IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 April 2023, accepted 23 May 2023, date of publication 31 May 2023, date of current version 7 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3281560

METHODS

RAIN: Risk Assessment Framework Based on an Interdependent-Input Propagation Network for a 5G Network

CHE-TSUNG KUO[1], HONG-YEN CHEN[2], AND TSUNG-NAN LIN[3,4], (Senior Member, IEEE)

[1]Master Program in Cybersecurity, Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan
[2]Doctoral Program in Cybersecurity, Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan
[3]Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan
[4]Graduate Institute of Communication Engineering, National Taiwan University, Taipei 10617, Taiwan

Corresponding author: Tsung-Nan Lin (tsungnan@ntu.edu.tw)

This work was supported in part by the Ministry of Science and Technology, Taiwan, under Grant MOST 111-2221-E-002-157-MY2 and Grant NSTC 111-2218-E-002-017-MBK; and in part by the "DDoS Attack Detection under GTP (GPRS Tunneling Protocol) Protocol" of the Chunghwa Telecom, Taiwan.

ABSTRACT It is essential for mobile network operators to provide effective protective measures for assets in 5G networks to mitigate various threats, and risk assessment plays an important role in decision-making for protective measures. Organizations refer to risk assessment to determine the priority for protective measures, and multiple studies have proposed assessments that take various aspects and methodologies into consideration. Nevertheless, these efforts are not sufficiently useful in a practical sense. Existing studies lack numerical results to make cost-efficient decisions and cannot be automatically updated when the security policy is altered. Finally, a unified assessment framework is necessary. Hence, we propose a quantitative risk assessment framework, RAIN, to solve these problems for the 5G network. A customized weighted network combined with an interdependent-input weighting method enables the framework to provide holistic and quantitative assessment results and can be used for any scenario in a 5G network. With the assessment results, organizations can prioritize the implementation of protective measures for the target assets. In addition, the framework is flexible for policy changes and suitable for different systems in 5G networks. We implement our framework on a 5G stand alone core network system with different scenarios.

INDEX TERMS 5G security, 5G SA, risk assessment.

I. INTRODUCTION

Five generation standalone (5G SA) systems, which include enhanced mobile broadband (eMBB), ultra-reliable low latency communications (uRLLC), and massive machine type communications (mMTC), three types of traffic classes, provide Gbps order data rates, low latency, increase in base station capacity, and considerable improvement in users' quality of service (QoS) [1]. However, telecommunication standardization organizations, such as the 3rd generation partnership (3GPP) or European Telecommunications Standards Institute (ETSI) are working on integrating networking techniques into telecommunication networks. Examples include using multiaccess edge computing (MEC) to provide localized real-time service [2], [3] using software defined networking (SDN) to customize network routing [4], network slicing (NS) to perform custom QOS for each customer [5], and network function virtualization (NFV) and cloud computing techniques to establish flexible and programmable core services for mobile network operators (MNO).

As 5G combines internet technologies (IT) and communication technologies (CT), there are more potential risks, including communication protocol vulnerability [6], [7] and SDN vulnerabilities [8]. 5G brings such unique and diverse security challenges; hence, it is necessary to

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

provide protective measures against these threats. To provide protective measures for the 5G network, risk assessment plays an important role. Risk assessment helps organizations identify, analyze, and evaluate weaknesses in their processes and systems. By performing a risk assessment, organizations can prioritize their efforts to address the most critical risk and mitigate the risks they pose to the organization's assets. Currently, several works have made risk assessments for different systems in 5G networks, such as MEC and the core network. We classified them into three types: qualitative risk assessment [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], attack graph risk assessment [22], [23], and quantitative risk assessment [24], [25].

All of the related works addressed security issues related to 5G technology or the components in the 5G network, such as network functions and MEC servers. Some also list the threat issue's risk level (e.g., critical, high, moderate, and low). However, these works are not effective for practical use. The problems are as follows:

- **Without cost-effectiveness:** In practice, a risk assessment must be used to make decisions for protective measures, and commonly, protection resources, such as cost, are limited. That is, the most powerful protective measure can only be used for some assets. Therefore, managers need to make cost-effective decisions when they have to implement protective measures, and the more fine-grained assessment results would ease managers in classifying different protection levels for various assets, which means that the numerical result is more detailed than the level-based result. However, none of the related works provide numerical results.
- **Without flexibility:** The manager's security policy or tendencies may change (e.g., to cooperate with government policies); hence, risk assessment results should also be changed in time. Nevertheless, these works cannot directly affect the assessment results when the security policy or tendency changes; they require experts to reassess the risk level of each asset based on new policies.
- **Without a unified framework:** The current works addressed the risk from different aspects of the 5G system and made risk assessments. However, the methodology for each study cannot be used for the various subsystems or different aspects. In other words, there needs to be a unified assessment framework.

Therefore, we propose a risk assessment framework, RAIN, illustrated in Figure 1, which takes assets, protective measures, and security policy as input factors. With these factors, experts create a self-defined weighted network used to holistically assess asset risks while considering security policy, which we call the security propagation network. Through the security propagation network, the assessment report is generated and contains a numeric risk score for each asset, and the manager knows the priority of implementing protective measures. In addition, by adjusting the self-defined parameters in the framework, it is flexible for generating

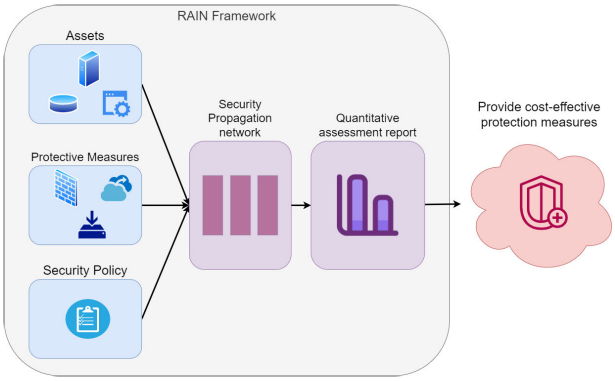

FIGURE 1. RAIN framework application view. Using assets, protective measures, and security policy as input, we generate quantitative assessment results via a customized security propagation network, thereby offering cost-effective protective measures.

different results for various scenarios. This work utilizes the 5G model as a prototype to perform risk evaluation and deliver effective correction results. Table 1 shows the main contributions of both the related works and our frameworks, and map them to different assessment types.

We also conducted experiments comparing traditional qualitative analysis with the RAIN framework. Considering different protective measures and security policies, we evaluate each common network function in three scenarios in the 5G core network environment. In scenario 2 (Table 7), we noticed that traditional qualitative assessment mistakenly identified the NEF having the risk level ''critical'', which is same as the AMF when focusing on confidentiality. This is because it uses a fixed risk-level scale as its evaluation criterion, making it hard to generate accurate assessments under all conditions. By contrast, RAIN can adjust the corresponding parameters according to different scenarios, resulting in more sensible assessment. Moreover, in scenario 1 (Table 6), the traditional assessment solely relying on level-based results leads to several network functions having the same risk level, which cannot provide resource allocation judgments when resources are limited. Nevertheless, RAIN produces numerical results to aid decisions. The following are the framework's contributions:

- Given limited resources, managers must make the most effective choices to lessen security risks within the organization. However, earlier studies [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21] utilized qualitative techniques for risk assessment, which could not furnish precise anticipation of risk correction outcomes. For instance, Ranaweera et al. [16] provided detailed threat descriptions for each asset and interface in the MEC system; however, the literature cannot determine which asset or interface should put more emphasis on protection, and executives can not assess the protective effect from the literature when they have new protection strategy to MEC system, they must actually apply reinforcement measures to attain results.

Mohan et al. [20] listed potential cyber threat vectors for 5G networks and provided corresponding countermeasures such as mitigation or prevention solutions; however, the literature cannot evaluate the effect of the mitigation measures on the threat vectors, executives need to implement the mitigation practically to measure countermeasure effect. On the other side, The proposed framework is capable of offering risk correction results in advance through quantitative evaluation with the interdependent-input weighting method; that is to say, executives could adjust the parameter functions inside the framework to attain the results without really applying reinforcement measure, thus enabling executives to intuitively obtain investment advantages and reduce the chance of investment misuse.

- An organization's information security policy is often altered by external influences. In previous work, managers needed to go through reevaluations, which was a burden on business operations. However, the proposed work structure offers parameter functions, so managers can adapt to policy requirements and lighten the load on the organization by modifying the parameters. Later, in this work, the efficacy of this feature is substantiated in the 5G domain.
- There are different fields or systems in the organization that need to conduct risk assessment. In the previous work, an integrated assessment framework could not be provided. When managers want to conduct analysis and assessment, they must put in effort to redefine the assessment method. However, using our framework, experts can analyze any system they want without defining new methods, reducing the burden on managers to design new evaluation methods.

The remainder of this paper is organized as follows. Section II provides the fundamentals of the service-based architecture for the 5G SA core network, common network functions, and MEC system. We describe collecting the recent works related to 5G risk assessment and classifying them into three types in Section III. Section IV provides our framework, and we implement it in the 5G SA core system in Section V. We present the framework's flexibility by changing the security policy and protective measure in Section VI, and provide comparison experiments between the RAIN framework and the traditional assessment in Section VII. Finally, the paper is concluded in Section VIII.

II. BACKGROUND

It is necessary to have domain knowledge of the 5G SA core network and MEC to provide quantitative assessments for the 5G network. Therefore, in the following, we introduce the 5G core network SBA architecture and the MEC architecture.

A. 5G SA CORE SERVICE-BASED ARCHITECTURE

The core network is mainly responsible for authentication management, mobility management, roaming, accounting, etc. The 5G SA core network architecture adopts a service-based architecture (SBA), as shown in Figure 2. This architecture differs from the core network architecture in the previous generation, which integrates many functionalities into one instance. Each network node is split based on the network function (NF), which is beneficial to achieve network load balancing, flexibility and upgradability. Each network function represents different services. In the following, we introduce common network functions in the core network according to the definition from 3GPP TS 23.501 [26]:

1) ACCESS AND MOBILITY MANAGEMENT FUNCTION (AMF)

AMF is mainly responsible for registration management, connection management, reachability management, mobility management, charging, security and access management, and authorization functions. According to 3GPP TR 33.926 [27], application programs exist that execute AMF software, related software packages, and programs related to the orchestration and administration management (OAM) process. Therefore, the key assets to be protected include AMF applications, mobility management materials, AMF service-based interface (SBI), Console interface, OAM interface, and AMF Software.

2) USER PLANE FUNCTION (UPF)

A UPF is mainly responsible for data plane packet transmission, upstream and downstream packet routing, filtering, forwarding, and QoS flow processing. There are two types of UPFs. One is a PSA-UPF (PDU Session Anchor-UPF), and the other is an intermediated UPF. PSA-UPF records the UE session and is connected to the DN. The intermediate UPF multihome to more than one PDU session anchor (PSA) is responsible for forwarding the PDU to the specific PSA-UPF. According to 3GPP TR 33.926 [27], the key assets to be protected include application programs, user plane data, session-related data (e.g., CN Tunnel information, packet detection rules, network usage, traffic detection information, etc.), and cryptographic materials for the N3, N4, and N9 interfaces.

3) SESSION MANAGEMENT FUNCTION (SMF)

SMF is responsible for session management, such as establishing, modifying, or releasing sessions, UE IP allocation management (requires DHCP service), control and selection of UPF (such as control UPF proxy ARP response), charging functionality, etc. According to 3GPP TR 33.926 [27], the critical assets in SMF are the application program, session-related data (e.g., subscriber identities, network usage, charging data records, etc.), and user plane data.

4) UNIFIED DATA MANAGEMENT (UDM)

UDM manages network user data and verifies authentication-related information to ensure the legitimacy of users. UDM stores the certificates of the 5G AKA registration authentication mechanism (restores SUCI, GUTI to SUPI and

TABLE 1. The contribution summary and assessment types for related works in the 5G SA/MEC system.

Ref	Main Contribution	Relevance to 5G/MEC security	Assessment method
[24]	Generating attack graph with a Quantitative vulnerability analysis approach using the TOPSIS multidecision-making method.	Relevance to 5G security and MEC security	Quantitative, Attack graph
[9]	From the security and privacy perspective, present the core techniques related to 5g, such as SDN, NFV, MEC, NS; and PHY layer; and discuss activities in standardization bodies.	Relevance to 5G security and MEC security	Qualitative
[10]	From a holistic perspective, provide a detailed analysis of the security of edge paradigms.	Relevance to MEC security	Qualitative
[11]	Study the security of 5G in comparison with traditional cellular networks, and propose a 5G wireless security architecture.	Relevance to 5G security	Qualitative
[12]	Address the challenge and solution for mobile cloud, SDN, NFV, and privacy in 5G.	Relevance to 5G security	Qualitative
[13]	The security features, requirements, vulnerabilities, and corresponding solutions are described in detail according to the five security aspects in the 3GPP 5G security architecture.	Relevance to 5G security	Qualitative
[14]	Provide an overview of 5G security technology, vulnerabilities, solutions, and challenges according to OSI model layers.	Relevance to 5G security	Qualitative
[15]	Introduce the security challenges and solutions or future directions of 5G technologies (MIMO, SDN, NFV, Cloud), and also discuss the changes in privacy and security from 1G to 4G.	Relevance to 5G security	Qualitative
[22]	Proposed modular security metrics based on an attack graph to aggregate different parties such as RAN, Core network, and MEC provider's local security metrics.	Relevance to 5G security and MEC security	Attack graph
[16]	Focus on MEC risk assessment, which investigated the MEC architecture, and functional layers; and discussed the open issues such as traffic isolation, cloudnative security, and trust management.	Relevance to 5G security and MEC security	Qualitative
[17]	Proposed a methodology based on the EN-ISO/IEC 27005 standard to develop 5G security regulations based on different risk scenarios.	Relevance to 5G security and MEC security	Qualitative
[18]	Provide a survey of MEC data security domains and an overview of the related works in each domain.	Relevance to MEC security	Qualitative
[19]	5G security vulnerabilities in different use case scenarios (e.g. mMTC, eMBB, V2V, XR, UAV) according to MEC.	Relevance to MEC security	Qualitative
[23]	Utilize the machine learning and a constraint satisfaction problem (CSP) formulation for the attack graph analysis which contain various attack vectors of 5G protocols, SDN, and NFV.	Relevance to 5G security	Attack graph
[25]	Perform vulnerability assessment for SDN mobile network base on attack graph using AHP and TOPSIS approach.	Relevance to 5G security	Quantitative, Attack graph
[20]	Categorized the cyber attack related to 5G into physical, local, and remote three types.	Relevance to 5G security	Qualitative
[21]	Propose security threats and provide corresponding mitigation measures for SDN, NFV, and NS technologies.	Relevance to 5G security	Qualitative
Our Study	Provide a quantitative risk assessment framework for 5G network, capable of offering risk correction results with the interdependent-input weighting method and compatible with different scenarios in 5G.	Relevance to 5G security and MEC security	Qualitative, Quantitative

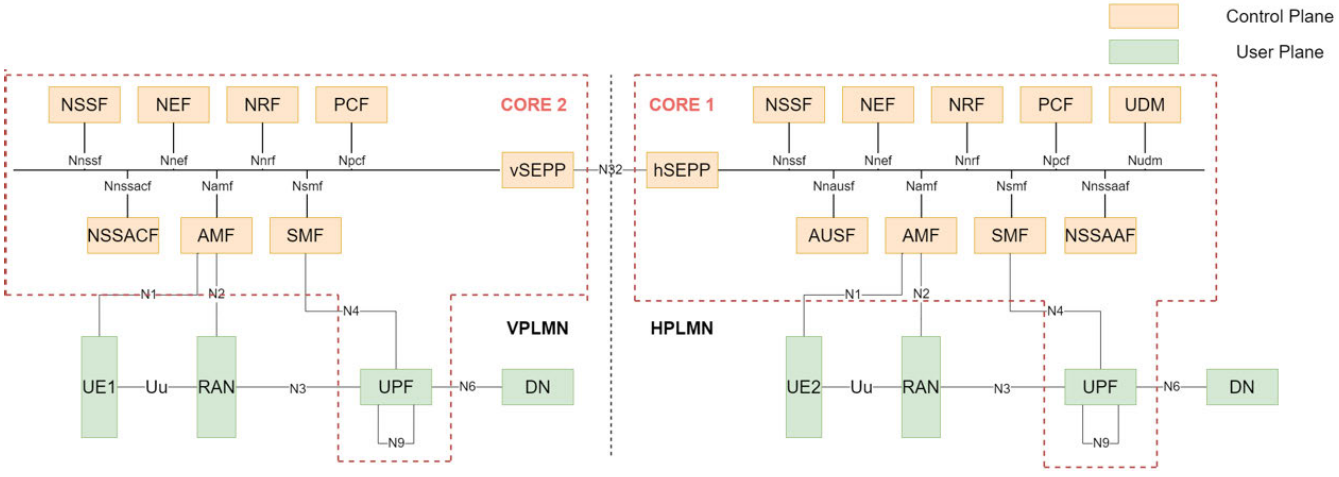

FIGURE 2. 5G SA core network service-based architecture.

checks the correctness). According to 3GPP TR 33.926 [27], the critical assets specific to the UDM to be protected are the UDM application program, user subscription data (e.g., SUPI and access and mobility subscription data) and authentication status.

5) NETWORK EXPOSURE FUNCTION (NEF)

The NEF is mainly responsible for handling external and internal information communication. It exposes events and network functions externally, provides information inside the core network to third parties, and provides information from external applications to the 3GPP network. 3GPP TR 33.926 [27] has specified the critical asset below: NEF application, Network functions, such as capabilities or events, and user data retrieved from the Unified Data Repository (UDR).

6) NETWORK REPOSITORY FUNCTION (NRF)

The NRF is responsible for network function service discovery and registration functions, receiving NF discovery requests from NF instances and notifying subscribed NFs of new, updated, or deleted NF instances. NRF also maintains NF configuration files and the health status of NF instances. According to 3GPP TR 33.926 [27], the critical assets in NRF are NRF applications and NF profiles of available NF instances, e.g., NF instance ID, NF type, PLMN ID, network slice-related identifiers, IP address of NF, NF capacity information, and location information for the NF instance.

7) SECURITY EDGE PROTECTION PROXY (SEPP)

SEPP is an entity located at the periphery of the mobile network, acting as a nontransparent proxy node, filtering and relaying the control plane signaling of the inter-PLMN. SEPP can also hide the internal network topology from the outside network. According to 3GPP TR 33.926, the critical assets specific to the SEPP to be protected are the SEPP application, the control plane message to be sent/received over N32, the internal topology information, and the protection policies, such as the data encryption policy.

B. MEC ARCHITECTURE

Multi-access edge computing (MEC) is a network architecture developed by ETSI in 2014 to provide information technology (IT) services using a front-end radio access network combined with cloud computing resources. By providing computing capabilities at the edge of the mobile network, the client can directly receive the remote server's data without going through the core network, thus reducing the delay and obtaining a better QoS. Hence, the MEC architecture greatly facilitates the development of services that require extremely low latency. Figure 3 shows the MEC architecture defined by ETSI [28], which can be roughly divided into the MEC system level and the MEC host level. The MEC system level is mainly responsible for server management, deployment management, and providing an application service operator interface for configuring their MEC application.

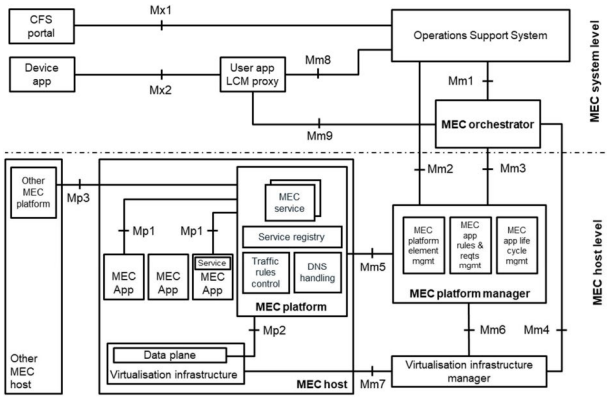

FIGURE 3. ETSI MEC reference architecture.

III. RELATED WORK

There are several assessments related to 5G security or MEC security. We collected these related works and classified them into the following categories: qualitative-based, attack-graph-based, and quantitative-based. We also summarize the related works on the 5G or MEC system in Table 1 to take comparison with our proposed framework. In Table 1, we outline the main contributions of both the related works and our frameworks, and map them to different assessment types. We introduce related works based on three evaluation methods in the following.

A. QUALITATIVE BASE RISK ASSESSMENT IN 5G

Among the three types of assessment, qualitative assessment works account for the majority. A qualitative assessment is the target assessment by experts based on the information collected by themselves and their own experiences; hence, it requires much experience and domain knowledge. It also has different aspects of assessment methodologies due to the expertise of experts. For instance, S. Sullivan [14] combined the knowledge of 5G and network OSI layers to provide 5G vulnerabilities, solutions, and future challenges for each OSI layer; Cao et al. [13] provided threat descriptions in five security domains to 5G networks based on the 3GPP security architecture; Mohan et al. [20] classified the attack vectors related to 5G into three types, which are the attacks initiated wirelessly or through the Internet, the attacks within local area networks, and the attacks from physical access; and Batalla et al. [17] evaluated the 5G system based on the methodology from the EN-ISO/IEC 27005 standard, and the assessment results indicate the corresponding risk level (Low, Medium, High, Critical) for each risk scenario in the 5G network.

Since the 5G network is composed of many different technologies and systems, the related works also carried out risk assessment for different targets. For instance, Ranaweera et al. [16] collected several papers related to MEC systems and provided detailed threat descriptions for each asset and interface; the other literature from the same authors [19] describes an investigation into security vulnerabilities of 5G use cases such as critical infrastructure-based

services, eMBB, mMTC, V2V connections, AR/VR/MR, and UAVs that deployed in accordance with MEC-based scenarios; and Hasneen and Sadique. [21] discussed the security issue for SDN, NFV, and NS technologies in 5G network and provided corresponding mitigation measures.

Although these qualitative assessments provided sufficient information on security issues, they did not effectively provide managers with assistance in practice. First, managers could not easily make comparisons from the large amount of information provided by qualitative analysis. Second, coarse-grained assessment results lead to many items being marked on the same level. Therefore, managers cannot directly understand which components in the system need to invest more in implementing protective measures. In addition, the results of the qualitative assessments are subjective; they were influenced by the bias and personal perception of the assessor. Therefore, it is considered to lack objectivity.

B. ATTACK GRAPH BASE RISK ASSESSMENT IN 5G

An attack graph is a directed graph-based structure that represents all possible attack paths against the target network. Vertices represent system assets, edges representing the existence of communication between assets, and the final state indicates that the attacker has successfully destroyed the target [29]. Currently, several works provide attack graph-based risk assessment for 5G systems. For instance, Zhao et al. [22] proposed a method to integrate local security metrics of different providers (e.g., RAN provider, core network provider, MEC provider) to form overall 5G system attack graph-based security metrics; Saha et al. [23] proposed a framework to perform attack graph analysis with machine learning and a constraint satisfaction problem (CSP) formulation to scale to more extensive infrastructures, and the proposed framework generated 119 novel possible exploits that are exclusive to 5G networks. However, this kind of assessment only focuses on exploitation, and when facing different scenarios, it has to redraw the attack graph, which is usually time-consuming work.

C. QUANTITATIVE BASE RISK ASSESSMENT IN 5G

Quantitative assessment is the least of the three types. In contrast from qualitative assessments, quantitative assessments are statistical and provide numeric results. For instance, Luo et al. [25] proposed a vulnerability assessment mechanism for SDN-based mobile network using attack graphs, and the attack graph generation is based on analytic hierarchy process (AHP) decision approaches to derive the weights for each attack action; similarly, Kholidy's work [24] leverages TOPSIS (Technique for Order Preference by Similarity to an Ideal Solution), a multiple criteria decision-making approach, to derive quantitative scores for each attack action (e.g., CVE vulnerabilities) and use them to build attack graphs. Both related works utilized a decision approach to quantify the analysis; However, this work focuses on how to generate the attack graph rather than on the risk assessment of the overall system. At present, we have not found any related work for quantitative risk assessment of the 5G network.

IV. METHODOLOGY: RAIN FRAMEWORK

As mentioned in the previous section, three types of existing works have their own deficiencies. The qualitative assessment lacks numeric and objective assessment results, the attack graph base assessment lacks comprehensive assessment and flexibility for different scenarios, and the existing quantitative assessment is only proposed for attack graph generation. In addition, all three types of existing assessments lack a unified framework, which means that their methodologies are customized to specific systems.

Hence, in this section, we present a unified assessment framework, RAIN, as depicted in Figure 1. Compared with previous related works, our framework is a quantitative assessment, flexible for adjustment, and available for various scenarios. Moreover, we incorporate the interdependent-input weighting method, an objective way to depict subjective judgment, to prioritize assets and risks. This framework takes three factors as inputs, namely, assets, protective measures, and security policy, where:

- Assets refer to the resources and components that constitute a target scenario or target's infrastructure. These assets can include hardware (e.g., servers and workstations), software (e.g., operating systems and docker containers), and data (e.g., files, databases, and configurations).
- Protective measures are measures taken to safeguard computer systems, networks and devices from potential threats, such as viruses, malware, and malicious hacking attempts. Examples of these types of protective measures include firewall implementation, backup service provision, and data encryption implementation.
- Security policy is a set of guidelines or criteria that are employed to guarantee the security of an organization's systems, networks, and data. It is usually established by the organization's management team and is typically congruent with standards, such as ISO/IEC 27001, or the organization's individual security requirements and priorities.

Utilizing these factors, experts create a security propagation network, which is a self-defined weighted network used to holistically analyze assets while considering compliance with security policy. With the security propagation network, experts generate a vector including each asset's risk score. By considering these scores, the expert can then rank the protection priority for each asset, resulting in more cost-effective protective measure decision-making. The procedures of the framework can be divided into four steps. The first step is security propagation network establishment; the expert establishes the architecture of the security propagation network to comply with the security policy. The second step is weight determination for risk type; risk type represents the nodes in the network, and the expert determines the weight for the risk types in the security propagation network. The

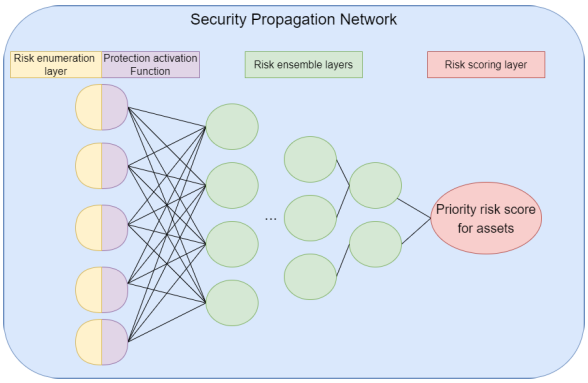

FIGURE 4. Security propagation network architecture contains four components, which are a risk enumeration layer, protection activation functions, risk ensemble layers, and a risk scoring layer.

next step is defining the assets' risk value for each risk, considering the severity of the impact or the likelihood of occurrence; the expert defines a risk value for the asset of each risk. The final step is network forward propagation; the expert transmits the risk value along the network and then produces the priority risk score for each asset. The following subsections describe the security propagation network and the procedures of the framework in more detail.

A. SECURITY PROPAGATION NETWORK: THE NETWORK TRANSFORMS QUALITATIVE RISK ASSESSMENTS INTO NUMERICAL RISK SCORES

The security propagation network, as shown in Figure 4, is designed to transform qualitative risk assessments of assets into numerical risk scores that comply with the organization's security policy. It consists of four components: a risk enumeration layer, protection activation functions, risk ensemble layers, and a risk scoring layer. In the risk enumeration layer, the expert identifies the risks in the assets and uses protection activation functions to mitigate specific risks. Subsequently, the risk value is propagated by the network in the risk ensemble layers, implying the combination of the risk values from each risk to the security policy-related risk type. Finally, the risk scores from each risk type are aggregated together to obtain the holistic risk score for each asset. The functionalities of each of the components are as follows:

- **Risk enumeration layer**: The risk enumeration layer is responsible for listing risks for the given assets. Experts typically initiate the process with a qualitative assessment to identify the various risk factors that can affect the assets. These risks are then arranged in the risk enumeration layer, with each risk depicted as a node. Every asset is then allocated a risk value for each risk node, producing a vector of size 3*1 (in the event that there are three assets). This vector demonstrates the risk profile for each asset in connection with the identified risk nodes.
- **Protection activation function**: Protective measures, including data encryption and backups, can be used to reduce certain risks associated with specific assets. In a security propagation network, these protective measures are depicted by protection activation functions, which can either increase or decrease the risk value for a particular asset. These activation functions can be implemented through a variety of options, such as sigmoid functions, ReLU functions, or pulse functions, to determine how successful the protective measures are in minimizing the risk associated with the assets. For example, in (1), we consider the situation where three assets (A_1, A_2, and A_3) need to be assessed for risk R_1. Each asset has its own risk value (V_1, V_2, V_3) for R_1. If a protection method (P) is in place for asset A_1 that helps to mitigate the impact of R_1, a pulse function (2) can be used to model the effect of this protection. This would result in $V_{p1} = 0$, thus showing that the protection has totally offset the risk for A1, while $V_{p2} = V_2$ and $V_{p3} = V_3$ shows that the risks for A2 and A3 have not been mitigated.

$$V_p = \begin{bmatrix} V_{p1} \\ V_{p2} \\ V_{p3} \end{bmatrix} = V \times P = \begin{bmatrix} V_1 \\ V_2 \\ V_3 \end{bmatrix} \times \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \tag{1}$$

$$P_a = \begin{cases} 0, & \text{if the risk for the asset } A_i \text{ is mitigated} \\ 1, & \text{otherwise} \end{cases} \tag{2}$$

- **Risk ensemble layers**: To abide by a security policy, it is necessary to group the risks listed in the risk enumeration layer into various risk types and provide different weights to these risk types depending on the policy's priorities. For example, a manager can state in a security policy that confidentiality is particularly important. One can distinguish confidentiality, integrity, and availability as three different risk types. These risk types can be utilized to assess the general security posture of the assets in question, with the weights showing the relative importance of each risk type in the policy. In addition, a multilayered structure may need to be constructed to aggregate the concrete risks into abstract risk types. This can help to provide a more comprehensive and organized view of the risks facing the assets.
- **Risk scoring layer**: The risk scoring layer produces a risk-priority score for each asset based on the output from the last layer in the risk ensemble layers. This result is a comprehensive score reflecting the weight of all the factors considered by the expert in their assessment. Subsequently, these scores can be used to prioritize the assets based on their risk level and to identify which assets may require additional protective measures or risk mitigation strategies.

B. SECURITY PROPAGATION NETWORK ESTABLISHMENT

There are four steps to establish a security propagation network architecture that conforms to the security policy.

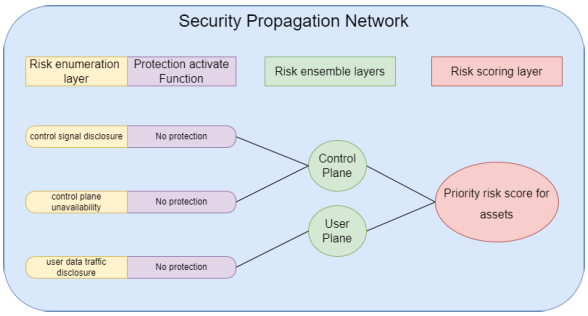

FIGURE 5. Use case for the security propagation network using the AMF and UPF as assets and using a security policy that focuses on the control plane but without any protective measure.

First, experts analyze assets and enumerate risks based on their domain knowledge. Second, existing protective measures are mapped to corresponding protection activation functions. Third, risk types in the risk ensemble layer are determined according to the security policy and linked to corresponding risks. Finally, the nodes of the last layer of the risk ensemble layers are connected to the node in the risk scoring layer. For example, if an expert wants to evaluate two network functions, AMF and UPF, and the manager has issued a security policy that focuses on the control plane but there are no existing protective measures, the expert would first need to complete the risk enumeration layer by identifying risks, such as control signaling disclosure, control plane unavailability, and user data traffic disclosure. Next, since there are no protective measures in place, there is no need to define any activation functions. The expert would then complete the risk ensemble layer by defining the control and user planes as risk types and connecting the risks to the corresponding types. Finally, the risk scoring layer is completed, and the control and user planes are connected to the priority risk score for assets. Figure 5 illustrates the resulting security propagation network for this example.

C. WEIGHT DETERMINATION FOR RISK TYPE

In the previous step, we establish the architecture of the security propagation network. Now, the expert must ascertain which risk type is more critical and assign the corresponding weights to satisfy the security policy. It is generally more accurate to assess all the input nodes together rather than individually, providing a comprehensive outlook of the risks. To identify the comparative importance of the different risk types, we employ the interdependent-input weighting method, which can be based on the analytic hierarchy process (AHP) approach [30], an effective method for objectively describing people's subjective judgments. The method is divided into three steps. First, a fundamental scale must be established for evaluating different risk types. Second, a comparison matrix is created using the fundamental scale. Finally, the matrix is standardized, and the vector value is computed to obtain the weights for each risk type. The individual steps are described below:

- **Defining the fundamental scale** According to Saaty's definition [30], the fundamental scale values are from one to nine, which represents the degree of importance or preference, as detailed in Table 2. For instance, a value of nine means that there is enough evidence to definitely prove that one is more important than another.
- **Generate the comparison matrix** We create a pairwise comparison matrix for each layer's risk type or risk, meaning that if there are n risks, we need to perform n(n-1)/2 pairwise comparisons, as seen in matrix M in (3). Table 2 illustrates the scale we use for the comparison, and its result is situated in the upper triangle part of the matrix, with the lower triangle's value being the reciprocal of the upper's relative position value.

$$M = \begin{bmatrix} 1 & a_{12} & \dots & a_{1n} \\ 1/a_{12} & \dots & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 1/a_{1n} & 1/a_{2n} & \dots & 1 \end{bmatrix} \tag{3}$$

- **Standardizing the matrix and obtaining the weight** After the matrix is established, the vector values need to be calculated to obtain the weight. The average of normalized columns technique is utilized for this purpose, as shown in 4. Here, w_i is the weight, m_{ij} is the element in the pairwise comparison matrix, and n is the number of risk types or risks included in the matrix.

$$W_i = \frac{1}{n} \sum_{j=1}^{n} \frac{m_{ij}}{\sum_{i=1}^{n} m_{ij}} \tag{4}$$

D. DEFINING ASSETS' RISK VALUE FOR EACH RISK

In the previous step, the security propagation network is completed. Now, the expert needs to define the initial risk value for each asset as the input for further calculation in the security propagation network. Each asset has a unique value for every risk in the risk enumeration layer based on factors, such as the severity of the impact or the likelihood of exposure. These values may vary for different risks and differ for the same risk on the different assets. Experts must determine which assets are most critical for a given risk to obtain a more comprehensive and precise assessment of the risks confronting the assets. To do this, the interdependent-input weighting method can be used to calculate the value of each asset for the associated risk, similar to calculating the weights of the various risk types.

E. NETWORK FORWARD PROPAGATION: AGGREGATING THE RISK VALUE TO THE HOLISTIC RISK SCORE

With the interdependent-input weighting method in the previous step, the expert has the asset risk value matrix A, with size n * m (n representing the number of assets and m representing the number of risks). The expert needs to aggregate the risk value of each asset into a single comprehensive risk score to obtain a holistic assessment and ensure that it meets the security policy. Thus, the following

TABLE 2. The fundamental scale [30] for evaluating comparison importance.

Intensity of importance	Definition	Explanation
1	Equal importance	The contributions of the two are of equal importance.
3	Moderate importance of one over another	Experience and judgment slightly favor one over another
5	Essential or strong importance	Experience and judgment strongly favor one over another.
7	Very strong importance	Strongly favor one over another, and its dominance is demonstrated in practice.
9	Extreme importance	There is enough evidence to definitely favor one over another. prove
2,4,6,8	Intermediate values	

step is to propagate these values through the network, producing the final assessment result and priority risk score for each asset. Every layer of propagation carries its own importance, which is explained subsequently:

- **Protection activation function processing:** The introduction of the security propagation network highlighted the fact that protective measures can decrease the value of each asset for every risk. The protection activation function was used to simulate this reduction and can be symbolized as a matrix P. This matrix is then multiplied elementwise with the initial asset value matrix A to create a new matrix A_p. This matrix reflects the reduced risk value of each asset for every risk, as expressed in (5).

$$A_p = A \times P \tag{5}$$

- **Ensemble of risk values:**
Once the protective activation procedure is applied, the risk values of each asset are aggregated (weighted sum) to create the risk values of each asset for every risk type. In (6), E_i represents a node in each layer in the ensemble layers, I is an input matrix with size n * m (where n is the number of assets and m is the number of input nodes for E_i), and W is a weighting matrix with size m * 1. This aggregation process helps to provide a more comprehensive perception of the risks facing the assets by considering the relative importance of every risk type and the individual risk values for each asset.

$$E_i = I \times W \tag{6}$$

- **Generating the risk score:** Finally, the values of each asset for every risk type are aggregated (weighted sum) into the priority risk score for each asset. In (7), R represents the priority risk score for each asset, I is an input matrix with size n * m (where n is the number of assets and m is the number of nodes at the last layer of the ensemble layers), and W is a weighting matrix with size m * 1. This last step of aggregation merges the values for every risk type into one single score that displays the complete risk profile for each asset. This score can be used to prioritize the assets and identify which ones may require extra protective measures or risk mitigation strategies.

$$R = I \times W \tag{7}$$

F. GENERATING RISK LEVEL CORRESPONDING TO RISK SCORE

To help executives identify the degree of risk associated with assets, we have created a procedure that assigns quantitative risk scores to different levels of risk (such as Low, Medium, High, and Critical). To start with, all of the protective activation functions must be disabled and the risk score is calculated. Subsequently, the range between highest and lowest values from the risk scores should be split into four equal quarters that correspond to Low, Medium, High, and Critical levels of risk from least to most severe. After that switch on the protective activation function so as to match the scenarios, and generate the risk scores. Finally, the risk scores could be mapped to the corresponding risk level based on the intervals it lies on. The Assets labeled as critical need prompt action such as providing protective measure; and those labeled as high should be prioritized for attention.

V. 5G SA CORE RISK ASSESSMENT

In this section, we apply our framework to the common network functions of the 5G core network, namely, AMF, UPF, SMF, UDM, NEF, NRF, and SEPP. The security policy is assumed to focus on confidentiality in the CIA triad, and there are no protective measures for these assets. In contrast to previous studies, the proposed framework offers objective, quantitative assessments and prioritizes the assets that require protection. Therefore, to produce quantitative risk assessment results, we first referred to the documents from 3GPP [27], [31], [32], [33], [34], [35], [36], [37], [38] and ENISA [39], [40], and then conducted a qualitative risk analysis of each core network function. Then, we construct a security propagation network and obtain quantitative risk assessment results through the network.

A. QUALITATIVE RISK ANALYSIS

First, we survey the key assets and potential threats of each network function from technical report 3GPP TR 33.926 [27] and the ENISA threat report [39], [40] and then consulted the detailed security issues for each network function according to the security requirements specification in 3GPP. Finally, according to the collected information, we explore the risks of common network functions, namely, AMF, UPF, UDM, SMF, NEF, NRF, and SEPP, from four directions: confidentiality, integrity, availability, and the likelihood of being an attacked surface. The following are the risk descriptions.

1) ACCESS AND MOBILITY FUNCTION (AMF)

- **Confidentiality**: If suffering from bidding down attacks on the security mode command (SMC) procedure or base station handover procedure, the low-level NAS ciphering algorithm may be used and cause the disclosure of a UE's communication traffic. If the AMF does not allocate a new 5G-GUTI in certain scenarios, an attacker may keep tracking the user using the old 5G-GUTI.
- **Integrity**: If suffering from bidding down attacks on the security mode command procedure or base station handover, the low-level NAS integrity algorithm may be used and cause tampering with the communication data. In addition, if the AMF does not verify whether the received S-NSSAIs are within the safelist stored at the AMF, an attacker can include the improper S-NSSAIs in the request and access the slice.
- **Availability**: An attacker can keep handcrafting some invalid requests and responses to AMF in 5G-AKA procedures, resulting in wasting system resources and denying legitimate user access to the system. Suppose the security mode complete message is not confidentiality protected. In that case, the AMF cannot be certain that the SMC is executed correctly, wasting system resources and denying legitimate user access to the system.
- **Likelihood of being an attacked surface**: We can directly communicate with the AMF through our UE; hence, the likelihood of an being attacked surface is high. In addition, if an additional exposed control interface (such as a remote OAM interface) exists, it may also be an attacked surface.

2) USER PLANE FUNCTION (UPF)

- **Confidentiality**: In a UPF, weak protection for user plane data and signaling data can be subject to eavesdropping.
- **Integrity**: Weak protection for user plane data can be subject to tampering. In addition, an attacker (e.g., Insider or malicious switch) may use the same TEID as the normal user, causing charging errors.
- **Availability**: Malformed GTP-U messages and handcraft-specific packets would consume the processing resource of the victim UPF or make the corresponding program crash.
- **Likelihood of being an attacked surface**: We cannot directly communicate to the UPF through our UE, but the UPF can parse/analyze our user plane packet; hence, the likelihood of being an attacked surface is high.

3) SESSION MANAGEMENT FUNCTION (SMF)

- **Confidentiality**: If the local UP security policy takes priority and no protection is indicated in the local UP security policy at the SMF, then the user plane data will be sent over the air without any protection.
- **Integrity**: If the SMF sets TEID without an identity or existing malicious SMF, an attacker uses the same TEID as the regular user, causes charging errors, or is unauthorized using a specific QoS. However, if SMF sets a charging ID without an identity or existing malicious SMF, attackers can use the same ID as the regular user, causing charging errors.
- **Availability**: If the SMF does not ensure the security policy in the gNB, the gNB might suffer from bidding down attacks. In addition, a malicious SMF may interfere with the UPF and gNB session settings, causing a lower QoS.
- **Likelihood of being an attacked surface**: There is no direct access method, but it may be accessible when a remote OAM interface exists.

4) UNIFIED DATA MANAGEMENT (UDM)

- **Confidentiality**: There are many sensitive data, such as user subscription data (e.g., subscriber's identities (SUPI)) and subscription-related data (e.g., credentials, authentication status, etc.) in UDM or, more precisely, in UDR.
- **Integrity**: Incorrect security enforcement configurations may cause user planes to not use security policies based on specific scenarios, such as time-sensitive communication (TSC). At the same time, incorrect authentication status storing implementation may cause attackers to successfully register the roughened AMF. Finally, improper UDM protection may cause user subscription data tampering.
- **Availability**: User Subscription Data in a UDM that is unavailable may cause all of the UE to not use the 5G network, and improper SUCI concealment may cause AMF to obtain a different SUPI than UE itself, causing the SMC procedure to fail. In addition, a large number of invalid requests from AUSF or forwarded by AUSF may cause DOS/DDOS.
- **Likelihood of being an attacked surface**: There is no direct access method, but it may be accessible when a remote OAM interface exists.

5) NETWORK EXPOSURE FUNCTION (NEF)

- **Confidentiality**: Network function and user data exist in NEF, such as NF capabilities and events, network, and user-sensitive information (DNN, S-NSSAI). They need to be prevented from exposure.
- **Integrity**: Network function and user data may be tampered with if unauthorized access vulnerabilities exist.
- **Availability**: A considerable number of invalid requests from third parties may cause DOS/DDOS attacks.
- **Likelihood of being an attacked surface**: NEF is usually accessed by third parties. Hence, it is possible to make NEF an attacked surface when existing attackers are third parties.

6) NETWORK REPOSITORY FUNCTION (NRF)

- **Confidentiality**: NRF contains network function profiles of available NF instances, such as NF instance ID,

NF type, PLMN ID, network slice-related identifiers, and an IP address of NF. They need to be prevented from exposure.

- **Integrity**: Improper discovery authorization may cause the NF profile to be tampered with, misleading the discovery procedure.
- **Availability**: If NF discovery authorization for a specific slice is not supported by the NRF, the NF instance in one slice can discover NF instances belonging to other slices, rendering the system to be easily attacked, as well as wasting resources.
- **Likelihood of being an attacked surface**: It would be an attacked surface when attackers are insiders, or it is accessible when a remote OAM interface exists.

7) SECURITY EDGE PROTECTION PROXY (SEPP)

- **Confidentiality**: SEPP may contain service messages to be sent/received over N32 and internal topology information. They need to be prevented from exposure.
- **Integrity**: Misusing cryptographic material of peer SEPPs and IPX providers may cause forged IPX providers or forged vSEPP, leading to tampered messages in the N32 interface. In addition, if the SEPP performs incorrect handling when detecting that the PLMN-ID in the incoming N32 message mismatches the PLMN-ID in the related N32 context, it may cause NF consumers to use hPLMN's NF without authorization.
- **Availability**: SEPP service or related data unavailability may cause roaming failure.
- **Likelihood of being an attacked surface**: It can be accessed from IPX provider (third party) or vSEPP (other operators).

B. QUANTITATIVE ASSESSMENT

According to the qualitative risk descriptions, we can enumerate the risks. We listed 24 risks, illustrated in Table 3. Then, to meet the security policy, "focus on confidentiality," four risk types are defined on the risk ensemble layer: confidentiality, integrity, availability, and the likelihood of being an attacked surface, and the related risks are connected to the corresponding risk types. Then, the four nodes are connected to the priority risk score for assets of the risk scoring layer to complete the construction of the security propagation network. Finally, the weights of all risk types and risks are set. The weight determination has been mentioned in section four. Figure 6 shows the overall security propagation network.

After the security propagation network is established, we use the interdependent-input weighting method mentioned in Section IV to define the risk value of each asset for every risk; the result is shown in Table 4. In Table 4, we can observe that UDM has the highest risk value in almost all risks since UDM keeps subscribers' credentials and other sensitive information, and UDM is responsible for authentication procedures for UE. However, NEF has the highest risk value in the likelihood of being an attacked surface since NEF is the interface network function between the 5G core network and the third-party application servers, and it can potentially be targeted by attackers as a way to gain access to the core network. After defining the risk value, we propagate these values through the network, and finally, we obtain the risk score of each asset, as shown in Figure 7. According to the numerical results, the UDM is the riskiest among the core network functions, with a risk score of 0.315. Hence, UDM needs to be the priority to implement protective measures. However, NRF, UPF, and SEPP have lower risk scores than others, so they would not be the priority for the protective measure.

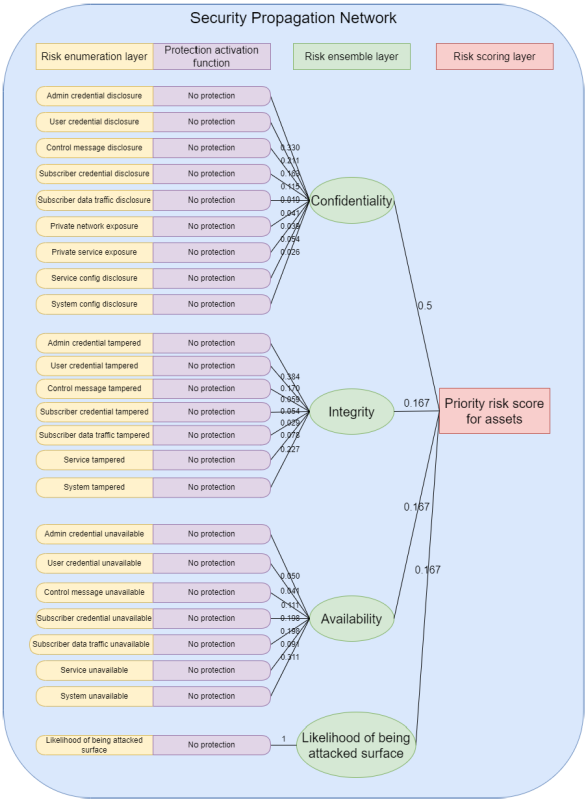

FIGURE 6. Security propagation network for 5G SA core network functions.

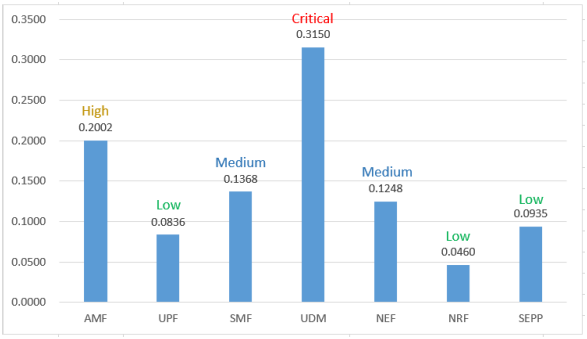

FIGURE 7. 5G SA core network function assessment result. The results show that the UDM holds the greatest risk of all the core network functions, with a risk score of 0.315.

TABLE 3. Risk enumeration and description for 5G SA core network functions.

Risk	Risk description
Likelihood of being an attacked surface	It indicates the likelihood of becoming an attacker's contact. If the asset has an interface for external communication, it is more likely to become an attacked surface.
Admin credential disclosure	The target asset's administrator or high-privileged account credentials being leaked or stolen.
User credential disclosure	The target asset's low-privilege account credentials being leaked or stolen.
Control message disclosure	Control-related signaling, such as mobility-related information or session management information, is eavesdropped on or leaked.
Subscriber credential disclosure	Subscribers' credentials, such as SUPI, and IMSI, are leaked or stolen.
Subscriber data traffic disclosure	The data traffic from the subscribers through the mobile network is eavesdropped on or stolen.
Private network exposure	Private network domains of mobile network operators are exposed through malicious behavior.
Private service exposure	Private services of mobile network operators are exposed through malicious behavior.
Service config disclosure	Service configs of mobile network operators, such as docker YAML or website version configs, are exposed through malicious behavior.
System config disclosure	System configs of mobile network operators, such as boot configs, are exposed through malicious behavior.
Admin credential tampered	The target asset's administrator or high-privileged account credentials are tampered.
User credential tampered	The target asset's low-privileged account credentials are tampered.
Control message tampered	Control-related signaling, such as mobility-related information or session management information, is tampered.
Subscriber credential tampered	Subscribers' credentials, such as SUPI, and IMSI, are tampered.
Subscriber data traffic tampered	The data traffic from the subscribers through the mobile network is tampered.
Service tampered	The service which working on the component cannot be tampered without authorization or can be quickly discovered after tampering. e.g., Website, docker service.
System tampered	Component's corresponding system can't be tampered without authorization or can be quickly discovered after tampering. e.g., system's boot config, system's network config.
Admin credential unavailable	The target asset's administrator or high-privileged account credentials are breached.
User credential unavailable	The target asset's low-privileged account credentials are breached.
Control message unavailable	Control-related signaling, such as mobility-related information or session management information, is breached.
Subscriber credential unavailable	Subscribers' credentials, such as SUPI, and IMSI, are breached.
Subscriber data traffic unavailable	The data traffic from the subscribers through the mobile network is breached.
Service unavailable	The service which working on the component not being available and accessible to the customers during the time you promised to keep the service available. e.g., website, docker service.
System unavailable	The hosting system which working on the component not being available during the time you promised to keep the target service available. e.g., server, cloud instance.

TABLE 4. 5G SA core network function risk value for each risk.

	AMF	UPF	SMF	UDM	NEF	NRF	SEPP	Total
Likelihood of being attacked surface	0.241	0.167	0.023	0.070	**0.420**	0.030	0.049	1.000
Admin credential disclosure	0.174	0.033	0.174	**0.473**	0.033	0.020	0.093	1.000
User credential disclosure	0.196	0.047	0.196	**0.360**	0.047	0.031	0.123	1.000
Control message disclosure	**0.322**	0.029	0.151	0.235	0.063	0.076	0.124	1.000
Subscriber credential disclosure	0.193	0.031	0.193	**0.455**	0.031	0.031	0.066	1.000
Subscriber data traffic disclosure	0.067	**0.600**	0.067	0.065	0.067	0.067	0.067	1.000
Private network exposure	0.055	0.055	0.055	0.054	**0.374**	0.266	0.141	1.000
Private service exposure	0.049	0.049	0.049	0.050	**0.337**	0.190	0.276	1.000
Service config disclosure	0.327	0.022	0.120	**0.328**	0.061	0.043	0.099	1.000
System config disclosure	0.327	0.022	0.120	**0.328**	0.061	0.043	0.099	1.000
Admin credential tampered	0.174	0.033	0.174	**0.473**	0.033	0.020	0.093	1.000
User credential tampered	0.196	0.047	0.196	**0.360**	0.047	0.031	0.123	1.000
Control message tampered	0.256	0.029	0.131	**0.314**	0.076	0.063	0.131	1.000
Subscriber credential tampered	0.237	0.034	0.171	**0.456**	0.034	0.034	0.034	1.000
Subscriber data traffic tampered	0.067	**0.598**	0.067	0.067	0.067	0.067	0.067	1.000
Service tampered	0.327	0.022	0.120	**0.328**	0.061	0.043	0.099	1.000
System tampered	0.327	0.022	0.120	**0.328**	0.061	0.043	0.099	1.000
Admin credential unavailable	0.174	0.033	0.174	**0.473**	0.033	0.020	0.093	1.000
User credential unavailable	0.196	0.047	0.196	**0.360**	0.047	0.031	0.123	1.000
Control message unavailable	0.190	0.027	0.151	**0.396**	0.059	0.071	0.106	1.000
Subscriber credential unavailable	0.237	0.034	0.171	**0.456**	0.034	0.034	0.034	1.000
Subscriber data traffic unavailable	0.067	**0.600**	0.067	0.065	0.067	0.067	0.067	1.000
Service unavailable	0.038	0.038	0.196	**0.453**	0.095	0.059	0.121	1.000
System unavailable	0.042	0.035	0.197	**0.452**	0.111	0.065	0.098	1.000

VI. 5G SA CORE RISK ASSESSMENT WITH DIFFERENT SCENARIOS

The information security policy of an organization can be altered by external influences. In contrast to previous studies, the proposed work structure offers parameter functions, so managers can adapt to policy requirements more easily. By adjusting the security propagation network in the framework according to different situations, we obtain

the corresponding assessment results without re-evaluation. In the following, we employ protective measure alteration and security policy modification from the prior evaluation as examples.

A. 5G SA CORE RISK ASSESSMENT WITH PROTECTIVE MEASURES

In this subsection, we assume that the manager decided to focus on the UDM protection based on the risk assessment results in section five. According to 3GPP TR 33.926, the critical assets of the UDM include user subscription data such as SUPI, access and mobility subscription data, and other status data, such as authentication status. Hence, the manager implements the protective measure that provides encryption techniques for these data in rest, transit, and process for the UDM.

Given the protective measure, experts only need to modify the protection activation function in the original security propagation network and perform network forward propagation again. The first step is to model the protective measure. Valid data encryption can effectively mitigate risks in the UDM related to data confidentiality, such as admin credential disclosure, user credential disclosure, control message disclosure, subscriber credential disclosure, subscriber data traffic disclosure, and system config disclosure. To model the mitigation effect of these risks, we use the pulse function; that is, the risk value of the UDM for a specific risk will be multiplied by 0, and the rest will be multiplied by 1, which means that the same risk value remains. The updated security propagation network is shown in Figure 8. Finally, we obtain new risk assessment results after network forward propagation, as shown in Figure 9, compared with the assessment result in the previous section. As seen in Figure 9, the risk score of the UDM has been effectively mitigated, and AMF has replaced the UDM as the network function with the highest protection priority. Therefore, through the assessment result, managers can intuitively understand the effect of protective measures on specific assets.

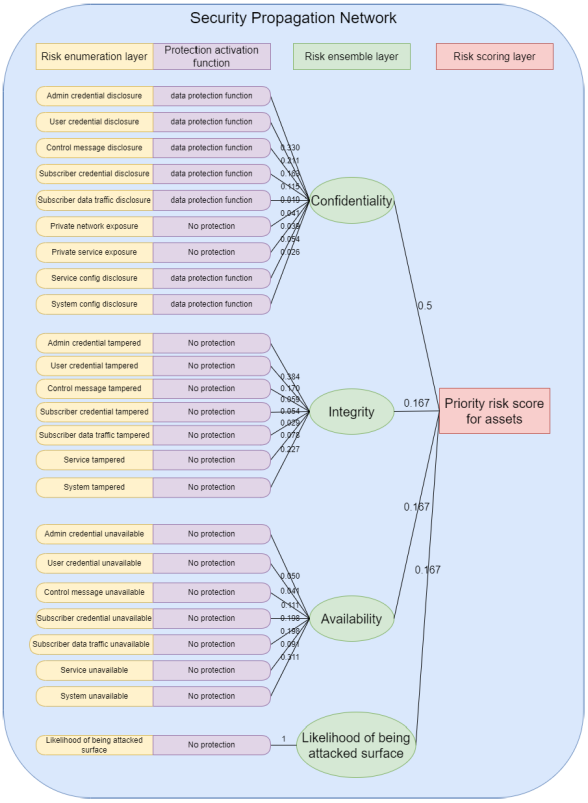

FIGURE 8. Security propagation network for 5G SA core network functions with an updated protective measure.

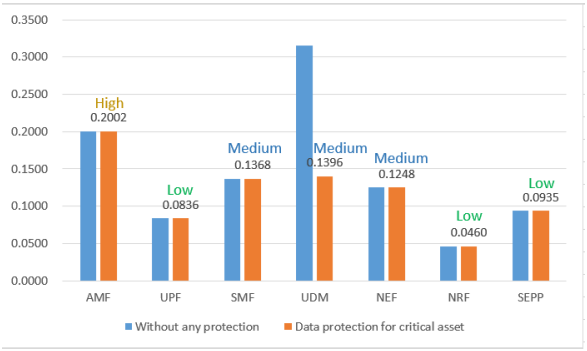

FIGURE 9. 5G SA core network function with protective measure assessment results. The risk score for the UDM has been substantially reduced, and AMF is now the network function with the top priority for protection.

B. 5G SA CORE RISK ASSESSMENT WITH DIFFERENT SECURITY POLICIES

In this subsection, we assume that the manager's security policy changes and decides to put more emphasis on the likelihood of being an attacked surface. Therefore, the risk score for the network functions that are easily exposed to the external network, such as NEF and AMF, should be increased.

Given the security policy, experts only need to adjust the parameters in the original security propagation network, increase the corresponding weight in the risk type, and perform network forward propagation again. The first step is the weight adjustment. According to the interdependent-input weighting method mentioned in section four, we increase the likelihood of being an attacked surface to 0.5. The updated security propagation network is shown in Figure 10. Finally, we obtain new risk assessment results after network forward propagation, which are compared with the assessment results in the fifth section, as shown in Figure 11. In Figure 11, the risk score of NEF has been dramatically increased since the network function is responsible for communicating with third-party application servers. However, the risk score of the UDM drops considerably. Compared with other network functions, the UDM has fewer opportunities to communicate with the outside world. Therefore, under the emphasis on the likelihood of being an attacked surface, the UDM is no longer the highest risk network function, and NEF becomes the priority for implementing the protective measure.

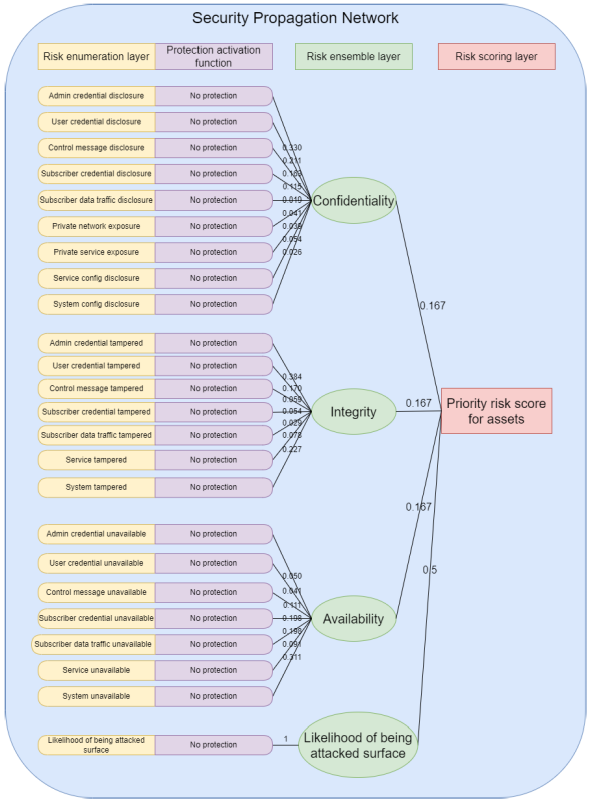

FIGURE 10. Security propagation network for 5G SA core network functions with updated security policies.

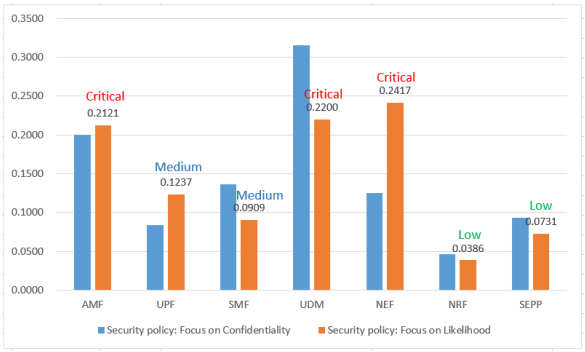

FIGURE 11. 5G SA core network function with an updated security policy assessment result. The results show that the NEF is the riskiest of all the core network functions, with a risk score of 0.2417.

VII. COMPARISON WITH THE TRADITIONAL ASSESSMENT

To compare the traditional assessment with the RAIN framework, we applied the traditional qualitative assessment methodology to the three scenarios (Section V, Section VI-A, Section VI-B) mentioned in our article to compare the proposed framework. We design scenario 2 versus scenario 1 with protection measures as the manipulated variable and scenario 3 versus scenario 1 with security policies as the manipulated variable. These settings allow inter-scenario and intra-scenario comparisons for results from two assessments. The results of this comparison are illustrated in Table 6, Table 7, and Table 8. The following subsections introduced the methods used for the traditional qualitative assessment and explained the three experimental scenarios again. Then, we present a comparison between both assessment techniques from these tables.

TABLE 5. The risk-level scale from Jordi Mongay Batalla's work [17].

Consequence \ Likelihood	Hard to imagine	Might happen	Certainly happen
Moderate	Low	Medium	High
Significant	Low	High	Critical
Catastrophic	Medium	Critical	Critical

A. TRADITIONAL ASSESSMENT

Traditional assessments often use the Risk-level scale to consider different risk factors (such as the consequences and likelihood of occurrence) and then use tables to define the risk levels corresponding to various risk factors. For instance, Batalla et al. utilizes the Risk-level scale table 5 to measure risks associated with 5G networks [17]. This kind of approach leads to coarse-grained assessment results, and can only focus on specific risk factors and not be flexible enough for changing conditions. Further discussion is found in section VII-C.

B. EXPERIMENT ENVIRONMENT

We provide three experimental scenarios, all of which use common network functions in the 5G core network service-based architecture as assets. In the first scenario, no protective measures are implemented and the security policy focuses on confidentiality. The second and third scenarios are different from the first scenario in protective measures and security policies respectively. The second scenario implements data confidentiality protective measure on the UDM, and the third scenario's security policy focuses on the likelihood of becoming an attacked surface instead. We used the assessments for these three environments to see whether the assessment results for different environments were accurate and reasonable. For the traditional assessment part, we refer to the qualitative risk analysis in section V and assign a risk level for each asset based on Table 5. In scenario 2, UDM has implemented protective measures for confidentiality which reduces the consequence degree from "Catastrophic" to "Significant" as it is only mitigating the issue related to confidentiality, thus lowering the risk level to "High". In addition, Scenario 3 produces an assessment result identical to that of Scenario 1. For RAIN framework, we used the assessment results in sections V, VI-A, and VI-B.

C. COMPARISON OBSERVATION

The experimental results are presented in Table 6, Table 7, and Table 8. Each of these tables contains information regarding the scenario settings (including protective measures and security policies), assets (common network functions), assessment results from traditional assessment (level-based) and RAIN framework (both numeric-based and level-based), as well as the risk level difference number between two

TABLE 6. Comparison between traditional assessment and RAIN framework based on Scenario in Section V.

Scenario / **Protective measure** / **Security policy**	Scenario 1 (Sec V.) None Focus on confidentiality		
NF \ Assessment	Traditional	RAIN	
AMF	Critical	High	0.2002
UPF	High	Low	0.0836
SMF	High	Medium	0.1368
UDM	Critical	Critical	0.3150
NEF	Critical	Medium	0.1248
NRF	Low	Low	0.0460
SEPP	Low	Low	0.0935
Difference	4		

TABLE 7. Comparison between traditional assessment and RAIN framework based on Scenario in Section VI-A.

Scenario / **Protective measure** / **Security policy**	Scenario 2 (Sec VI-A) Encryption techniques for the UDM Focus on confidentiality		
NF \ Assessment	Traditional	RAIN	
AMF	Critical	High	0.2002
UPF	High	Low	0.0836
SMF	High	Medium	0.1368
UDM	High	Medium	0.1396
NEF	Critical	Medium	0.1248
NRF	Low	Low	0.0460
SEPP	Low	Low	0.0935
Difference	5		

assessment results. From our analysis of these tables, we have noticed four key observations:

- From Table 8, the RAIN framework produced similar assessment results as traditional assessment. The level scale (Table 5) used by Jordi Mongay Batalla's work [17] puts more emphasis on the likelihood of becoming an attacked surface, which matches the security policy in scenario 3; hence the assessment result is similar as the one from RAIN framework.
- From Table 7, it can be found that traditional assessment cannot adapt to security policies, resulting in inaccurate assessment results. For instance, the NEF have the risk level "critical" in the traditional assessment, but the consideration security policy is biased to focus on confidentiality issues rather than the likelihood of becoming an attacked surface. Consequently, the NEF does not have the same level of security breaches related to confidentiality as the AMF (like subscriber credential disclosure (SUCI, SUPI)) and should not be assigned a "critical" risk level. In addition, the UPF has the risk level of "High" in the traditional assessment; however, it does not have sensitive data related to subscribers; hence from the perspective of confidentiality, the UPF should not have the risk level of "High."
- From Table 6 and 7, the traditional assessment is not sensitive to the protective measure. UDM has implemented protective measures for confidentiality issues in scenario 2; however, the traditional assessment focuses more on the likelihood of becoming an attacked surface. Hence the risk level is only decreased to "High" level. On the other hand, the RAIN framework responded sensitively to the mitigation, which reduced the risk level to "Medium."
- From Table 6, executives cannot decide which of AMF, UDM, or NEF should be prioritized for protective resource allocation when the resources are limited. On the other hand, the RAIN framework provides numeric results to assist executives in understanding that UDM is the priority of providing protective resources.

TABLE 8. Comparison between traditional assessment and RAIN framework based on Scenario in Section VI-B.

Scenario / **Protective measure** / **Security policy**	Scenario 3 (Sec VI-B.) None focus on Likelihood		
NF \ Assessment	Traditional	RAIN	
AMF	Critical	Critical	0.2121
UPF	High	Medium	0.1237
SMF	High	Medium	0.0909
UDM	Critical	Critical	0.2200
NEF	Critical	Critical	0.2417
NRF	Low	Low	0.0386
SEPP	Low	Low	0.0731
Difference	2		

VIII. CONCLUSION

We construct a quantitative assessment framework, RAIN, for a 5G network. Given the assets, protective measures, and security policies, the framework enables the manager to obtain fine-grained assessment results. According to the security policy, it can quickly generate updated assessment results by changing the weight of the corresponding security types. According to different protective measures, experts can update assessment results by changing the protection activation functions. Finally, the framework can also be applied to various subsystems. We apply our framework to the 3GPP-defined 5G core network and present a method to directly update assessment results when facing protection strategy or security policy changes.

ACKNOWLEDGMENT

The authors would like to thank Professor Yeali S. Sun. This work would not have possibly proceeded well without her advice and discussion.

REFERENCES

[1] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.

[2] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.

[3] A. Filali, A. Abouaomar, S. Cherkaoui, A. Kobbane, and M. Guizani, "Multi-access edge computing: A survey," *IEEE Access*, vol. 8, pp. 197017–197046, 2020.

[4] F. Z. Yousaf, M. Bredel, S. Schaller, and F. Schneider, "NFV and SDN—Key technology enablers for 5G networks," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2468–2478, Nov. 2017.

[5] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.
[6] S. R. Hussain, M. Echeverria, O. Chowdhury, N. Li, and E. Bertino, "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019, pp. 1–15.
[7] Y. Cheng and C. Shen, "A new tracking-attack scenario based on the vulnerability and privacy violation of 5G AKA protocol," *IEEE Access*, vol. 10, pp. 77679–77687, 2022.
[8] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, "Security in SDN: A comprehensive survey," *J. Netw. Comput. Appl.*, vol. 159, Jun. 2020, Art. no. 102595.
[9] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 196–248, 1st Quart., 2020.
[10] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog: A survey and analysis of security threats and challenges," *Future Gener. Comput. Syst.*, vol. 78, pp. 680–698, Jan. 2018.
[11] D. Fang, Y. Qian, and R. Q. Hu, "Security for 5G mobile wireless networks," *IEEE Access*, vol. 6, pp. 4850–4874, 2018.
[12] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Sep. 2017, pp. 193–199.
[13] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, and L. Xiong, "A survey on security aspects for 3GPP 5G networks," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 170–195, 1st Quart., 2020.
[14] S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G security challenges and solutions: A review by OSI layers," *IEEE Access*, vol. 9, pp. 116294–116314, 2021.
[15] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and beyond," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 4, pp. 3682–3722, 4th Quart., 2019.
[16] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 1078–1124, 2nd Quart., 2021.
[17] J. M. Batalla, E. Andrukiewicz, G. P. Gomez, P. Sapiecha, C. X. Mavromoustakis, G. Mastorakis, J. Zurek, and M. Imran, "Security risk assessment for 5G networks: National perspective," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 16–22, Aug. 2020.
[18] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *IEEE Access*, vol. 9, pp. 18706–18721, 2021.
[19] P. Ranaweera, A. Jurcut, and M. Liyanage, "MEC-enabled 5G use cases: A survey on security vulnerabilities and countermeasures," *ACM Comput. Surveys*, vol. 54, no. 9, pp. 1–37, Oct. 2021.
[20] J. P. Mohan, N. Sugunaraj, and P. Ranganathan, "Cyber security threats for 5G networks," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (eIT)*, May 2022, pp. 446–454.
[21] J. Hasneen and K. M. Sadique, "A survey on 5g architecture and security scopes in SDN and NFV," in *Proc. Appl. Inf. Process. Syst. (ICCET)*. Singapore: Springer, 2022, pp. 447–460.
[22] L. Zhao, M. S. Oshman, M. Zhang, F. F. Moghaddam, S. Chander, and M. Pourzandi, "Towards 5G-ready security metrics," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2021, pp. 1–6.
[23] T. Saha, N. Aaraj, and N. K. Jha, "Machine learning assisted security analysis of 5G-network-connected systems," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 4, pp. 2006–2024, Oct. 2022.
[24] H. A. Kholidy, A. Karam, J. L. Sidoran, and M. A. Rahman, "5G core security in edge networks: A vulnerability assessment approach," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Sep. 2021, pp. 1–6.
[25] S. Luo, J. Wu, J. Li, L. Guo, and B. Pei, "Toward vulnerability assessment for 5G mobile communication networks," in *Proc. IEEE Int. Conf. Smart City/SocialCom/SustainCom (SmartCity)*, Dec. 2015, pp. 72–76.
[26] *System Architecture for the 5G System (5GS)*, document 3rd Generation Partnership Project TR 23.501, 2022.
[27] *Security Assurance Specification (SCAS) Threats and Critical Assets in 3GPP Network Product Classes*, document 3rd Generation Partnership Project TR 33.926, 2022.
[28] *Multi-Access Edge Computing (MEC); Phase 2: Use Cases and Requirements*, document European Telecommunications Standards Institute GS MEC 002, Sophia Antipolis, France, Jan. 2022.
[29] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Proc. 15th IEEE Comput. Secur. Found. Workshop. (CSFW-15)*, Jun. 2002, pp. 49–63.
[30] T. L. Saaty, "Decision making with the analytic hierarchy process," *Int. J. Services Sci.*, vol. 1, no. 1, pp. 83–98, 2008.
[31] *Security Architecture and Procedures for 5G System*, document 3rd Generation Partnership Project TS 33.501, 2022.
[32] *5G Security Assurance Specification (SCAS), Access and Mobility Management Function (AMF)*, document 3rd Generation Partnership Project TS 33.512, 2022.
[33] *5G Security Assurance Specification (SCAS), User Plane Function (UPF)*, document 3rd Generation Partnership Project TS 33.513, 2022.
[34] *5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) Network Product Class*, document 3rd Generation Partnership Project TS 33.514, 2022.
[35] *5G Security Assurance Specification (SCAS) for the Session Management Function (SMF)*, document 3rd Generation Partnership Project TS 33.515, 2022.
[36] *5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP)*, document 3rd Generation Partnership Project TS 33.517, 2022.
[37] *5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF)*, document 3rd Generation Partnership Project TS 33.518, 2022.
[38] *5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF)*, document 3rd Generation Partnership Project TS 33.519, 2022.
[39] *ENISA Threat Landscape For 5G Networks: Updated Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)*, document European Union Agency for Cybersecurity (ENISA), Dec 2020.
[40] *ENISA THREAT LANDSCAPE FOR 5G NETWORKS: Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)*, document European Union Agency for Cybersecurity (ENISA), Nov 2019.

CHE-TSUNG KUO received the B.S. degree in electronics engineering from National Taiwan University, Taipei, Taiwan, in 2021, where he is currently pursuing the M.S. degree with the Master Program in Cybersecurity, Department of Electrical Engineering. His research interests include cybersecurity and 5G security.

HONG-YEN CHEN received the B.S. degree in electronics engineering from National Taiwan Normal University, Taipei, Taiwan, in 2019. He is currently pursuing the Ph.D. degree with the Doctoral Program in Cybersecurity, Department of Electrical Engineering, National Taiwan University, Taipei. His research interests include cybersecurity, machine learning, and deep learning.

TSUNG-NAN LIN (Senior Member, IEEE) received the B.S. degree from National Taiwan University, Taipei, Taiwan, in 1989, and the M.S. and Ph.D. degrees from Princeton University, Princeton, NJ, USA, in 1993 and 1996, respectively. Then, he joined EPSON Research and Development Inc., San Jose, CA, USA, and EMC Corporation, Hopkinton, MA, USA. Since February 2002, he has been with the Department of Electrical Engineering, Graduate Institute of Communication Engineering, National Taiwan University. He has also been the Director of the Division of Network Management of Computer and Information Networking Center, National Taiwan University, and the Vice President and the General Director of the Cybersecurity Technology Institute, Institute for Information Industry. He is a member of the Phi Tau Phi Scholastic Honor Society.