Research on 5G Core Network Trust Model Based on NF Interaction Behavior

Ying Zhu[1], Caixia Liu[1,2*], Yiming Zhang[1], and Wei You[1]
[1] PLA strategic support army Information engineering university
Zhengzhou Henan, 450001, China
[e-mail: ouyangxiyu16@163.com, zym913914944@163.com]
[2] Institute of Systems Engineering, Academy of Military Sciences
Beijing, 100091, China
[e-mail: lcxtxr@163.com]
*Corresponding author: Caixia Liu

Received May 28, 2022; revised September 18, 2022; accepted September 23, 2022; published October 31, 2022

Abstract

The 5G Core Network (5GC) is an essential part of the mobile communication network, but its security protection strategy based on the boundary construction is difficult to ensure the security inside the network. For example, the Network Function (NF) mutual authentication mechanism that relies on the transport layer security mechanism and OAuth2.0's Client Credentials cannot identify the hijacked NF. To address this problem, this paper proposes a trust model for 5GC based on NF interaction behavior to identify malicious NFs and improve the inherent security of 5GC. First, based on the interaction behavior and context awareness of NF, the trust between NFs is quantified through the frequency ratio of interaction behavior and the success rate of interaction behavior. Second, introduce trust transmit to make NF comprehensively refer to the trust evaluation results of other NFs. Last, classify the possible malicious behavior of NF and define the corresponding punishment mechanism. The experimental results show that the trust value of NFs converges to stable values, and the proposed trust model can effectively evaluate the trustworthiness of NFs and quickly and accurately identify different types of malicious NFs.

Keywords: 5G, 5G Core Network, trust model, time decay, punishment mechanism, trust transmit

1. Introduction

The large-scale deployment of the 5th generation mobile network (5G) brings a better communication experience to users. Meanwhile, operators are also placing higher demands on 5G network security. As an essential part of the mobile network, abnormalities in the Network Function (NF) of the 5G core network (5GC) not only endanger the security and stability of 5GC and affect the regular operation of the mobile communication network, but also lead to the inability of users to communicate and even cause the leakage of user information. The current boundary-based security protection model for mobile networks is difficult to resist attacks from inside the network, and there is an urgent need to explore new security mechanisms to enhance further the security of the mobile network [1].

Researchers have analyzed and proposed various solutions to the potential security threats in 5GC. Trust management as a security enhancement scheme has been noticed and introduced into mobile communication networks. In recent years, trust models have been applied to quantify and manage trust in many fields, such as finance[2], wireless sensor networks[3-5], vehicular networks[6-12], edge computing[13-15], cloud computing[16-17], Internet of Things (IoT) [18-19], and 5G network slicing[20]. The main methods used by researchers to build trust models include Bayesian theory [5-6], D-S theory [13], fuzzy logic [21], machine learning [22-23], and graph theory [24-25]. At present, the research on trust model is relatively mature, and the methods for building trust models are diverse. However, facing the increasing security requirements of mobile networks, researchers qualitatively propose that the security of 5GC can be enhanced by combining trust management, but a quantitative trust management scheme is lacking. To enhance the security of 5GC, this paper designs a trust model suitable for 5GC, and realizes the identification of malicious NFs by evaluating the trust level of NFs.

To quantitatively implement trust evaluation in the system, the trust model should be designed in a targeted manner from the actual characteristics of the system and the purpose of the evaluation. There are two challenges in introducing the trust model into 5GC:

1. How can adequate trust evidence be extracted from a large amount of data so that the quantification of NF trust can be accomplished? If trust is quantified based on NF interaction data and context awareness, it is known that messages from different NFs and messages requesting various services have different contents. We need to explore a unified standard to quantify trust.
2. How can the trust assessment module be deployed appropriately so that the reliability of the assessment results can be assured? The evaluation center greatly influences the centralized trust model, and the information collection process occupies a lot of resources. Due to the limitation of information collection granularity, the evaluation center may not obtain detailed trust evidence. How to determine the reliability of the trust evaluation results of each evaluation module in the distributed trust model is a problem that many scholars continue to study.

Based on the characteristics of 5GC and combining the advantages of the distributed and centralized trust models, this paper designs a lightweight trust model suitable for 5GC. With each NF as the evaluation subject, the credibility of other NFs in the network is scored based on the interaction behavior of the NF. As the evaluation center, the Network Repository Function (NRF) summarizes and adjudicates the trust evaluation results and low-scoring trust evidence of each evaluation module and obtains the recommended trust of NF by synthesizing the reliable evaluation results.

The main contributions of this paper are as follows:

1. A Trust Model applicable to 5GC is proposed. Each NF is deployed with a trust

evaluation module which contains four parts: direct trust, indirect trust, time decay, and punishment mechanism. NRF acts as an evaluation center to aggregate and adjudicate the trust evaluation results of each evaluation module. It avoids the waste of resources caused by collecting a large amount of data by the evaluation center and ensures the reliability of the distributed evaluation results.

2. A dynamic trust evaluation algorithm suitable for 5GC is proposed. By taking the interaction behavior and context information of NF as the basis of trust evaluation, the interaction frequency proportional trust and interaction behavior trust are proposed to realize the quantification of NF trust. The malicious behaviors of NF are classified, and the corresponding punishment mechanism is defined according to the degree of harm of the behavior.
3. A core network prototype system is constructed in simulation experiments to analyze the influence of each parameter in the trust evaluation algorithm on the effectiveness of the evaluation mechanism, and to test the ability of the trust model to identify malicious NFs under different malicious behaviors to achieve verification of the effectiveness and robustness of the trust model.

2. Related Work

The 3rd Generation Partnership Project (3GPP) standardization organization continues to update and improve the 5G communication technology standards, describes the security architecture of the 5G system in detail [26], and analyzes the Service Based Architecture (SBA) potential security vulnerabilities [27]. Liu et al. [28] evaluated the security of 5G networks and security protocols based on the Lowe taxonomy. By analyzing 5G security specifications, Roger et al. [29] proposed that 5G networks are vulnerable to the Long Term Evolution (LTE) adversarial attacks due to the implicit trust in messages before identity authentication. Holtrup et al. [30] described the security mechanisms of 5G systems, analyzed 12 threat scenarios for the wireless access and network core, and discussed possible security measures. New services and new technologies bring higher security requirements to 5G. China Communications Standards Association (CCSA) constructively introduced the concept of Zero Trust into mobile communication networks [1]. ZTE researchers [31] proposed the application of Single Package Authorization (SPA), NF trust evaluation, authorization revocation, and other methods to enhance the security of 5GC. Lu et al. [32] proposed to decouple NF communication logic and service logic to enhance fast and reliable communication between NFs. The researchers of China Telecom proposed to realize the hiding of network topology based on the Service Communication Proxy (SCP) to ensure efficient and reliable communication of NF [33]. Although scholars have begun to pay attention to the communication security of NFs in 5GC, few studies have evaluated the trustworthiness of NFs themselves.

Current research efforts on trust in 5G are focused on the critical technologies of 5G, such as network slicing, edge computing, and Massive Machine Type Communication (mMTC), which is an important application scenario for 5G. Researchers [13-15] respectively studied the use of trust evaluation in edge computing for ensuring the reliability of edge data collection, guaranteeing resource management and collaborative optimization, and realizing direct management of terminal nodes. Matin et al. [16] studied the use of trust evaluation to select trusted cloud service providers in the cloud environment. Yu et al. [17] constructed a cloud computing security assessment model based on trust management and quantitative trust criteria. Huang et al. [18] proposed a mechanism to verify trust for IoT data devices actively

and then constructed a verifiable trust evaluation scheme for intelligent network systems. Aiming at the security problem of IoT edge servers, an algorithm for aggregated reputation was proposed by integrating information entropy theory [19]. Niu et al. [20] presented the concept of network slicing trust degree and established a slice trust degree model for 5G network slicing. In these works, the trust model is proven to be an effective security mechanism to enhance system reliability. Therefore, we introduce the trust model into 5GC to ensure the security of the NFs by evaluating the trustworthiness of the NFs within 5GC.

3. Problem Background and Analysis

3.1 Overview of NF Security Mechanisms

The mutual authentication between NFs in 5GC is based on the transport layer security mechanism and the Client Credentials of OAuth2.0 of the application layer. The transport layer security mechanism is the transport protection mode of Transport Layer Security (TLS). When communicating between NF instances, the Public Key Infrastructure (PKI) system is used to authenticate the server and the client, and TLS encryption protects the transmitted messages. The Certificate Authority (CA) in the operator domain is the core of PKI, responsible for signing, authenticating, and managing TLS entity certificates for NF. The identity of NF in the service access process will change according to the change in service requirements, so NF should support both server certificates and client certificates.

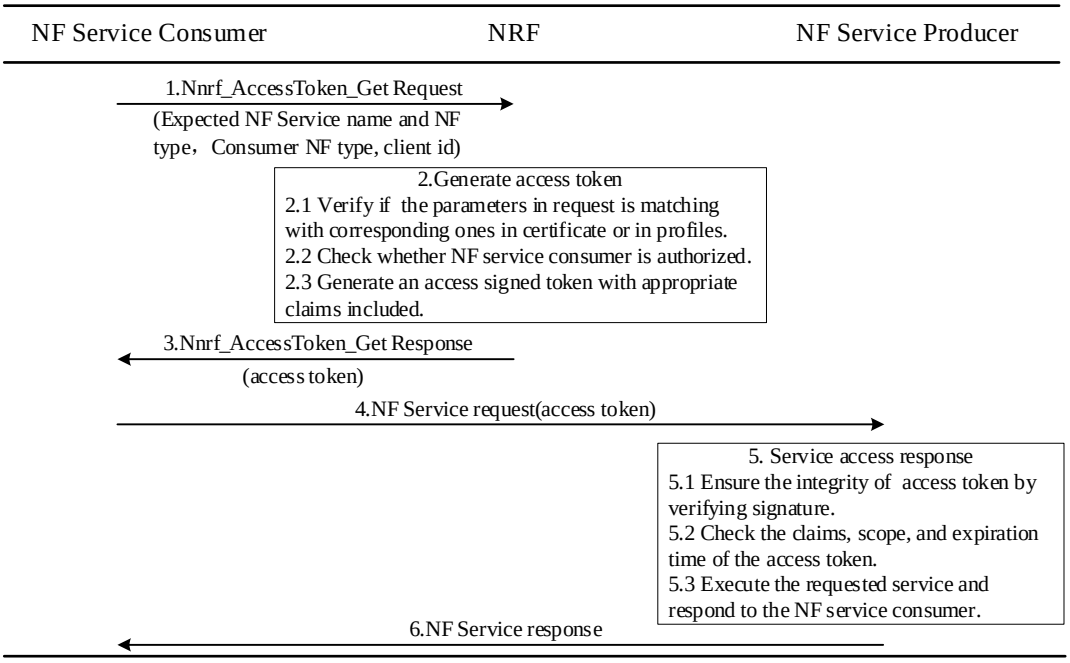


Fig. 1. NF service access process [23]

The service access process of NFs in 5GC is designed based on the Client Credentials mechanism of OAuth2.0. As shown in **Fig. 1**, before the NF accesses the service to other NFs, it must request an access token from the NRF. At this time, the NRF is equivalent to the authentication server, which is responsible for verifying the request message of the NF and deciding whether to issue an access token to the NF. The NF requesting the access token from

the NRF is called the NF service consumer, and the accessed NF is called the NF service producer. The NF service consumers can request services from the NF service producers only after obtaining the access token of NRF.

3.2 Design of Trust Model Based on 5GC Topology

Fig. 2 is the schematic diagram of the 5GC topology after combining the trust model. The Access and Mobility Management Function (AMF), the Session Management Function (SMF), the Unified Data Management (UDM), the Authentication Server Function (AUSF), the User Plane Function (UPF), the Policy Control Function (PCF), and NRF in the figure are the basic NFs of the 5G core network. 3GPP describes the service functions of each NF and provides the principles for NF service discovery and selection. When an NF instance goes online in 5GC, it needs to register with NRF, which stores the profile of the NF. The profile includes the identity information of the NF, including the NF type, IP address, and services provided, the information about the NF that is allowed to be accessed, including the NF type, Instance ID, IP address, and the service functions it is entitled to request.

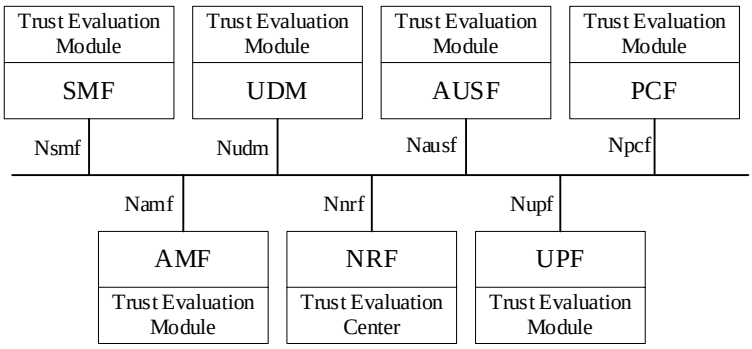


Fig. 2. NF topology combined with the trust model

In the deployed 5GC, each NF will initiate or process many request messages per unit time, and the services provided by the NF are interrelated. The reliability of each NF is directly related to the safe and efficient operation of 5GC. Therefore, a trust evaluation module can be deployed on each NF to quantify the trust of other NFs based on the interaction behavior.

NRF supports the registration of NF instances, provides service discovery functions, stores the configuration files of NF instances, and plays a crucial role in the NF service access process. Therefore, NRF can be used as a trust evaluation center, which is responsible for aggregating and adjudicating the evaluation results of each NF and the trust evidence for low values, so as to obtain the recommended trust for each NF.

Based on the above analysis, when designing the trust model in this paper, the trust model is divided into two parts: the trust evaluation module and the trust evaluation center module. Based on the interactive behavior of NF, the trust evaluation module evaluates the trust value of other NFs, and the evaluation center summarizes and judges the validity of the evaluation results of each evaluation module. After the NF goes online on 5GC, the trust value of the NF will increase or decrease according to the subsequent interaction behavior of the NF.

3.3 NF Interaction Analysis

In the actual service procedures, the interaction frequency between different NFs is quite different. The end-to-end information flow between NFs can be sorted out by the system process defined in 23.502 [34], and the interaction relationship of NF in the process can be

obtained, as shown in **Fig. 3**.

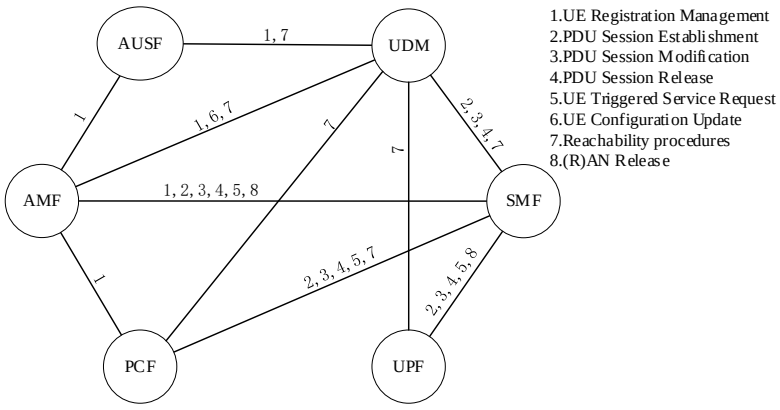


Fig. 3. NF interaction relationship based on procedures

NF evaluates the trust value of each other based on historical interaction information and context awareness. Based on historical interaction information, communication behavior and communication frequency can be evaluated. Based on context awareness, it can be evaluated whether the actual IP address, Instance ID, and NF type of the NF match the information in the request message and whether the serviced UE is in the SUPI list.

4. Trust Model Based on Interaction Behavior

4.1 An Overview of the Trust Model

The trust model architecture of this paper is shown in **Fig. 4**. The trust evaluation module includes five components: direct trust, indirect trust, time decay, punishment mechanism, and comprehensive trust.

Specifically, the trust between NFs is defined as follows:

Definition 1: Direct trust. Based on historical interaction information, NF quantifies the trust of NFs from the two dimensions of interaction frequency ratio and interaction behavior reliability and integrates the trust values of the two dimensions to obtain direct trust in other NFs.

Definition 2: Indirect trust. Based on the trust value transmitted by the non-direct interaction trust path between *NFi* and *NFj*, the indirect trust value of *NFi* and *NFj* can be obtained by trust inference.

Definition 3: Time decay. The more recent the trust evaluation time, the more reliable the result. The decay factor is a set of parameters that adjust the weight of the trust evaluation result at different sampling times. The evaluation module combines the time decay factor to update the trust value of NF.

Definition 4: Punishment mechanism. The malicious behavior of NF is classified, and the penalty scores of different malicious behaviors are defined according to the degree of harm of the malicious behavior.

Definition 5: Comprehensive trust. The comprehensive trust value of *NFi* to *NFj* is obtained by combining the direct trust, indirect trust after time decay, and punishment mechanism.

Definition 6: Recommended trust. The evaluation center aggregates and adjudicates the trust evaluation results of each evaluation module and obtains the recommended trust of NF.

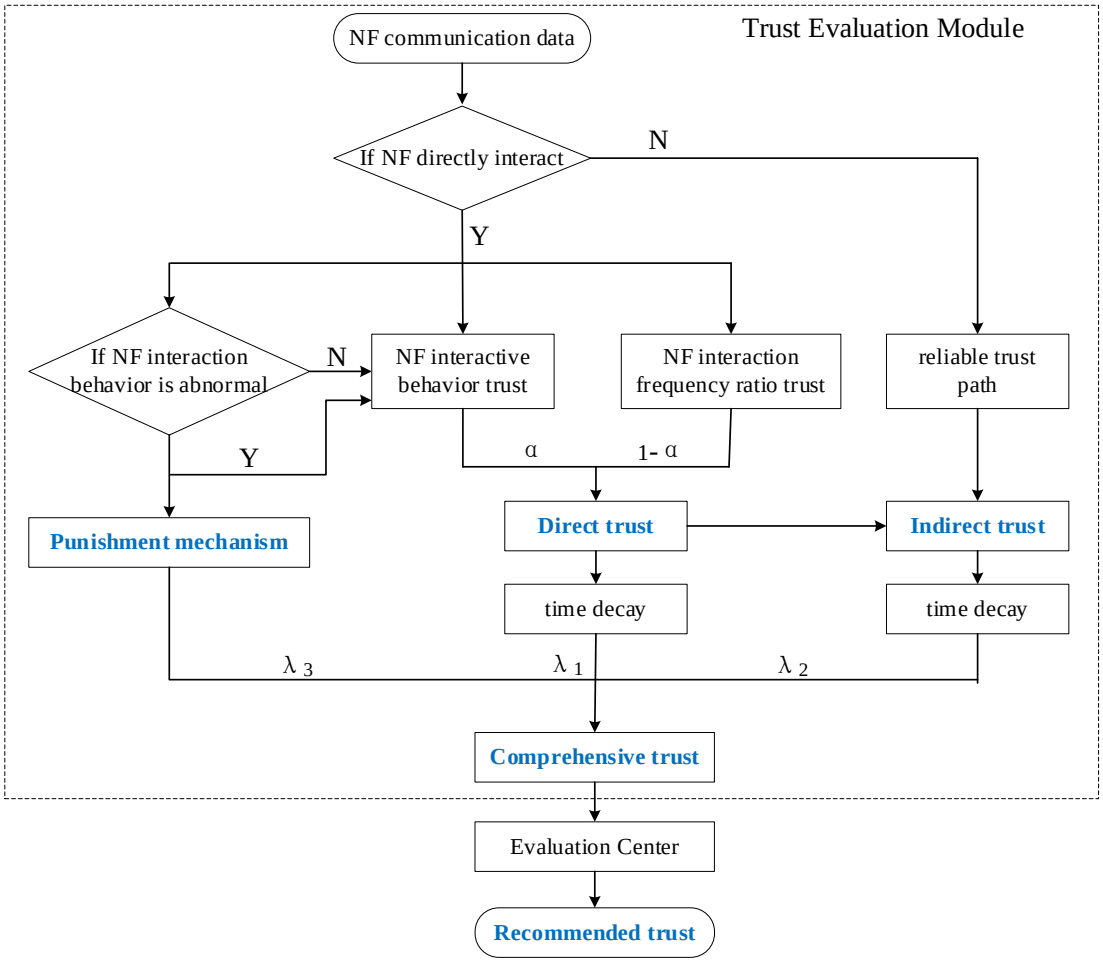


Fig. 4. Trust model architecture diagram

The symbol definitions used in the model are shown in **Table 1**.

Table 1. Model Symbol Definition

Symbol	Definition
S_i	Set of NFs that have direct communication with *NFi*
M	Set of all NFs contained within the domain
Δt	Time window
$N_i(\Delta t)$	Total number of request messages received by *NFi* within Δt
θ_{ij}	The expected value of the ratio of request messages sent by *NFj* to *NFi* to the total received messages by *NFi*
$num_{ij}(\Delta t)$	The total number of request messages sent by *NFj* to *NFi* within Δt
σ	Parameter to adjust the rate of decrease in the frequency ratio trust degree

s	The number of successful interactions between *NFj* and *NFi* within Δt
f	The number of failed interactions between *NFj* and *NFi* within Δt
α	The weight of interactive behavior trust in direct trust
S_{ij}	The intersection of collection S_i and collection S_j
ω_l	Between *NFi* and *NFj*, the weight of the lth reliable path
ρ	Time decay factor
P	The number of trust evaluation results that can be aggregated by the time decay module
k	Number of malicious behaviors in *NFi*
$\lambda_1, \lambda_2, \lambda_3$	Direct trust weight, indirect trust weight, punishment mechanism weight
η_l	The punishment score corresponding to the lth malicious act

4.2 Trust Evaluation Module

4.2.1 Direct Trust Evaluation

The interaction relationship between NFs in 5GC procedure is fixed, and the interaction relationship between NFs can be determined by the proportion of different procedures initiated by users during this period. Based on the statistical data of user behavior, the service needs of users at different periods can be obtained. Even though the network access conditions of UEs in different periods in the actual network are quite different, the interaction frequency between different NFs has a specific correlation. In any period of time in an ideal state, the ratio of the number of interactive messages between *NFj* and *NFi* to the total number of *NFi* interactive messages is fixed. Therefore, interaction frequency ratio trust can be used to measure the rationality of NF interaction behavior.

We modify the probability density function of the normal distribution to fit the interaction frequency ratio trust. Therefore, the smaller the deviation between the interaction frequency ratio and the expected value, the higher the trust degree. Suppose *NFi* has *N* NFs that communicate directly, so $S_i = \{NF_{i1}, NF_{i2}, NF_{i3}, \cdots, NF_{iN}\}$. The expected value of the number of request messages sent by *NFj* to *NFi* is $\theta_{ij} * N_i(\Delta t)$ within Δt. Then the interaction frequency ratio trust of *NFi* to *NFj* can be expressed as:

$$F_{\Delta t}(i, j) = \frac{1}{e} * \exp\left(-\frac{\left(num_{ij}(\Delta t) - \theta_{ij} * N(\Delta t) \right)^2}{2\sigma^2} \right) \quad i \in M, j \in S_i \tag{1}$$

Another critical dimension for evaluating NF trust is the reliability of NF behavior. In this paper, the interaction success rate [15] is used to measure the reliability of interaction behavior, and the interaction behavior trust of *NFi* to *NFj* is defined as:

$$R_{\Delta t}(i, j) = \frac{s}{s + f} \qquad s+f \neq 0 \tag{2}$$

A successful request and response are regarded as a successful interaction; if the NF does not respond because the received request message is incomplete or unreasonable, it is recorded as an interaction failure, then $num_{ij}(\Delta t) = s + f$.

If within Δt, no message is sent from $NFj \in S_i$ to *NFi*, let the value $R_{\Delta t}(i, j)$ be 0.5. That is, within Δt, if there is no communication between NFs that have a direct interaction relationship,

the trust in each other's interaction behavior will drop to 0.5.

Combining the trust values of the two dimensions of interaction frequency and interaction behavior, the direct trust of *NFi* to *NFj* is defined as:

$$DT_{\Delta t}(i,j) = \alpha R_{\Delta t}(i,j) + (1-\alpha) F_{\Delta t}(i,j) \qquad 0<\alpha<1 \tag{3}$$

Where α and (*1- α*) represent the weight of the interaction behavior trust and the weight of the interaction frequency ratio trust, respectively.

From formula (1) and formula (2), we can know that the value range of $F_{\Delta t}(i,j)$ is $(0,1]$ and the value range of $R_{\Delta t}(i,j)$ is $[0,1]$, so the value range of $DT_{\Delta t}(i,j)$ is $(0,1]$.

4.2.2 Indirect Trust evaluation

Indirect trust is the synthesis of trust values delivered by other communication paths other than the direct communication path [6]. The significance of indirect trust is to provide a trust reference for NFs without direct communication and to enable the initial NF to refer to the trust value of the adjacent NF to the target NF to obtain a more comprehensive trust evaluation result. Let the NF performing the trust evaluation be the initial NF, and the evaluated NF be the target NF.

In an existing large network, there are multiple paths between the initial NF and the target NF, and any NF on the path may be attacked by an attacker. Therefore, the more NFs passed by the path, the higher the possibility of NF being attacked on the path, and the lower the reliability of the trust value transmitted by the path. Therefore, when conducting an indirect trust evaluation between NFs, the path passing through only one intermediate NF is regarded as a reliable path.

Obviously, for the initial NF, the trust value transmitted by the trusted intermediate NF with high interaction frequency is more reliable, so that the path weight can be represented by the interaction frequency between the initial NF and the intermediate NF. Based on all reliable paths between NFs, the initial NF combines the path weight and the trust of the path transmit to calculate the indirect trust value for the target NF.

S_{ij} = {NF_{ij1}, NF_{ij2}, NF_{ij3}, ⋯, NF_{ijN}} represents the NF set that has direct interaction with *NFi* and *NFj*. Then there is only one reliable path connecting *NFi* and *NFj* through any NF in S_{ij}, and there are *M* non-interfering reliable paths for transmitting indirect trust between *NFi* and *NFj*.

Then the trust value passed on the lth path is expressed as：

$$IDT^{l}_{\Delta t}(i,j) = DT(i,l) * DT(l,j) \quad l \in S_{ij} \tag{4}$$

It is known that the trust weight of each path is $\omega_1, \omega_2, \omega_3 \cdots \omega_M$, then the indirect trust of *NFi* to *NFj* is:

$$IDT_{\Delta t}(i,j) = \sum_{b=1}^{M} \frac{\omega_b * IDT^{b}_{\Delta t}(i,j)}{\sum_{a=1}^{M} \omega_a} \tag{5}$$

4.2.3 Time Decay Module

In NF trust value calculation, the evaluation module should not only evaluate the current trust basis, but also refer to the historical trust value, such that Δt exerts no influence on the trust evaluation results. The latest interaction behavior and context information should reflect the current credibility of NF more than the corresponding information in the past [19].

The moments when *NFi* conducts trust evaluation on *NFj* are: $T_1, T_2, \cdots, T_P$, the time intervals are $\Delta t_1, \Delta t_2, \cdots, \Delta t_P$, the direct trust values are $DT_{\Delta t1}(i,j), DT_{\Delta t2}(i,j), \cdots, DT_{\Delta tP}(i,j)$, and the indirect trust values are $IDT_{\Delta t1}(i,j), IDT_{\Delta t2}(i,j), \cdots, IDT_{\Delta tP}(i,j)$.

The time decay factor of the *q*th trust evaluation result is expressed as:

$$\rho_q = \frac{1}{P-q+1} \quad 1 \le q \le P \tag{6}$$

Then the time decay factors from T_P to T_1 time are respectively $1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{P}$.

Combined with time decay, the direct trust of *NFi* to *NFj* normalized [25] is expressed as:

$$DT_{Tp}(i,j) = \frac{\sum_{q=1}^{P} DT_{\Delta tq}(i,j) * \rho_q}{\sum_{a=1}^{P} \rho_a} = \frac{\sum_{q=1}^{P} DT_{\Delta tq}(i,j) * \frac{1}{P-q+1}}{\sum_{a=1}^{P} \frac{1}{P-a+1}} \tag{7}$$

The indirect trust of *NFi* to *NFj* is described as:

$$IDT_{Tp}(i,j) = \frac{\sum_{q=1}^{P} IDT_{\Delta tq}(i,j) * \rho_q}{\sum_{a=1}^{P} \rho_a} = \frac{\sum_{q=1}^{P} IDT_{\Delta tq}(i,j) * \frac{1}{P-q+1}}{\sum_{a=1}^{P} \frac{1}{P-a+1}} \tag{8}$$

4.2.4 Punishment Mechanism

The punishment mechanism is an essential part of identifying malicious NFs. If *NFj* commits malicious behavior to *NFi*, *NFi* will punish *NFj* according to the degree of harm of its behavior. When the initial NF receives an abnormal message from the target NF, if the initial NF determines that the interaction behavior of the target NF is malicious, it will deduct the corresponding trust value of the target NF. When the NRF aggregates the trust value, the initial NF should package its abnormal punishment evidence and send it to the NRF, and the NRF will adjudicate. NRF verifies that the evaluation results from the initial NF are reliable before accepting the results of the initial NF.

Based on the description of the security mechanism and access process of NF service access in 3GPP protocol TS.33501 [26], We analyze the malicious behavior of malicious NF in the following categories: Fraudulent identity, unauthorized access, and illegal access.

Specifically, according to the operational difficulty of malicious behavior, the concealment of behavior, and the degree of maliciousness, the punishment scores for different malicious behaviors are defined, as shown in **Table 2**.

Table 2. Malicious behavior classification and punishment score

Behavior Type	Behavior Target	Malicious Behavior	Punishment Score
Fraudulent identity	NRF	When NF requests a discovery service/access token from the NRF, the IP address does not match the IP address in its certificate or profile.	0.5
		When NF requests an access token from the NRF, the NF type in the request message does not match the corresponding information in its certificate or profile.	0.4
		When NF requests the access token from the NRF, the NF Instance ID in the request message does not match the corresponding information in the certificate or profile.	0.3

	NF Service Producer	When NF accesses the NF Service Producer, its IP address does not match the IP address in the certificate.	0.5
		When NF requests a service from a producer, the NF type in the request message does not match the corresponding information in its certificate or access token.	0.4
		When NF requests a service from a producer, the NF Instance ID in the request message does not match the corresponding information in its certificate or access token.	0.3
Unauthorized access	NRF	NF requests access to services beyond the authorized scope of the NF.	0.2
	NF Service Producer	NF is not authorized to access this producer.	0.4
		NF requests unauthorized service from the producer.	0.3
		The service requested by the NF to the producer exceeds the authorization scope of the access token.	0.3
		The service requested by the NF is beyond its service scope, where the permission verification is relatively loose when authorized by the token.	0.2
Illegal access	NRF	Replay attack or DDoS attack	0.7
		Unregistered NF requests services are other than registration services.	0.5
		Format of NF request message is an error.	0.3
		The NF request message does not carry the necessary parameters.	0.2
	NF Service Producer	Replay attack or DDoS attack.	0.7
		Unregistered NF requests access.	0.5
		The format of the NF request message is an error.	0.3
		The expired access token is carried in the NF request message.	0.3
		The NF request message does not carry the necessary parameters	0.2
	NF Service Consumer	NF refuses to respond to other NF service requests	0.5
		NF responds incorrectly to request message	0.3

The IP address of the NF does not match the certificate, which is a relatively hidden and imperceptible behavior in the NF service request process. The information verified by the NRF before authorization does not include the IP address of the NF [23], and thus defines the highest punishment score for this type of fraudulent identity. If the NF type or Instance ID does not match, the NRF can determine the abnormality when the NRF verifies the NF request message. It is more harmful to use different types of NF identities, so the punishment for NF type mismatch is more severe.

NF requests for services beyond the authorized scope can be regarded as unauthorized access, which could easily be identified in the service request process. Among the unauthorized access behaviors listed in the table, the behavior of NF requesting service from unauthorized access NF is the most malicious, followed by the requested service exceeding the scope of token authorization.

Illegal access includes failure of NF authentication, request messages that do not meet requirements, incorrect responses, and attacks. The maliciousness of the attack is evident, so the punishment score is the highest. Unregistered NFs requesting services other than registration can be directly regarded as malicious NF access, and the punishment score is also higher.

In the existing system, due to the network bandwidth limitation, there will be delay and packet loss when NFs send request messages, resulting in incomplete message content, missing part of the information, and repeated sending of the same request message. That is, standard NF may also behave maliciously in some environments. The format error of the request message and without the necessary parameters can be regarded as the request message does not meet the requirements, considering that the lack of required parameters may be caused by NF processing failure or packet loss. Hence, we set the punishment score of those behaviors small. If an NF occurs with lots of format errors, leading to a low trust value and classified as untrusted, we regard it as an abnormal NF.

The punishment mechanism can be expressed as:

$$P_{T_P}(i,j)=\sum_{l=1}^{k}\eta_l \tag{9}$$

Where k represents the number of malicious behaviors of NF in the historical interaction information and η_l is the punishment score corresponding to the lth malicious behavior. The initial NF can score the malicious behavior of the target NF only when there is a direct interaction between NFs. The more malicious behavior occurs, the higher the cumulative score of the punishment mechanism and the lower the trust value of the NF.

The weight of the punishment mechanism can be determined based on the probability of abnormal behavior of standard NFs. The trust model, after adding the punishment mechanism, can effectively identify malicious NFs and reduce the possibility of misjudging standard NFs as malicious.

4.2.5 Trust Synthesize

By combining the time decay and punishment mechanism, the trust of *NFi* to *NFj* at T_P can be expressed as:

$$T_{T_P}(i,j)=\lambda_1 * DT_{T_P}(i,j)+\lambda_2 * IDT_{T_P}(i,j)-\lambda_3 * P_{T_P}(i,j) \quad 0<\lambda_1,\lambda_2,\lambda_3<1 \tag{10}$$

Where $\lambda_1,\lambda_2,\lambda_3$ respectively represent the weight of direct trust value, indirect trust value, and punishment mechanism when calculating comprehensive trust, and $\lambda_1+\lambda_2=1$.

The weight should take an appropriate value so that the comprehensive trust value can quickly and accurately reflect whether the NF is credible. When there is no direct interaction between *NFi* and *NFj*, take λ_1、$\lambda_3=0$, and the effective trust source of the trust value is the indirect trust value. Due to the existence of the punishment mechanism, the trust value may be negative, and the scope of the comprehensive trust value of *NFi* to *NFj* is $(-\infty,1]$. For the consideration of normalization, when *NFi* evaluates that the trust value of *NFj* is less than 0, let the comprehensive trust value be 0.

The comprehensive trust of *NFi* to *NFj* after normalization is expressed as:

$$CT_{T_P}(i,j)=\begin{cases}T_{T_P}(i,j) & T_{T_P}(i,j)>0\\ 0 & T_{T_P}(i,j)\le 0\end{cases} \tag{11}$$

4.3 Trust Evaluation Center

The trust evaluation center summarizes the evaluation results of each trust evaluation module and verifies whether the evaluation results of the NF are reliable. For the reliable evaluation results of *NFj* by different trusted NFs, the evaluation center only refers to the comprehensive trust values of the NFs in the set S_j for *NFj*. If the malicious NFs access NF1 without direct

interaction in the protocol procedure, the evaluation center adds NF1 to the set of NFs having direct interaction with the malicious NF and obtains the recommended trust for the malicious NFs by combining the evaluation results of the NF1. Based on the trust value of the initial NF, the evaluation center performs a weighted average of the evaluation results of each initial NF to obtain the recommended trust of the evaluation center for the target NF.

The recommended trust of the evaluation center to *NFj* is expressed as:

$$T_{center}^{n}(j)=\sum_{i\in S_j}\frac{T_{center}^{n-1}(i)*CT_{Tn}(i,j)}{\sum_{l\in S_j}T_{center}^{n-1}(l)} \tag{12}$$

$T_{center}^{n}(j)$ represents the recommended trust for *NFj* calculated by the evaluation center for the nth time. Let $T_{center}^{0}(j)=0.8$, that is, the initially recommended trust of *NFj* just launching in 5GC is 0.8.

According to the trust value, NF can be divided into three categories: trusted, suspicious, and untrusted. The specific trust level classification is shown in **Table 3**.

Table 3. Trust level

Trust value	NF trust level
$0.8\le T<1$	Trusted
$0.6\le T<0.8$	Suspicious
$T<0.6$	Untrusted

If the trust value of *NFi* to *NFj* is less than 0.6, *NFj* will be marked as untrusted. If the evaluation center verifies that the evaluation result of *NFi* is reliable, the evaluation center will accept the untrusted judgment of *NFj*. The evaluation center will warn the administrator to request to delist *NFj*, and notify other NFs to reject the message from *NFj*. Before *NFj* goes offline, the evaluation center will no longer refer to its trust evaluation results for other NFs. If the evaluation result is unreliable, the evaluation center marks the *NFi* for evaluation as suspicious and records its trust value as 0.6.

5. Experiment Analysis

In this section, we construct a simple core network architecture based on NF interaction. Then we test the influence of parameters such as the interactive behavior trust weight, the direct trust weight, and the punishment mechanism weight in the trust model on the trust evaluation results and use this architecture to evaluate the effectiveness of the trust model.

5.1 Experimental Setup

Based on the schematic diagram of the NF topology in **Fig. 2** and the NF interaction in **Fig. 3**, we define instance functions for AMF, SMF, UDM, AUSF, UPF, PCF, and NRF, respectively, in the experiment and implement service function access between NFs. When the NF receives the request message, it verifies the identity and access rights of the NF service consumer according to the specific content of the request message. If the verification succeeds, the NF matches the service function required by the consumer. If the verification fails, the NF matches its malicious behavior type based on the wrong request.

According to the procedures defined by 3GPP, the request message of UE is forwarded by the gNB to 5GC [34]. When AMF receives the UE request message delivered by gNB, it

initiates the corresponding procedure and accesses different NF services according to the specific content of the UE request. The trust model proposed in this paper is to quantify the trust value of NF by evaluating the interaction behavior of NF. Therefore, the role of the UE triggering service procedure is ignored in the experiment, and AMF is used as the starting point of the service procedure. Meanwhile, in the NF list, a registered malicious NF is defined such that the identity of this malicious NF is SMF, and named SMF2, then the malicious NF has access to all NFs in the topology graph except AUSF matching its identity.

During a trust evaluation cycle, AMF randomly triggers one of the service procedures multiple times and accesses the NF services corresponding to the procedure. At the same time, the malicious NF is made to call the services of other NFs randomly. At the end of the trust evaluation period, each NF evaluates the trust values of other NFs. The NRF summarizes the evaluation results of the NFs and calculates the recommended trust of the NFs.

Algorithm1: Trust Evaluation Algorithm Process

Input: Service access relationship between NFs.
Output: Recommended trust value of NFs.
Initialization:

1) Generate a simulated core network, and define the service functions of each NF and malicious NF.

2) Initialize the interaction frequency θ_{ij} of any *NFj* to *NFi*, the trust transfer path and path weight ω of NFi, the weights $\lambda_1, \lambda_2, \lambda_3$ of the trust evaluation sub-module, and the punishment mechanism.

for evaluation time from 1 to *M*:

Step1: AMF triggers service procedures for *N* times.

Step2: NF counts the number of successful interactions *s* and the number of failed interactions *f* with other NFs.

Step3: Evaluation module computes trust in other NFs

Step4: Calculate the direct trust $DT(i,j)$ by formula (3).

Step5: Calculate the indirect trust $IDT(i,j)$ by formula (5).

Step6: Calculate the punishment score $P(i,j)$by formula (9).

Step7: Combined with the time decay factor ρ, calculate the comprehensive trust $\mathrm{CT}(i,j)$by formula (10)

Step8: NRF summarizes the trust evaluation results of each NF, and calculate the recommended trust $T_{center}^{n}(i)$ by formula (13).

End

The algorithm will output the recommended trust $T_{center}^{n}(i)$ for *NFi* obtained by *M* times of trust evaluation.

The experimental environment configuration is Intel Core i7-6700 3.4GHz CPU, 16G memory, python version 3.6. The simulation parameters in the experiment are set as shown in **Table 4**.

Table 4. Simulation parameters

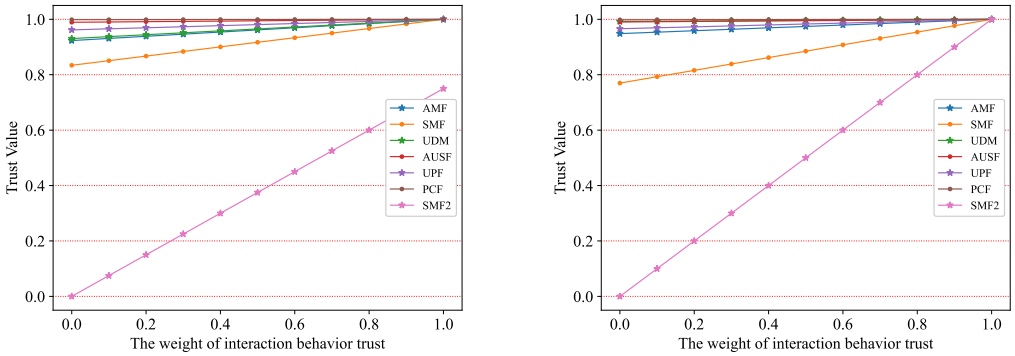
Description	Value
The number of times AMF executes service procedures	56
The number of trust evaluation *P*	10
The initial recommended trust value T_{center}^{0}	0.8
The weight of interactive behavior trust α	$(0,1)$
The weight of interaction frequency ratio trust *1-*α	$(0,1)$
The weight of direct trust λ_1	$(0,1)$
The weight of punishment mechanism λ_3	$[0,1]$

5.2 Experimental Results and Analysis

In the experiment, to evaluate the effect of the model more accurately, we assume that the interactions of standard NF are always successful, and the interaction of malicious NF according to its identity can also be completed.

5.2.1 Direct Trust Module

It can be seen from formula(3) that an important parameter affecting the direct trust value of NF is the weight of interactive behavior trust α. When the number of SMF2 accesses to other NFs is 200, the trust curves of standard NFs are significantly different. Evaluate the trust evidence sampled simultaneously, set α from 0 to 1, and each step is 0.1, and obtain a set of NF trust values corresponding to different α values. **Fig. 5(a)** and **5(b)** are the trust curves in different α values of SMF2 random access NFs with and without AUSF, respectively.



(a)SMF2 random access with AUSF (b)SMF2 doesn't access AUSF

Fig. 5. NF trust curve in different value of α

It is known that SMF2 accesses other NFs many times. The total number of service accesses in a cycle counted by *NFi* is $N_i(\Delta t) = N_i^f(\Delta t) + N_i^b(\Delta t)$, where $N_i^f(\Delta t)$ represents the number of accesses of standard NFs and $N_i^b(\Delta t)$ represents the number of accesses of malicious NFs. Obviously, due to the access of SMF2, the total number of accesses calculated by *NFi* is high, and the ratio of actual interaction frequency of standard NF calculated is lower than the ideal value. When there is no malicious NF interference, the expected value of the number of accesses by *NFi* to *NFj* is $\theta_{ij} * N_i^f(\Delta t)$. Due to the existence of malicious NF, the exact calculated expected value is $\theta_{ij} * N_i(\Delta t)$. The deviation between the expected value of the ideal number of accesses of *NFj* and the expected value of the actual number of accesses of *NFj* is $\theta_{ij} * [N_i^f(\Delta t) - N_i(\Delta t)]$, which is equal to $-\theta_{ij} * N_i^b(\Delta t)$. In the experiment, the total number of malicious NFs accessing other NFs is fixed, so $N_i^b(\Delta t)$ is stable at a specific constant. In the actual simulation, the total number of NF interactions is limited by the number of service executions, and there is a specific deviation between the exact number of NF accesses and the theoretical number of accesses. Therefore, combined with formula (1), we can infer that the interaction frequency ratio trust value of *NFi* to *NFj* fluctuates around a fixed value. When the service requested by the NF is within the authorized scope, the value of the interaction behavior trust is always 1. So the trust curve of NF grows approximately linearly.

Let the task failure rate of *NFi* be $FR(i) = \frac{f_i}{total_i}$, where f_i represents the number of failed access requests by *NFi*, and $total_i$ represents the total number of access requests initiated by *NFi* to other NFs. By increasing the number of malicious NFs, the task failure rate of NFs is shown in **Fig. 6**.

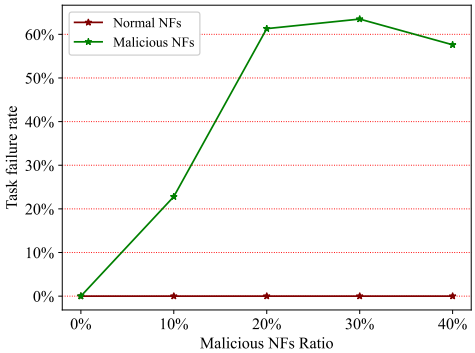


Fig. 6. The task failure rate in different malicious NF ratio

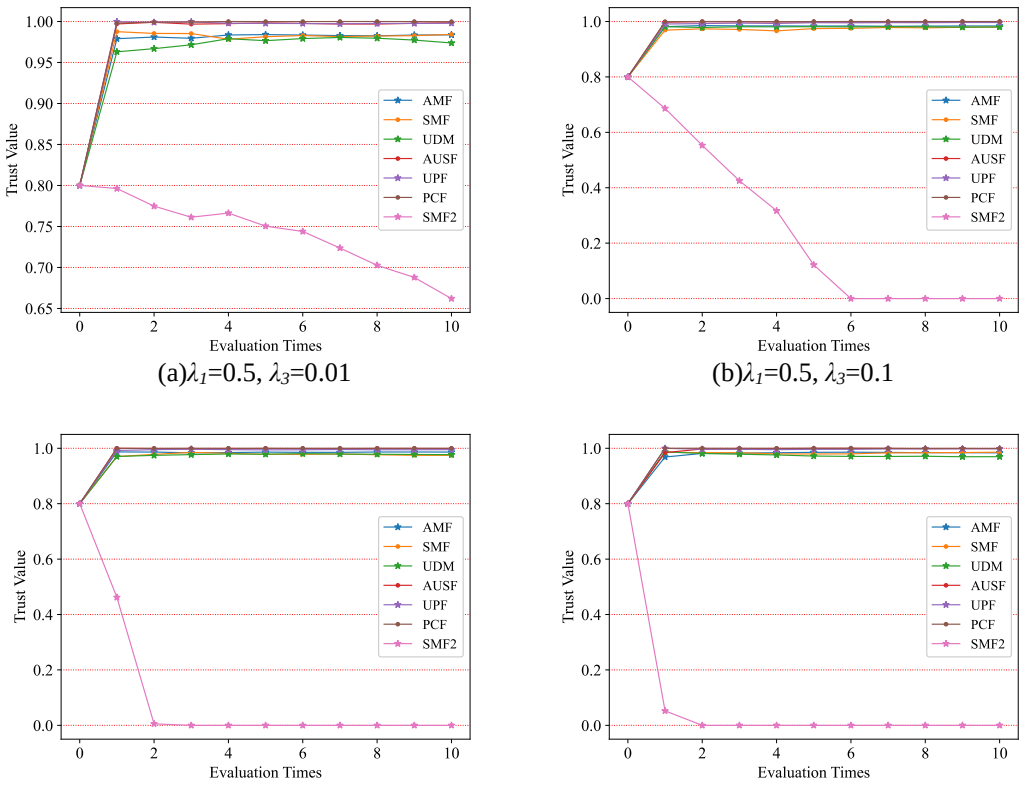
The task failure rate of standard NF is always 0. That is, the interaction behavior trust value of standard NF is always 1. However, due to the different malicious behaviors of malicious NFs, the task failure rate varies significantly with the malicious NFs ratio. Still, the average failure rate remains at a high level.

It can be seen from **Fig. 5** that when the malicious behavior of NF changes, the effective discrimination range of the evaluation mechanism for malicious NF rapidly reduces, and the appropriate value range of α is highly correlated with the specific malicious behavior of NF, which is realized only by direct trust. The robustness of the trust evaluation mechanism is not enough to deal with the complex and diverse attack methods that malicious NF may carry out. In the following experiments, indirect trust, time decay, and punishment mechanism are implemented, and the trust model is further improved to enhance its effectiveness and robustness.

5.2.2 Comprehensive Trust Evaluation

This section introduces the indirect trust and the punishment mechanism into the trust model and observes the impact of the punishment mechanism on the trust model's ability to identify malicious NFs.

We adjust the frequency of SMF2 initiating NF accesses and let SMF2 randomly access 50 times other NFs within a trust evaluation period. Let the weight of direct trust λ_1=0.5, the weight of the punishment mechanism λ_3 take 0.01, 0.1, 0.3, and 0.5, respectively, and we get the trust curves of NF as shown in **Fig. 7**.



(a)λ_1=0.5, λ_3=0.01 (b)λ_1=0.5, λ_3=0.1

(c)λ_1=0.5, λ_3=0.3 (d)λ_1=0.5, λ_3=0.5

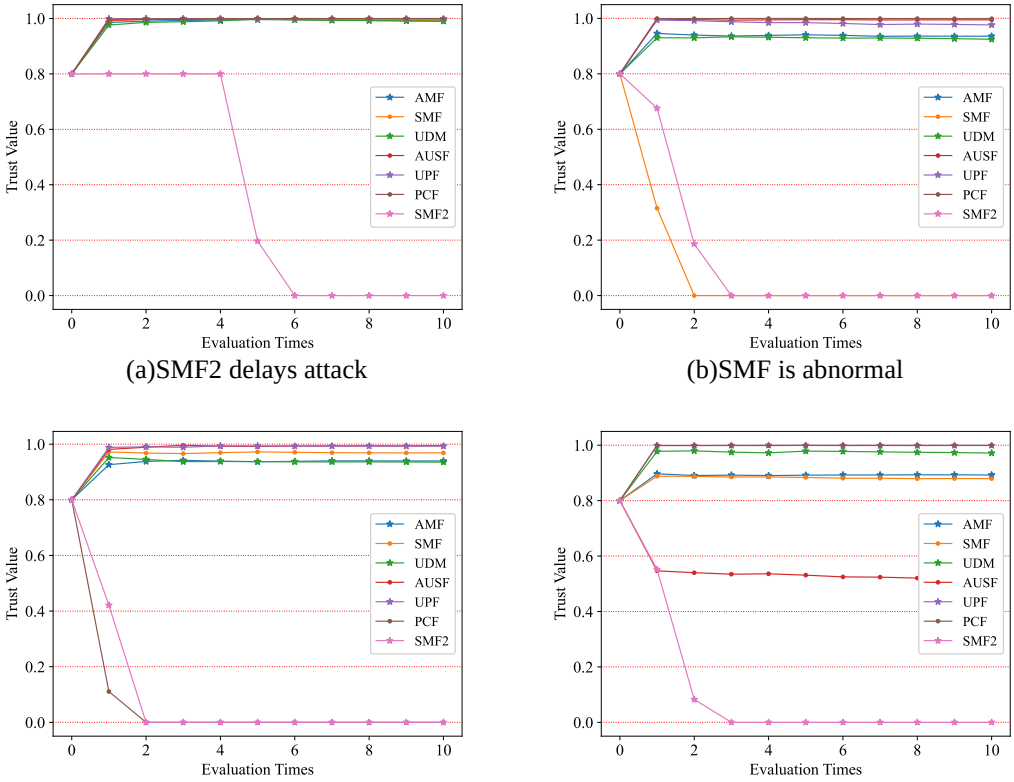
Fig. 7. NF trust curves in different punishment mechanism weights

Obviously, the larger the value of the punishment mechanism weight, the stronger the trust model's ability to distinguish malicious behavior. It is known that standard NF may behave maliciously, and the trust model should have certain fault tolerance for standard NF behavior. When applying the trust model in the actual 5GC, appropriate punishment mechanism parameters should be selected according to the frequency of malicious behavior of standard NFs, to quickly identify malicious NFs and reduce the possibility of misjudging standard NFs as malicious.

5.2.3 Effectiveness of the Trust Model

In this section, we further verify the effectiveness of the trust evaluation mechanism proposed in this paper.

We test the trust model's ability to identify hijacked standard NFs. Let α=0.3, λ_1=0.5, λ_3=0.3, and the number of malicious accesses of SMF2 in each trust evaluation cycle is 50. If the SMF is hijacked, it will randomly access the services of PCF, UDM, AUSF, and UPF after responding to the access request. When the PCF is hijacked, it will randomly access the services of SMF, UDM, AUSF, and UPF after the response. When the AUSF is hijacked, it only invokes the services of UDM after the response. We test the NF trust curves when SMF2 starts malicious behavior in the fifth evaluation period, SMF is hijacked, PCF is hijacked, and AUSF is hijacked. Then a set of NF trust curves is obtained, as shown in **Fig. 8**.



(a)SMF2 delays attack (b)SMF is abnormal

(c)PCF is abnormal (d)AUSF is abnormal

Fig. 8. NF trust curve graph with different ab abnormal NFs

It can be seen from **Fig. 8** that the trust value decays rapidly when the abnormal NF starts malicious behavior, and the trust level of abnormal NF at the next evaluation time is untrusted. When the SMF or PCF is abnormal, it randomly accesses other NF services, including unauthorized services. The punishment mechanism can identify the abnormal behavior of the SMF or PCF, so that the corresponding trust value will decay rapidly. The AUSF only calls authorized services, but the calling frequency is abnormal. Because the access request of the AUSF is legitimate, when its request is not identified as a replay attack or DoS attack, the punishment mechanism cannot determine its abnormality. At this time, the interaction frequency ratio trust in the trust model plays a vital role in distinguishing abnormalities of the AUSF. Combining different NF trust curves in **Fig. 8**, it can be seen that the trust model can identify not only malicious NFs that trigger the punishment mechanism, but also malicious NFs with abnormal access frequency.

In the experiment, since the request message does not carry the UE information, the NF does not distinguish whether the consecutively received request messages are the same. If the trust evaluation module is deployed in the actual 5GC to implement punishment for various malicious behaviors, the ability of the trust model to identify malicious NFs with abnormal access frequency will be further improved.

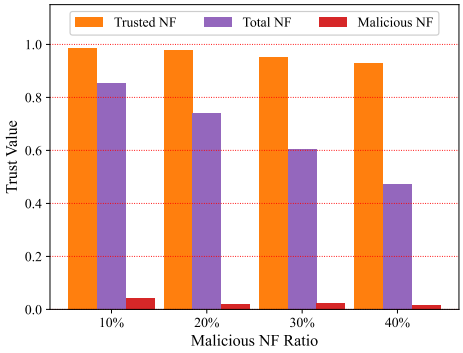


Fig. 9. NF trust values under different malicious NF ratios

Fig. 9 shows the change in the mean trust value of trusted NFs, all NFs, and the malicious NFs, respectively, as the ratio of malicious NFs increases from 10% to 40%. As the malicious NFs ratio increases, the trust means of trusted NFs decreases slightly, but always maintains a high trust score; the mean trust of malicious NFs is close to 0. The increased ratio of malicious NFs has little effect on the trust value of trusted NFs or malicious NFs.

In summary, the trust model proposed in this paper can quickly identify malicious NFs with illegal access and efficiently identify the NFs with abnormal interaction behavior after being hijacked in 5GC. It has good reliability and robustness.

6. Conclusion

To address the potential security threats in 5GC, this paper proposes a quantifiable trust model to identify the malicious NF. According to the characteristics of 5GC and the service access relationship between NFs, a trust evaluation module is deployed on each NF. The interaction frequency ratio trust and the interaction behavior trust are introduced to achieve the quantification of NF trust. The malicious behaviors in NF interactions are classified, and the corresponding punishment scores are defined. Trust transmit is introduced so that NFs could comprehensively refer to the trust values of NFs with a direct interaction relationship to the target NF when evaluating the trust of the target NF. The NRF aggregates and adjudicates the trust evaluation results and low-scoring evidence of each NF, then calculates the recommended trust of the trust evaluation center for NFs. This scheme not only overcomes the problem that the reliability of the evaluation results of the distributed trust module is difficult to verify, but also greatly reduces the resources required by the evaluation center to collect information. Simulation experiments show that the trust model proposed in this paper can effectively identify malicious NFs with abnormal behaviors from many NFs in 5GC. In the next step, we will further study how to refine the authorization granularity and strengthen the management of NF access rights.

Acknowledgment

The authors sincerely thank the anonymous reviewers for their valuable comments that helped improve the readability and clarity of this paper. This work was supported by the National Key R&D Program of China (Grant No. 2020YFB1806607).

References

[1] CCSA, "Research on Zero Trust Security Applied in Mobile Network," Mar. 12, 2021.

[2] A. Nasser, D. Keshav, "Multi-Dimensional E-commerce Trust Evaluation Method," in *Proc. of SKIMA*, 2018. Article (CrossRef Link)

[3] G. A. Kumar, K Rakesh, "A Robust Trust Model for Wireless Sensor Networks," in *Proc. of UPCON*, 2018. Article (CrossRef Link)

[4] D. S. Sundeep, N. Manisha J, "Multihop Trust Evaluation using Memory integrity in Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4092-4100, Dec. 2021. Article (CrossRef Link)

[5] Z. Miao, "Trust computation model based on improved Bayesian for wireless sensor networks," in Proc. of ICCT, 2017. Article (CrossRef Link)

[6] R. M. Khalid, Y. Fan, A. Imran, "A multidimensional trust inference model for the mobile Ad-Hoc networks," in *Proc. of WOCC*, 2019. Article (CrossRef Link)

[7] G. Theodorakopoulos, J. S Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 318-328, Feb. 2006. Article (CrossRef Link)

[8] F. Farhan, K. Fatih, A. Asma, "MARINE: Man-in-the-middle Attack Resistant trust model IN connEcted vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310-3322, Apr. 2020. Article (CrossRef Link)

[9] Z. Lu, W. Liu, Q. Wang, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655-45664, Apr. 2018. Article (CrossRef Link)

[10] Z Liu, J Ma, J Weng, "LPPTE: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications," *Information Fusion*, vol. 73, pp. 144-156, Mar. 2021. Article (CrossRef Link)

[11] Z Liu, J Weng, J Ma, "TCEMD: A trust cascading-based emergency message dissemination model in VANETs," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4028-4048, May. 2020. Article (CrossRef Link)

[12] Z Liu, F Huang, J Weng, "BTMPP: balancing trust management and privacy preservation for emergency message dissemination in vehicular networks," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5386-5407, Apr. 2021. Article (CrossRef Link)

[13] W. Mo, T. Wang, S. Zhang, "An active and verifiable trust evaluation approach for edge computing," *J Cloud Comp*, vol. 9, no. 2, pp. 51, Dec. 2020. Article (CrossRef Link)

[14] X. H. Deng, P. Y. Guan, "Integrated Trust Based Resource Cooperation in Edge Computing," *Journal of Computer Research and Development*, vol. 55, no. 3, pp. 449-477, Feb. 2019. Article (CrossRef Link)

[15] T. Wang, H. Luo, X. Zheng, "Crowdsourcing mechanism for trust evaluation in CPCS based on intelligent mobile edge computing," *ACM TIST*, vol. 10, no. 6, pp. 1-19, Nov. 2019. Article (CrossRef Link)

[16] C. Matin, J. N. Nima., "Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms," *Journal of Electrical Systems and Information Technology*, vol. 5, no. 3, pp. 608-622, Dec. 2018. Article (CrossRef Link)

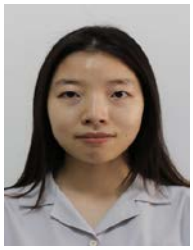
[17] Z. Yu, "Research on Cloud Computing Security Evaluation Model Based on Trust Management," in *Proc. of IEEE ICCC*, 2018. Article (CrossRef Link)

[18] S. Huang, A. Liu, S. Zhang, "BD-VTE: A novel baseline data based verifiable trust evaluation scheme for smart network systems," *IEEE transactions on network science and engineering*, vol. 8, no. 3, pp. 2087-2105, Jul. 2021. Article (CrossRef Link)

[19] L. Zhang, X. Y. Wei, "Trust evaluation algorithm of IoT edge server based on cooperation reputation and device feedback," *Journal on Communications*, vol. 43, no. 1, pp. 118-130, Feb. 2022. Article (CrossRef Link)

[20] B. Niu, W. You, H. Tang, "5G network slice security trust degree calculation model," in *Proc. of IEEE ICCC*, 2017. Article (CrossRef Link)

[21] T. Li, A. Q. Hu, “Mobile trusted hierarchical model and its applications,” in *Proc. of IEEE CSC*, 2014. Article (CrossRef Link)
[22] Z. Kang, P. Li, “A Machine Learning Based Trust Evaluation Framework for Online Social Networks,” in *Proc. of IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, 2014. Article (CrossRef Link)
[23] J. W. Wang, X. Y. Jing, Z. Yan, “A survey on trust evaluation based on machine learning,” *ACM Computing Surveys*, vol. 53, no. 5, pp. 1-36, Sep. 2021. Article (CrossRef Link)
[24] W. J. Jiang, G. J. Wang, M. Z. A. Bhuiyan, “Understanding graph-based trust evaluation in online social networks: Methodologies and challenges,” *ACM Computing Surveys*, vol. 49, no. 1, pp. 1-35, Mar. 2017. Article (CrossRef Link)
[25] W. Z. Yang, C. Huang, W. Bo, “A General Trust Model Based on Trust Algebra,” in *Proc. of International Conference on Multimedia Information Networking & Security*, 2009. Article (CrossRef Link)
[26] Security Architecture and Procedures for 5G System, 3GPP Standard TS33.501, 2021.
[27] Study on security aspects of the 5G Service Based Architecture (SBA), 3GPP Reference TR33.855, 2020.
[28] C. X. Liu, X. X. Hu, “Security Analysis of 5G Network EAP-AKA ‘Protocol Based on Lowe’s Taxonomy,” *Journal of Electronics & Information Technology*, vol. 41, no. 8, Aug. 2019. Article (CrossRef Link)
[29] R. P. Jover and V. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications," *IEEE Access*, vol. 7, pp. 24956-24963, Feb. 2019, Article (CrossRef Link)
[30] G. Holtrup, W. Lacube, D. P. David, “5G System Security Analysis,” *arXiv preprint arXiv:2108.08700*, Aug. 2021. Article (CrossRef Link)
[31] J. H. Liu, “Research on Security Improvement of 5G Core Network Based on Zero Trust Architecture,” *Designing Techniques of Posts and Telecommunications*, no. 9, pp. 75-78, 2020.
[32] J. Lu, L. Xiao, Z. Tian, “5G Enhanced Service-based Core Design,” in *Proc. of WOCC*, 2019. Article (CrossRef Link)
[33] H. Wang, “5G Core network service-based architecture evolution,” *Application of Electronic Technique*, vol. 46, no. 11, pp. 48-51, 2020. Article (CrossRef Link)
[34] Procedures for the 5G System (5GS), 3GPP Standard TS23.502, 2021.



Ying Zhu received the B.E. degree from Shanghai Jiao Tong University in 2020. She is currently working towards the M.E. degree in Information Engineering University. Her research interest includes mobile communication network security, 5G core network security analysis, and access control.

Caixia Liu received the M.S. and Ph.D degrees from Information Engineering University, China. She is a researcher at Academy of Military Sciences. Her main research interests include new network technologies, network security, and information security.

Yiming Zhang received the B.E. from Beijing Institute of Technology in 2019, and received the M.E. degree from Information Engineering University in 2022. His current main research interests include network security, abnormal traffic detection.

Wei You received the M.S. and Ph.D degrees in cryptology from Information Engineering University, China. He is currently an associate professor of Information Engineering University. His major research interests include New-generation mobile communication systems, and mobile communication network security.