

Retraction

Retracted: A Novel Variable Pseudonym Scheme for Preserving Privacy User Location in 5G Networks

Security and Communication Networks

Received 31 October 2023; Accepted 31 October 2023; Published 1 November 2023

Copyright © 2023 Security and Communication Networks. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

- (1) Discrepancies in scope
- (2) Discrepancies in the description of the research reported
- (3) Discrepancies between the availability of data and the research described
- (4) Inappropriate citations
- (5) Incoherent, meaningless and/or irrelevant content included in the article
- (6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.






The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

- [1] M. M. Saeed, R. A. Saeed, R. A. Mokhtar, H. Alhumyani, and E. S. Ali, "A Novel Variable Pseudonym Scheme for Preserving Privacy User Location in 5G Networks," *Security and Communication Networks*, vol. 2022, Article ID 7487600, 11 pages, 2022.

Research Article

A Novel Variable Pseudonym Scheme for Preserving Privacy User Location in 5G Networks

Mamoon M. Saeed ¹, Rashid A. Saeed ², Rania A. Mokhtar ², Hesham Alhumyani ², and Elmustafa Sayed Ali ³

¹Communications and Electronics Engineering Department, Faculty of Engineering, University of Modern Sciences, Sanaa, Yemen

²Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

³Department of Electrical and Electronics Engineering, Faculty of Engineering, Red Sea University, Port Sudan, Sudan

Correspondence should be addressed to Elmustafa Sayed Ali; elmustafasayed@gmail.com

Received 8 January 2022; Revised 28 January 2022; Accepted 25 February 2022; Published 30 March 2022

Academic Editor: Muhammad Arif

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

Due to the development in 5G mobile communications, user privacy becomes the main challenge, especially with the multiplicity of services and applications that can be accessed. Location privacy is related to the user privacy in terms of the possibility of tracking and unwanted advertisements, as well as the possibility of exposure to suspicious activities and terrorist attacks based on the user location. Accordingly, previous mobile systems use pseudonyms instead of a permanent identity to preserving the user's location privacy in mobile networks, by what is known as the Cellular Radio Network Temporary Identifiers (C-RNTIs). The C-RNTI protects the user privacy relatively, but it faces some problems due to the clear text of the user in CRNI exchange, which will make the user easily trackable by man-in-the-middle attack. This article aims at proposing a new algorithm that improves the user's location privacy and enhances the capabilities of the 5G infrastructure in terms of confidentiality and privacy. The idea is based on the use of a novel variable pseudonym (V-RNTI) algorithm that acts as a radio channel identifier for the user, which improves the allocation of pseudonyms to identify users. The proposed algorithm uses different V-RNTI values by the UE and can be changed frequently to improve the pseudonym allocation procedure. This approach can be implemented in 3GPP standard architecture by upgrading UEs and eNB by minor modifications. During this study, the proposed 5G V-RNTI authentication protocol model was built. And then, the automated analysis of the protocol model is performed by using ProVerif Model Checker. The results showed that the model works well without any noticeable problems.

1. Introduction

Because of the advantages of 5G networks such as high data rate, low latency, high capacity, and wide coverage, it has rapidly grown to become the main core network [1]. The 5G network requires an enhancement in security and privacy to ensure transferring information in a safe manner. As user privacy is the main issue in 5G networks, the location privacy is considered much more important for user privacy [2]. Recognizing the characteristics of certain services for consumers in 5G technology requires the provision of secure

network services. The privacy requirements of the 5G network may change according to the services provided by the network [3]. Meanwhile, service-oriented privacy requirements can be enabled by 5G technology. In some 5G applications, for example, in the healthcare Internet, a higher degree of privacy will be required to secure users' information. Furthermore, a higher level of privacy protection and site privacy protection may be required [3, 4]. And a lower degree of privacy may be required in other applications, such as searching for some type of location information.

In 3GPP cellular technology, the protective privacy of user location in mobile systems has received an increasing interest more particularly. By comparing previous standards for 5G cellular networks, recently proposed by 3GPP, it was found that each had improved in the security and privacy levels [5]. Although 3GPP introduced enhancing the privacy of user identity, the location privacy of the user is still vulnerable to privacy attacks [6, 7]. For instance, in 3GPP networks, various different temporary identities such as Global User Temporary Identifier (GUTI) are allocated instead of permanent identity for identifying the user in the network by the Home Subscriber Subsystem (HSS). In such networks, Mobile Management Entity (MME) uses Temporary Mobile Subscriber Identifier (TMSI) for paging users in the network [8]. And Cell Radio Network Temporary Identifier (C-RNTI) is used for user location updating in the coverage area of evolved node B (eNB).

In location updating, C-RNTI is used to a single user equipment (UE), which mitigates the location attack and protects the privacy of the user in the network [9]. However, the C-RNTI is probably to be attacked, because C-RNTI is sent in clear text and always used more than one time in the same coverage area of eNB [9, 10]. A hacker can easily trace the user and collect information about him/her. The 5G network is the first standard to benefit from location information, that is, sufficiently precise to be leveraged in the wireless network design and optimization [11]. Due to this fact, the 5G network must consider the privacy and security challenges and resist location hackers by improving the mechanism of location update, which will tend to improve user privacy [12]. This article provides a location privacy scheme to enhance the pseudonym allocation procedure for identification and user privacy protection.

The rest of the article is organized as follows. User privacy and location privacy are discussed in Section 2. Location procedure privacy issues in 5G networks are described in Section 3. In Section 4, a summary of related work is given. The proposed solution and its privacy analysis are presented in Sections 5–8. Section 9 concludes the study.

2. User and Location Privacy

In mobile communication, there are many updates and developments in user privacy and location privacy. Authentication process and location update in 3GPP are implemented between these parties: Home Subscriber Server (HSS) and UE for authentication and evolved node base station (eNB) and UE for location update (see Figure 1) [13]. The message comprises the IMSI sent to the service network by UE [14]. In authentication vector (AV), the service network (Mobile Management Entity (MME)) sends a message comprised of IMSI to the HSS.

In the first attachment, the HSS responds to AV requests by calculating the sequence number (SQN) from generating a changeable random challenge (RAND). Next, by using the network authentication function (f_1), the message authentication code (MAC) is computed by utilizing authentication management field (AMF), SQN, and RAND [15]. After that, the ciphering key (CK), the integrity key (IK), the anonymity

key (AK), and the expected response (XRES) are computed by using f_2 , f_3 , f_4 , and f_5 over RAND challenges. By XORing the authentication token (AUTN) that contains the SQN with the MAC, the AK and AMF are generated.

Finally, the HSS creates the AV, which consists of CK, IK, XRES, AUTN, and RAND. The HSS sends the AV to the MME, and then, the MME forwards the AUTN and the RAND within an authentication request to the UE and saves XRES. After that, the MME uses the TMSI to page the UE [16]. In cell coverage, the eNB uses the C-RNTI to update the location of UE. The C-RNTI is constant in the same cell coverage area, whereas it changes if the UE moves from one coverage area to another as shown in Figure 2 [17, 18].

3. User Location Issues in 5G Network

In 3GPP, the privacy of subscribers must be protected by cellular systems from risks associated with knowing subscriber's identities by attackers as a third party [7, 13]. Location tracking (LT) tracks the movements of a specific user by a third party, which is one of the main privacy challenges in 3GPP networks. In mobile systems, different temporary identities are assigned to every user equipment (UE) by serving the network during movement from one cell to another within eNB's coverage area [19]. This strategy will ensure the untraceability of users. The use of various C-RNTIs improves the performance of location tracking but does not eliminate the attacks.

The assignment of C-RNTIs to user UE is possible to be linked by an attacker. The passive attacker who is monitoring the radio channel of UE can initiate an attach procedure, which possibly links various C-RNTIs assigned to UE through eNB with permanent identity (IMSI) [20, 21]. Due to this kind of attack, the invasion of user's privacy becomes more obvious. Meanwhile, the locations visited by the target user can be recorded, and the user profile history can be saved by the attacker as shown in Figure 3.

The location tracking poses a serious threat to users' privacy. In fact, the passive attacker can attack the UE radio channel at the moment of validation. The passive attacker maintains a specific user location and keeps tracking it, while the C-RNTI is sent in plain text where attackers can violate privacy [7, 14].

4. Related Work

Many research studies have discussed location privacy in 5G networks and suggested different solutions for protecting privacy [22, 23]. A related work presented by S. Gang et al. attempts to solve the location privacy issue in 5G. The study proposed an algorithm based on a region-of-interest division to preserve the location privacy for mobile device users in location-based cyber services [24]. The algorithm generates a dummy location by considering the semantic information of those locations. The generated locations enable to exclude or reduce the exposure of a user's real location [16].

Xudong et al. proposed a location privacy method-based k-anonymity to prevent privacy disclosure in location-based encryption (LBE) constrained in incomplete

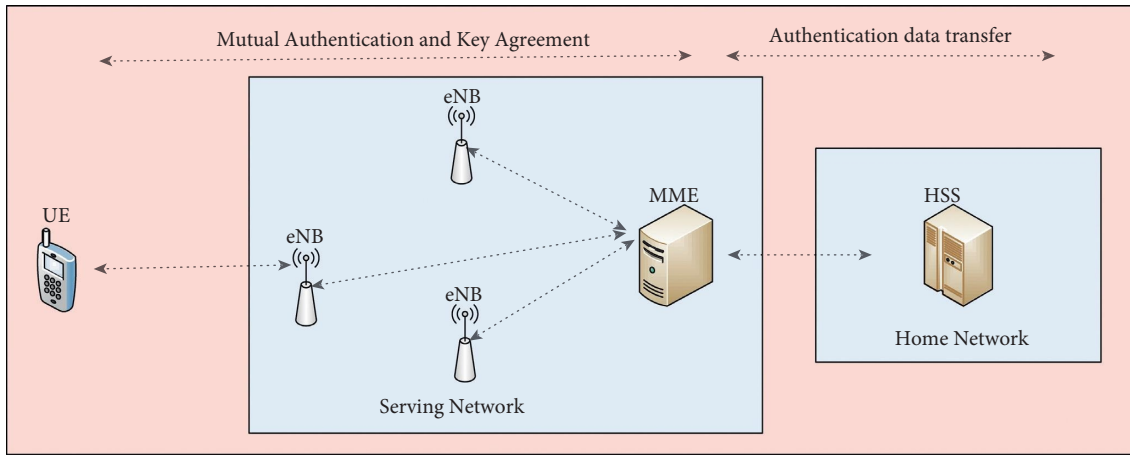


FIGURE 1: 3GPP privacy architecture.

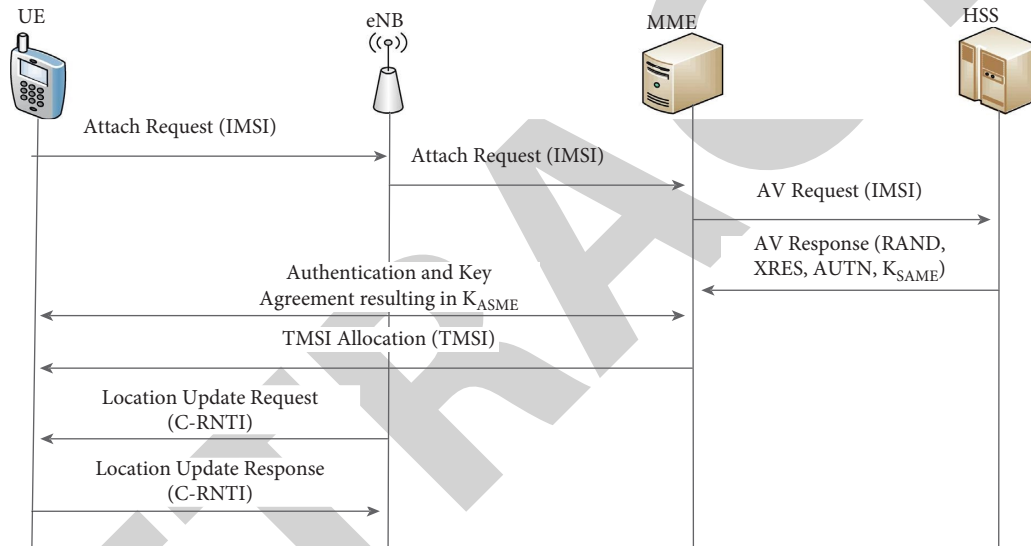


FIGURE 2: Authentication and location update in 3GPP.

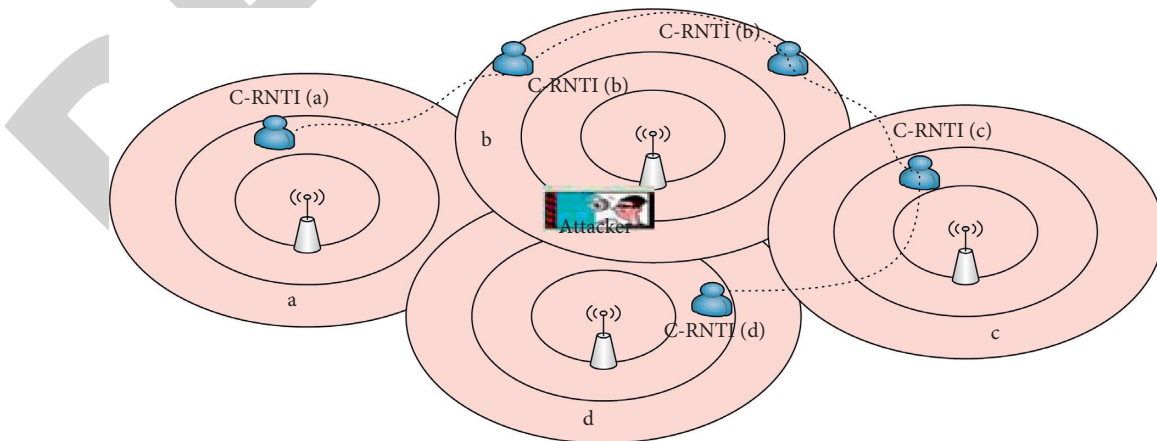


FIGURE 3: Location tracking attack using the C-RNTI.

data collection. In the process of constructing the anonymous set, and against background attacks, the proposed scheme can provide effective location privacy

protection [25, 26]. The problem of incomplete data collection of location can be solved by a constructing a method for anonymous candidate set (ACS) with

compressing sensing technology. The differential privacy mechanism to construct the anonymous set (AS) with the ACS is adapted to prevent the privacy disclosure in the process [19].

Zhongyang et al. proposed a location privacy-preserving mechanism (CKD) by combining k-anonymity and differential privacy-preserving to prevent mobile user's location privacy from being leaked. [21]. Liang et al. 2017 presented a certain cryptographic solution for security and privacy of positioning, in addition to location-based services in IoT [22, 27].

Catania and Corte investigated location privacy derived from the densification of both mobile nodes and access nodes in the context of ultradense networks. The study points that more ambiguity in the information about the node and access point in addition to time correlations reached by the opponent will make the location determining tasks more difficult [28].

Laoudias et al. 2018 reviewed the localization algorithms that need to be combined with complementary technologies including accurate height estimation. The authors present an example of three-dimensional locations, reliable user mobility classification, and efficient indoor mapping solutions to fully exploit the potential of location awareness and enable new advanced location-based services [29, 30]. They presented solutions based on wireless local area networks (WLANs) and cellular localization systems, including recent results on 5G localization, and highlighted the capability of computing 3D location in multifloor indoor environments [31]. Moreover, the authors presented estimation techniques for user mobility, which could improve tracking accuracy and localization. [32].

Hailu and Saily (2017) proposed hybrid location tracking and paging scheme where both core network and random access network are involved in location tracking and paging of radio resource channel (RRC)-inactive UEs [33].

5. Preserving Privacy Location by Using Variable Pseudonym Scheme

In the variable pseudonym scheme, a range of Variable-Radio Network Temporary Identify (V-RNTI) values enable UE to use frequently varying V-RNTI instead of fixed C-RNTI to protect against location tracking (LT) attacks [34–37]. The range of V-RNTI values is initially allocated by serving the network to each UE within eNB's coverage area. As in the standard protocol, eNB supplies UE with one V-RNTI during the RRC setup procedure [38]. The user equipment then derives from received V-RNTI minimum and maximum values of the range of V-RNTI, that is, VI_{MIN} and VI_{MAX} . The UE treats received V-RNTI as VI_{MIN} and computes VI_{MAX} from VI_{MIN} using the following equation:

$$VI_{MAX} = VI_{MIN} + \text{extract}(VI_{MIN}, 8). \quad (1)$$

The UE extracts at least 8 bits from VI_{MIN} by using function `extract` and adds the result to VI_{MIN} to yield VI_{MAX} . Subsequently, within the allocated range, a fresh V-RNTI (VI_{UE}) is generated by UE and transmitted to eNB that

included handover message request whenever UE moves between different cells within eNB's coverage area [39]. The arriving VI_{UE} value is verified by eNB in an attempt to identify UE. The UE is granted required resources if VI_{UE} verification is passed and UE has been identified; otherwise, no resource is granted to UE, and the request is discarded.

An adversary cannot track the movement of a specific UE, because the V-RNTI value that is used by UE always keeps changing [40]. The design of the proposed scheme is used to achieve security objectives without any modification imposed on any other network node except minimal modifications at two network nodes, that is, UE and eNB [23, 41, 42]. The storage capabilities and computational power of UE and eNB are considered.

This scheme ensures the unlinkability of UEs with minimal modifications at eNB, as shown below. Besides that, it introduces a negligible computation overhead at UE and an affordable computation overhead at eNB [40, 43, 44]. This scheme can easily be integrated with current mobile technology, and thus, location tracking is protected by it with a minimal cost.

6. The Enhanced Algorithm in eNB

The enhanced algorithm in eNB is extended to store three 16 bit V-RNTI values, VI_{RCV} , VI_{MIN} , and VI_{MAX} , to allocate V-RNTI for each UE. The VI_{RCV} is the V-RNTI that was last used by UE, whereas VI_{MIN} and VI_{MAX} represent the boundaries of the allocated V-RNTI range. Table 1 known as VI-table that kept by eNB, which stores values of C-RNTI for each UE in its coverage area [45–47]. A V-RNTI range allocated to one UE is contained by each entry in VI-table contains. There are two phases, setup and V-RNTI management, that can be described by the proposed scheme as shown in Table 1.

6.1. Setup Phase (the Initial Allocation). The initial V-RNTI range allocation to UEs is performed within eNB's service area. The setup phase must be completed successfully before the management phase is executed and is executed only once at the very beginning. The setup phase has many steps; the major steps are as follows:

- (i) Initialize VI-pool with V-RNTI information: to initialize VI-pool with boundaries of V-RNTI ranges [48], the `Init-VI-Pool` algorithm is run by eNB as shown in Algorithm 1.
- (ii) Allocate V-RNTI ranges to UEs: within eNB's coverage area, the `Allocate-V-RNTIRange` algorithm per each UE is run by eNB [49]. Then, to supply concerned UEs with the boundaries of their V-RNTI range (VI_{MIN} and VI_{MAX}), eNB initiates a preamble procedure toward each UE as shown in Algorithm 2. The eNB performs the following steps to allocate V-RNTI ranges to UEs:

Step 1. An empty table called VI-pool is created, which has three columns— VI_{STATUS} , VI_{MIN} , and VI_{MAX} , as shown in

TABLE 1: VI-table for UEs.

IMSI	VI_{RCV}	VI_{MIN}	VI_{MAX}
$IMSI_1$	VI_{RCV1}	VI_{MIN1}	VI_{MAX1}
...
...
$IMSI_k$	VI_{RCV_k}	VI_{MIN_k}	VI_{MAX_k}
...
...
$IMSI_m$	VI_{RCV_m}	VI_{MIN_m}	VI_{MAX_m}

Input: limits of range length MAX and MIN

- (1) Set Avail = 2^{16}
- (2) Set Stop = 0
- (3) Set $S = 0$
- (4) While Avail \geq min do
- (5) Generate a random M between MAX and MIN ($MIN \leq M \leq MAX$)
- (6) If Avail $<$ MIN then
- (7) $M = Avail$
- (8) End if
- (9) $S = Stop$;
- (10) Stop = Stop + (2/3) * M
- (11) Generate a new record at VI-pool
- (12) Insert a tuple (S, M) into new record at
- (13) VI-pool
- (14) Avail = Avail - M
- (15) end while

ALGORITHM 1: VI-Pool initialization algorithm.

Table 2. The VI_{STATUS} against each range indicates whether the range is free for use or not. Value 1 against a particular range means that range is allocated to some UE, whereas value 0 in VI_{STATUS} indicates that the corresponding V-RNTI range is free for use. The minimum and maximum V-RNTI values of V-RNTI range are stored by VI_{MIN} and VI_{MAX} , respectively.

Step 2. An ordered sequence of 16 bit V-RNTI values (ranging from 1 to 65523) is used for initializing the VI-pool table with V-RNTI range information. A set of nonoverlapping partitions called V-RNTI ranges is partitioned in the V-RNTI sequence. The VI is created from the V-RNTI sequence, and a new record is created at VI-pool, which will store the range's boundaries VI_{MIN} and VI_{MAX} for each range. Value 0 is initialized to each record field in VI_{STATUS} [50].

Step 3. The VI-table stores' boundaries of Vis intervals, which are created in Step 1. The boundaries of one VI range (VI_{MIN} and VI_{MAX}) shall be contained in a record in the VI-table. The field VI_{RCV} is initially set to zero.

Step 4. During the run of random access procedure, randomly not-in-use VI range from VI-pool is selected by eNB and VI's boundaries (VI_{MIN} and VI_{MAX}) are included in random access response (RAR) that will be transmitted to

UE minimum and maximum V-RNTI values of the V-RNTI range, which are stored by VI_{MIN} and VI_{MAX} , respectively.

6.2. The V-RNTI Phase of Management (Monitor and Update). Through the phase of management, ongoing processes and activities of monitoring UE's movements are performed by eNB, and V-RNTI identities are handled in the VI-table and VI-pool accordingly. For allocation and de-allocation of V-RNTI ranges, consistency of contents of VI-table and VI-pool is maintained by eNB through employing different algorithms.

- (i) Allocation of V-RNTI range: After successful runs of procedures—random access RAR and handover to eNB, a new V-RNTI range (VI) is allocated by eNB to UE as shown in Algorithm 2.
- (ii) De-allocation of V-RNTI range: After a successful run of handover to another eNB or when a UE is re-attached to another eNB without having properly detached from eNB, the V-RNTI range (VI) allocated to a UE is de-allocated by eNB as shown in Algorithm 3.

Validation of V-RNTI location: As shown in Algorithm 4, eNB verifies that the request is initiated by a genuine UE using the validate request algorithm when a UE sends a request including the V-RNTI to eNB (e.g., in the case of an

Input: IMSI identifier of UE (IMS_{UE}) Set Avail = 216

- (1) If there are free V-RNTI ranges at VI-pool, then
- (2) Select one free V-RNTI range i (S, M) from
- (3) VI-pool
- (4) Update STATE = 1
- (5) Allocate UE ($S_i = M_i$)
- (6) Else
- (7) Let range x (S_x, M_x) be an V-RNTI range
- (8) Allocated to a UE $_z$ where
- (9) $TAL(UE) \cap TAL(UE_z) = \varnothing$ TAL is (Tracking Area List)
- (10) UE ($S_x = M_x$)
- (11) End if
- (12) Create a new blank record at VI-table
- (13) Insert tuple (IMSI, VIRC, VIMIN, VIMAX) into new record

ALGORITHM 2: Allocation of V-RNTI range algorithm.

TABLE 2: VI-pool.

IMSI	VI_{MIN}	VI_{MAX}
1	VI_{MIN1}	VI_{MAX1}
0	VI_{MIN2}	VI_{MAX2}
1	VI_{MIN3}	VI_{MAX3}
...
1	VI_{MINi}	VI_{MAXi}
...
0	VI_{MINb}	VI_{MAXb}
...
0	VI_{MINn}	VI_{MAXn}

Input: IMSI identifier of UE

- (1) Locate P-table for IMSI
- (2) Get limitations of V-RNTI range S and M
- (3) Remove UE's record from V-table
- (4) Locate V-table for another copies of S and M
- (5) If no match is found then
- (6) locate V-RNTI -pool for record that contains S and M
- (7) Update STATUS = 0
- (8) End if

ALGORITHM 3: De-allocation of V-RNTI range algorithm.

Input: IMSI, V-RNTI value VUE received from **UE**

(ii) Output: Boolean value stored in variable Valid

- (1) Valid = false
- (2) Locate V-table for V-RNTI range where:
- (3) $SUE \leq VUE \leq (SUE + MUE)$
- (4) If a particular range is found
- (5) If ($VUE \neq SUE$ and $VUE \neq MUE$)
- (6) Valid = True
- (7) End if
- (8) End if
- (9) Return Valid

ALGORITHM 4: Validate request algorithm.

authentication request using Global User Temporary Identify (GUTI) [51] or Radio Resource Channel (RRC) request) [52].

7. The Enhanced Algorithm in UE

For an enhanced algorithm in UE, to store three 16 bit V-RNTI values— VI_{SND} , VI_{MIN} , and VI_{MAX} , UE is extended for that. The VI_{SND} is the V-RNTI that was last used by UE, whereas VI_{MIN} and VI_{MAX} represent the boundaries of the allocated V-RNTI range. As shown in equations (2) and (3), a random V-RNTI value (VI_{Fresh}) that satisfies conditions is generated by UE during RRC request, as part of the RRC procedure. Then, the newly generated V-RNTI value is stored by UE as shown in the following equation [53]:

$$VI_{MIN} \leq VI_{Fresh} \leq VI_{MAX}, \quad (2)$$

$$VI_{Fresh} \neq VI_{SND}. \quad (3)$$

The UE then updates VI_{SND} :

$$VI_{SND} = VI_{Fresh}, \quad (4)$$

where VI_{Fresh} represents a random V-RNTI value, whereas VI_{MIN} and VI_{MAX} the represent boundaries of the allocated V-RNTI range and VI_{SND} is the V-RNTI that was last used by UE [54].

8. Proposed Scheme Analysis and Key Features

In this section, privacy analysis and key features of the suggested scheme are provided.

8.1. Privacy Analysis Using ProVerif Tool. In this section, the privacy of the suggested solution is analyzed using the automatic security verification tool ProVerif to formally verify its capabilities against several attacks and in terms of unlinkability, anonymity, and untraceability [45, 46]. ProVerif is a widely used automatic privacy protocol verifier. In the next section, a few vulnerable are examined, and it has been proven that our scheme is secure after analysis, where the adversary cannot get the parameters of the V-RNTI and its values. All related events are executed normally.

C-RNTI is clear text and uses in the same cell without change. Table 3 shows the process of the eNB and the UE in the proposed solution. Finally, the following pseudocode is used to start the verification process (Algorithm 5).

8.1.1. Replay Attack. The suggested scheme defends the user against a replay attack. Suppose that, during a successful run of the location update procedure, an assailant has previously intercepted V-RNTI destined for a particular user. If any are attempting to resend the V-RNTI to eNB or user by the attacker, then by comparing the V-RNTI stored at eNB and user with the V-RNTI that was in the token, eNB and user would easily detect such attack. The received V-RNTI, in such case, is not in range or would be replayed [55].

TABLE 3: V-RNTI verification.

* (events *)	(* queries *)
event eNB()	query attacker (V-RNTI).
event UE()	query attacker (V-RNTI).
	query inj-event (eNB ())==>
	inj-event(UE()).
event end().	query inj-event (end ())==>
	inj-event(UE()).

8.1.2. Unlinkability of the User. The possibility of linking between permanent location and temporary identities of users is referred to as linkability. The user linkability is eliminated, and the user is protected against tracking attack by providing the unlinkability of 5G network subscribers by this proposed scheme. Instead of a fixed C-RNTI, which can be tracked and linked to a specific UE, UE is assigned a sequence of temporary identities (V-RNTIs).

As shown in Figure 4, the privacy of the user increases by increasing the number of location updates because the V-RNTI changes in every location update, while the privacy of the user decreases when using the C-RNTI because it does not in the same cell coverage area.

8.1.3. Anonymity of User. The user location is a significant feature of the privacy of the user. The suggested scheme offers a great level guarantee of preserving user location. It is clear that an assailant could not know the V-RNTI of a specific user because V-RNTI never retransmitted or replayed as it is available only to serving network eNB and mobile user (SIM card) and is not known by other parties in the network. In regard to V-RNTI, it is changed by eNB continuously.

The strategy adopted by the proposed scheme with respect to V-RNTI selection gives a user a privilege to preserve the anonymity of the user and prevent assailants from breaching the anonymity of the user. The V-RNTI is utilized only once by UE; when UE is successfully location-updated by the network, a fresh V-RNTI is assigned by UE, which is different from the current V-RNTI that was last used. The UE assigns a fresh V-RNTI, which is random and is unrelated to the most recently used V-RNTI by UE. The V-RNTIs assigned to a particular UE look like random bitstreams that cannot be linked to a certain UE; this is from the point of view of an attacker. Therefore, the highest level of location anonymity is provided because the attacker cannot identify the target subscriber.

8.1.4. Untraceability of User. The possibility of identifying past location requests and responses of the same subscriber is referred to as traceability. In the proposed scheme, user traceability is eliminated and the user is protected against tracking attack by enhancing the characteristics of, and allocation procedures of, pseudonyms (V-RNTIs) and introducing pseudonyms that replace user permanent identifier (IMSI). Moreover, the presented scheme adopts allocation procedures of V-RNTI pseudonyms to prevent tracking of the user. In each request message, a random pseudonym (V-RNTI according to location request type) is


```

(1) new VRNT1a: bitstring; new VRNT2a: bitstring;
(2) new VRNT1b: bitstring; new VRNT2b:
(3) bitstring;
(4) (
(5)   !MS (A, choice[VRNT1a, VRNT1b] |
(6)     !MS (B, choice[VRNT1b, VRNT1a] |
(7)     !SN (choice[A, B]))
(8) -- Observational equivalence
(9)Initial clauses:
(10) Clause 0: v_31 <> true && attacker2(v_31, true)
(11)   && attacker2(@ mayfail_32, @ mayfail_33) ->
(12)     attacker2(false, @mayfail_33)
(13) (The attacker applies function &&.)
(14) Clause 1: v_37 <> true && attacker2(true, v_37)
(15)   && attacker2(@mayfail_36, @mayfail_38) ->
(16)     attacker2(@mayfail_36, false)
(17) (The attacker applies function &&.)
(18) RESULT Observational equivalence is true (bad
(19) not derivable).

```

ALGORITHM 5: 5G security and privacy.

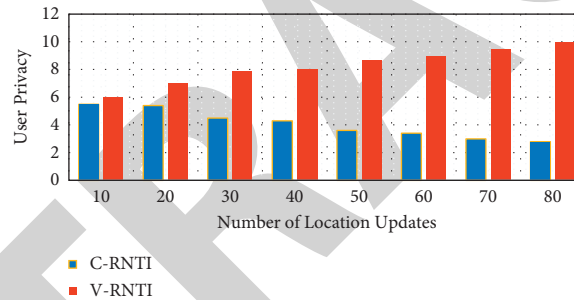


FIGURE 4: User privacy comparison between C-RNTI and V-RNTI.

chosen from within ranges of V-RNTIs, which is assigned to the user. Furthermore, by the respective network parties, each pseudonym is utilized only once. The pseudonyms selection process is random and unrelated, which makes it difficult to identify location requests by an observer, and to respond destined the same user as pseudonyms exchanged in the network.. Subsequently, past location requests and responses of the same user cannot be identified by the observer, and the user's untraceability is provided (Table 4).

8.2. The Key Features of Results. The scheme enhances the characteristics of the V-RNTI assigned to UE, as (1) it generates the V-RNTI independently from any previous allocated V-RNTI and IMSI and GUTI. The collected V-RNTI cannot be correlated with a particular UE by an attacker, who is monitoring location update channel; (2) it is unpredictable to calculate; (3) it is limited by lifetime; (4) it is frequently changed and is not reused; (5) in allocation areas, there are no collisions; and (6) if the identifier of concerned UE is included in V-RNTI message, it can easily verify. (7) The length of ranges is varying; however, the operator determines the length of each V-RNTI range by the lower limit

TABLE 4: ProVerif results on the current 5G procedure.

Properties	C-RNTI	V-RNTI
Unlinkability	X	✓
Anonymity	X	✓
Untraceability	X	✓

Note. ✓ proved to hold, ✗ attack found

and upper limit. As lengths of V-RNTI ranges are variable, so for an adversary, linking the collected V-RNTI with a specific range and specific UE would be more difficult.

8.2.1. Minimal System Impact. The messages and messaging system have a little change by this proposed solution, which makes it obvious to intercessor networks.

8.2.2. Minimal Computation Overhead. The majority of computation overhead is placed on eNB, while a minimal computation is placed on UE. The overhead on eNB is negligible since the computation power of eNB is unlimited,

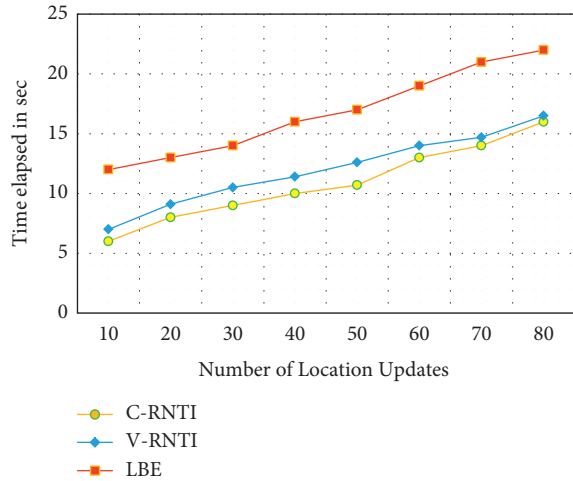


FIGURE 5: Location updates overhead at eNB.

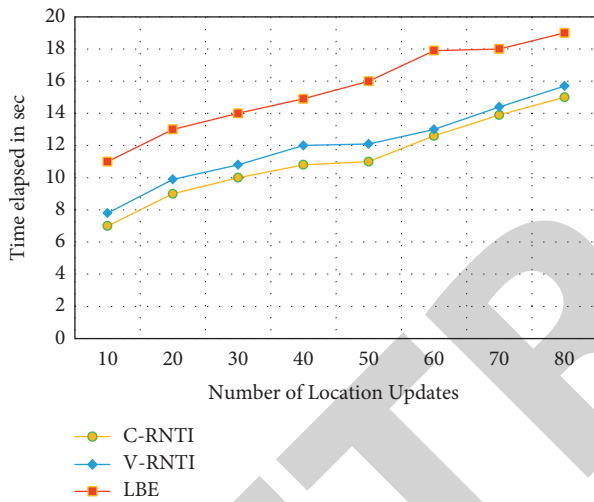


FIGURE 6: Location updates overhead at UE.

in addition to that computation overhead at UE is negligible since most of the computation overhead is placed on eNB. Figures 5 and 6 show the overhead on eNB and UE by using the C-RNTI, V-RNTI, and LBE.

8.2.3. Compatible with Previous Standard Architecture. As the proposed solution imposes minimal modifications on network parties, it can fit easily in previous standard architecture.

9. Conclusions

The study presents a convenient solution to the problem of preserving user's location privacy in 5G. Through a secure identification scheme, it allows a user to be uniquely identified by serving network (eNB) while the user remains anonymous within the network, location privacy is maintained, and thus, adversaries are prevented from being able to identify a user. The proposed solution easily fits within previous standards architecture and derives its advantages from the fact that it is compatible with previous standards of mobile cellular

technology. With minimal modifications at both network and UE and low computation overhead on part of the network and negligible computation overhead on part of UE, the proposed solution preserves user location privacy in 5G by introducing variable pseudonyms (V-RNTIs) that replace user temporary identities (C-RNTIs).

The time delay in executing the location updates procedures in the proposed solution is very close to the standard method rather than the encryption method. It is concluded that the proposed solution provided a high level of protection to the user privacy in 5G networks with a time delay closer to the standard compared to the encryption method. The security scheme presented in this study provides a sufficient guarantee for protecting user privacy in mobile cellular networks and enhances the privacy preserving capability of the mobile cellular networks. The security scheme can be extended in several directions. The following outlines the possible future works:

- (i) Minimizing the computation efforts required to manage the pseudonymous.
- (ii) Full integration of the enhanced protocols.
- (iii) Minimizing the number of messages exchanged between the network parties.

10. Appendix: Formal Verification of Enhanced V-RNTI Re-Allocation

For automatically examining the safety of cryptographic protocols, an instrument called ProVerif is used for that procedure, which is not limited to cryptographic primitives but supports hash functions, asymmetric and symmetric encryption, and digital signatures evidence. ProVerif is accomplished to prove spread capability possessions, declarations, and observational and communication correspondence. These competencies are essentially valuable to the security and privacy domains since they authority studying and examining validation and private possessions.

Moreover, evolving possessions such as traceability, verifiability, and privacy could also be deliberated. Analysis of protocol is deliberated with deference to an infinite numeral of sittings and an infinite space of message. Also, the instrument is accomplished of modernization of attack: whenever possessions could not be verified, ProVerif attempts to rebuild an implementation suggestion, which fabricates wanted possessions [45].

The proposed scheme for V-RNTI re-allocation indeed preserves privacy (i.e., untraceability and unlinkability), which is the main result of this study. An attacker outside the observer sees no difference in the output of two executions of the protocol that they differ only in user identities; this is the underlying idea behind the proof. By using observational equivalence, the proof is proceeded [46, 56].

Data Availability

The datasets generated and/or analyzed during this study are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare that they have no known competing financial interest or personal relationships that could have appeared to influence the work reported in this article.

Authors' Contributions

The codes generated during this study are available from the corresponding author on reasonable request.

Acknowledgments

This research was supported by Taif University Researchers Supporting Project (Grant no. TURSP-2020/216), Taif University, Taif, Saudi Arabia

References

- [1] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, 2018.
- [2] T. Kumar, M. Liyanage, I. Ahmad, A. Braeken, and M. Ylianttila, "User privacy, identity and trust in 5G," in *A Comprehensive Guide to 5G Security*, M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, Eds., Wiley Online Library, Hoboken, NJ, USA, 2018.
- [3] A. muthana, M. Saeed, A. Ghani, and R. Mahmood, "Enhancing privacy of paging procedure in LTE," *International Journal of Engineering Science Invention*, vol. 7, no. 2, 2018.
- [4] M. M. Saeed, R. A. Saeed, and E. Saeid, "Preserving privacy of paging procedure in 5G using identity-division multiplexing," in *Proceedings of the 2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, pp. 1–6, Hadhramout, Yemen, December 2019.
- [5] I. Ahmad, T. Kumary, M. Liyanage, J. Okwuibex, M. Ylianttila, and A. Gurtov, "5G security: analysis of threats and solutions," in *Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, September 2017.
- [6] H. Choudhury, B. Roychoudhury, and D. Saikia, "Enhancing user identity privacy in LTE," in *Proceedings of the IEEE 11th International Conference on Security and Privacy in Computing and Communications (TrustCom)*, pp. 949–957, Liverpool, UK, June 2012.
- [7] H. Ghafghazi, A. El-Mougy, and H. Mouftah, "Enhancing privacy of LTE-based public safety networks," in *Proceedings of the 13th Annual IEEE Workshop on Wireless Local Networks*, Nagoya Japan, December 2014.
- [8] R. Taranto, L. Muppirisetty, R. Raulefs, D. Slock, T. Svensson, and H. Wymeersch, "Location-AWARE Communications for 5g Networks," *IEEE Signal Processing Magazine*, vol. 102, 2014.
- [9] 3Gpp T. S. 23.003, "Digital Cellular Telecommunications System (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, Addressing and Identification, ETSI TS 123 003 V16.3.0 (2020-10), Sophia Antipolis, France," 2016.
- [10] 3Gpp T. S. 33.106, *Universal Mobile Telecommunications System (UMTS); LTE; Digital Cellular Telecommunications System (Phase 2+) (GSM); 3G Security; Lawful Interception Requirements*, ETSI TS 133 106 V16.0.0 (2020-08), Sophia Antipolis, France, 2016.
- [11] 3Gpp T. S. 33.107, *3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Lawful Interception Architecture and Functions (Release 13)*, 3GPP TS 33.107 V13.4.0 (2016-09), Sophia Antipolis, France, 2016.
- [12] S. K. Gupta, J. Y. Khan, and D. T. Ngo, "An LTE-direct-based communication system for safety services in vehicular networks," in *Moving Broadband Mobile Communications Forward - Intelligent Technologies for 5G and beyond* IntechOpen, London, UK, 2020.
- [13] U. Jang, H. Lim, and H. Kim, "Privacy-enhancing security protocol in LTE initial attack," *Symmetry*, vol. 6, no. 4, pp. 1011–1025, 2014.
- [14] S. Rafiul Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5G. Reasoner: a property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)*, pp. 669–684, Association for Computing Machinery, London, UK, November 2019.
- [15] S. Gang, C. Shuai, Y. Hongfang et al., "Location privacy preservation for mobile users in location-based services," *IEEE ACCESS*, vol. 28, 2019.
- [16] C. Hiten, "Enhanced anonymity: customized for roaming and non-roaming IoT-devices in 5G mobile network," in *Proceedings of the 3rd ISEA Conference on Security and Privacy (ISEA-ISAP)*, IEEE, Guwahati, India, February 2020.
- [17] G. Ikram, S. Salima, and Z. Faouzi, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks," *IET Information Security*, vol. 14, no. 1, pp. 21–29, 2020.
- [18] L. Jiang, X. Chang, J. Bai, J. Mistic, and Z. Chen, "Dependability analysis of 5G-AKA authentication service from server and user perspectives," *IEEE Access*, vol. 8, pp. 89562–89574, 2020.
- [19] Y. Xudong Yang, G. Ling Gao, Z. Jie Zheng, and W. Wei, "Location privacy preservation mechanism for location-based service with incomplete location data," *Digital Object Identifier*, vol. 8, Article ID 2995504, 2020.
- [20] L. Huibin, L. Xu, and Z. Yali, "An efficient location privacy-preserving authentication scheme for cooperative spectrum sensing," *Digital Object Identifier*, vol. 8, 2017.
- [21] C. Zhongyang, W. Yingjie, H. Yan, and T. Xiangrong, "The novel location privacy-preserving CKD for mobile crowdsourcing systems," *Digital Object Identifier*, vol. 6, Article ID 2783322, 2017.
- [22] C. Liang, T. Sarang, J. Kimmo et al., "Robustness, security and privacy in location-based services for future IoT: a survey," *Digital Object Identifier*, vol. 5, Article ID 2695525, 2017.
- [23] Z. J. Haddad, S. Taha, and I. A. Saroit, "Anonymous authentication and location privacy preserving schemes for LTE-A networks," *Egyptian Informatics Journal*, vol. 18, no. 3, pp. 193–203, 2017.
- [24] W. Jinbao, L. Yingshu, Y. Donghua, G. Hong, L. Guangchun, and L. Jianzhong, "Achieving effective k-anonymity for query privacy in location-based services," *IEEE Access*, vol. 5, pp. 24580–24592, 2017.
- [25] L. Ting, L. Yuxin, X. Neal N, L. Anfeng, C. Zhiping, and S. Houbing, "Privacy-preserving protocol for sink node location in telemedicine networks," *Digital Object Identifier*, vol. 6, Article ID 2858274, 2018.

- [26] H. Zhisheng, Y. Xiai, L. Yaping, X. Zhou, and L. Feng, "A secure and efficient privacy-preserving range query scheme in location-based services," *Digital Object Identifier*, vol. 6, Article ID 2882399, 2018.
- [27] Z. Shiwen, Y. Tingting, L. Wei, S. Voundi Koe Arthur, and L. Kuan-Ching, "An efficient privacy-preserving multi-keyword query scheme in location based services," *Digital Object Identifier*, vol. 8, Article ID 3018417, 2020.
- [28] E. Catania and A. Corte, "Location Privacy in Virtual Cell-Equipped Ultra-dense Networks," in *Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–4, IEEE, Paris, France, February 2018.
- [29] M. A. Zurbaran, A. Salazar, M. A. Brovelli, and W. Pedro M, "An evaluation framework for assessing the Impact of location privacy on geospatial analysis," *IEEE Access*, vol. 8, pp. 158224–158236, 2020.
- [30] K. Huguenin, I. Bilogrevic, J. S. Machado et al., "A predictive model for user motivation and utility implications of privacy-protection mechanisms in location check-ins," *IEEE Transactions on Mobile Computing*, vol. 17, no. 4, 2018.
- [31] Z. Lijuan, Y. Huanhuan, L. Zhaoxuan, P. Xiao, W. Mei, and Y. Fan, "K-anonymity location privacy algorithm based on clustering," *Digital Object Identifier*, vol. 6, Article ID 2780111, 2017.
- [32] C. Laoudias, A. Moreira, S. Kim, S. Lee, L. Wirola, and C. Fischione, "A survey of enabling technologies for network localization, tracking, and navigation," *IEEE Communications Surveys & Tutorials*, vol. 20, 2018.
- [33] S. Hailu and M. Saily, "Hybrid paging and location tracking scheme for inactive 5G UEs," in *Proceedings of the IEEE European Conference on Networks and Communications (EuCNC)*, Oulu, Finland, June 2017.
- [34] L. Gaolei, Z. Qiaolun, L. Jianhua, W. Jun, and Z. Peng, "Energy-efficient location privacy preserving in vehicular networks using social intimate fogs," *Digital Object Identifier*, vol. 6, Article ID 2859344, 2018.
- [35] Y. Dan and S. Yiran, "Location- and relation-based clustering on privacy-preserving social networks," *Tsinghua Science and Technology*, vol. 23, no. 4, pp. 453–462, 2018.
- [36] Z. Konglin, Y. Wenke, Z. Wenqi, C. Liyang, Z. Lin, and O. Eiji, "Cyber-physical-social aware privacy preserving in location-based service," *Digital Object Identifier*, vol. 6, Article ID 2871158, 2018.
- [37] Y. Ke, L. Guangchun, Z. Xu, T. Ling, and V. Akshita Maradapu, "A comprehensive location-privacy-awareness task selection mechanism in mobile crowd-sensing," *Digital Object Identifier*, vol. 7, Article ID 2921274, 2019.
- [38] Z. Liu, L. Wu, J. Ke, W. Qu, H. Wang, and W. Hao, "Accountable outsourcing location-based services with privacy preservation," *IEEE Access*, vol. 7, pp. 117258–117273, 2019.
- [39] K. Youssef, F. Jingyao, Z. Sencun, and C. Guohong, "Preserving personalized location privacy in ride-hailing service," *Tsinghua Science and Technology*, December, vol. 25, no. 6, pp. 743–757, 2020.
- [40] R. Dewoprabowo, M. Arzaki, and Y. Rusmawati, "Formal verification of divide and conquer key distribution protocol using ProVerif and TLA+," in *Proceedings of the International Conference on Advanced Computer Science and Information Systems (ICACSIS)*, Yogyakarta, Indonesia, October 2018.
- [41] C. Xiang, L. Jun, G. Daqing, and W. Rui, "Preserving location privacy in spatial crowdsourcing under quality control," *Digital Object Identifier*, vol. 7, Article ID 2949409, 2019.
- [42] I. N. Jagdale and N. S. Gawande, "Hybrid model for location privacy in wireless ad-hoc networks," *International Journal of Computer Network and Information Security*, vol. 5, no. 1, pp. 14–23, 2013.
- [43] B. Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif," *Foundations and Trends in Privacy and Security*, vol. 1, no. 1-2, pp. 1–135, 2016.
- [44] J. Zhang, L. Yang, W. Cao, and Q. Wang, "Formal analysis of 5G EAP-TLS authentication protocol using proverif," *IEEE access*, vol. 8, 2020.
- [45] D. Forsberg, H. Leping, K. Tsuyoshi, and S. Alanara, "Enhancing security and privacy in 3GPP E-UTRAN radio interface," in *Proceedings of the IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications*, pp. 1–5, Athens, Greece, September 2007.
- [46] M. Arapinis and L. Ilaria Mancini, "New privacy issues in mobile telephony: fix and verification," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 205–216, Raleigh, CA, USA, October 2012.
- [47] T. N. Weerasinghe, I. A. M. Balapuwaduge, and F. Y. Li, "Priority-based initial access for URLLC traffic in massive IoT networks: schemes and performance analysis," *Computer Networks*, vol. 178, Article ID 107360, 2020.
- [48] A. Angelogianni, I. Politis, F. Mohammadi, and C. Xenakis, "On identifying threats and quantifying cybersecurity risks of mnos deploying heterogeneous rats," *IEEE Access*, vol. 8, pp. 224677–224701, 2020.
- [49] Q. Hao, L. Sun, S. Guo, H. Liu, D. Qian, and X. Zhu, "Improvement of EAP-TLS protocol based on pseudonym mechanism," in *Proceedings of the 2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, pp. 23–28, Hangzhou, China, August 2021.
- [50] R. A. Saeed, M. M. Saeed, R. A. Mokhtar, H. Alhumyani, and S. Abdel-Khalek, "Pseudonym mutable based privacy for 5G user identity," *Journal of Computer Systems Science and Engineering*, vol. 29, pp. 1–14, 2021.
- [51] R. Ali, Z. Zulqarnain, S. W. Kim, and H. Seok Kim, "Exponentially distributed random access in LTE-A networks," in *Proceedings of the 2020 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–5, Montreal, QC, Canada, December 2020.
- [52] K. Koutlia, R. Ferrús, E. Coronado et al., "Design and experimental validation of a software-defined radio access network testbed with slicing support," *Wireless Communications and Mobile Computing*, vol. 2019, Article ID 2361352, 17 pages, 2019.
- [53] C. Yu, S. Chen, F. Wang, and Z. Wei, "Improving 4G/5G air interface security: a survey of existing attacks on different LTE layers," *Computer Networks*, vol. 201, Article ID 108532, 2021.
- [54] Vu Thi Hoang Ahn and M. Ma, "A secure authentication protocol with performance enhancements for 4G LTE/LTE-A wireless networks," in *Proceedings of the 3rd International Electronics Communication Conference (IECC)*, vol. 28–36, July 2021.
- [55] M. Abualigah, T.-D. Huy, A. Younes Shdefat et al., "An efficient 5G data plan approach based on partially distributed mobility architecture," *Sensors*, vol. 22, no. 1, p. 349, 2022.
- [56] F. Fifi, A. Yasmin, and R. Rawya, "Efficient privacy-preserving scheme for location based services in VANET system," *Digital Object Identifier*, vol. 8, Article ID 2982636, 2020.