Dependability Analysis of 5G-AKA Authentication Service From Server and User Perspectives

LILI JIANG, XIAOLIN CHANG, JING BAI, JELENA MIŠIĆ, VOJISLAV MIŠIĆ, AND ZHI CHEN

1Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China
2Computer Science Department, Ryerson University, Toronto, ON M5B 2K3, Canada

Corresponding author: Xiaolin Chang (xlchang@bjtu.edu.cn)

The work of Lili Jiang, Xiaolin Chang, Jing Bai, and Zhi Chen was supported in part by the National Natural Science Foundation of China under Grant U1836105, and in part by the Fundamental Research Funds for the Central Universities under Grant 2019YJS042. The work of Jelena Mišić and Vojislav Mišić was supported in part by the National Science and Engineering Research Council (NSERC) of Canada through Discovery Grants.

ABSTRACT The fifth generation (5G) technology offers a set of security services in order to provide secure communication to a large number of various devices. 5G Authentication and Key Agreement (5G-AKA) authentication service acts as the first step of securing the 5G network communication. This paper aims to quantitatively analyze the dependability of 5G-AKA authentication service. We develop the continuous-time Markov chain (CTMC) models to capture the operational details of the 5G-AKA authentication services when facing the service failure. We also derive formulas for calculating metrics of interest, including Defects Per Million (DPM), authentication service’s first restoration time from failure and total cost of ownership (TCO). Extensive numerical analysis is applied to investigate the impact of parameters on the evaluation metrics.

INDEX TERMS 5G-AKA protocol, availability, defects per million, first restoration time, total cost of ownership.

I. INTRODUCTION The tremendously increased capacities of the 5th-Generation (5G) networks [1] enable 5G to offer ultra-reliable and affordable broadband access to a huge number of various devices, including mobile hand-held, Machine-to-Machine communication (M2M), Internet of Things (IoT) [2], and Cyber-Physical Systems (CPSs) devices [3]. Moreover, 5G system offers several security services for secure communication [4]. The “5G Authentication and Key Agreement” (5G-AKA) protocol, which is used to authenticate and establish keys between the involved parties in 5G network, acts as the first step of securing the 5G network communication [5]. Designing authentication and access control mechanisms for 5G networks should consider service-specific security requirements. For example, fast communications need the design of fast AKA procedures [6].

FIGURE 1 illustrates three security entities in the 5G Core Network (5GC), which are involved in the 5G-AKA authentication service provisioned to User Equipment (UE) [7]. These entities are Security Anchor Function (SEAF), Authentication Server Function (AUSF), and Authentication credential Repository and Processing Function (ARPF). It is known that the design flows, misconfiguration, and implementation bugs of 5G system can cause 5G system failures. Furthermore, those entities are facing software aging problem like other software. No matter which problem happens will lead to the failure of the entity and the failure of the whole protocol process, and finally result in loss of authentications, i.e., newly arriving UE authentication requests will be dropped. Backup entity can alleviate this authentication request loss but increase cost to
This paper explores an analytical modeling approach to quantitatively analyze the dependability of 5G-AKA authentication service from the perspectives of both service provider and end user. Without loss of generality, we only consider the SEAF failure and assume that all the other entities will never fail. That is, 5G-AKA authentication service fails only due to SEAF entity failure. Notice that, AUSF and ARPF in 5G-AKA authentication service also suffer from failure. The model proposed in this paper is also suitable to the scenario where AUSF or ARPF fails. We choose SEAF as an example because SEAF is the first functional element for the UE accessing the 5GC. Also, the SEAF receives the anchor key, $K_{\text{SEAF}}$, from the AUSF upon a successful primary authentication procedure in each serving network, and the SEAF shall never transfer $K_{\text{SEAF}}$ to an entity outside the SEAF. Keys for more than one security context can be derived from $K_{\text{SEAF}}$ without the need of the running of a new authentication [7]. Finally, the channel between UE and SEAF is more likely been attacked by adversaries which makes SEAF more prone to failure [5].

The main contributions of this paper are summarized as follows:

- We develop continuous-time Markov chain (CTMC) models for capturing the behaviors of 5G-AKA service that suffers from failure under non-backup and backup policies, respectively. The details of these two policies are given in Section III. The availability models will be applied for deriving the formulas for computing metrics of interest. Note that CTMC modeling is an evaluation approach for quantitatively analyzing the target performance, dependability and security [24].
- We quantitatively analyze the user-oriented dependability of 5G-AKA by deriving the formulas for computing defects per million ($DPM$) computation under each policy. $DPM$ denotes the number of authentication requests not served per million as in [8].
- We quantitatively analyze the service-provider-oriented dependability of 5G-AKA by deriving the formulas for computing the 5G-AKA authentication service’s first restoration time from SEAF failure and total cost of ownership (TCO) under each policy. The later includes infrastructure cost, power consumption and cooling cost, operation cost and drop cost.

The rest of the paper is organized as follows. Section II introduces background and related work. Section III provides a brief description and presents the proposed model. Section IV presents the experimental results. Finally, we conclude this paper and possible directions for future work in Section V.

II. BACKGROUND AND RELATED WORK

This section first introduces the 5G-AKA protocol developed by 3GPP [7]. Then we present the existing studies of AKA protocol which are closely related to our research.

A. 5G-AKA PROTOCOL

5G-AKA protocol developed by the 3rd Generation Partnership Project (3GPP) [7] is an essential security protocol in 5G networks in order to ensure the communication security, and its authentication procedure is shown in FIGURE 2 [7]. It is an evolution of the AKA variants used in 3G and 4G [7]. It is used to authenticate and establish keys between the involved parties [5] in 5G networks. AUSF compares the received RES* with the stored XRES*. If RES* and XRES* are equal, the authentication is successful from the home network point of view. Anyone who wants to use 5G network needs to complete the protocol before accessing the network. FIGURE 1 describes the main security entities involved in the 5G-AKA authentication. The channel between UE and SEAF belongs to Radio Access Network and other two channels belong to 5G core network (5GC). Unlike 3G or 4G network, those function modules are virtualized software functions on a unified platform, not specialized hardware.

B. RELATED WORK

There was no real secure authentication [9]. Many researches have been carried out to analyze or/and address this weakness by improving or modifying AKA protocol. Gupta et al. [10] proposed a dynamic group based efficient and secure (DGBES-AKA) protocol for M2M communication in LTE/LTE-A network, which improved some overhead. Li et al. [11] proposed the group-based AKA (GR-AKA) protocol which not only could authenticate several communication devices simultaneously, but also made the system to dynamically update its access-policy in an efficient way. Parne et al. [12] proposed the security enhanced group-based (SEGB) AKA protocol for M2M communication in LTE/LTE-A network, which overcame the problem of the single key, signaling congestion and high bandwidth consumption. Parne et al. [13] proposed the performance and security enhanced (PSE-AKA) protocol for LTE/LTE-A network, which generated the authentication vectors with small overhead. 5G AKA protocol enhances the AKA protocol of 4G LTE [14] [15] by providing the next party and channel with proof of successful authentication of the UE from the visited network [16]. Idrissi et al. [17] proposed enhancement of AKA protocol in order to meet the requirements of authentication and authorization in 5G networks by using a new key framework, which not only improved performance, but also enabled fast re-authentication during handover. Basin et al. [18] analyzed the 5G AKA algorithms and demonstrated that the protocol failed in meeting several security goals, which were explicitly required, and then made explicit recommendations for the attacks and weaknesses with finding. Differently, in this paper we analyze the...
dependability of 5G-AKA authentication service when facing the failure of SEAF service, which can be used to help the assessment of the capability of the aforementioned protocols.

Note that researchers have investigated the reasons for the authentication requests to be dropped in the authentication process. Some researchers focused on the authentication failure, which caused the requests to be dropped. Abdoet et al. [19] considered that RandomEncKey, RandomIntKey, UESeccapabilities and some other information were encrypted by using the Home network’s public key stored in UICC, in order to get A. Then A was checked for integrity in EC-AKA2 signaling messages. If failing, Home Subscriber Server (HSS) dropped the request and replied with an error code. Differently, we consider the failure of SEAF entity of 5G-AKA protocol will result in the loss of authentication and provide the Authentication Request Loss (ARL) model for the failure.

Finally, TCO can help providers make decisions to minimize their costs. There is a crucial need to provide TCO for analyzing the services. Zhang et al. [20] evaluated the authentication cost of RUSH based on the computation cost, the communication overhead and the storage cost. Sun et al. [21] analyzed the performance of proposed scheme in terms of computational cost, signaling overhead and communication overhead. Cao et al. [22] proposed a fast mutual authentication and data transfer scheme for massive NB-IoT devices, and compared the signaling cost, the transmission cost and the total computational cost of existing policies. Differently, we consider the failure and recovery of SEAF entities of 5G-AKA protocol, and then define different components for TCO of authentication service, i.e., infrastructure cost, power consumption and cooling cost, operation cost and drop cost. Moreover, the formula of the different component costs is given.

To the best of our knowledge, we are the first to consider DPM, the first restoration time and TCO by developing the model to capture the failure of 5G-AKA authentication service. Our work can be divided into two tasks. We first propose the model under non-backup and backup policies, and give the formulas of DPM, the first restoration time and TCO. Then we investigate the relationships among parameters and the impact of parameters on evaluation measures.

III. MODELS OF NON-BACKUP AND BACKUP POLICIES

This section first presents the availability models under non-backup and backup policies, respectively. Then we present the methods for computing DPM and service’s first restoration time from failure in Section III-B and Section III-C, respectively. In Section III-D, we discuss how to calculate TCO. TABLE 1 gives the definition of variables to be used.
TABLE 1. Definition of variables.

| Notation | Description                                      | Value                  |
|----------|--------------------------------------------------|------------------------|
| $\lambda$ | Authentication request arrival rate              | 748.8 users/s [23]     |
| $1/\gamma$ | Mean time for failure                           | 3 days [24]            |
| $1/\delta$ | Mean time for failure detection                 | 1 sec [25]             |
| $1/\tau$  | Mean time for recovery                          | 15 sec [25]            |
| $1/\tau_f$ | Mean time for failover                         | 2 sec [25]             |
| $T_{a}, T_{b}, T_{c}$ | The time to the absorbing state                  |                        |
| $F_{a}(t)$ | The cumulative distribution function for $T_{a}$ |                        |
| $n_{i}$  | The number of SEAF entity                       |                        |
| $C_{p}$  | The capital expenditure per SEAF entity         | $800$ $\$/               |
| $C_{c,r}$ | The capital expenditure of mean time for failure| $80$ $\$/               |
| $C_{nf}$ | The infrastructure cost                        |                        |
| $C_{e}$  | The power consumption and cooling cost in dollar per Watt-hour | $3.6 \times 10^{-4}$ $\$/Wh [26] |
| $P(x)$   | The steady state probability of having $x$ non-failed SEAF entities |                        |
| $C_{per}$ | The power consumption and cooling cost          |                        |
| $W_{c,x}$ | The power consumption with $x$ non-failed SEAF entities |                        |
| $h_{dc}$ | The idle power consumption                      | 6 Watt                 |
| $V_{dc}$ | The power consumption of a SEAF entity during its average utilization | 3 Watt               |
| $C_{o}$  | The operation cost (include detection, failover and recovery cost) per unit time after each failure | 2 $\$/                |
| $C_{op}$ | The operation cost                             |                        |
| $C_{de}$ | The penalty cost for each request not accepted by the service provider | 0.01 $\$/          |
| $C_{drop}$ | The drop cost                                  |                        |
| $L$      | The operational period                         |                        |
| TCO      | The total cost of ownership                    |                        |
| $T_{f}$  | The first restoration time into state $k$ starting from state $i$ |                        |
| $T_{r,ak}$ | The first restoration time to state $k$ starting from state $i$ |                        |

in the rest of the paper. The details of the two policies are given as follows:

**Non-backup**
- **Policy.** Under this policy, there is only one SEAF entity. When the entity fails, it will take time to detect and repair the failure. The authentication service is not provisioned to end users until the failing entity completes its repairing.

**Backup policy.** Under this policy, there are two homogeneous SEAF entities, which process the arriving authentication requests in parallel. When one fails, the failure detection is first made and then the failover [24] is applied such that the other SEAF entity can handle all arriving requests. Finally, it is repaired. During these three processes, the other SEAF entities may also fail.

A. AVAILABILITY MODELS

1) NON-BACKUP POLICY

FIGURE 3 describes the CTMC availability model for capturing one SEAF entity state transitions, namely, 5G-AKA authentication service state transition. State 0 denotes the healthy state and then all incoming authentication requests can be processed. The SEAF entity can fail at the rate $\gamma$ and then enters state 1. SEAF at state 1 is considered unavailable to work. Detecting the SEAF entity failure takes an exponentially distributed time with rate $1/\delta$. The system reaches state 2 in which recovery is initiated. The recovery time from state 2 to state 0 is exponentially distributed with rate $1/\tau$. Then we get the steady-state probabilities of three states: $\pi_0 = \left[1 + \frac{\gamma}{\delta} + \frac{\gamma}{\tau}\right]^{-1}$, $\pi_1 = \left[1 + \frac{\delta}{\gamma} + \frac{\delta}{\tau}\right]^{-1}$ and $\pi_2 = \left[1 + \frac{\tau}{\gamma} + \frac{\tau}{\delta}\right]^{-1}$, which are to be used later.

2) BACKUP POLICY

Under this policy, there are two SEAF entities processing authentication requests in parallel. FIGURE 4 shows the CTMC model for capturing the behaviors of two SEAF entities. The arrival rate is $\lambda/2$ for each SEAF entity. In this model, state 0 represents that both SEAF entities are up for handling incoming authentications. Either of them can fail with rate $1/\gamma$. When failure occurs to one of the SEAF entities, the system goes to state 1 with rate $2\gamma$, (i.e., one SEAF entity is down). The failure is detected at rate $\delta$ upon which the system enters state 2. During the failure detection, the other SEAF entity may fail. Hence, if another failure occurs before the detection of the first failure, the system goes to state 5 with rate $\gamma$. Then we get the steady-state probabilities of three states: $\pi_0 = \left[1 + \frac{\gamma}{\delta} + \frac{\gamma}{\tau}\right]^{-1}$, $\pi_1 = \left[1 + \frac{\delta}{\gamma} + \frac{\delta}{\tau}\right]^{-1}$ and $\pi_2 = \left[1 + \frac{\tau}{\gamma} + \frac{\tau}{\delta}\right]^{-1}$, which are to be used later.
State 5 represents that both SEAF entities are down. The failures are detected and the system enters state 6 with rate $\delta$. State 6 represents that both failures are detected. Since both SEAF entities have failed, two recovery processes need to be started independently with rate $\tau$. When the failures are recovered, the system enters state 0 with rate $\tau$.

In state 3, when the failure is recovered and the system enters state 0 with rate $\tau$. In addition, if another failure occurs before the recovery, the system goes to state 4 with rate $\gamma$. Eqs. (1)-(7) give the steady-state probabilities of all states, which are used later.

$$
\pi_0 = \frac{\delta(\delta + \gamma)(\tau + \gamma)\Psi}{\Psi} (1)
$$

$$
\pi_1 = \frac{2\delta(\tau + \gamma)(\tau + \gamma)\tau \gamma}{\Psi} (2)
$$

$$
\pi_2 = \frac{2\delta^2 \tau \gamma(\tau + \gamma)}{\Psi} (3)
$$

$$
\pi_3 = \frac{2\gamma \tau \delta^2}{Z} (4)
$$

$$
\pi_4 = \frac{2\tau \gamma^2(\tau + \tau + \gamma)}{\Psi} (5)
$$

$$
\pi_5 = \frac{2(\tau + \gamma)(\tau + \gamma)\tau \gamma^2}{\Psi} (6)
$$

$$
\pi_6 = \frac{2\delta \gamma^2(\tau + \tau + \gamma + \delta)(\tau + \tau + \delta + \tau f)(\tau + \tau + f)}{Z} (7)
$$

where $\Psi = (2\delta + 2\tau + \gamma)\gamma^2 + (2\tau^2 + (2\tau + 77\delta + 2\delta(\tau + \delta))\gamma^3 + (((2\tau + 58\delta + 2\delta(\tau + \delta))\gamma^3 + (2\tau^2 + 7\delta(\tau f) + 2\tau^2 f)\gamma^2 + 3\tau \delta(\tau + \delta) + \tau + \delta)^2 f + 2(\tau + \tau + f))\gamma^2 + (2\tau^2 + 5\tau + 5)\delta^2 + (5\tau^2 + 7\tau + \delta + 2\tau^2 f)\gamma^2 + 3\tau \delta((\tau f + \tau f) + \tau + \tau f)\gamma + \delta^2 \tau f \tau f$.

### B. DPM COMPUTATION

1) NON-BACKUP POLICY

This section first discusses how to calculate the number of authentication request loss per Failure and then presents DPM computation.

#### a: NUMBER OF AUTHENTICATION REQUEST LOSS PER FAILURE

We consider the ARL model shown in FIGURE 5, which is developed from FIGURE 3. It shows the state transitions after the failure occurrence. State 1 and 2 are defined as same as in FIGURE 3. State H is an absorbing state, denoting that SEAF entity has successfully recovered from failure. Define $T_d$ to denote the time to state H from state 1. From FIGURE 5, we can obtain its cumulative distribution function $F_{T_d}(t) = \pi_H(t)$, where $\pi_H(t)$ is the transient probability that the CTMC is in state H at time t. According to the Kolmogorov equation, we can get:

$$
F_{T_d}(t) = \pi_H(t) = 1 - \frac{\delta}{\delta - \tau} e^{-\tau t} + \frac{\tau}{\delta - \tau} e^{-\delta t}, t \geq 0 (8)
$$

Eq. (8) indicates that the cumulative distribution function of $T_d$ is a two stage Hypo-exponential distribution $HYPO(\delta, \tau)$. Therefore, we obtain the mean number of authentication request loss due to the SEAF entity failure as in Eq. (9):

$$
n_{no_{-}ba} = \int_0^\infty \lambda tdF_{T_d}(t) = \lambda \int_0^\infty t d\pi_H(t) = \lambda (\frac{1}{\delta} + \frac{1}{\tau}) (9)
$$

#### b: DPM COMPUTATION

The failure frequency of the availability model in FIGURE 3 is $f = \pi_0 \gamma$, where $\pi_0 = [1 + \frac{\gamma}{\delta} + \frac{\gamma}{\tau}]^{-1}$ is the probability of SEAF in state 0. With the definition of $DMP = f \cdot n_{no_{-}ba} \frac{10^6}{\lambda}$ given in [25], we get the DPM caused by SEAF failure as in Eq. (10):

$$
DPM = \frac{10^6 \gamma(\tau + \delta)}{\delta \tau + \tau \gamma + \delta \gamma} (10)
$$

2) BACKUP POLICY

When one SEAF entity fails, the system goes to state 1 in FIGURE 4. Subsequently, three scenarios may occur:

- (S1). Only one SEAF entity fails (with probability $\delta(\gamma + \delta)$): the transition follows 1→2→3;

- (S2). The other SEAF entity fails before completing the detection of the first failure (with probability $\gamma(\gamma + \delta)$): the transition follows 1→5→6→0;

- (S3). The other SEAF entity fails before the recovery of the first failure (with probability $[\delta(\gamma + \delta)] \cdot [\gamma(\gamma + \delta)] \cdot [\gamma(\gamma + \delta)]$: the transition follows 1→2→4→6→0 or 1→2→3→4→6→0.

The authentication losses in these three scenarios are different and hence we compute the authentication loss for these three scenarios separately and then combine them in the total DPM computation. We also find that the sojourn time for the system in state 1 is exponentially distributed with parameter $\delta + \gamma$, based on which FIGURE 6 and FIGURE 7 are constructed.

The rest of this section first discusses how to calculate the number of authentication request loss per failure and then presents DPM computation.
To compute the mean number of newly arriving authentication request loss due to one SEAF entity failure, we consider the CTMC ARL models shown in FIGURE 6, FIGURE 7, FIGURE 8 and FIGURE 9, which illustrate the state transitions. \( H_1 \) is an absorbing state, which is obtained by merging states 0 and 3 from model in FIGURE 4. \( H_2, H_3 \) and \( H_4 \) are the absorbing states, which are the states obtained by merging state 0 from model in FIGURE 4.

We assume that the first failure occurs at time 0. Hence the system of FIGURE 4 enters state 1 in scenario (S1). The cumulative distribution function of \( T_{d1} \) can be computed in the way similar to that of non-backup policy. Thus, we can obtain:

\[
F_{T_{d1}}(t) = 1 - \frac{\delta + \gamma}{(\delta + \gamma) - \tau f} e^{-\gamma t} + \frac{\tau f}{(\delta + \gamma) - \tau f} e^{-(\delta + \gamma)t}, \quad t \geq 0 \quad (11)
\]

With Eq. (11), we can calculate the mean number of authentication request loss due to one SEAF entity failure in Eq. (12).

\[
n_{ba1} = \int_0^\infty \frac{\lambda}{2} t dF_{T_{d1}}(t) = \frac{\lambda}{2} \left( \frac{1}{\delta + \gamma} + \frac{1}{\tau f} \right) \quad (12)
\]

So the mean number \( n_{sc1} \) of authentication request loss for scenario (S1) can be computed as in Eq. (13).

\[
n_{sc1} = \frac{\delta}{\gamma + \delta} n_{ba1} \quad (13)
\]

We assume that the first failure occurs at time 0. Hence the system of FIGURE 4 enters state 1 in scenario (S2). The cumulative distribution function of \( T_{d21} \) can be computed from the CTMC in the way similar to that of non-backup policy. Eq. (14) describes \( F_{T_{d21}}(t) \).

\[
F_{T_{d21}}(t) = 1 + \frac{\delta}{\gamma} \frac{t}{\tau - (\delta + \gamma)} e^{-(\delta + \gamma)t} - \frac{\delta + \gamma}{\gamma} \frac{\tau}{\tau - \delta} e^{-\delta t} - \frac{\delta + \gamma}{\delta - (\delta + \gamma) - \tau} e^{-\tau t}, \quad t \geq 0 \quad (14)
\]

Eq. (14) indicates that the cumulative distribution function of \( T_{d21} \) is a three-stage Hypo-exponential distribution \( HYPO((\delta + \gamma), \delta, \tau) \). We then can compute the mean number \( n_{ba21} \) of authentication request loss due to the SEAF entity failure as in Eq. (15).

\[
n_{ba21} = \int_0^\infty \frac{\lambda}{2} t dF_{T_{d21}}(t) \quad (15)
\]

If the second failure occurs at time 0, the system of FIGURE 4 enters state 5 in scenario (S2). The cumulative distribution function for \( T_{d22} \) can be computed as in Eq. (16):

\[
F_{T_{d22}}(t) = 1 - \frac{\delta}{\delta - \tau} e^{-\tau t} + \frac{\tau}{\delta - \tau} e^{-\delta t}, \quad t \geq 0 \quad (16)
\]

The mean number \( n_{ba22} \) of authentication request loss due to the SEAF entity failure is computed in Eq. (17).

\[
n_{ba22} = \int_0^\infty \frac{\lambda}{2} t dF_{T_{d22}}(t) = \frac{\lambda}{2} \left( \frac{1}{\delta} + \frac{1}{\tau} \right) \quad (17)
\]

Eq. (18) gives the mean number \( n_{sc2} \) of authentication request loss for scenario (S2).

\[
n_{sc2} = \frac{\gamma}{\gamma + \delta} (n_{ba21} + n_{ba22}) \quad (18)
\]

If the second failure occurs at time 0, the system of FIGURE 4 enters state 4 in scenario (S3). The cumulative distribution function of \( T_{d3} \) can be computed as in Eq. (19).

\[
F_{T_{d3}}(t) = 1 - \frac{\delta}{\delta - \tau} e^{-\tau t} + \frac{\tau}{\delta - \tau} e^{-\delta t}, \quad t \geq 0 \quad (19)
\]

We get the mean number \( n_{ba3} \) of authentication request loss due to the SEAF entity failure in Eq. (20) and then obtain the mean number of authentication request loss for scenario (S3) as in Eq. (21)

\[
n_{ba3} = \int_0^\infty \frac{\lambda}{2} t dF_{T_{d3}}(t) = \frac{\lambda}{2} \left( \frac{1}{\delta} + \frac{1}{\tau} \right) \quad (20)
\]

\[
n_{sc3} = \frac{\gamma}{\gamma + \delta} \left( \frac{\gamma f}{\gamma + \tau f} + \frac{\gamma}{\gamma + \tau} \right) + \frac{\tau f}{\gamma + \tau} \quad (21)
\]
The failure frequency of the availability model in FIGURE 4 is $f = \pi_0 2 \gamma$, where $\pi_0 = \frac{(\delta + \gamma)(\tau_f + \gamma)(\tau_f + \gamma)}{\psi}$ is the probability that the system is in state 0. We get DPM caused by the SEAF entity failure as in Eq. (22).

$$DPM = f \cdot n_{ba} \frac{10^6}{\lambda}$$

$$= \pi_0 2 \gamma (n_{sc1} + n_{sc2} + n_{sc3}) \frac{10^6}{\lambda}$$

$$= \pi_0 2 \gamma (\frac{\delta}{\gamma + \delta} n_{ba1} + \frac{\gamma}{\gamma + \delta} (n_{ba21} + n_{ba22})) \frac{10^6}{\lambda}$$

$$+ \pi_0 2 \gamma (\frac{\delta}{\gamma + \delta} + \frac{\tau_f}{\gamma + \tau_f} + \frac{\gamma}{\gamma + \tau_f}) n_{ba3} \frac{10^6}{\lambda}$$

(22)

### C. The First Restoration Time of Authentication Service from Failure

The first restoration time for authentication service is crucial. Providers can make that the service is recovered faster to its healthy state (i.e., state 0) via configuring parameters (e.g., mean time for recovery) after the failure occurring, which causes the increasing of the associated costs. Therefore, it is necessary to analyze the first restoration time. In this section, we describe how to calculate the first restoration time under each policy.

1) Non-Backup Policy

Let $X(t)$ with finite State-Space $S_{no, ba} = \{0, 1, 2\}$ denote the system state at time $t$. Eq. (23) gives the rate matrix $R = [r_{ij}], (i, j \in S_{no, ba})$, for the CTMC model of FIGURE 3.

$$R = \begin{bmatrix}
0 & \gamma & 0 \\
0 & 0 & \delta \\
\tau & 0 & 0
\end{bmatrix}$$

(23)

The expected value of the random time at which the system passes into each of the states $\{0, 1, 2\}$ for the first time can be calculated by using first passage times of FIGURE 3. The first passage time $T_k$ into state $k$ starting from state $i$ is defined as $T_k = E(T|X(0) = i)$. Here, $E$ is the expected value, $T = \min\{t \geq 0 : X(t) = k\}$ and $k \in S_{no, ba}$.

Define $t_{i \to k} = E[T_k|X(0) = i]$ to denote the mean time for the first passage from $i$ to $k$. Here, $k \in S_{no, ba}$. For each $k$, the first passage time for FIGURE 3 satisfies the equation

$$r_{i k} t_{i \to k} = 1 + \sum_{j \in S_{no, ba} \not= i} (r_{ij} \cdot t_{j \to k}), i \not= k$$

[27]. Here, $i \in S_{no, ba}$ and $r_1 = \sum_{i \in S_{no, ba}} r_{1i}$.

State 0 denotes the healthy state and Eq. (24) gives the calculation of the first restoration time of the model of FIGURE 3. The detailed derivation processes are given in Appendix A-1.

$$\begin{cases}
\delta t_{1 \to 0} = 1 + \delta t_{2 \to 0} \\
\tau t_{2 \to 0} = 1
\end{cases}$$

(24)

By solving Eq. (24), we get $t_{1 \to 0} = \frac{\delta + \tau}{\delta}$ and $t_{2 \to 0} = \frac{1}{\tau}$, denoting the first restoration time to state 0 starting from states 1 and 2 respectively.

2) Backup Policy

Let $X(t)$ with finite State-Space $S_{ba} = \{0, 1, 2, \ldots, 6\}$ denote the state of the system at time $t$. Eq. (25) describes the rate matrix $R = [r_{ij}], i \in S_{ba}, j \in S_{ba}$ for the CTMC of FIGURE 4.

$$R = \begin{bmatrix}
0 & 2 \gamma & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \delta & 0 & 0 & \gamma & 0 \\
0 & 0 & 0 & \tau_f & \gamma & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \delta \\
0 & 0 & 0 & 0 & 0 & 0 & \delta \\
\tau & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

(25)

The expected value of the random time at which the system passes into each of the states $\{0, 1, 2, \ldots, 6\}$ for the first time can be calculated by using first passage times of FIGURE 4. Therefore, the first restoration time for state 0 will be as Eq. (26) in the model of FIGURE 4, and the detailed derivation processes are given in Appendix A-2.

$$\begin{cases}
(\delta + \gamma) t_{1 \to 0} = 1 + \delta t_{2 \to 0} + \gamma t_{3 \to 0} + \gamma t_{4 \to 0} + \gamma t_{5 \to 0} + \gamma t_{6 \to 0} \\
(\tau_f + \gamma) t_{2 \to 0} = 1 + \tau_f t_{3 \to 0} + \gamma t_{4 \to 0} + \gamma t_{5 \to 0} + \gamma t_{6 \to 0} \\
(\tau + \gamma) t_{3 \to 0} = 1 + \gamma t_{4 \to 0} + \gamma t_{5 \to 0} + \gamma t_{6 \to 0} \\
\delta t_{4 \to 0} = 1 + \delta t_{6 \to 0} \\
\delta t_{5 \to 0} = 1 + \delta t_{6 \to 0} \\
\tau t_{6 \to 0} = 1
\end{cases}$$

(26)

By solving Eq. (26), we get Eqs. (27) - (32):

$$t_{1 \to 0} = \frac{(\gamma^2 + (\tau + \delta + \gamma) \gamma^2 + (\tau + \gamma) \delta + \tau \gamma)}{\delta \tau (\tau_f + \gamma)(\tau + \gamma)}$$

(27)

$$t_{2 \to 0} = \frac{(\delta + \gamma)(\tau_f + \gamma)(\tau + \gamma)}{\delta \tau (\tau_f + \gamma)(\tau + \gamma)}$$

(28)

$$t_{3 \to 0} = \frac{\delta \tau + \gamma \delta + \gamma \tau}{\delta \tau (\tau + \gamma)}$$

(29)

$$t_{4 \to 0} = \frac{\delta + \tau}{\delta \tau}$$

(30)

$$t_{5 \to 0} = \frac{\delta \tau + \gamma \tau}{\delta \tau}$$

(31)

$$t_{6 \to 0} = \frac{1}{\tau}$$

(32)

where $t_{1 \to 0}$, $t_{2 \to 0}$, $t_{3 \to 0}$, $t_{4 \to 0}$, $t_{5 \to 0}$ and $t_{6 \to 0}$ are the first restoration times to state 0 starting from states 1, 2, 3, 4, 5 and 6 respectively.

### D. Total Cost of Service Provider (TCO)

High availability for 5G-AKA protocol is crucial. A few minutes of service failure can cause a large loss of revenue and
business reputation. While providers try to achieve reduce DPM (or reduce the first restoration time) via several means (e.g., recovery strategies), the associated costs also increase. Hence, understanding the trade-offs between cost and DPM is an important issue. In this section, we describe our assumptions in terms of cost components and show how to compute them using the ARL model.

We define different components for TCO, as follows:

- Infrastructure Cost \( C_{\text{inf}} \). Define \( n_s \) as the number of SEAF entities in service, \( C_s \) ($/hr) as the capital expenditure (CapEx) per SEAF entity and \( C_{s,y} \) ($) as the capital expenditure of mean time for failure. We define the infrastructure cost as \( C_{\text{inf}} = n_s \cdot (C_s + C_{s,y} \cdot \frac{x}{2}) \).

- Power Consumption and Cooling Cost \( C_{\text{pow}} \). Define \( C_p \) ($/Wh) as the power consumption and cooling cost in dollar per Watt-hr, and \( p(x) \) as the steady state probability with \( x \) non-failed SEAF entities in service. The power consumption and cooling cost \( C_{\text{pow}} \) ($) [28] over the operational period \( L \) (hr) is defined as \( C_{\text{pow}} = \sum_{x=0}^{\infty} p(x)W_p(x) \cdot C_p \cdot L \). Here \( W_p(x) \) (Watt) is the power consumption with \( x \) non-failed SEAF entities in service. When there are \( x \) SEAF entities running simultaneously on service, the reward rate of each state of CTMC is \( h_{\text{idle}} + x \cdot v_s \), where \( h_{\text{idle}} \) (Watt) is the idle power consumption and \( v_s \) is the power consumption of a SEAF entity during its average utilization. If there are \( n_s \) SEAF entities, we define power consumption in \( x \) non-failed SEAF entities as \( W_p(x) = n_s \cdot (h_{\text{idle}} + x \cdot v_s) \) [29].

- Operation Cost \( C_{\text{ope}} \). Let \( C_o \) ($/hr) be the operation cost (include detection, failover and recovery cost) per unit time after each failure. With \( C_o \), we can compute the operation cost \( C_{\text{ope}} = C_o \cdot \gamma \cdot (L/24) \cdot t \). Here, \( t = \sum_{i \in S} t_{i \to 0} p_i \), \( S \) is finite State-Space without state 0, and \( p_i = \pi_i \sum_{j \in S} \pi_j \).

- Drop Cost \( C_{\text{dro}} \). Let \( C_d \) ($/hr) be the penalty cost for an authentication request is dropped. With \( C_d \), the formula for computing the drop cost \( C_{\text{dro}} \) ($) during the operational period \( L \) as \( C_{\text{dro}} = C_d \cdot \rho_{\text{dro}} \cdot \lambda \cdot L \cdot 3600 \), where \( \rho_{\text{dro}} = \text{DPM} / 10^6 \).

- TCO. TCO ($) can be computed as: \( C_{\text{TCO}} = C_{\text{inf}} + C_{\text{pow}} + C_{\text{ope}} + C_{\text{dro}} \).

### IV. NUMERICAL ANALYSIS

This section aims to compare two policies in terms of DPM, the first restoration time and TCO. Default values of the model parameters are summarized in TABLE 1 for numerical analysis. Several default values are set according to [23]–[26]. Numerical analysis is conducted on MAPLE [30]. The results and discussions of DPM computation, the first restoration time and TCO are presented in Section IV-A, IV-B and IV-C, respectively.

#### 1) Effect of Failure Rate (1/\( \rho \))

\( 1/\rho \) varies from 1 to 6 days and let \( 1/\delta = 1 \) sec and \( 1/\tau_f = 2 \) sec. FIGURE 10 (a) and (b) show the results of DPM over \( \gamma \) under two policies. More explanations of results are given as follows.

FIGURE 10 shows that DPM decreases with the increasing \( 1/\rho \), and increases with the increasing \( 1/\tau \) under both policies. We illustrate these phenomena by taking an example of FIGURE 10 (a). The reason is that the SEAF entity is less prone to failure and then DPM decreases when the failure time \( 1/\rho \) increases. \( \text{DPM}_{(\rho)} = 10^6 f (\tau + \delta) \), so \( (\text{DPM}_{(\rho)})' = 10^6 f (\rho + \delta) \). \( \gamma \) plays a decisive role due to the existence of the square, so there is always \( (\text{DPM}_{(\rho)})' > 0 \), i.e., the DPM decreases with the increasing \( 1/\rho \).

FIGURE 10 shows that the DPM under backup policy is much smaller than under non-backup policy for each \( \gamma \). The reason is that there are two SEAF entities in backup policy, which leads to fewer authentications being dropped. Thus, DPM under backup policy is less than DPM under non-backup policy.

#### 2) Effect of Failure Detection Rate (\( \delta \)) and Recovery Rate (1/\( \tau_f \))

\( 1/\delta \) varies from 1 to 3 sec and \( 1/\tau_f \) varies from 10 to 20 sec. Let \( 1/\gamma = 3 \) days and \( 1/\tau_f = 2 \) sec. FIGURE 11 (a) and (b) show the impact of \( \delta \) and \( \tau \) on DPM computation under each policy, respectively.

From FIGURE 11 (a), we observe:

- FIGURE 11 (a) shows that the increasing \( 1/\delta \) results in the increasing DPM under non-backup policy. This is...
because the failure is detected slowly. Then, the time from failure to recovery is longer. Therefore, $DPM = 10^6 \gamma (\tau + \delta)$, so $(DPM(\delta))' = \frac{-10^6 \gamma^2}{(\delta + \tau + \gamma + \delta)^2}$. $\delta$ plays a decisive role due to the existence of the square, so there is always $(DPM(\delta))' < 0$, i.e., the $DPM$ increases with the increasing $1/\delta$.

- FIGURE 11 (a) shows that the increasing $1/\tau$ results in the increase of $DPM$ under non-backup policy. This is because the failure is recovered slowly. The time from failure to recovery is longer. Therefore, $DPM$ increases with the increasing $1/\tau$. $DPM = 10^6 \gamma (\tau + \delta)$, so $(DPM(\tau))' = \frac{-10^6 \delta^2 \gamma}{(\delta + \tau + \gamma + \delta)^2}$. $\tau$ performs a decisive role due to the existence of the square, so there is always $(DPM(\tau))' < 0$, i.e., the $DPM$ increases with the increasing $1/\tau$.

From FIGURE 11 (b), we observe:
- FIGURE 11 (b) shows that the increasing $1/\delta$ results in the increasing of $DPM$ under non-backup policy. This is due to $(DPM(\delta))' < 0$, i.e., $DPM$ increases with the increasing $1/\delta$.
- FIGURE 11 (b) shows that the increasing $1/\tau$ results in the increasing of $DPM$ under backup policy. This is due to $(DPM(\tau))' < 0$, $DPM$ increases with the increasing $1/\tau$.

**B. THE FIRST RESTORATION TIME**

This section presents the first restoration time by varying $\tau$. $1/\tau$ varies from 10 to 20 sec. Let $1/\gamma = 3$ days, $1/\delta = 1$ sec and $1/\tau_f = 2$ sec. FIGURE 12 shows the first restoration time under each policy, respectively. More explanations of results are given as follows.

FIGURE 12 shows that the first restoration time increases with the increasing $1/\tau$ under each policy. The reason for non-backup policy is that with mean time for recovery $1/\tau$ increases, the time from failure to recovery is longer, so the time into state 0 from state 1, state 2 and other states are increases. Therefore, the first restoration time increases with the increasing $1/\tau$.

Under each policy, with the increasing $1/\tau$, the first restoration times into state 0 from other states are almost different. The first restoration time from state 1 to state 0 is always higher than the first restoration time of other states to state 0. The reason is that the system enters state 1 and then enters other states for fixed $1/\tau$ when one failure occurs. So the first restoration time from state 1 to state 0 is higher than the first restoration time from other states to state 0.

**C. THE TOTAL COST OF OWNERSHIP (TCO)**

Section IV-A and IV-B analyze the $DPM$ and the first restoration time under two policies. According to $DPM$ and the first restoration time, we analyze the TCO below.

1) EFFECT OF FAILURE RATE ($\gamma$)

The parameter settings are the same as in Section IV-A-1). In order to better reflect the impact of a policy on TCO, we set $L = 70$ hours under non-backup policy and $L = 700$ hours under backup policy. FIGURE 13 (a) and (b) show the results of TCO under each policy for each $\gamma$, respectively.

FIGURE 13 (a) and (b) show that the TCO decreases first and then increases with the increasing $1/\gamma$. The reason is explained by using FIGURE 14 with $1/\tau = 15$ sec. $C_{TCO}$ is composed of four elements: (i) $C_{inf}$, denoted as “$C_{inf}$” in FIGURE 14, represents the infrastructure cost.
(ii) $C_{\text{pow}}$ represents the power consumption and cooling cost. Note that $C_{\text{pow}}$ is very small and then it is not considered in the following. (iii) $C_{\text{ope}}$, denoted as “$C_{\text{ope}}$” in FIGURE 14, represents the operation cost. (iv) $C_{\text{dro}}$, denoted as “$C_{\text{dro}}$” in FIGURE 14, represents the drop cost.

From FIGURE 14 (a), we observe:

- When $1/\gamma$ is less than 2 and $1/\tau$ is fixed, “$C_{\text{inf}}$” increases and “$C_{\text{ope}}$” decreases slowly with the increasing $1/\gamma$. And “$C_{\text{dro}}$” decreases and plays a dominant role in decreasing TCO with the increasing $1/\gamma$. The reason is that the failure rate decreases when $1/\gamma$ increases. Then, the SEAF entity is less prone to failure, which leads to the number of authentication requests being dropped decreases, i.e., “$C_{\text{dro}}$” decreases. But the margin of “$C_{\text{dro}}$” decrease is greater than that of “$C_{\text{inf}}$” increase. Therefore, TCO decreases with the increasing $1/\gamma$.

- When $1/\gamma$ is more than 2 and $1/\tau$ is fixed, “$C_{\text{ope}}$” decreases slowly and “$C_{\text{dro}}$” decreases with the increasing $1/\gamma$. And “$C_{\text{inf}}$” increases and plays a dominant role in increasing TCO with the increasing $1/\gamma$. The reason is that the margin of “$C_{\text{inf}}$” increase is greater than that of “$C_{\text{dro}}$” decrease. So TCO increases with the increasing $1/\gamma$.

From FIGURE 14 (b), we observe:

- When $1/\gamma$ is less than 3 and $1/\tau$ is fixed, “$C_{\text{inf}}$” increases with the increasing $1/\gamma$. And “$C_{\text{dro}}$” and “$C_{\text{ope}}$” also decrease and play a dominant role in decreasing TCO with the increasing $1/\gamma$. The reason is that the failure rate decreases when $1/\gamma$ increases. Then, the SEAF entity is less prone to failure, which leads to the number of authentication requests being dropped decreases. Thus, the drop cost and operation cost decrease. But the margin of “$C_{\text{dro}}$” and “$C_{\text{ope}}$” decrease is greater than that of “$C_{\text{inf}}$” increase. Therefore, TCO decreases with the increasing $1/\gamma$.

- When $1/\gamma$ is more than 3 and $1/\tau$ is fixed, “$C_{\text{dro}}$” and “$C_{\text{ope}}$” decrease with the increasing $1/\gamma$. But “$C_{\text{inf}}$” increases and plays a dominant role in increasing TCO with the increasing $1/\gamma$. The reason is that the margin of “$C_{\text{inf}}$” increase is greater than that of
“C_dro” and “C_ope” decrease. Thus, TCO increases with the increasing $1/\tau$.

2) EFFECT OF FAILURE DETECTION RATE ($\delta$) AND RECOVERY RATE ($\tau$)

The parameter settings are the same as in Section IV-A-2. We set $L = 700$ hours under two policies. FIGURE 15 (a) and (b) show the impact of $\delta$ and $\tau$ on TCO under non-backup policy and backup policy, respectively.

FIGURE 15 shows that the TCO increases with both the increase of $1/\delta$ and $1/\tau$ no matter which policy is applied. We first explain the reason of non-backup policy by using FIGURE 16(a) of $1/\delta = 1$ sec. From FIGURE 16(a), we can observe that with the increasing $1/\tau$, “C_inf” is unchanged and “C_ope” and “C_dro” increase. The reason is that, with the increasing $1/\tau$, the time from the failure state of the SEAF entity to its healthy state increases. Hence, “C_ope” increases. The time from the state of failure occurrence to healthy state increases, which leads to the number of authentication requests being dropped increases, i.e., “C_dro” increases. Therefore, TCO increases with the increasing $1/\tau$.

Now we explain the results of backup policy by using FIGURE 16(b) of $1/\delta = 1$ sec. From FIGURE 16(b), we can observe that with the increasing $1/\tau$, “C_inf” is unchanged and “C_ope” increases. And “C_dro” increases slowly with the increasing $1/\tau$. The reason is that there are two SEAF entities in backup policy. With the increasing $1/\tau$, the number of authentication requests being dropped increases slowly. So “C_dro” increases slowly. Therefore, TCO increases with the increasing $1/\tau$.

V. CONCLUSION AND FUTURE WORK

This paper explores analytical modeling approaches to quantitatively analyze the dependability of 5G-AKA authentication service. We first present the availability models under non-backup and backup policies, respectively. Then we present the methods for computing DPM and service’s first restoration time from failure. Finally, we discuss the TCO, including infrastructure cost, power consumption and cooling cost, operation cost and drop cost. Extensive numerical analyses are applied to illustrate the impact of various parameters on DPM, the first restoration time and TCO.

This paper assumes that all time intervals are exponentially distributed. Future work will relax this assumption and explore the semi-Markov process that the time intervals follow general distributions in order to make the models better capture the operational details of the 5G-AKA authentication services when facing the service failure. In addition, recover policy can affect the authentication service availability. We plan to consider the recovery policy in our model. Finally, we will extend our model to the simultaneous failure of multiple entities.

APPENDIX

THE FIRST RESTORATION TIME OF AUTHENTICATION SERVICE FROM FAILURE

3) NON-BACKUP POLICY

We can get $k = 0$ according to the first restoration time for state 0. Based on Eq. (23) and $r_{i:i\rightarrow k} = 1 + \sum_{j\in S_{no,ba}, j\neq i} (r_{i,j} \cdot t_{j\rightarrow k})$, $i \neq k$ [27], where $i \in S_{no,ba} = \{0, 1, 2\}$ and $r_1 = \sum_{l\in S_{no,ba}} r_{1,l}$.

- When $i = 1$, $r_1 = \sum_{l\in S_{no,ba}} r_{1,l} = \delta$, so we can get $\delta t_{1\rightarrow 0} = 1 + \delta t_{2\rightarrow 0}$.
- When $i = 2$, $r_2 = \sum_{l\in S_{no,ba}} r_{2,l} = \tau$, so we can get $\delta t_{1\rightarrow 0} = 1 + \delta t_{2\rightarrow 0}$.

Therefore in the model of FIGURE 3, the first restoration time for state 0 will be as follows:

$$
\begin{align*}
\delta t_{1\rightarrow 0} &= 1 + \delta t_{2\rightarrow 0} \\
\tau t_{2\rightarrow 0} &= 1
\end{align*}
$$

(A.1)

4) BACKUP POLICY

We can get $k = 0$ according to the first restoration time for state 0. Based on Eq. (25) and $r_{i:i\rightarrow k} = 1 + \sum_{j\in S_{ba}, j\neq i} (r_{i,j} \cdot t_{j\rightarrow k})$, $i \neq k$ [27], where $i \in S_{ba} = \{0, 1, 2, \ldots, 6\}$ and $r_1 = \sum_{l\in S_{ba}} r_{1,l}$.

- When $i = 1$, $r_1 = \sum_{l\in S_{ba}} r_{1,l} = \delta + \gamma$, so we can get $(\delta + \gamma) t_{1\rightarrow 0} = 1 + \delta t_{2\rightarrow 0} + \gamma t_{5\rightarrow 0}$.
- When $i = 2$, $r_2 = \sum_{l\in S_{ba}} r_{2,l} = \gamma + \tau$, so we can get $(\tau + \gamma) t_{2\rightarrow 0} = 1 + \gamma t_{3\rightarrow 0} + \gamma t_{4\rightarrow 0}$.
- When $i = 3$, $r_3 = \sum_{l\in S_{ba}} r_{3,l} = \tau + \gamma$, so we can get $(\tau + \gamma) t_{3\rightarrow 0} = 1 + \gamma t_{4\rightarrow 0}$.
- When $i = 4$, $r_4 = \sum_{l\in S_{ba}} r_{4,l} = \delta$, so we can get $\delta t_{4\rightarrow 0} = 1 + \delta t_{6\rightarrow 0}$.
- When $i = 5$, $r_5 = \sum_{l\in S_{ba}} r_{5,l} = \delta$, so we can get $\delta t_{5\rightarrow 0} = 1 + \delta t_{6\rightarrow 0}$.
- When $i = 6$, $r_6 = \sum_{l\in S_{ba}} r_{6,l} = \tau$, so we can get $\tau t_{6\rightarrow 0} = 1$. 

FIGURE 16. Detailed effect of recovery rate ($\tau$).
Therefore in the model of FIGURE 3, the first restoration time for state 0 will be:

\[
\begin{align*}
(\delta + \gamma)\tau_{1-0} & = 1 + \delta t_{2-0} + \gamma t_{5-0} \\
(\tau + \gamma)\tau_{2-0} & = 1 + \tau t_{3-0} + \gamma t_{4-0} \\
(\tau + \gamma)\tau_{3-0} & = 1 + \tau t_{4-0} \\
\delta t_{4-0} & = 1 + \delta t_{6-0} \\
\delta t_{5-0} & = 1 + \delta t_{6-0} \\
\tau_{6-0} & = 1
\end{align*}
\]  \hspace{1cm} (A.2)

REFERENCES

[1] J. Tang, H. Wen, K. Zeng, R.-F. Liao, F. Pan, and L. Hu, “Light-weight physical layer enhanced security schemes for 5G wireless networks,” IEEE Netw., vol. 33, no. 5, pp. 126–133, Sep. 2019.

[2] Y.-P.-E. Wang, X. Lin, A. Adhikary, A. Grovlen, Y. Sui, Y. Blankenship, A. Orsino, A. Ometov, G. Fodor, D. Moltchanov, L. Militano, S. Andreev, Y. Koucheryavy, “Effects of heterogeneous mobility on D2D- and drone-assisted mission-critical MTC in 5G,” IEEE Commun. Mag., vol. 55, no. 2, pp. 79–87, Feb. 2017.

[3] Security Architecture and Procedures for 5G System, document TS 33.501, 3rd Generation Partnership Project, 2019.

[4] C. Cremers and M. Dehnel-Wild, “Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion,” in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2019, pp. 425–431.

[5] Y. Sun, J. Cao, M. Ma, H. Li, B. Niu, and E. Liu, “Privacy-preserving device discovery and authentication scheme for D2D communication in 3GPP 5G HetNet,” in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Feb. 2019, pp. 425–431.

[6] J. Cao, P. Yu, M. Ma, and W. Gao, “Fast authentication and data transfer protocol for massive NB-IoT devices in 3GPP 5G network,” IEEE Internet Things J., vol. 6, no. 2, pp. 1561–1575, Apr. 2019.

[7] S. M. Baskaran, G. Raja, A. K. Bashir, and M. Murata, “QoS-aware frequency-based 4G+ relative authentication model for next generation LTE and its dependent public safety networks,” IEEE Access, vol. 5, pp. 21977–21991, 2017.

[8] X. Chang, T. Wang, R. J. Rodríguez, and Z. Zhang, “Modeling and analysis of high availability techniques in a virtualized system,” Comput. J., vol. 61, no. 2, pp. 180–198, Feb. 2018.

[9] S. K. Mondal, X. Yin, J. K. Muppala, J. A. Lopez, and K. S. Trivedi, “Defects per million computation in service-oriented environments,” IEEE Trans. Services Comput., vol. 8, no. 1, pp. 32–46, Jan. 2015.

[10] V. G. Kulkarn, Introduction to Modeling and Analysis of Stochastic Systems, 2nd ed. Berlin, Germany: Springer, 2012.

[11] R. Ghosh, V. K. Naik, and K. S. Trivedi, “Stochastic model driven capacity planning for an infrastructure-as-a-service cloud,” IEEE Trans. Services Comput., vol. 7, no. 4, pp. 667–680, Oct. 2014.

[12] A. B. M. Baskaran, G. Raja, A. K. Bashir, and M. Murata, “QoS-aware Secure Comput.,” vol. 33, no. 5, pp. 126–133, Sep. 2019.

[13] R. Ghosh, F. Longo, R. Xia, V. K. Naik, and K. S. Trivedi, “Power-performance trade-offs in IaaS cloud: A scalable analytic approach,” in Proc. IEEE/ACM 41st Int. Conf. Dependable Syst. Netw. Workshops (DSN-W), Jun. 2011, pp. 152–157.

[14] Maplesoft. (2019). The Essential Tool for Mathematics. [Online]. Available: http://www.maplesoft.com/products/maple

- LILI JIANG is currently pursuing the Ph.D. degree with the School of Computer and Information Technology, Beijing Jiaotong University. Her research interests include edge/cloud computing and performance modeling.

- XIAOLIN CHANG (Member, IEEE) is currently a Professor with the School of Computer and Information Technology, Beijing Jiaotong University. Her current research interests include edge/cloud computing, network security, and security and privacy in machine learning.

- JING BAI is currently pursuing the Ph.D. degree with the Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University. Her research interest includes software reliability and availability.
JELENA MIŠIĆ is currently a Professor of computer science with Ryerson University, Toronto, ON, Canada. She has published four books, over 125 articles in archival journals, and more than 190 articles with international conferences in the areas of computer networks and security. She is a member of ACM. She serves on the editorial boards of the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, the IEEE INTERNET OF THINGS JOURNAL, the IEEE Network, Computer Networks, and Ad hoc Networks.

VOJISLAV MIŠIĆ (Senior Member, IEEE) is currently a Professor of computer science with Ryerson University, Toronto, ON, Canada. He is a member of ACM. He serves on the editorial boards of the IEEE TRANSACTIONS ON CLOUD COMPUTING, Ad hoc Networks, Peer-to-Peer Networking and Applications, and the International Journal of Parallel, Emergent and Distributed Systems.

ZHI CHEN is currently pursuing the Ph.D. degree with the Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University. His research interests include cloud computing, information security, and moving target defense.

* * *