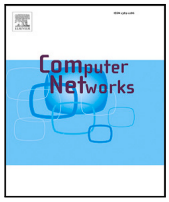
Computer Networks 240 (2024) 110165

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet



Base station gateway to secure user channel access at the first hop edge

Sang-Yoon Chang [a,*], Arijet Sarker [a], Simeon Wuthier [a], Jinoh Kim [b], Jonghyun Kim [c], Xiaobo Zhou [a]

[a] University of Colorado Colorado Springs, Colorado Springs, CO 80918, USA
[b] Texas A&M University-Commerce, Commerce, TX 75428, USA
[c] Electronics and Telecommunications Research Institute, Daejeon, 34129, Republic of Korea

ARTICLE INFO

Keywords:
Mobile computing
Telecommunications network
5G
Base station
Channel access control
Security

ABSTRACT

In mobile networking, the base station is the first hop from the user and serves as the bridge gateway between wireless and wired networking, while the security control and implementations are offloaded to the core network farther in the network. However, implementing the security control at the network edge can provide significant advantages in limiting the attacker's networking traffic and impacts, such as against DDoS. We design and build the base station gateway (BSG) to implement a security gateway on the base station, the first hop from the user, by constructing token-based secure channel access. We take a systems approach for our research to distinguish from other generic security control in edge computing. BSG is designed for efficiency (practical for mobile users) and compatibility with the existing standardized mobile networking protocol (which has traditionally challenged the mobile/cellular technology's adoption of the security research). BSG thus uses an existing protocol data field in the 4G/5G (the temporary ID of TMSI) to encode and deliver the BSG channel token and builds on the existing 5G networking protocol to incur no additional real-time communication overheads. BSG is also asymmetric between user/core network (generating the tokens) and base station (can only verify). We analyze BSG's requirement compatibility with 5G and the token security. We implement BSG between a phone and a computer to validate its design and efficiency, e.g., BSG incurs less than 0.1 microseconds overhead for the online computing on phone. We also experiment with real-world 5G networking systems to measure and estimate the defense gains of implementing BSG on the first-hop base station as opposed to on the core network.

1. Introduction

Mobile devices use telecommunications/cellular technology, e.g., 4G and 5G, to network and connect to the Internet and remote services. The cellular service provider is comprised of base stations and core network, which jointly provide the networking infrastructure and the connectivity service to the users equipped with mobile/wireless devices. Nevertheless, the base stations and the core network serve different purposes and functionalities for cellular service provision. The *base stations* are equipped with radios and directly communicate with the mobile user and serve as bridge gateways between wireless and wired networking, while the *core network* provides the digital control and networking, including the subscription/registration verification, security setup/parameter control, and the digital connections to the networking to the application end destinations beyond the cell service provider. Because of the wireless range limitation of the wireless signals for the communications between the users and base stations, the base stations are closer to the users and thus greater in number than the core network. The base stations on the edge of the network are the first-hop and the last-hop connection from/to the mobile user.

The base station vs. core network division in the purposes and functionalities has driven the separations of R&D in base station vs. in core network. The base station focuses on wireless communications and their advancements (e.g., mmWave, multiple-input and multiple-output/MIMO, spectrum-aware, and spectrum-agile medium access control/MAC). In contrast, the digital security control has been developed and implemented on the core network. The core network takes active measures based on security and authorization control, such as denying the connectivity, but not the base station (the base station's packet dropping and communication denial are rather accidental due to communication or channel/noise failures).

Building security intelligence and control on the base station located at the networking edge (the immediate hop from the user) can provide significant advantages in limiting the attacker's networking traffic and impacts. The edge-based defense can provide distributed defense to

* Corresponding author.
E-mail address: schang2@uccs.edu (S.-Y. Chang).

https://doi.org/10.1016/j.comnet.2023.110165
Received 3 July 2023; Received in revised form 13 December 2023; Accepted 21 December 2023
Available online 27 December 2023

limit the effectiveness (the number of attacker sources the defense agent encounters, e.g., against distributed denial-of-service or DDoS) and the threat impacts (in the number of routers/servers affected and the threat time duration). To achieve such security advantages from the edge-based defense, we build security control on the base station.

We design and build token-based secure channel access at the base station and call our scheme *Base Station Gateway* (BSG). BSG is distinguishable from the traditional base stations, as BSG implements digital security control using token-based virtualization (the token credentials are presented and verified to access the secure channel). Our work in BSG therefore builds security control on the furthest edge of the network in the base station (which is the first hop from the user) and provides the security benefits from edge computing (including quicker threat mitigation and reduced threat impact than implementing the security control on the farther core network). We however distinguish our BSG work from other generic edge-based security solutions by taking a systems approach to build on the existing telecommunications networking system, i.e., the 5G New Radio (NR) standardized technology by 3rd Generation Partnership Project (3GPP), and incorporate BSG into the telecommunications system. Our work therefore involves the computing and communications between the user (the client of the connectivity provision) and the base station and core network (distinct parts of the provision infrastructure). BSG utilizes the existing information, protocol, and infrastructure and incurs no real-time communication transmission overhead during the online communications to facilitate practicality and the deployment of our work on the current and future telecommunication systems.

We design BSG to achieve the following goals. First, BSG effectively defends against unauthorized cellular channel access, enabling edge-based and distributed defense to limit the threat impacts. Second, we design BSG to be secure against threats attacking the BSG itself and its integrity so that the attacker cannot manipulate or nullify/bypass the BSG security. Third, BSG is lightweight in protocol execution and changes over the existing 5G implementation, facilitating its practicality and deployment. To achieve such feats, we build on the cryptographic primitives and design and incorporate the channel-access token randomization in BSG (to enable greater frequency in token changes while ensuring lightweight verification operations). Furthermore, BSG builds on the existing 5G protocol and infrastructure to introduce zero communication overhead (i.e., no networking bytes or packets but only computing overhead). More specifically, BSG utilizes the existing TMSI (the temporary ID for 4G/5G) as the data field to encode and deliver the token and the MSIN (the permanent ID) to generate the token. BSG uses such encoding and delivery and integrates to the 5G protocol to introduce zero communication overhead over the existing 5G protocol between the base station and mobile user. BSG implementation adds computing overhead but no networking bytes or packets. BSG does introduce communication between the core network and base station during the phone registration in the offline setup but not after the setup when the mobile user becomes active for use.

BSG design inherits the asymmetry between the base station and the core network; while the user and the core network can generate the BSG tokens, the base station can only verify the token. Despite using the existing networking protocol and information and incurring no additional networking overheads when the phone/user becomes active, BSG enables token verification and the corresponding channel access control on the base station. In contrast, the traditional 5G base stations have no security control, i.e., does not drop or deny channel access. While BSG is effective in securing channel access (analogous to spreading spectrum in wireless security but without the spectrum channel-resource costs due to spreading), it does not replace the other security functionalities that the core network provides, e.g., key setup and authentication.

We make the following contributions in this paper.

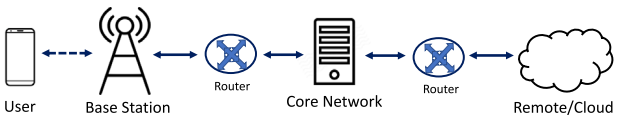


Fig. 1. The user and networking service provider infrastructure including base station and core network. The communication link between user and base station is wireless (dotted arrow), while the other communication links are wired (solid arrows).

- We design BSG to defend against unauthorized communications, e.g., DDoS, by implementing the security control at the first-hop base station to mitigate the threat impacts and amplify the defense gains.
- We design the BSG's underlying token protocol so that it is computationally efficient and practical to mobile users. We build on the well-established cryptographic primitives and building blocks to secure the integrity of BSG against the threats on the BSG itself.
- We design BSG so that it is specific to cellular base station and compatible to the existing 5G protocol. We also incorporate the BSG into the 5G protocol. By building on the 5G protocol and using the existing communication fields, we introduce no additional real-time/online communication overhead.
- We implement BSG on a phone and a computer to validate and test its efficiency.
- We estimate the BSG's defense gain and effectiveness by measuring the real-world 5G networking in practice.
- We discuss BSG and the relevant future work directions to encourage and facilitate future research and development to build practical solutions for securing mobile networking.

The rest of the paper is organized as follows. Section 2 describes the system model, threat model, and the assumptions we build on for our work. Section 3 designs the BSG scheme. We analyze the BSG, including its appropriateness and advancements of the temporary ID of TMSI and the token security against tracking/eavesdropping and injection adversaries, in Section 4. We further implement BSG on a phone and a computer for its correctness and to show its efficiency focusing on the overheads that BSG introduces beyond the existing 5G networking in Section 5. We also estimate the BSG defense gain based on experimental measurements on the real-world 5G networking deployment in Section 6. Section 7 discusses the related research to our work, and Section 8 identifies potential future directions to encourage and call for greater research to secure mobile networking including 5G and the upcoming 6G, and Section 9 concludes our paper.

2. System model, threat, and assumptions

2.1. Mobile system overview: User, base station, core network

The *user*, mobile and connected wirelessly, is the client of the networking service, while the base station and the core network jointly comprise the networking service provider infrastructure. The *base station* communicates directly with the users via wireless communication (and thus is the *first hop* in the user's networking path) and acts as a bridge gateway between the wireless and wired domains to connect to the other nodes beyond the wireless-transmission reach using wired links, including the core network. The base station forwards the networking packets to the *core network* which then forwards and routes the packets to the Internet for the remote services. To set up such connections and networking prior to forwarding the packets, the core network resolves the digital credentials of the user, e.g., service provision registration and subscription.

Fig. 1 describes the networking architecture involving these entities. Between the user and the base station, the communication links are wireless. The users use radio-specific identifiers, pre-amble signals, and base-station- or cell-specific identifiers, e.g., Cell-Radio Network

Temporary Identifier/C-RNTI in 5G. Beyond the base station, the communications are wired communications. The communications involving the backend core network enable access to remote services and digital applications and involve digital registration/subscription verification and security establishment. The user identifier credentials in such digital domain used by the core network include the global-network-level identifiers (e.g., Global Unique Temporary Identifier in 5G New Radio/3GPP) as well as those used for global connectivity based on the TCP/IP protocol (e.g., IP address).

The core network in 5G NR includes multiple logical entities, including unified data management (UDM) generating the authentication and key credentials, authentication server function (AUSF) acting as the authentication server, and access and mobility management function (AMF) managing the user connection/mobility including the user's temporary ID generation. For example, the authentication process involves the intra-core-network communications between AUSF, UDM, and AMF as well as the challenge-and-response protocol communications between UDM and the user being authenticated [1]. In our work, we do not focus on intra-core-network communications and thus do not separate the multiple logical entities within the core network; instead, we focus on the communications between user, base station, and core network.

2.2. Threat model

Our threat model is comparable to those used in the previous cellular base station threat research described in Section 7. We consider the threat injecting networking with spoofed of fake identities/credentials, pretending to be another legitimate user or a new user. Empowered by such capabilities, an attacker can launch threats against availability by injecting denial-of-service (DoS) packets. Our work thus includes the classical DoS techniques based on source address spoofing using fake IDs, which enables reflection and amplification and is used popularly in the DoS attack implementations. (BSG effectively defends against such threat by denying the channel access. If the attacker still launches DoS, it is reduced to DoS attack without spoofing. Such reduction of the attacker capability reduces the DoS risk and impacts, because the attacker cannot launch reflection or amplification, and makes the DoS detection and mitigation substantially easier, enabling rate-blocking and blacklisting due to the attacker using its own ID.)

Our goal of making our scheme compatible to the existing 5G networking protocol adds additional complexity and challenge for our threat consideration. We inherit the 5G mobile user threat model where an unauthorized attacker tracks and compromises the user privacy, e.g., to track the mobile user's whereabouts and transactions. Addressing such privacy threats has been a critical requirement for mobile networking since the incorporation of pseudonym-like temporary IDs in 2G [2]. (BSG is compatible to the ID privacy requirement of the existing 5G and actually improves the user privacy by enabling quicker updates in the TMSI.)

Our work focuses on the attackers implemented as users. The insider threats compromising the base stations, the core networks, or the user registration and the permanent-ID setup are out of the scope of our threat model. Compromising the users (so that the attacker participates in the networking as users) has greater threat feasibility and lower scrutiny than compromising the public cellular service provider entities.

To analyze the integrity and security effectiveness of our scheme of BSG, we consider an attacker trying to bypass the integrity of BSG without the authorization and registration in the offline phase. A mobile user who goes through the proper registration and MSIN allocation is a legitimate subscriber/user and therefore has the proper authorization for mobile channel access; such a mobile user is not an attacker by definition. In addition to the injection capabilities to send the packets with the spoofed IDs/tokens, the attacker can monitor/track the tokens. (BSG builds on the secure user subscription/registration, which occurs before the user becomes active for communications and networking. More specifically, BSG relies on the confidentiality of the mobile user's permanent ID of MSIN for the security of our scheme; the key/seed for the BSG tokens is derived from MSIN.)

2.3. Building blocks and assumptions

BSG builds on and adapts multiple technologies, including pseudo-random-number-generator (PRNG)-based randomization, hash chain, and TMSI (to be used to encode the security token for BSG). We rely on the underlying cryptographic primitives for the security of these technologies (since these are well-established and anchors the security of our current-day digital security technologies and cryptographic protocols, we briefly identify and discuss them in this section). More specifically, we rely on the computational hardness assumptions of the public key cipher (for the confidentiality of the seed for our BSG token generation, as described in Section 3.2) and the pseudo-random, one-way, and the collision-resistance property of the hash chain (the latter two of which we will more precisely define and use for the BSG token security in Sections 4.3 and 4.4). We also assume the existing cellular technology (more specifically, the 5G New Radio standardization) for the reference design of BSG, including the core network generating the TMSI and the TMSI data structure (e.g., 32 bits in length). We further build on the privacy and confidentiality of the user's permanent ID of Mobile Subscriber Identification Number (MSIN), a part of Subscription Permanent Identifier (SUPI), for the security of the initial input/seed s_n of the BSG token chain, as discussed in Section 4.1.

3. Base Station Gateway

Base Station Gateway (BSG) is unique in the following ways. First, it is distinguishable from the traditional technique using the base station only as a bridge gateway from wireless to/from digital domains, since it uses the random temporary ID field to encode tokens for securing the channel access. Second, BSG is distinguishable from the security control at the core network, since it implements the security control at the base station, which is the first hop from the user and closer to the user at the network edge. Third, it builds on the base station protocol (more specifically, on 5G NR in the 3GPP standard) and supports compatible and efficient operations.

Section 3.1 provides an overview of the BSG protocol, described in Fig. 2, while the rest of the section describes and explains BSG in greater details.

3.1. BSG overview and offline vs. control communication vs. and data communication

BSG utilizes a novel token for security control at the base station. The *token* provides the channel access for the secure channel and is denoted by s_t at the tth session where $t > 0$. The token is encoded in the TMSI field, which has traditionally been pseudo-random and only been used to identify the user temporarily (the traditional base station does not use the TMSI to deny access for security). BSG is designed to allow access to the channel when the legitimate token is presented while denying access otherwise, including against the threats in Section 2.2 attempting to violate the BSG integrity. The first session and token use are at $t = 1$. On the other hand, $t = 0$ is offline, e.g., for registration, subscription, the permanent ID establishment, before the user becomes active for connectivity service. While the traditional TMSI is static until an event/protocol triggers its change, BSG automatically updates it with dynamic s_t where t is updated and incremented for every communication session. The TMSI field carrying the BSG token thus changes much more frequently than the traditional TMSI.

BSG builds on the existing 5G NR protocol [1,3,4]. Fig. 2 depicts the BSG overview building on the existing 5G NR protocol where the existing 5G NR is color-coded in green/non-black. The phases from top

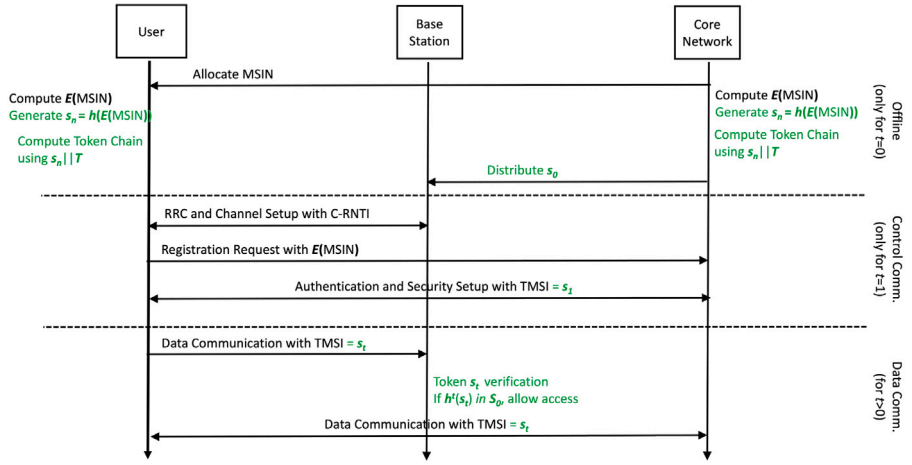


Fig. 2. BSG overview building on the existing 5G NR protocol. The existing 5G protocol is color-coded in black, while our newer BSG additions are in green. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

to bottom are divided between offline (before the user becomes active for cellular use) and online (control communications and data communications), while the figure omits the setup-suspend and setup-release phases after the data communications. After offline (e.g., registration), the user uses the s_t for the t-the communication session. The control communications at $t = 1$ occur once and does not repeat for the data communications at $t > 1$.

BSG only incurs computing-based overheads at the user for building the secure channel. The BSG implementation between the user and the cellular service provider (comprised of base station and core network) only incurs intra-node computing on the nodes and no inter-node communications. However, within the service provider, BSG does include communications within the cellular service provider between the base station and core network.

The rest of this section describes the brief and relevant 5G protocol overview and the BSG scheme in greater detail and is divided into phases, including a priori *offline* process before the user is active and the *online* process after the user becomes active and ready for accessing the cellular connectivity service. The online is further divided into the *control communication* for setting up the data communications, and the *data communication* for the downlink/uplink communications for accessing the connectivity service provided by the cellular service provider.

3.2. Existing 5G: From permanent ID to temporary ID

BSG builds on the existing 5G NR protocol [1,3,4]. This section briefly describes the existing 5G protocol which is the most relevant to our work in BSG.

In offline, i.e., before the user is active and ready for communications and connectivity services, the user gets assigned a mobile subscriber identification number (MSIN) which is a 10-digit number and is a part of the subscription permanent identifier (SUPI) for 5G (and a part of the international mobile subscriber identity (IMSI) for 4G/LTE). Both the SUPI/MSIN and the public key of the core network are shared via the universal subscriber identity module (USIM), which is often hardware- or chip-based [3]. Once the user is ready to communicate and connect in 5G having registered with USIM, the MSIN value is hidden and never directly used due to the user privacy against user tracking (which issue has been highlighted since 2G in 3GPP).

Multiple mechanisms are in place for the protection of MSIN confidentiality. First, MSIN is never communicated in plaintext but is encrypted using a public-key cipher, and the public key of the core network (E(MSIN) where E(.) is the ciphertext output of the Elliptic Curve Integrated Encryption Scheme or ECIES used in 5G NR [3]).

Fig. 3. The token generation based on the token chain using the hash function h. The generation of the tokens s is from left to right, while the use of the token s is from right to left starting from s_1 (s_0 is not used as a token for the secure channel access but rather for the token verification on the base station).

E(MSIN) is a part of the Subscription Permanent Concealed Identifier (SUCI) in 3GPP [1,3]. We build on the registration/subscription process involving the key/MSIN exchange via USIM from the existing 5G protocol, enabling the user's computation of E(MSIN), and omit it from Fig. 2 focusing on our BSG contribution (our paper presentation focuses more in details on the novel parts of BSG).

Second, the permanent ID of MSIN is quickly replaced with the temporary ID for the rest of the communications, while the mapping between the MSIN and the temporary ID is only known to the core network. The temporary ID is the temporary mobile subscriber identity (TMSI) generated by the core network (AMF to be more specific) in response to the user registration request and verification using E(MSIN). TMSI is 32 bits long and is a part of the global unique temporary identifier (GUTI) in 5G networking (as well as 4G).

3.3. BSG protocol with user

3.3.1. Token generation at $t = 0$

The BSG token generation is inspired by S/Key for one-time password [5] and TESLA for broadcasting-based source authentication [6–8]. More specifically, the BSG token chain shares similarities with TESLA and S/Key in that the token-chain construction builds on the one-way chain while the use of the tokens is in the reverse order of its creations. The subscripts for the token t is therefore in the reverse order of its construction. The seed for constructing the token chain is s_n (not used as a token for channel access), which is the input of the token generation via the token chain. The token chain generates the tokens as its output, and there are $n - 1$ tokens generated from s_1 to s_{n-1}. Fig. 3 describes the token generation algorithm, i.e., the token chain construction using the hash function h. h is a popular one-way function due to its efficiency and the security properties identified in Section 2.3.

In offline at $t = 0$ before the user becomes active, the core network and the user generate the token chain. To build on the existing 5G protocol without incurring separate seed exchange (MSIN is already allocated to the user by the core network), we use the hash output

Algorithm 1 Token Verification

Input: S_0, s_t // s_t is the token presented
Control: n
Output: $\mathcal{A}$ // $\mathcal{A} = 1$ is authenticated

$\mathcal{A} = 0$; // Initialization; no access by default

$x = h^t(s_t)$; // Apply h function t times
If find(x,S_0)==1 **then** $\mathcal{A} = 1$; // S_0 is the list of s_0

return $\mathcal{A}$;

of E(MSIN) (described in Section 3.2) as the input/seed of the token chain, i.e., $s_n = E(\text{MSIN})$. $s_n \parallel T$ is the input for the token chain computation where T is the timestamp to refresh and vary each token chain computation. The token chain outputs the tokens s_t from $t = n$ (s_n) to $t = 1$ (s_1), which are presented in the reverse-chronological order by the user for accessing the channel access at t communication. n is a control parameter that determines the number of tokens per connection, i.e., $n - 1$ tokens from s_1 to s_{n-1} before the connection release. s_t is used as t increases, e.g., s_1 is the first token to use, while s_0 is only used for verification, described in Section 3.3.3.

3.3.2. Channel setup and TMSI encoding in control communication at $t = 1$

The control communication is to construct a communication/networking channel and ensure its reliability and security prior to the data communications for carrying payloads or accessing the networking services/assets [9,10]. In the 5G protocol, the control communication's functionalities include constructing a wireless channel at the PHY and link layers of the OSI communication model, verifying the user's subscription verification, etc. The most relevant to our work in BSG however is its functionality to allocate a temporary ID of TMSI/GUTI, as described in Section 3.2. (The control communication to release/pause a communication session is omitted from Fig. 2.)

BSG builds on such 5G control communications but with a small modification of encoding the s_t in the TMSI data field in the networking protocol. The control communications need to only occur once when a new TMSI gets allocated (TMSI = s_1 in BSG), e.g., the user moves to a new tracking area (TA) or a base station or at the periodic registration. It only occurs again when the 5G protocol triggers a TMSI update or the token chain gets exhausted (i.e., $n - 1$ tokens are used), at which a new token chain gets constructed and t gets reset to $t = 0$. These events either occurred significantly less than t updates or can be controlled by BSG by selecting a larger n.

3.3.3. TMSI-token use and BSG control in data communication at $t > 0$

The BSG security implementation gets executed during the data communications which follow the control communications. The user uses the token s_t for the BSG virtual channel access for data communications. Once a session ends, t increments, and a new token is used. The BSG base station checks s_t upon the user's first packet by computing $h^t(s_t)$ and comparing it with the list of s_0, denoted with S_0. s_0 entries in S_0 correspond to the registered users for the secure channel access. For example, in the second data-communication session ($t = 2$), the BSG base station applies the hash function twice on the provided token s_2 to compute $h^2(s_2)$ and checks if it is equal to one of the s_0 in the list. If there is a match, then BSG allows the channel access yielding the Boolean $\mathcal{A} = 1$; if no match, BSG denies the access and $\mathcal{A} = 0$. Algorithm 1 describes the verification algorithm for verifying the user's token s_t.

3.4. BSG protocol between core network and base station

Our presentation of BSG and the later analyses focus on the base station and the user interactions and their setup because most of our research contributions and innovations affect the changes in these processes. However, in this section, we describe the secure "distribution of s_0" at $t = 0$ (before the user becomes active in communications) between the core network and base station in Fig. 2 using the standard public-key digital signature for completeness and clarifications. The core network sending s_0 to the base station enables the token verification on the base station.

BSG is designed to offload *some* intelligence and control from the core network to the base station. While the core network (having generated the token chain) can identify the token by mapping the token to the user's permanent ID, BSG is designed so that the base station only has the verification capability to distinguish whether a token is among the list of the virtual channel authorized users or not. To achieve such a feat, only s_0 to provide the verification capability of the legitimate virtual channel access, as opposed to the permanent ID or its derivative (e.g., E(MSIN)), is shared from the core network to the base stations.

The secure distribution of s_0 uses the public-key digital signature, which use protects the sender integrity (so that an attacker cannot inject s_0 messages spoofing as core network or base station) and the message authentication (the attacker cannot manipulate the s_0 value). The core network sends s_0 after digitally signing it with its private key to the base station in offline at $t = 0$ (before the data communications and BSG execution for security control). The base station receives the s_0 and verifies the core network's digital signature using the core network's public key. The base station then sends an acknowledgment to the core network by sending a response including the hash digest of s_0. s_0 confidentiality is not necessary for the security of our scheme, since knowing s_0 only provides the verification capability (for example, the attacker can verify that the legitimate user is transmitting).

4. Security analyses

Our security analyses of the proposed BSG scheme build on the cryptographic primitives and assumptions, including those described in Section 2.3.

4.1. TMSI requirements and privacy amplification

BSG uses the TMSI field of the 5G networking protocol to encode the token for security control. TMSI is the temporary ID valid for the radio connection at the time, and such use of the temporary ID has been used since 2G in the year 1991 [2] to protect the privacy of the mobile user against tracking in both the user location and service-application. Previous research in cellular temporary ID, including the TMSI and those equivalent before 5G, specify the privacy requirements [11–13], including *frequent updating of ID by core network*, *unpredictable ID reallocation*, *allocation of unique ID's to the users*, and *low computation and memory overhead*. To use the TMSI field and also serve as temporary IDs, BSG tokens are designed to inherit and support these requirements. For the uniqueness and unpredictability requirements, the use of the cryptographic hash function for BSG token generation resolves the uniqueness (due to collision resistance) and the unpredictability (due to the output's pseudo-randomness). For computation and memory overhead, we show in our proof-of-concept evaluations to show that BSG and the BSG token generations are appropriate for the user-simulating phone and laptop.

While BSG merely satisfies and supports the other requirements, it advances the frequency and the unpredictability of the ID because its frequency for changing increases. By introducing a token construction, the frequency gets amplified by n, i.e., the TMSI encoding the BSG token changes n times faster than the existing 5G protocol. Such greater frequency will help mitigate the threats in cellular security research, e.g., [4,14,15], caused by the relatively static nature of the current TMSI [11].

4.2. s_n Security for key/seed for token chain

s_n serves as the symmetric key for our BSG scheme and the BSG security relies on the secrecy of s_n against the unauthorized attacker. While s_n needs to be known between the user and the core network, the base station does not need to know s_n despite its BSG token verification capability (i.e., can check the legitimacy of the token when the token is being used).

s_n secrecy/confidentiality is well-protected against the unauthorized attacker and its secrecy level is comparable to that of the permanent ID of mobile users and that of a private key in the public-key cryptosystem. In BSG, s_n is derived from the permanent ID of MSIN, which has been shared between the user and the core network in the offline mobile registration process and its security/privacy is well-protected and highly guarded as described in Section 3.2. The s_n information is also kept in the local machine and not communicated outside of the machines. This significantly reduces the security risk when the information is getting networked and communicated across the machines and provides the security assurance level of a private key in a public-key cryptographic system (which also relies on the fact that it is stored and kept in the local computer for its secrecy).

4.3. Token security: Forward confidentiality of s_t

BSG requires the *forward confidentiality* of s_t, i.e., the unauthorized attacker cannot know s_t before the user uses it at time t and knowing the past s_i, $\forall i < t$ does not provide additional information about s_t.

Theorem 1. *BSG achieves the forward confidentiality of s_t if h is pseudo-random and preimage-resistant.*

Proof. We assume h which is pseudo-random and preimage-resistant (or "one-way"), such as a cryptographic hash function, e.g., SHA. The modern-day cryptographic systems using cryptographic hash functions build on this standard computationally hardness/infeasibility assumption. If h is *pre-image resistant*, then given any hash output y, it is computationally infeasible to find x such that $h(x) = y$.

At the time t when the user uses s_t for the channel token, an attacker can monitor the past s_i values where $i < t$ (can include s_0 as s_0, unlike s_n, is communicated across the nodes). An attacker cannot use s_{t-1} to find s_t because h is preimage-resistant, i.e., given s_{t-1}, the attacker cannot find s_t such that $h(s_t) = s_{t-1}$. The knowledge of the previous s_i also does not provide the information about s_t because h is pseudo-random and, more specifically, the s_t value is statistically independent to all s_i where $\forall i < t$. □

4.4. Token security: Attacker cannot generate another s'_t passing BSG verification

For verifying s_t at time t, the BSG base station computes $h^t(s_t)$ and checks if $h^t(s_t) = s_0$. From Theorem 1, an attacker cannot know the value of s_t. However, if an attacker can generate $s'_t \neq s_t$ such that $h^t(s'_t) = h^t(s_t) = s_0$, then it can generate a token s'_t which passes the BSG verification, thus violating the BSG integrity.

Theorem 2. *Given the legitimate token s_t, attacker cannot generate a $s'_t \neq s_t$ such that $h^t(s'_t) = h^t(s_t) = s_0$ if h is weakly collision resistant.*

Proof. We assume h which is weakly collision resistant (also called the second preimage resistance), which is a standard computational-hardness assumption for cryptographic hash functions on which the modern-day cryptographic systems rely. If h is *weakly collision resistant*, for any given x, it is computationally infeasible to find $z \neq x$ such that $h(z) = h(x)$.

We prove by induction that, given the legitimate token s_t, attacker cannot generate a $s'_t \neq s_t$ such that $h^t(s'_t) = h^t(s_t) = s_0$.

Table 1
Implementation platform specifications.

Simulating	Processor	Memory	OS
User (Phone)	Samsung Exynos 9820, 2.84 GHz	8 GB	Android 12
Core Network	AMD Ryzen 3960X, 4.5 GHz	64 GB	Windows 10

When $t = 1$, an attacker cannot generate a $s'_t \neq s_t$ such that $h(s'_t) = h(s_t)$ if h is weakly collision resistant.

Let us assume that, when $t = k$, an attacker cannot generate a $s'_t \neq s_t$ such that $h^k(s'_t) = h^k(s_t) = s_0$.

Let us show that the statement holds for $t + k + 1$. Let us prove by contradiction. Suppose an attacker, given the legitimate token s_t, can find $s'_t \neq s_t$ such that $h^{k+1}(s'_t) = h^{k+1}(s_t)$. The attacker can compute $h^k(s_t)$ from the given s_t. If the attacker can find such s'_t, the attacker can also find $h^k(s'_t)$. Therefore, such attacker, given the legitimate token s_t and deriving the $h^k(s_t)$, can find $h^k(s'_t)$ such that $h(h^k(s'_t)) = h(h^k(s_t))$. This violates the h's weakly collision resistance property; the two input hash arguments from the definition earlier in this proof are $x = h^k(s_t)$ and $z = h(^k s'_t)$. Therefore, there is a contradiction and the statement is true for $t = k + 1$ if it is true for $t = k$. □

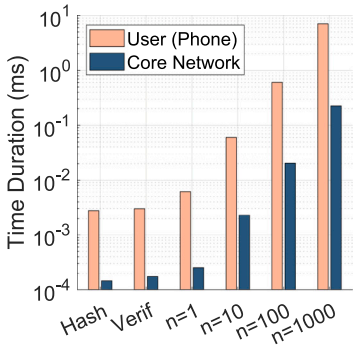
4.5. Base station defense gain

BSG implements the security control at the farthest of the networking edge in the cellular service provider, which is the base station. Because BSG limits the propagation of the attack networking, it limits the threat impact for the attacker-generated networking, which is especially important for the DoS or DDoS threats attacking the system availability. We quantify such defense gain by G which is the inverse ratio of the threat impact when BSG is used and the security implemented at the base station vs. the threat impact when the security is implemented at the core network. Since the threat impact is less for BSG and it is in the denominator of the defense-gain ratio, the greater the defense gain G the less the threat impact (better defense). We apply such defense gain in multiple performance metrics and denote it with G_i where the subscript i indicates the performance metric. For example, in our later implementation and experiment, we estimate the defense gain in time (G_T), the number of routers/switches/servers impacted on the path in hops (G_H), and the number of attack-source nodes the defense implementer faces (G_N). The defense gain values and their interpretations depend on the system application, and we measure and estimate the defense gains in our later experiments and analyses.

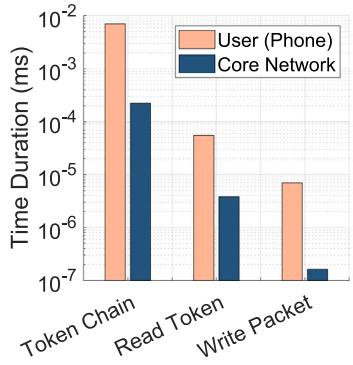
5. BSG implementation and computing

We implement BSG to test and validate the design and measure the performance. This section focuses on the networking protocol between the user and the core network and on the computing performances and the overheads, as the BSG additions beyond the existing 5G protocol are limited to computing (i.e., BSG does not incur additional networking) and the overheads are especially important for the token and its carrier in the temporary ID for the mobile users, as described in Section 4.1. BSG module can be implemented in different platforms/machines and support different hash functions (can different hash functions with different hash lengths, as long as the hash function meets cryptographic requirements described in Section 2.3).

We use a mobile phone to simulate the user while using a server computer for the core network, which platforms are representative of these entities, and the machine specifications are in Table 1. For the results presented, we average the measurements over 10^5 experimental samples, use SHA-256 for h, and $n = 1000$, unless otherwise noted.



(a) Computing overhead for hash-function computation ("Hash"), token verification ("Verif"), and tokens generation while varying $n \in \{1, 10, 100, 1000\}$.



(b) Computing overhead of the online operations during the control communication ("Read Token" and "Write Packet") compared to the offline tokens generation ("Token Chain").

Fig. 4. BSG implementation overhead.

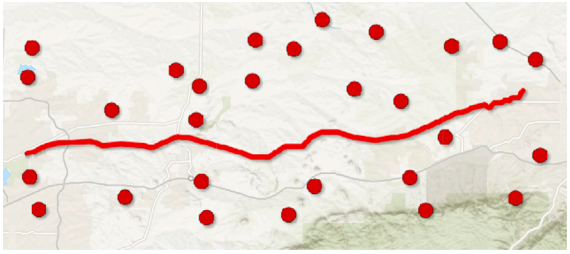
5.1. BSG token chain generation (offline) and verification

Our BSG scheme is compatible and builds on the existing 5G networking protocol, including using the existing TMSI field to encode and deliver the BSG token. BSG thus only incurs additional computing-based overheads. We focus on the new computations introduced by our BSG scheme, which are the BSG token chain generation (occurring offline before there is data to send) and the token verification. We generally observe that the computing overhead in time duration decreases as the processor capability increases.

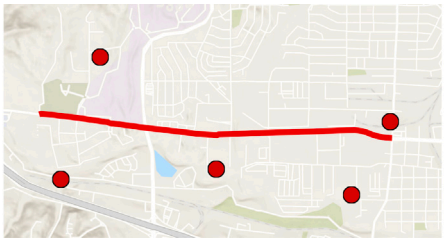
Fig. 4(a) focuses on these new computational operations of BSG, including the token verification and the token chain generation. The average hash function computations by itself ("Hash") without the additional overheads for constructing the token chain is also measured for a comparison reference. The token verification is designed for efficiency as it only involves a hash computation and comparison for checking the token's legitimacy (both operations are known to be efficient). The token verification takes 2.97 μs for phone-based users and 0.176 μs for the core network, which is only 6.8% and 19.7% greater than the hash function for the user and core network, respectively. The token verification is also two to three orders of magnitude more efficient than the tokens generation via the token chain construction if $n \geq 100$ ($n = 1$ and $n = 10$, although feasible, is not recommended as they would require frequent updates on the offline token-chain construction). More specifically, for the phone-based user, the verification overhead is $\frac{606}{2.97} = 204$ times smaller than the token chain construction when $n = 100$ and $\frac{7044}{2.97} = 2370$ times smaller when $n = 1000$. For the core network, the difference is more drastic; the token verification overhead is $\frac{20.2}{0.176} = 115$ times smaller than the tokens generation when $n = 100$ and $\frac{226}{0.176} = 1280$ times smaller when $n = 1000$.

Focusing on the resource-constrained phone user (rather than the much quicker server computing simulating the core network), the token verification takes only 2.97 μs for the resource-constrained phone user. The token verification will be even smaller for the less-resource-constrained base stations, which makes the online/real-time BSG token verification feasible on the base station. The tokens generation via the token-chain construction on the user is also manageable at 606 μs and 7040 μs with $n = 100$ and $n = 1000$, respectively, especially because the tokens generation operation occurs offline before there is data to transmit in the cellular networking.

Fig. 4(a) also compares the tokens generation overheads via the token-chain construction when varying n. The computing overheads are proportional to n, the number of tokens generated.



(a) Highly Mobile (28 base stations)



(b) Mobile (5 base stations)

Fig. 5. Geographical map showing the user mobility (via driving) and the base stations (in red dots) for our real-world 5G experiments.

5.2. The online operations

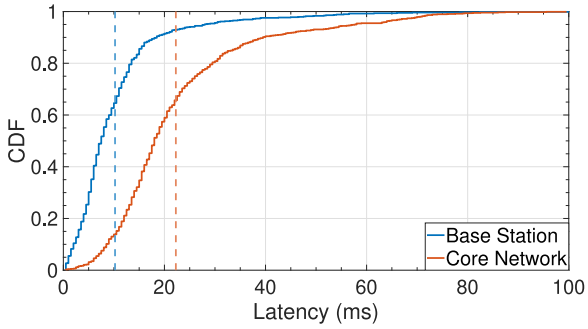
While offline operations can be performed any time before the application data transfer and the use of the networking services, online operations add real-time delays to transferring data and using the networking services. We therefore analyze the online operations of BSG. Fig. 4(b) measures overheads for reading the token from the token chain ("Read Token") and writing the token on the networking packet ("Write Packet") while including the offline token chain generation for comparison. Because of their operational simplicity, the online operations have significantly smaller overheads than the offline tokens generation. For the phone-based user, the time overhead is 0.0549 μs for accessing the token from the token-chain data and 0.00698 μs for encoding that token on the packet; for the core network, it is 0.0038 μs for accessing and reading the token and 0.000164 μs for writing the token on the packet. These are two to three orders of magnitude smaller than the offline token construction when $n = 1000$ and are even simpler and cheaper overheads than the verification (which can be online and offline) which are in the order of microseconds for user/phone and tenths of microseconds for core network/computer.

6. Base station defense gain measurement and estimation

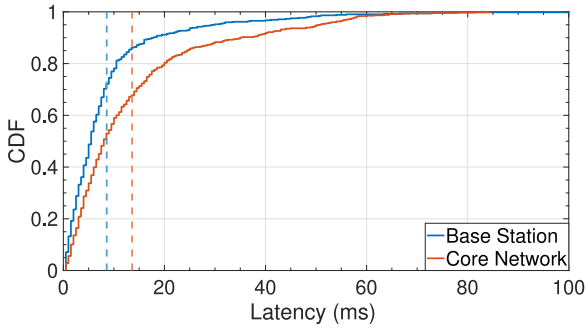
While Section 5 implements and tests the BSG design, efficiency, and the feasibility on phone, we take the networking measurements in the real-world 5G deployment in this section. We use these measurements to estimate BSG's defense gains. The gains quantify the increased security effectiveness of BSG over the existing scheme of authenticating the user on the backend core network, as there is currently no scheme authenticating the user or implementing security against malicious user on the base station.

Table 2
BSG gain G over the current scheme, estimated based on our measurements.

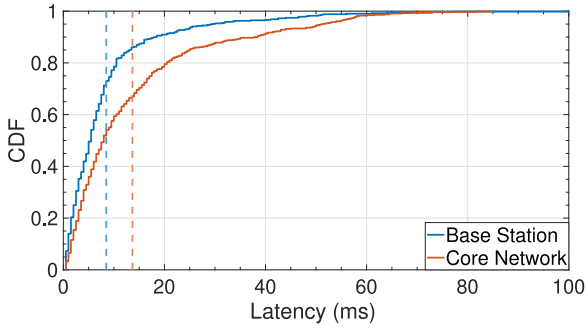
	Time duration, G_T	Number of hops, G_H	Number of attack nodes, G_N
G	1.61 – 2.19	4 – 6	100+
Depends on	Network topology, base station location	Network topology, user location	Number of base stations deployed



(a) Highly Mobile (28 base stations)



(b) Mobile (5 base stations)



(c) Static (1 base station)

Fig. 6. BSG ("Base Station") vs. existing scheme ("Core Network") gain performances for G_T. These are based on our real-world 5G experimental latency measurements in CDF, and the vertical dashed lines show the averages.

6.1. Experimental methodology and observations

6.1.1. Base stations vary

In our experiments, we observe that the cellular service provider network ranges from the first hop up to 4–6 hops, depending on the user location and the base station getting accessed (i.e., different user location has different base station available). The first-hop base station is local, while the rest of the hops for the core network use the registered public IP addresses by the cellular service provider and the servers are located in different cities in the nation. While the base stations vary as we move the user in our mobile experiments, the core network remained the same, i.e., all the base stations processed the networking on the same core network.

6.1.2. Mobility experiments

To vary the base stations, we conduct mobile experiments and move the user locations by driving it on a vehicle. We experiment with varying degrees of mobility: *Highly Mobile* where we move quickly at 65–80 miles per hour across 28 base stations, *Mobile* where we move at 25–35 miles per hour and access 5 base stations, and *Static* in a fixed location. While both the Mobile experiments and the Static experiments are taken in the same city (the Mobile experiment is conducted within the city), the Highly Mobile experiment involved driving between the two largest cities in the Colorado state (Denver and Colorado Springs). Fig. 5(a) shows the geographical coverage of our driving experiment and the base stations accessed in red dots for our Highly Mobile experiment and Fig. 5(b) for the Mobile experiment.

6.1.3. Destinations do not affect our results

We experiment using different destination servers using the popular application destinations. These destinations include Google, YouTube, Facebook, Twitter, Instagram, Baidu, Wikipedia, Yandex, Yahoo, and WhatsApp. While we vary the destinations, our experimental measurements up to the core network remain the same since all the traffic gets relayed to the core network. The results we present in this section are not affected by the networking destination, since we focus on the core network while the destination affects the routing and forwarding beyond the core network.

6.2. Defense gain: BSG on base station vs. Current scheme authenticating user on core network

We measure and estimate the defense gains described in Section 4.5. We measure the defense gains with respect to the metrics critical against a DoS threat, which are the time duration of the attacker injection G_T, the number of routers/servers impacted on the path in hops G_H, and the number of potential attack-source nodes G_N. Table 2 outlines our gain estimations, described in this section.

BSG implements the token verification on the network edge closer to the user and more specifically on the first-hop base station from the user to provide quicker security control. Figs. 6(a), 6(b), and 6(c) show the distribution (cumulative distribution function or CDF) of our empirical measurements for the Highly Mobile, Mobile, and Static experiments, respectively. The BSG's base station implementation can enable channel access control in 10.2 ms, 8.58 ms, and 8.49 ms in the Highly Mobile, Mobile, and Static experiments, respectively, and limit the threat duration. These are quicker than the core-network-based implementation which takes 22.3 ms, 13.6 ms, and 13.7 ms in the Highly Mobile, Mobile, and Static experiments, respectively. Thus, $G_T = 2.19, 1.59, 1.61$ in the Highly Mobile, Mobile, and Static experiments, respectively.

The BSG's base station implementation can also limit the number of routers/servers impacted as the threat does not go beyond the first-hop base station. In contrast, the threat impacts the service provider's network up to 4–6 hops if the BSG security control were implemented on the core network. Thus, G_H ranges from 4 to 6.

DDoS increases the number of attack sources/devices to amplify its DoS traffic and impacts. As greater attack sources/devices can generate larger traffic, the DDoS botnet size is used as the measure for the potential impact of the DDoS threat. BSG enables distributed defense and the implementation on the greater number on base stations as opposed to the on the smaller number of core network can limit such DDoS impact because the individual BSG defense-agent encounters and defends against fewer attack-source nodes. We estimate the BSG's

defense gain in the attack-source nodes G_N by the potential number of users/devices which can be targeted to be a part of the DDoS network, which is the number of user entities served by and encountered by the security implementer. Given a cellular service provider, the ratio between the average number of users served by a core network and that by a base station is equal to the ratio between the number of base stations and the core networks. Unlike the previous G_T and G_H which are based on our experimental measurements, G_N is derived from the estimates. The 5G cellular service provider accessed in our experiment is AT&T, which has an estimated 75 core network servers [16] and an estimated 33,000 base stations (100,000 base stations split across three major service provider companies [17]) in USA. For 5G AT&T in USA, the estimated G_N is thus $G_N = 440$. More conservatively, the BSG defense gain G_N is at least two orders of magnitude greater than implementing the security control on the core network, i.e., $G_N > 100$.

6.3. Comparison between mobility experiments

Our measurements in Figs. 6(b) and 6(c) are very similar for the Mobile and Static experiments, e.g., the latency measurements are within 2% difference for both the base stations and the core network, because they are taken within the same city. However, we observe greater differences between the Highly Mobile experiment (Fig. 6(a)) and the Mobile/Static experiments (Figs. 6(b) and 6(c)), because the Highly Mobile experiment physically spans across two largest cities in a US state and includes the rural areas in between the two cities where the base stations are more sparse and farther away. The latency measurements are generally longer in the Highly Mobile experiment than the Mobile or Static experiments; the base station latency is $\frac{10.22}{8.578} = 1.19$ times greater and the core network latency $\frac{22.26}{13.6} = 1.64$ times greater in the Highly Mobile experiment involving rural areas than the Mobile experiment.

7. Related work

7.1. Edge computing security and authentication

Previous research in edge computing implemented security and authentication on the network edge closer to the client mobile device than the cloud. Most relevant to our research in security functionality and purpose are those implementing wireless authentication at the edge link, i.e., authenticating the wireless communication link directly connected to the end node user, e.g., [6–8,10,18,19]. These previous research consider a similar threat model as ours in DoS (Section 2.1), which motivates the efficiency and low latency of our scheme. Part of our work (more specifically, the token generation in Section 3.3) is inspired by the TESLA authentication and adapts a similar hash-chain construction [6–8].

However, we distinguish our work from previous research in two ways. First, BSG is specific to the telecommunications/cellular protocol and builds on the 5G protocol. Second, BSG utilizes the existing data field of 5G base stations, as opposed to providing separate authenticator inputs as is the case in the previous research for efficient authentication. Because there are no separate inputs/communications (i.e., encoding the token from the existing data fields in the protocol), BSG is a security gateway for constructing secure channel access, as opposed to the authentication requiring separate authenticator inputs. We also do not recommend that BSG replaces the traditional user authentication in 5G conducted by the core network; BSG is rather a supplementary mechanism enabling distributed defense and an additional layer of defense.

7.2. Base station security

In current 5G development and standardization, as described in Section 1, the core network conducts the user authentication after the TMSI has been established. However, such authentication is after the TMSI is established. Recent literature studied the vulnerability in TMSI and the threats enabled by the attacker spoofing the victim user's TMSI, including redirecting the victim to a malicious destination/websites and track the user's transactions [15,20], de-registering the victim to detach the victim from the base station and the core network [14], and tracking the TMSI to breach the user's location privacy using the silent phone calls or SMS [11,12,21]. Our work is motivated by such threats; BSG prevents such threats by implementing security on the base station and disabling the attacker from spoofing the TMSI (the encoded BSG token).

Previous research implemented security on the base station focusing on the wireless communication link between the base station and the user. Previous research built secure wireless channels using medium access control and channel randomization to ensure the wireless channel availability against wireless DoS threat in jamming [9,22,23]. In 5G NR standardized technology, the base station transmits the signal preamble over the Physical Random Access Channel (PRACH) which spreads the signal in both time and frequency [24]. BSG is inspired by the spread spectrum technologies but uses the digital token instead of randomizing the physical radio-channel frequency, code, or time channel locations for gaining access to the channel. To the best of our knowledge, our work is the first to implement a digital token-based secure channel access on the base station, as the base station has mostly been treated as a security-oblivious bridge gateway.

Other previous research in base station security studied security against rogue or malicious base stations, e.g., [25–29]. However, these previous research are orthogonal to our work, as we focus on malicious users in our threat model. In our threat model, the attacker launches the threats from the user perspective, while these previous research considers the malicious actor assuming the base station role.

8. Discussions and future work

While edge computing including those for security applications has been surging in general, the 5G-specific mechanisms for implementing such edge-computing approach has been limited. We discuss BSG and some relevant future work directions to encourage further research and development to build practical edge solutions for securing mobile networking.

8.1. BSG compatibility

BSG implementation is on a per-channel basis, and we present BSG focusing on a single channel between a user and base station/core network in this paper. BSG can therefore be implemented on any base station and it requires no coordination between base stations. For example, some base stations can implement BSG while others do not. Furthermore, within a base station supporting BSG, there can be users who use BSG and those who do not. When such users coexist, the base station can prioritize those users using BSG who have stronger security assurances, e.g., limit the rate/bandwidth for the non-BSG channels when the base station is overwhelmed.

8.2. More security functionalities at base station

BSG focuses on the gateway functionality to use tokens to enable or block/deny cellular channel access. BSG's security functionality is digital (the random token enables access) but analogous to the physical-layer spreading spectrum in wireless communications (the channel access dynamically varies in its frequency or code/processing where the channel selections are random to the attacker). The base station can

implement other security functionalities beyond BSG. These security functionalities can include security threat detection and identifications and the corresponding active control mechanisms, including channel misuse detection from a legitimate subscription/registration. BSG itself only distinguishes and filters based on the legitimacy of the subscription/registration, considering the subscribed/registered users as having access to the channel as described in Section 2.2. The base station can also potentially implement mechanisms to strengthen user privacy, which goal is outside of the scope of BSG (although BSG is compatible with the user-privacy requirements as described in Sections 3.2 and 4.1).

8.3. BSG for beyond 5G

While we build on the existing 5G New Radio protocol standard from 3rd Generation Partnership Project (3GPP) in this paper, BSG's underlying assumptions and building blocks in the mobile/cellular networking (including the temporary ID and the base station-core network asymmetry) has been used since 2G. We therefore envision BSG to be applicable to future mobile networking standards beyond 5G, e.g., 6G, with minor to no updates. Such BSG design can facilitate its practicality and deployment. We plan to work with the standardization bodies, including International Telecommunication Union (ITU-T) and 3GPP, in order to incorporate BSG and build security in 6G networking during the design and standardization. Enabled by such a security-by-design approach, future work includes further amplifying and enhancing BSG in its security benefits and properties to secure future mobile/cellular networking. The standardization can also help with wider deployment and implementation of BSG in practice.

9. Conclusion

We design and build a Base Station Gateway (BSG) protocol using a token to construct secure channel access at the first-hop edge of base station in mobile networking. BSG enables distributed defense and limits the networking injection/DoS threat impacts. BSG also builds on the well-established cryptographic primitives to secure its integrity and operations. BSG is distinguishable from the generic edge-based security solutions in that it is tightly integrated into the existing 5G NR standardized protocol, which enables compatibility and efficiency since it uses the existing 5G protocol data fields and the base station-core network infrastructure and communications. We design BSG and its integration to 5G so that BSG incurs no additional networking overhead in real-time communications when the user is transmitting data and accessing the cellular service; BSG only incurs computing overheads. We analyze both the BSG's compatibility with the security/privacy requirements of the temporary ID (on which we encode the BSG token) and the security of the BSG token against eavesdropping or injecting attackers. We further implement BSG to test its design and (lightweight) performances as well as conduct experiments on the current real-world 5G deployment to estimate the defense gains of implementing BSG on the first-hop base station against DDoS threats on the network availability.

CRediT authorship contribution statement

Sang-Yoon Chang: Conceptualization, Formal analysis, Funding acquisition, Investigation, Methodology, Project administration, Resources, Supervision, Validation, Visualization, Writing – original draft, Writing – review & editing. **Arijet Sarker:** Data curation, Investigation, Methodology, Software, Validation, Writing – review & editing, Resources, Writing – original draft. **Simeon Wuthier:** Data curation, Investigation, Methodology, Software, Validation, Writing – review & editing. **Jinoh Kim:** Conceptualization, Funding acquisition, Investigation, Supervision, Project administration. **Jonghyun Kim:** Conceptualization, Funding acquisition, Investigation, Resources, Project administration, Supervision. **Xiaobo Zhou:** Conceptualization, Investigation, Project administration, Supervision.

Declaration of competing interest

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

Data availability

Data will be made available on request.

Acknowledgments

This work was supported in part by National Science Foundation under Grant No. 1922410 (50%) and by Institute of Information & communications Technology Planning & Evaluation (IITP) grants funded by the Korea government (MSIT) (No. 2021-0-00796, Research on Foundational Technologies for 6G Autonomous Security-by-Design to Guarantee Constant Quality of Security, 50%).

References

[1] 3G.P.P. T.S. 33.501, 5G; Security architecture and procedures for 5G System, 2022.
[2] G.S.M. 3.20 version 3.3.2, European digital cellular telecommunication system (Phase1), 1991.
[3] 3G.P.P. T.S. 23.003, Numbering, addressing and identification, 2021.
[4] S.R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, E. Bertino, 5Greasoner: 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, 2019, pp. 669–684.
[5] L. Lamport, Password authentication with insecure communication, Commun. ACM 24 (11) (1981) 770–772, http://dx.doi.org/10.1145/358790.358797.
[6] A. Perrig, R. Canetti, J.D. Tygar, D. Song, Efficient authentication and signing of multicast streams over lossy channels, in: Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000, 2000, pp. 56–73, http://dx.doi.org/10.1109/SECPRI.2000.848446.
[7] A. Perrig, R. Canetti, J. Tygar, D. Song, The TESLA broadcast authentication protocol, RSA CryptoBytes 5 (2002) http://dx.doi.org/10.1007/978-1-4615-0229-6_3.
[8] D. Liu, P. Ning, S. Zhu, S. Jajodia, Practical broadcast authentication in sensor networks, in: The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005, pp. 118–129, http://dx.doi.org/10.1109/MOBIQUITOUS.2005.49.
[9] S.-Y. Chang, Y.-C. Hu, N. Laurenti, SimpleMAC: A jamming-resilient MAC-layer protocol for wireless channel coordination, in: Proceedings of the 18th Annual International Conference on Mobile Computing and Networking, Mobicom '12, Association for Computing Machinery, New York, NY, USA, 2012, pp. 77–88, http://dx.doi.org/10.1145/2348543.2348556.
[10] S.-Y. Chang, Y.-C. Hu, SecureMAC: Securing wireless medium access control against insider denial-of-service attacks, IEEE Trans. Mob. Comput. 16 (12) (2017) 3527–3540, http://dx.doi.org/10.1109/TMC.2017.2693990.
[11] B. Hong, S. Bae, Y. Kim, GUTI reallocation demystified: Cellular location tracking with changing temporary identifier, in: NDSS, 2018.
[12] D.F. Kune, J. Koelndorfer, N. Hopper, Y. Kim, Location leaks on the GSM air interface, 2012, ISOC NDSS (Feb 2012).
[13] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, J.-P. Seifert, Practical attacks against privacy and availability in 4G/LTE mobile communication systems, 2015, arXiv preprint arXiv:1510.07563.
[14] H. Kim, J. Lee, E. Lee, Y. Kim, Touching the untouchables: Dynamic security analysis of the LTE control plane, in: 2019 IEEE Symposium on Security and Privacy, SP, IEEE, 2019, pp. 1153–1168.
[15] D. Rupprecht, K. Kohls, T. Holz, C. Pöpper, Breaking LTE on layer two, in: 2019 IEEE Symposium on Security and Privacy, SP, IEEE, 2019, pp. 1121–1136.
[16] AT&T, AT&T Inc. Data Center Map, 2023, https://www.datacentermap.com/company/at-t-inc_map.html. (Accessed: 04 January 2023).
[17] 5G Observatory, Table: Comparison of 5G rollout in international markets, 2023, (Accessed: 04 January 2023).
[18] S.-M. Chang, S. Shieh, W.W. Lin, C.-M. Hsieh, An efficient broadcast authentication scheme in wireless sensor networks, in: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, ASIACCS '06, Association for Computing Machinery, New York, NY, USA, 2006, pp. 311–320, http://dx.doi.org/10.1145/1128817.1128864.

[19] B.-R. Chen, Y.-C. Hu, Mitigating denial-of-service attacks on digital contact tracing: Poster abstract, in: Proceedings of the 18th Conference on Embedded Networked Sensor Systems, Association for Computing Machinery, New York, NY, USA, 2020, pp. 770–771.

[20] S. Bae, M. Son, D. Kim, C. Park, J. Lee, S. Son, Y. Kim, Watching the watchers: Practical video identification attack in {LTE} networks, in: 31st USENIX Security Symposium, USENIX Security 22, 2022, pp. 1307–1324.

[21] S.R. Hussain, M. Echeverria, O. Chowdhury, N. Li, E. Bertino, Privacy attacks to the 4G and 5G cellular paging protocols using side channel information, in: Network and Distributed Systems Security (NDSS) Symposium2019, 2019.

[22] G.R. Cooper, R.W. Nettleton, A spread-spectrum technique for high-capacity mobile communications, IEEE Trans. Veh. Technol. 27 (1978) 264–275.

[23] M. Lichtman, R.M. Rao, V. Marojevic, J.H. Reed, R.P. Jover, 5G NR jamming, spoofing, and sniffing: Threat assessment and mitigation, in: 2018 IEEE International Conference on Communications Workshops, ICC Workshops, 2018, pp. 1–6.

[24] 3GPP, 5G; NR; Physical Channels and Modulation, Technical Specification (TS) TS 38.211, 3rd Generation Partnership Project (3GPP), 2020, URL: https://www.etsi.org/deliver/etsi_ts/138200_138299/138211/16.02.00_60/ts_138211v160200p.pdf, Version 16.2.0.

[25] S.R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, E. Bertino, Insecure connection bootstrapping in cellular networks: The root of all evil, in: Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '19, Association for Computing Machinery, New York, NY, USA, 2019, pp. 1–11, http://dx.doi.org/10.1145/3317549.3323402.

[26] A. Singla, R. Behnia, S.R. Hussain, A. Yavuz, E. Bertino, Look before you leap: Secure connection bootstrapping for 5G networks to defend against fake base-stations, in: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, in: ASIA CCS '21, Association for Computing Machinery, New York, NY, USA, 2021, pp. 501–515, http://dx.doi.org/10.1145/3433210.3453082.

[27] J. Deng, R. Han, S. Mishra, Enhancing Base Station Security in Wireless Sensor Networks, Technical Report, University of Colorado, 2003.

[28] A.B. Seyi, F. Jafaar, R. Ruhl, Securing the authentication process of LTE base stations, in: 2020 International Conference on Electrical, Communication, and Computer Engineering, ICECCE, 2020, pp. 1–6, http://dx.doi.org/10.1109/ICECCE49384.2020.9179227.

[29] X. Yan, M. Ma, A lightweight and secure handover authentication scheme for 5G network using neighbour base stations, J. Netw. Comput. Appl. 193 (2021) 103204, http://dx.doi.org/10.1016/j.jnca.2021.103204, URL: https://www.sciencedirect.com/science/article/pii/S1084804521002095.

Sang-Yoon Chang received the BS, MS, and Ph.D. degrees from the Department of Electrical and Computer Engineering at University of Illinois at Urbana-Champaign in 2007, 2009, and 2013, respectively. He has been working at the Computer Science Department at University of Colorado Colorado Springs since 2016 and is currently an associate professor there. He was a postdoctoral fellow with the Advanced Digital Sciences Center from 2013 to 2016. His research is in security, networking, wireless/mobile, cyber–physical systems, and applied cryptography.

Arijet Sarker received his BS and MS degree in information technology from Institute of Information Technology, Jahangirnagar University, Dhaka, Bangladesh in 2013 and 2015 respectively. He was a lecturer in Bangladesh at Dhaka City College and Daffodil International University from 2015 to 2016. He is currently pursuing his Ph.D. degree in security at University of Colorado Colorado Springs, CO, USA. His research interests include 5G/6G wireless security, blockchain, vehicular privacy, software assurance and wireless sensor networking.

Simeon Wuthier is a Ph.D. student from the Department of Computer Science at the University of Colorado, Colorado Springs. His research is in theoretical computer science, cryptography, and distributed ledger technology.

Jinoh Kim received his Ph.D. degree in Computer Science from University of Minnesota, Twin Cities. He is currently an Associate Professor of Computer Science at Texas A&M University-Commerce and an Affiliate Faculty Scientist at Lawrence Berkeley National Laboratory. His main research interest lies in the area of networked/distributed systems with the focuses on performance, reliability, scalability, visibility, and security, with data-driven analytics and machine intelligence.

Jonghyun Kim received the M.S. degree and the Ph.D. degree in computer science from the University of Oklahoma, USA, in 2000 and 2005, respectively. He was a researcher with the Samsung Electronics in 1995–1997 and a system consultant with the Samsung SDS in 2000. He is currently a principal researcher with the Electronics Telecommunications Research Institute, Daejeon, Korea. He is currently working as a project leader of the Intelligence Security Group of the ETRI. He is also involved in standardization activities as a vice chair of WP1 and a rapporteur of Q.4 (cybersecurity) with ITU SG17. His research interests include information Security, Cyber Security, Cloud Security, AI-based malware detection and 5G/6G Security.

Xiaobo Zhou obtained the BS, MS, and Ph.D. degrees in Computer Science from Nanjing University, in 1994, 1997, and 2000, respectively. Currently he is a professor of the Department of Computer Science, University of Colorado, Colorado Springs. His research lies in Cloud computing and datacenters, BigData parallel and distributed processing, autonomic and sustainable computing. He was a recipient of the NSF CAREER Award in 2009.