOC2.

STEP 7: Then, AG-1 searches the core routing table and forwards new data packets to the core network.

STEP 8: After the data packet is forwarded through the core network to the AG-2 of the network egress router where the destination node is located, the CPM in AG-2 decapsulates the packet to obtain the original packet. In the original packet, the source address is EID1, and the destination address is EID2.

STEP 9: By searching the local routing table, AG-2 forwards the original packet to UE-2.

7. Blockchain Trusted Feedback Control Protocol

The blockchain trusted feedback control protocol is used to security control the behavior of UE. In the blockchain trusted feedback control protocol, the CPM receives the information of potential malicious UE detected or inferred by external modules (such as malicious traffic detection units, security knowledge bases), and calls the FCC interface to perform user historical reputation analysis. The FCC contract calculates the reputation value of potential malicious UEs, and formulates fine-grained security management and control strategies according to the calculated reputation value.

Figure 5 is the flowchart of the blockchain trusted feedback control protocol. It can be expressed in detail as the follows.

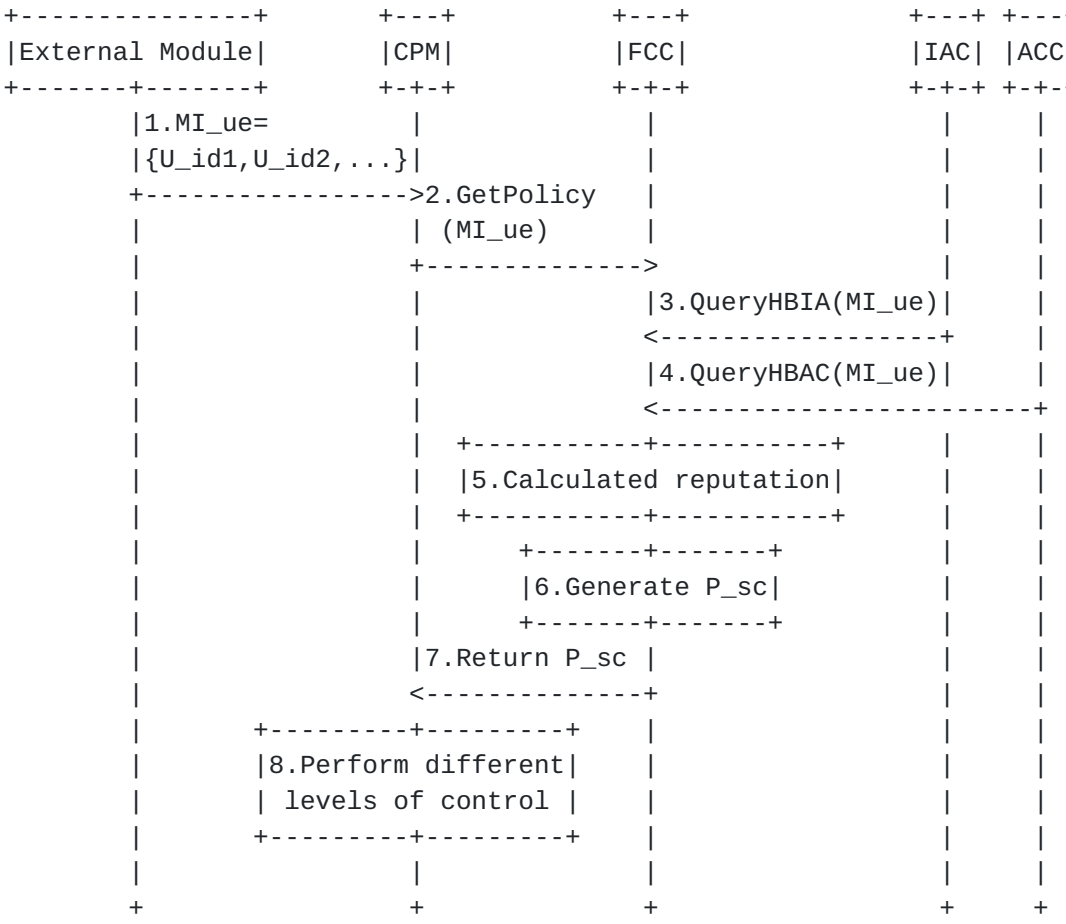

Figure 5 The blockchain trusted feedback control protocol

STEP 1: CPM continuously receives the potentially malicious UE information MI_ue sent by the external module. MI_ue is a set of identities of potential malicious UE, which can be expressed as follows. MI_ue = {U_id1, U_id2, ...}. U_id1 and U_id2 represents different UE identities.

STEP 2: After receiving potentially malicious UE information MI_ue, CPM invokes the GetPolicy() function of the FCC to obtain the fine-grained security control policies of the potential malicious UEs. The input of GetPolicy() is MI_ue.

STEP 3/4: FCC calls the interface with other smart contract (IAC, ACC) to obtain the historical behavior of potentially malicious UE, and conducts the reputation value according to the UE historical behavior. The interface to IAC is QueryHBIA(), and to ACC is QueryHBAC(). The

input of QueryHBIA() and QueryHBAC() is the identity information of the potentially malicious user MI_ue.

STEP 5: FCC calculated the reputation value of the potentially malicious UE based on the obtained historical behavior.

STEP 6: Then, FCC generates the fine-grained security control policies P_sc based on the calculated reputation values.

STEP 7: FCC returns the P_sc to CPM.

STEP 8: CPM performs different levels of control on malicious UE according to the received P_sc, such as invalidation of identity authentication information, revocation of access control permissions, etc., to achieve fine-grained real-time blocking of malicious attacks at the access gateway of the network.

8. IANA Considerations

This document has no IANA actions.

9. Security Considerations

The blockchain system needs to maintain the overall security of the system at the levels of data content, consensus algorithms, smart contracts, and peer-to-peer networks through technologies such as cryptography and network security. Possible security problems in cryptography include improper key management, vulnerabilities in cryptographic algorithms or components. In addition, the blockchain trusted protocol is deployed at the access gateway of the network, so the identity of the access gateway needs to be trusted.

10. References

10.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfceditor. org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2 Informative References

[ICN20] Jiang, C., Ge, N., Kuang, L., "AI-enabled next-generation communication networks: Intelligent agent and AI router, IEEE Wireless Communications", September 2020, <https://ieeexplore.ieee.org/abstract/document/9210134>.

[BTP22] Tu, Z., Zhou, H., Li, K., Song, H., Yang, Y., "A Blockchain-Enabled Trusted Protocol based on Whole-Process User Behavior in 6G Network, Security and Communication Networks", September 2022, <https://doi.org/10.1155/1970/8188977>.

[RFC6830] D. Farinacci, V. Fuller, D. Meyer, "The Locator/ID Separation Protocol (LISP)", RFC 6830, DOI 10.17487/RFC6830, January 2013, <https://www.rfc-editor.org/info/rfc6830>.

Acknowledgments

TBC

Author's Addresses

Jingfu Yan
Beijing Jiaotong University
Beijing
Phone: <86-18810753358>
Email: 22110030@bjtu.edu.cn

Huachun Zhou
Beijing Jiaotong University
Beijing
Phone: <86-13718168186>
Email: hchzhou@bjtu.edu.cn

Yuzheng Yang
Beijing Jiaotong University
Beijing
Phone: <86-15802201359>
Email: 21120151@bjtu.edu.cn

Zhe Tu
Beijing Jiaotong University
Beijing
Phone: <86-13146050755>
Email: zhe_tu@bjtu.edu.cn

Haoxiang Song
Beijing Jiaotong University
Beijing
Phone: <86-13161229322>
Email: 20120099@bjtu.edu.cn