

Preserving Privacy Location in 5G by Using Variable Pseudonym

^{1,2}Mamoon M. Saeed, ^{3,4}Rashid A. Saeed, ^{3,4}Rania A. Mokhtar, ³Hesham Alhumyani, ⁴Elmustafa Syed Ali

¹Electrical Engineering Department, Faculty of Engineering, Alzaiem Alazahri University, Sudan

²Communications and Electronics Engineering Department, Faculty of Engineering, Modern Sciences University,
Yemen

³Department of Computer Engineering, Taif University, Al Huwaya, Ta'if, Makkah Region 21974, Saudi Arabia

⁴College of Electronics Engineering, Sudan University of Science and Technology, Sudan.

mamoon530@gmail.com;

ABSTRACT

User privacy is one of the most issues addressed extensively in mobile communications evolutions, research literature, and standardization. Location privacy is a key parameter and crucial aspect for user privacy, where most of the tracking, Unsolicited advertising, malicious activities, and location-based terrorism attacks are depending on the location of the victims. For preserving location privacy, various methods in previous mobile networks use a pseudonym instead of permanent identity i.e. Cell Radio Network Temporary Identifiers (C-RNTI), However, these methods based on C-RNTI have been proved that faces many vulnerable due to the clear text used for C-RNTI exchange. A man-in-the-middle attack can easily trace users and collect information. The main objective of this paper is to propose a new location privacy algorithm that can greatly enhance the capabilities of the 5G architecture. The proposed algorithm introduces a novel variable pseudonym (V-RNTI) as an identifier for the user radio channel. Also, it provides an enhanced pseudonyms allocation procedure for identification. A new procedure that enabling UE to use different values for V-RNTI changed frequently using agreed equations to generate the values of the identifier. The proposed scheme is compatible with 3GPP standards architecture, where minor modifications/upgrades are needed for UEs eNB. Specifically, we build our model of the 5G V-RNTI authentication protocol and perform an automated security verification tool analysis of the protocol model by using the ProVerif model checker. Our analysis results show that the proposed procedure is working without flaws.

Keywords: 5G, Anonymity, linkability, traceability, IMSI, C-RNTI, V-RNTI, User Privacy and Location Privacy.

1 Introduction

Recently, the 5G network is rapidly grown to become the main core network, because of its capabilities in high data rate, low latency, high capacity, and wide coverage. Because of these capabilities, the 5G network requires an enhancement in security and privacy to ensure transferring information in a safe manner. User privacy is the main issue in 5G networks, in addition to location privacy which is considered much more important for user privacy [1]. For consumers, the realization of specific services characteristics in 5G technology, requires to provide secure network services. The privacy requirements in the 5G network might change according to the provided services. Meanwhile, service-oriented privacy requirements can be enabled by 5G technology. In some 5G applications i.e. in healthcare, a higher degree of privacy will be required to secure users' information. Moreover, an equally higher

DOI: 10.14738/tnc.85.9571

Publication Date: 10th January 2021

URL: <http://dx.doi.org/10.14738/tnc.85.9571>

level of privacy protection is required in some critical tasks. A low privacy degree may be required in other applications i.e. in searching for some kind of location information [1].

Recently, in 3GPP cellular technology, the protective privacy of user location in mobile systems has received an increasing interest more particularly. Comparing to preceding standards to the 5G cellular networks, which is recently proposed by 3GPP have an enhancement in security and privacy [2]. Although 3GPP introduced enhancing the privacy of user identity [2, 4], the location privacy of the user is still vulnerable to privacy attacks [5]. 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 Home Subscriber Subsystem (HSS). In such networks, Mobile Management Entity (MME) uses Temporary Mobile Subscriber Identifier (TMSI) for paging users in the network. And Cell Radio Network Temporary Identifier (C-RNTI) is used for user location updating in the coverage area of Evaluated Node B (eNB).

In location updating, C-RNTI is used to a single User Equipment (UE), which enables to mitigate the location attack and preserve the privacy of the user in the network, in addition, to enhance linkability and traceability. 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. Hacker can easily trace user and collect information about him/her [6,7].

The 5G network is the first standard to benefit from location information, that is sufficiently precise to be leveraged in wireless network design and optimization. Due to this fact, the 5G network must consider the privacy and security challenges and resistant location hackers by improving the mechanism of location update which will turns to improves user privacy [8]. This paper provides a location privacy scheme to enhance the pseudonyms allocation procedure for identification and user privacy protection.

The rest of the paper is organized as follows, user and location privacy discussed in section two. Location procedure privacy issue in 5G networks is described in section three. In section four, a summary of related work is given. The proposed solution and its privacy analysis are presented in sections five to eight. The concludes are in section nine.

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 as shown in Fig. 1.

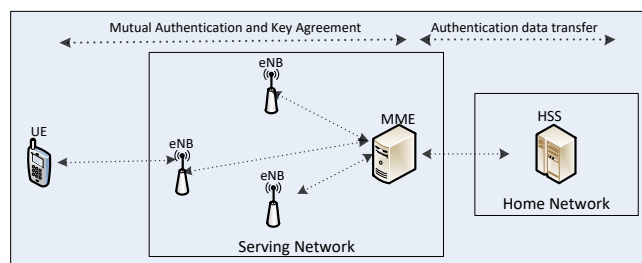


FIGURE 1: 3GPP privacy architecture.

The message comprises the IMSI sent to the service network by UE. In Authentication Vector (AV), the service network (Mobile Management Entity (MME)) sends a message comprises 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. 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) which contains the SQN with the MAC, the AK and AMF are produced. Finally, the HSS creates the AV which consists of CK, IK, XRES, AUTN, and RAND. The HSS sends the AV to the MME, 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. In cell coverage, the eNB uses the C-RNTI to update the location of UE. The C-RNTI stills fixed in the same cell coverage area, while it changes if the UE moves from one coverage area to another as shown in Fig. 2 [9 - 12].

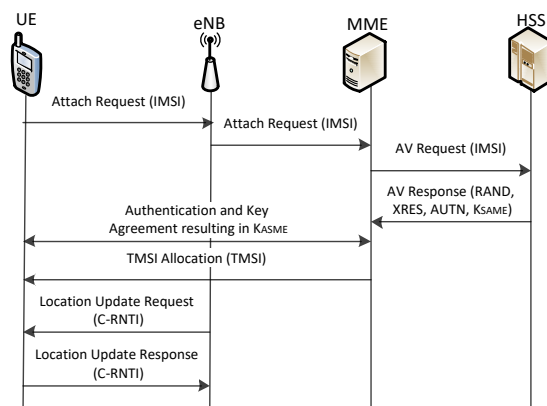


FIGURE 2: Authentication and Location update in 3GPP.

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) enables to track of 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. This strategy will ensure the un-traceability of users. The use of various C-RNTIs enables performance locating tracking but does not eliminate the attacks. The assignment of C-RNTIs to user UE possible to be linked by an attacker. The passive attacker how is monitoring the radio channel of UE can initiate an attach procedure, which possibly links various C-RNTI assigned to UE through eNB with permanent identity (IMSI). 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 Fig. 3.

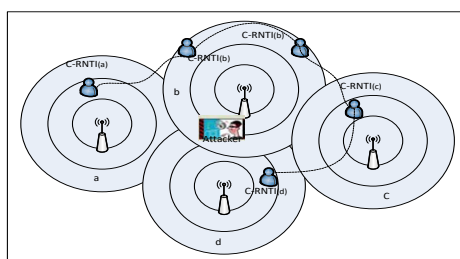


FIGURE 3: Location tracking attack using C-RNTI.

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 track of it, while the C-RNTI is sent in plain text where attackers can violate privacy [7, 14].

4 Related Work

Many research works have discussed location privacy in 5G networks and suggested different solutions for protecting privacy [15 - 39]. A related work presented by (S. Gang *et al*, 2019) 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. 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 [15].

(Xudong *et al*, 2020) proposed a location privacy method-based k-anonymity to prevent privacy disclosure in Location-Based Service (LBS) constrained in incomplete data collection. In the process of constructing the anonymous set, and against background attacks, the proposed scheme can provide effectively location privacy-preserving. The problem of incomplete data of collection location problem can be solved by a construct method for anonymous candidate set (ACS) with compressing sensing technology are designed. The differential privacy mechanism to construct the anonymous set (AS) with the ACS is adapted, to prevent the privacy disclosure in the process of construct anonymous [19].

(Zhongyang *et al*, 2017) proposed a location privacy-preserving mechanism CKD through combining k-anonymity and differential privacy-preserving to prevent mobile user's location privacy from being leaked. [29]. (Liang *et al*, 2017) present a certain cryptographic solution for security and privacy of positioning, in addition to location-based services in IoT [21].

(Catania and Corte, 2018) investigated on location privacy deriving from the densification of both mobile nodes and access nodes in the context of ultra-dense networks. The study points to the idea that more ambiguity in the information about the node to the access point and the time correlations reached by the opponent is one of the most difficult tasks in determining the location [40].

(Laoudias *et al*, 2018) reviewed the localization algorithms need to be combined with complementary technologies including accurate height estimation. The authors present an example about 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. They presented solutions based on Wireless Local Area Networks (WLAN) and cellular localization systems, including recent results on 5G localization, and highlighting the capability of computing 3D location in multi-floor indoor environments. Moreover, the authors presented estimation techniques for user mobility which could improve tracking accuracy and localization. [41]. (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 [42].

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 enabling UE to use frequently varying V-RNTI instead of fixed C-RNTI identifier to protect against Location Tracking (LT) attacks. The range of V-RNTI values is initially allocated by serving the network to each UE within eNB's coverage area. As in standard protocol, eNB supplies UE with one V-RNTI identifier during the RRC setup procedure. The user

equipment then derives from received V-RNTI minimum and maximum values of the range of V-RNTI, i.e. 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 identifier (VI_{UE}) is generated by UE and transmitted to eNB included handover message request whenever UE moves between different cells within eNB's coverage area. 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 a request is discarded.

An adversary cannot track the movement of a specific UE, because the V-RNTI value which is using by UE always keeps changing. 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, i.e. UE and eNB. 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. This scheme can be easily 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 identifier that was last used by UE while VI_{MIN} and VI_{MAX} represent boundaries of the allocated V-RNTI range. Table 1 called VI-table, kept by eNB, which stores values of V-RNTI for each UE in its coverage area. A V-RNTI range allocated to one UE is contained by each entry in VI-table contains. There are two phases, setup and V-RNTIs management can be described by the proposed scheme as shown in Table 1.

Table 1: VI-table for UEs

IMSI	VI_{RCV}	VI_{MIN}	VI_{MAX}
$IMSI_1$	VI_{RCV1}	VI_{MIN1}	VI_{MAX1}
...	...	...	...
...	...	...	...
$IMSI_k$	VI_{RCVk}	VI_{MINk}	VI_{MAXk}
...	...	...	...
...	...	...	...
$IMSI_m$	VI_{RCVm}	VI_{MINm}	VI_{MAXm}

A. 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 manage phase is executed and is executed only once at the very beginning. The setup phase has many steps; major steps as follows:

- Initialize VI-Pool with V-RNTI information: to initialize VI-Pool with boundaries of V-RNTI ranges, the Init-VI-Pool algorithm is run by eNB as shown in algorithm 1 below.

Algorithm 1: VI-Pool initialization algorithm

```

Input: limits of range length MAX and MIN
1.  Set Avail  $\rightarrow 2^{16}$ 
2.  Set Stop  $\rightarrow 0$ 
3.  Set S  $\rightarrow 0$ 
4.  While Avail  $\geq$  min do
5.    generate a random M between MAX and
6.    MIN ( $\text{MIN} \leq M \leq \text{MAX}$ )
7.    if Avail  $<$  MIN then
8.      M = Avail
9.    end if
10.   S = Stop;
11.   Stop = Stop + (2/3) * M
12.   generate a new record at VI-pool
13.   insert a tuple (S, M) into new record at
14.   VI-pool
15.   Avail = Avail - M
    end while

```

- Allocate V-RNTI ranges to UEs: Within eNB's coverage area, the Allocate-V-RNTI-Range algorithm per each UE is run by eNB. Then, to supply concerned UEs with the boundaries of their V-RNTI range (VI_{MIN} and VI_{MAX}), eNB initiates' preamble procedure toward each UE as shown in algorithm 2. The eNB performs the following steps to allocate V-RNTI ranges to UEs:

Algorithm 2: Allocation of V-RNTI range algorithm

```

Input: IMSI identifier of UE ( $\text{IMSI}_{\text{UE}}$ )
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 ( $\text{Si} \rightarrow \text{Mi}$ )
6.  else
7.    let range x ( $\text{Sz}, \text{Mz}$ ) be an V-RNTI range
8.    allocated to a UEz where:
9.     $\text{TAL}(\text{UE}) \cap \text{TAL}(\text{UEz}) = \phi$     TAL is (Tracking Area List)
10.   allocate UE ( $\text{Sz} \rightarrow \text{Mz}$ )
11.  End if
12.  create a new blank record at VI-table
13.  insert tuple ( $\text{IMSI}, \text{VI}_{\text{RCV}}, \text{VI}_{\text{MIN}}, \text{VI}_{\text{MAX}}$ ) into new record
14.

```

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 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, while value 0 in VI_{STATUS} indicates that the corresponding V-RNTI range is free for use. Whereas minimum and maximum V-RNTI values of V-RNTI range are stored by VI_{MIN} and VI_{MAX} respectively.

Table 2: VI-Pool

VI_{STATUS}	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}

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 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, while value 0 in VI_{STATUS} indicates that the corresponding V-RNTI range is free for use. Whereas min

Step 2: An ordered sequence of 16-bit V-RNTI values (range from 1 to 65523) is used for initializing the VI-Pool table with V-RNTI range information. A set of non-overlapping 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 shall store the range's boundaries VI_{MIN} and VI_{MAX} for each range. The value 0 is initialized to each record field in VI_{STATUS} .

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 VI-table. The field VIRCV 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 shall be transmitted to UE minimum and maximum V-RNTI values of V-RNTI range are stored by VI_{MIN} and VI_{MAX} respectively.

B. 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 at 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:

- 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.
- De-Allocation of V-RNTI range: After a successful run of Handover to another eNB or when a UE is re-attaching to another eNB without having properly detached from eNB, The V-RNTI range (VI) allocated to a UE is de-allocated by eNB as in algorithm 3.

Algorithm 3: De-allocation of V-RNTI range algorithm

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
9. end if

- Validation of V-RNTI identifier location: As shown in algorithm 4, eNB verifies that request is initiated by a genuine UE using the Validate-Request algorithm when a UE sends a request including V-RNTI identifier to eNB (e.g., in case of an authentication request using Global User Temporary Identify (GUTI) or Radio Resource Channel (RRC) request).

Algorithm 4: Validate request algorithm

Input: IMSI, V-RNTI value V_{UE} received from UE

Output: Boolean value stored in variable Valid

1. Valid = false
2. Locate V-table for V-RNTI range where:
3. $S_{UE} \leq V_{UE} \leq (S_{UE} + M_{UE})$
4. If a particular range is found
5. If ($V_{UE} \neq S_{UE}$ and $V_{UE} \neq M_{UE}$)
6. Valid = True
7. End if
8. End if
9. return Valid

I. The enhanced Algorithm in UE

For enhanced algorithm in UE, to store three 16-bit V-RNTI values: V_{SND}, V_{MIN}, and V_{MAX}, UE is extended for that. The V_{SND} is V-RNTI that was last used by UE, while V_{MIN} and V_{MAX} represent boundaries of allocated V-RNTI range.

As in equations (Eq. 2 and Eq. 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 (Eq. 4).

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

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

The UE then updates VI_{SND}

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

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

7 Proposed Scheme Analysis and Key Features

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

A. 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 [43 - 45]. ProVerif is a widely used automatic privacy protocol verifier. Next section, a few vulnerable are examined and have been proofed that our scheme is secure after analysis, where the adversary cannot get the parameters of V-RNTI and its values. All related events are executed normally.

Table 3: V-RNTI Verification

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

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 cod is used to start the verification process:

```
new VRNT1a: bitstring; new VRNT2a: bitstring;
new VRNT1b: bitstring; new VRNT2b: bitstring;
(
  !MS (A, choice[VRNT1a, VRNT1b]) |
  !MS (B, choice[VRNT1b, VRNT1a]) |
  !SN (choice[A, B]) )
```

-- Observational equivalence

Initial clauses:

Clause 0: $v_{31} \neq \text{true} \ \&\& \ \text{attacker2}(v_{31}, \text{true}) \ \&\& \ \text{attacker2}(\text{@mayfail_32}, \text{@mayfail_33}) \rightarrow \text{attacker2}(\text{false}, \text{@mayfail_33})$

(The attacker applies function &&.)

Clause 1: $v_{37} \neq \text{true} \ \&\& \ \text{attacker2}(\text{true}, v_{37}) \ \&\& \ \text{attacker2}(\text{@mayfail_36}, \text{@mayfail_38}) \rightarrow \text{attacker2}(\text{@mayfail_36}, \text{false})$

(The attacker applies function &&.)

RESULT Observational equivalence is true (bad not derivable). ■

▪ 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 V-RNTI to eNB or user by the attacker, then by comparing V-RNTI stored at eNB and user with V-RNTI that token, eNB and user would easily detect such attack. The received V-RNTI, in such case, not in range or would be replayed.

▪ Unlinkability of 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 through provide 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 Fig. 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 by using C-RNTI because it still fixed in the same cell coverage area.

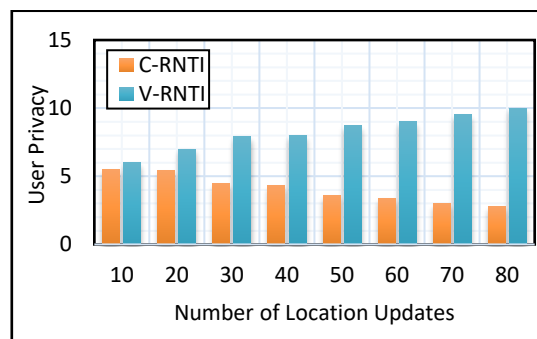


FIGURE 4: User privacy comparison between C-RNTI and V-RNTI.

▪ 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 except it is available only to serving network eNB and mobile user

(SIM card) and does not know 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-RNTIs selection and 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 updating 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 it is unrelated to most recently V-RNTI which is used by UE. The V-RNTIs assigned to a particular UE look like random bit-streams that cannot be linked to a certain UE, this from point of view of an attacker. Therefore, the highest level of location anonymity is provided because the attacker cannot identify the target subscriber.

▪ **Un- traceability 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 user protected against tracking attack through on enhancing characteristics of, and allocation procedures of, pseudonyms (V-RNTIs) and introducing of pseudonyms that replaces 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 chosen from within ranges of V-RNTIs which is assigned to the user. Furthermore, by respective network parties, each pseudonym is utilized only once. From the observer's viewpoint? are random and unrelated, this 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: ProVerif results on the current 5thG procedure.

Properties	C-RNTI	V-RNTI
Un-linkability	x	√
Anonymity	x	√
Un-traceability	x	√

√proved to hold x Attack found NA Not Applicable

B. The Key Features

The scheme enhances characteristics of V-RNTI identifier being assigned to UE, as (1) it generates V-RNTI identifier 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) V-RNTI identifier is unpredictable to calculate, (3) V-RNTI identifier is limited by a lifetime, (4) V-RNTI identifier is frequently changed and it 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 lower limit and upper limit. As lengths of V-RNTI ranges are variable, so for an adversary, linking of collected V-RNTI with a specific range and specific UE would be more difficult.

▪ **Minimal System Impact**

The messages and messaging system have a little change by this proposed solution, that makes it obvious to intercessor networks.

▪ 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, 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 LBS.

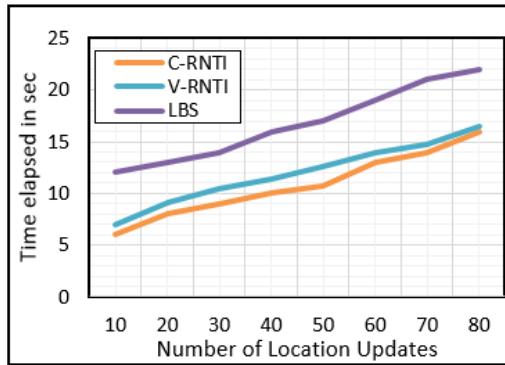


FIGURE 5: Location Updates overhead at eNB

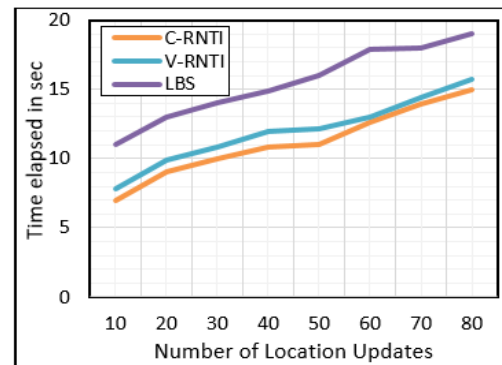


FIGURE 6: Location Updates overhead at UE

▪ Compatible with Previous Standards architecture

As the proposed solution imposes minimal modifications on network parties, it can fit easily in previous standards architecture.

8 Conclusions

The paper 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 through introducing variable pseudonyms (V-RNTIs) that replaces user temporary identities (C-RNTIs).

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

For automatically examining the safety of cryptographic protocols, an instrument ProVerif is used for that procedure, which is not limited to cryptographic primitives but supports hash functions, asymmetric and symmetric encryption, digital signatures evidence. ProVerif is accomplished to prove spread capability possessions, declarations, observational and communication correspondence. These competencies are essentially valuable to the security and privacy domain 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 [46].

The proposed scheme for V-RNTI re-allocation indeed preserves privacy (i.e., untraceability and unlinkability) is the main result of this paper. An attacker outside observer sees no difference in the output of two executions of protocol that they differ only in user identities, this underlying idea behind the proof. By using observational equivalence, the proof is proceeded [47].

REFERENCES

- [1] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, Overview of 5G Security Challenges and Solutions, 2471-2825/18/\$25.00 © 2018 IEEE IEEE Communications Standards Magazine • March 2018.
- [2] 3GPP, 3GPP System Architecture Evolution (SAE); Security architecture. 3GPP, TS 33.401, 2013.
- [3] A. muthana, M. Saeed, A. Ghani, R. Mahmod, Enhancing Privacy of Paging Procedure in LTE, www.ijesi.org || Volume 7 Issue 2 Ver. V || February 2018.
- [4] M. M. Saeed, R. A. Saeed and E. Saeid, "Preserving Privacy of Paging Procedure in 5G Using Identity-Division Multiplexing," 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), Hadhramout, Yemen, 2019, pp. 1-6.
- [5] I. Ahmad, T. Kumary, M. Liyanagez, J. Okwuibex, M. Ylianttila and A. Gurtovk, 5G Security: Analysis of Threats and Solutions, 978-1-5386-3070-9/17/\$31.00 ©2017 IEEE, 2017.
- [6] H. Choudhury, B.Roychoudhury and D. Saikia, Enhancing user identity privacy in LTE. In IEEE 11th International Conference on Security and Privacy in Computing and Communications (TrustCom), 2012. p. 949–957.
- [7] H. Ghafghazi, A. El-Mougy and H. Mouftah, Enhancing Privacy of LTE-based Public Safety Networks. In 13th Annual IEEE Workshop on Wireless Local Networks, Edmonton, Canada 2014.
- [8] R. Taranto, L. Muppirisetty, R. Raulefs, D. Slock, T. Svensson, and H. Wymeersch; LOCATION-AWARE Communications for 5g Networks; European Research Council under Grant No. 258418 (COOPNET), by European Union under ICT-248894 FP7 project WHERE2, and by Swedish Research Council under Grant No. 2011-6864 and 2009-4555.
- [9] 3GPP TS 23.003. Numbering, addressing and identification, 2016.
- [10] 3GPP TS 33.106. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements, 2016.
- [11] 3GPP TS 33.107. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions, 2016.
- [12] A. Muthana and M. Saeed "Analysis of User Identity Privacy in LTE and Proposed Solution, International Journal of Computer Network and Information Security (IJCNIS), Vol.9, No.1, pp.54-63, 2017.DOI: 10.5815/ijcnis. 2017.01.07

- [13] R. Mokhtar, S. Khatun, A. Borhanuddin, A. Ramli, R. A. Saeed "Authentication and user presence monitoring technique for mobile computers using JSR82," Proceeding of Brunei International Conference on Engineering and Technology (BICET 2005), Volume (2), pp. 133-136, Bandar Seri Begawan, Brunei, July 2005.
- [14] M. Saeed, R. Saeed. and E. Saeid; Survey of Privacy of User Identity in 5G: Challenges and Proposed Solutions. Saba Journal of Information Technology and Networking (SJITN)-ISSN:2312-4989, [S.I.], v.7. n.1. Jul.2019.ISSN:2312-4989.
- [15] S. Gang, C. Shuai, Y. Hongfang, M. Sabita, C. Victor, D. Xiaojiang, And G. Mohsen; Location Privacy Preservation for Mobile Users in Location-Based Services; IEEE ACCESS. June 28, 2019.
- [16] C. Hiten; Enhanced Anonymity: Customized for Roaming and Non-Roaming IoT-Devices in 5G Mobile Network, 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP) 978-1-7281-6708-4/20/\$31.00 ©2020 IEEE.
- [17] G. Ikram, S. Salima, Z. Faouzi; An efficient authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks; IET Inf. Secur., 2020, Vol. 14 Iss. 1, pp. 21-29.
- [18] J. Lili, C. Xiaolin, B. Jing, M. Jelena and M. Vojislav; Dependability Analysis of 5G-AKA Authentication Service from Server and User Perspectives; Digital Object Identifier 10.1109/ACCESS.2020.2993111.
- [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 10.1109/ACCESS.2020.2995504.
- [20] L. Huibin, Li Xu and Z. Yali; An Efficient Location Privacy-Preserving Authentication Scheme for Cooperative Spectrum Sensing; Digital Object Identifier 10.1109/ACCESS.2017.DOI
- [21] C. Liang, T. Sarang, J. Kimmo, S. Elena, A. Anette, L. Helena, M. Zahidul H. Bhuiyan, B. Shakila, F. Giorgia, H. Salomon, L. Jenna, R. Laura, K. Päivi and K. Heidi; Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey; Digital Object Identifier 10.1109/ACCESS.2017.2695525
- [22] W. Jinbao, L. Yingshu, Y. Donghua, G. Hong, L. Guangchun and L. Jianzhong; Achieving Effective k-Anonymity for Query Privacy in Location-Based Services; Digital Object Identifier 10.1109/ACCESS.2017.2766669
- [23] 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 10.1109/ACCESS.2018.2858274.
- [24] 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 10.1109/ACCESS.2018.2882399
- [25] 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 10.1109/ACCESS.2020.3018417.
- [26] Z. Mayra A., S. Augusto, B. Maria Antonia, and W. Pedro M.; An Evaluation Framework for Assessing the Impact of Location Privacy on Geospatial Analysis Digital Object Identifier 10.1109/ACCESS.2020.3019631.
- [27] K_evin Huguenin, I. Bilogrevic, J. Soares Machado, M. Stefan, S. Reza, D. Italo and H. Jean-Pierre; 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, APRIL 2018
- [28] Z. Lijuan, Y. Huanhuan, L. Zhaoxuan, P. Xiao, W. Mei and Y. Fan; k-Anonymity Location Privacy Algorithm Based on Clustering; Digital Object Identifier 10.1109/ACCESS.2017.2780111.

- [29] C. Zhongyang, W. Yingjie, H. Yan, and T. Xiangrong; The Novel Location Privacy-Preserving CKD for Mobile Crowdsourcing Systems; Digital Object Identifier 10.1109/ACCESS.2017.2783322.
- [30] 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 10.1109/ACCESS.2018.2859344
- [31] Y. Dan and S. Yiran; Location- and Relation-Based Clustering on Privacy-Preserving Social Networks; Tsinghua Science and Technology, August 2018, 23(4): 453–462
- [32] 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 10.1109/ACCESS.2018.2871158.
- [33] 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 10.1109/ACCESS.2019.2921274.
- [34] L. Zhaoman, W. Lei, K. Junming, Q. Wenlei, W. Wei and W. Hao; Accountable Outsourcing Location-Based Services with Privacy Preservation; Digital Object Identifier 10.1109/ACCESS.2019.2936582.
- [35] F. Fifi, A. Yasmin, And R. Rawya; Efficient Privacy-Preserving Scheme for Location Based Services in VANET System; Digital Object Identifier 10.1109/ACCESS.2020.2982636.
- [36] K. Youssef, F. Jingyao, Z. Sencun, and C. Guohong; Preserving Personalized Location Privacy in Ride-Hailing Service; Tsinghua Science and Technology, December 2020, 25(6): 743–757
- [37] C. Xiang, L. Jun, G. Daqing, And W. Rui; Preserving Location Privacy in Spatial Crowdsourcing Under Quality Control; Digital Object Identifier 10.1109/ACCESS.2019.2949409.
- [38] B. Jagdale, N. Gawande, "Hybrid Model for Location Privacy in Wireless Ad-Hoc Networks", IJCNIS, vol.5, no.1, pp.14-23, 2013.DOI: 10.5815/ijcnis.2013.01.02
- [39] 34Z. Haddad, S. Taha and I. Saroit; Anonymous authentication and location privacy preserving schemes for LTE-A networks; Egyptian Informatics Journal 18 (2017) 193–203.
- [40] E. Catania and A. Corte, Location Privacy in Virtual Cell-Equipped Ultra-Dense Networks, 978-1-5386-3662-6/18/\$31.00 ©2018 IEEE, 2018.
- [41] 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 · July 2018.
- [42] S. Hailu and M. Saily, Hybrid paging and location tracking scheme for inactive 5G UEs, 2017 IEEE European Conference on Networks and Communications (EuCNC).
- [43] Bruno Blanchet, Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif", Foundations and Trends in Privacy and Security, 2016, Volume 1, 4 issues, 2016
- [44] Ridhwan Dewoprabowo ; Muhammad Arzaki ; Yanti Rusmawati ", Formal Verification of Divide and Conquer Key Distribution Protocol Using ProVerif and TLA+", 2018 International Conference on Advanced Computer Science and Information Systems (ICACSIS), 2018.

- [45] Jingjing Zhang, Lin Yang, Weipeng Cao and Qiang Wang, "Formal Analysis of 5G EAP-TLS Authentication Protocol Using Proverif", IEEE access, Volume: 8, 2020.
- [46] B. Blanchet. Proverif: Cryptographic protocol verifier in formal model, <http://www.proverif.ens.fr/>, accessed on 13/06/2019.
- [47] M. Arapinis, et al., New privacy issues in mobile telephony: fix and verification. In ACM Conference on Computer and Communications Security, 2012.p. 205–216.