Journal of Information Security and Applications 61 (2021) 102943

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Toward securing the control plane of 5G mobile networks against DoS threats: Attack scenarios and promising solutions

Raja Ettiane [*], Abdelaali Chaoub, Rachid Elkouch

STRS Laboratory, MUSICS team, Institut National des Postes et Telecommunications (INPT), Rabat, Morocco

ARTICLE INFO

Keywords:
5G networks
Security flaws
Radio resource control
System information block
DoS attack

ABSTRACT

With the advent of the fifth generation (5G) technology, a plethora of revolutionary applications can now be supported. This tremendous growth will be certainly accompanied by a wider and fast-evolving security threat landscape, especially when the potential of massive devices connectivity will be fully unleashed. In this paper, we outline the security challenges faced by the 5G radio access network (5G-RAN) control plane as a result of the functional and architectural enhancements made at the radio resource control (RRC) protocol layer. We correspondingly analyze the dynamics of the new 5G RRC three-states model for a machine-type traffic pattern under an attack-free situation. Afterwards, we introduce and describe two RRC-based denial of service (DoS) attacks threatening the 5G-RAN resources availability. In the first threat scenario, the attacker maliciously manipulates the timing of state transitions in an attempt to overload the control plane. The second attack can be carried out through faking huge on-demand system information requests to prevent legitimate consumers from access to the cell and cause failed and interrupted 5G mobile services. Through numerical simulations, we measure the potential impact of these attacks on both 5G devices using the collision probability along with the access delay metrics, and on the critical gNB-centralized unit using the signaling overhead and the resource occupancy time metrics. Our observations reveal that both attacks can have disastrous effects on network stability and resiliency. Finally, some promising solutions are listed, with a special emphasis on injecting randomness into system parameters to complicate the task of designing such DoS attacks.

1. Introduction

1.1. Preliminary

Nowadays, mobile networks experience enormous traffic volumes emanating from diverse applications mainly with the advent of the 5G technology and the launch of the first 5G New Radio (5G NR) roll-outs worldwide. In order to meet the new desires of 5G customers, three new classes of services have been introduced, namely, massive machine-type communications (mMTC), enhanced mobile broadband (eMBB) and ultra-reliable low latency communications (URLLC) [1].

The new 5G era is embracing a set of disruptive paradigms (e.g. network densification). However, this trend can be regarded as a shift of a set of functionalities from the core to the access part for more network flexibility and elasticity. This will necessarily go with more complex interfaces coupled to excessive signaling overhead, resulting in a surge in malicious attacks mounted against radio access network (RAN) elements in particular the control plane. Such threats exploit the fact the air interface is particularly vulnerable due to the channel nature along with the fact that the focus of the previous mobile generations was to securely exchange signaling and user plane data while little attention have been paid to flooding attacks that jeopardize resource availability.

Lightweight signaling remains a key component of robust and ultra-lean 5G designs, continuous research activities are progressing in many fronts with the aim of reducing network complexity and unnecessary transmissions. Unlike the traditional monolithic approach, 5G and beyond networks call for new distributed and modular designs while partially keeping an optimal extent of centralized functions to reduce the signaling load over the interface between each distributed unit (DU) and its associated centralized unit (CU) (i.e. F1-C interface). This will entail a major change in the architecture of the next-generation radio access network (NG-RAN) part toward a dynamic, flexible and elastic infrastructure to avoid potential bottlenecks in the air interface. Indeed, several functional split options of the NG-RAN entity have been proposed by the 3rd Generation Partnership Project (3GPP) [2] depending on the set of signal processing functions that would be performed at DUs and those handled by the CUs. Moreover, a novel radio resource

[*] Corresponding author.
E-mail addresses: ettiane@inpt.ac.ma (R. Ettiane), chaoub@inpt.ac.ma (A. Chaoub), elkouch@inpt.ac.ma (R. Elkouch).

https://doi.org/10.1016/j.jisa.2021.102943

Available online 27 July 2021

control (RRC) inactive state RRC_{INACTIVE} have been introduced for NG-RAN [3] to enhance the energy efficiency and reduce the latency and signaling through optimizing the idle-to-connected transition. The new mobile technology also strives to minimize always-on transmissions to alleviate the traffic burden on common channels, and leave sufficient room for future enhancements. Henceforth, some signals (e.g. system broadcast information) are only transmitted when needed and explicitly requested by end-users.

This recent 5G evolution is clearly entailing a number of security implications. Despite the aforementioned RRC improvements (i.e. elastic RAN, new RRC state machine model and less always-on signals), there are still many challenges to overcome especially with the support of new verticals and the introduction of advanced mMTC use cases in the recently finalized 3GPP R16 and the next wave of innovative features expected in R17 and upwards. This will certainly trigger an unprecedented increase in the spreading of control signals over network resources and a permanent risk of signaling security lapses. The cellular paradigm needs to handle the huge signaling overhead, keep up with the rising customer desires and consolidate the protection perimeter accordingly.

1.2. Literature review

5G infrastructure is designed to be robust and more secure then 4G. However and according to [4], almost a dozen of 5G threats are discovered so far. These vulnerabilities could be exploited by malicious actors to jeopardize the security of various network elements. Indeed, the researchers reveal that an attacker can take advantage of paging protocol flaws to unveil the victim's real-time location (ToRPEDO), and identity (PIERCER), which can be used to mount a DoS attack against the paging channels to block the victim from receiving any pending traffic. The DoS signaling attacks raised in the former mobile network generations [5–7] can be also carried out against the 5G NG-RAN infrastructure [8] to overload the signaling control plane, which can disturb the network normal functioning and give rise to a loss of productivity from the network operator perspective. Different solutions have been proposed to defend against this type of DoS attacks in 3G/4G networks [9,10], but these threats are not tackled yet in 5G systems. The 5G fully IP-based architecture can also be exploited by malicious entities to launch attacks over the internet, including distributed DoS (DDoS) attacks. Indeed, as discussed in [11], a malicious Command and Control (C&C) entity could manage a large number of infected mMTC devices to launch a signaling DDoS attack against the 4G/5G RAN elements and make services inaccessible for the intended valid subscribers. Aiming at overwhelming the 4G/5G RAN signaling control plane by triggering malicious and frequent radio resource allocations and releases in a coordinated manner, such attacks may lead to a peak of signaling traffic that cannot be properly handled by the mobile infrastructure.

Nowadays, recent literature has proven an increasing interest in the topic of 5G security. However, little research efforts have been devoted to signaling-based threats causing network resources depletion in 5G contexts. Authors of [12,13] surveyed the 5G security architecture related to the primary protocols of the control plane signaling. Singla et al. [14] proposed a defense mechanism to secure the paging protocols against security and privacy attacks [4]. The proposed solution involves preventing the tracking of UE by introducing a new identifier randomizing the paging occasions, and designing a symmetric-key based broadcast authentication mechanism to protect 4G/5G devices from unauthorized/fake paging messages. Ahmed et al. in [15] studied the security challenges and solutions while covering the vast majority of mobile network generations, including the post-5G technologies. This work highlighted the problem of DoS attacks against signaling plane and other control plane security issues, and provided some security approaches to protect the 5G system against these threats. Indeed, the authors focused on physical layer security to protect the data information transmitted over the radio link and make the access more difficult for malicious parties.

Finally, we found enough support in the literature to consider that 5G security enhancements are not sufficient to deal with all the security challenges in particular those related to flooding the air interface using signaling messages that are common to a large set of subscribers. For instance, authors in [16] recognize that transmitting System Information Blocks (SIBs) without any authentication nor integrity protection as a part of RRC exchanges make them vulnerable to spoofing and tampering attacks. This research work has presented four potential threats against SIBs acquisition process, including a SIB_9-based spoofing attack. The latter exploits information related to Coordinated Universal Time (UTC) and Global Positioning System (GPS) time to disturb the time settings in 5G devices. This study was an attempt to give a general overview of potential vulnerabilities that still exist in 5G systems as a result of information exchanges, and no numerical results have been presented to outline how practical are these attacks and illustrate the inherent performance degradation. This kind of flaws supports our claims regarding the vulnerabilities of the 5G control plane against DoS attacks despite the new enhancements brought by 5G standardization (i.e. 3GPP releases 15 and 16 [16]).

Unfortunately, much work is still needed to make 5G mobile networks operate in truly ultra-lean designs while dealing with the huge 5G threats landscape especially the emerging and potential security issues compromising the control plane that will be the topic of this paper.

1.3. Contributions of the present work

This paper reviews a number of novel 5G features, aiming at increasing the overall network performance, with a special emphasis on exploring the inherent security challenges and implications. For instance, the 5G control plane has witnessed significant changes marked by great improvements such as an adaptive functional split, a new RRC state machine design and a new on-demand system information delivery mode. Diving deeper into these new capabilities, we pointed out a number of potential security breaches that can be exploited by any adversary holding a botnet to make 5G networks vulnerable to malicious large-scale offenses. More specifically, we introduce two new DoS attacks capable of exhausting the control plan of 5G mobile infrastructures by triggering excessive and heavy signaling procedures and making the network components struggling to respond to valid user solicitations. The first attack generates excessive inactive-connected transitions, whereas the second one forges huge massive false system information requests using SIB_9. To combat this malicious behavior, we investigate the impact of randomizing the involved system parameters on offering secure 5G services and demonstrate its effectiveness in making these parameters unpredictable by malicious actors. Through extensive numerical simulations, the proposed randomization-based solution has proven to be very efficient in terms of mitigating the signaling overhead and avoiding the unnecessary occupancy of network resources. This method offers a preventive framework that can avoid the occurrence of such attacks or at least alleviating their impact. A deep understanding of potential threat scenarios is of paramount importance to be able to identify the associated security vulnerabilities and eventually implement appropriate preventive (instead of reactive and costly) actions especially in the signaling plane. In the meantime, we provide some insights for future research directions to further immunize the control plane of future 5G networks.

To summarize, the main contributions of our work are listed as follows:

- We carry out a performance analysis of the major 5G RRC protocol enhancements and shed light on some efficiency concerns related to the control plane, in particular in the case of critical mMTC services.

- We introduce and deeply analyze the impact of two emerging attacks exploiting the new 5G RRC protocol enhancements. The first attack is inherited from the former mobile generations (i.e. 3G and 4G) and harness the 5G RRC state transitions to overload the NG-RAN control plane, whereas the second one is entirely new and relying on the system information (SI) acquisition procedures that can be initiated in on-demand basis and can lead to congestion and service failure issues if handled in a fraudulent way.
- We highlight some defense solutions to reduce the impact of the newly introduced signaling threats, including the randomization approach as a preventive solution to protect and secure the 5G control plane through increasing the complexity and the cost of launching DoS attacks that are based on prior knowledge and gained intelligence about system parameters.

The rest of the paper begins with Section 2 sketching an overview of the key NG-RAN architectural and functional improvements newly introduced in 5G systems notably at the RRC protocol level. Section 3 studies the attack-free scenario wherein the signaling efficiency of the recently introduced RRC features is assessed under a normal functioning of the system and thus a number of 5G RAN weaknesses and limitations are highlighted. Based on the identified limitations, two forms of signaling DoS attacks are designed in Section 4 exploiting the new RRC three-states model as well as the dedicated system information signaling, and seeking to exhaust the RAN resources. Later, both DoS attacks are discussed in greater detail and a performance evaluation is conducted for each of these attacks assuming a compromised network. Afterwards, we suggest to implement a randomization-based defensive strategy to increase the uncertainty for any malicious actor and decrease its chances to guess the operational system configurations used in launching the aforementioned DoS attacks. At the end of this section, some useful plots are provided for the case of RRC state dynamics-based DoS attack to confirm the robustness of 5G systems when endowed with the randomization feature to avoid ad-hoc and easy-to-guess system parameters. The last section concludes the paper and provides some insights for future works.

2. Background and motivations

5G systems continue to use the powerful RRC protocol in allocating and releasing radio resources between the network and the end-users. With the great variety of applications including intermittent and bursty traffics (e.g., mMTC), the signaling load generated from resource allocation and release procedures will increase significantly, thus overwhelming network entities. In 5G NR, a new RRC state named RRC_{INACTIVE} has been introduced. The objective of this new state is to minimize the latency by reducing the signaling exchanges triggered by the transition to RRC connected state $RRC_{\mathrm{CONNECTED}}$ through various 5G infrastructure elements. This novel state will also contribute to prolonging the battery life of 5G devices by minimizing the signaling load caused by frequent idle-to-connected transitions. Despite the new RRC inactive state and the lower number of generated RRC messages, the inherent signaling traffic remains significant for two main reasons: (1) latency-sensitive traffics (i.e., URLLC class) impose shorter inactivity timers to control the transition between the INACTIVE and the CONNECTED states [17] but at the detriment of more transition occurrences, and (2) other services (i.e., mMTC class) favor longer inactivity timers but the massive number of involved devices (e.g., sensors) leads to excessive overall signaling load. This will be further exacerbated if a DoS attack is being engineered against the RAN system and consequently the infected devices will act in a synchronized manner. Such threats can be easily mounted through sniffing or intelligently guessing (e.g., brute-force techniques) the inactivity timer parameter.

In 5G networks, the introduction of the novel RRC_{INACTIVE} state is not the only improvement introduced to reduce the RRC signaling load. For instance, always-on transmissions, in particular the SI delivery mechanisms, accentuate the energy inefficiency concerns of the RRC protocol especially with the new beam-based dimension of 5G networks. As a remedy, the fifth generation suggests to make a great part of this information available on demand using specific RRC signaling, as opposed to 4G wherein all system information is constantly broadcast. The on-demand SIBs comprise SIB_2 to SIB_9 messages, while SIB_1 is still periodically transferred. On the downside, on-demand SIBs necessitate five signaling messages to be provisioned in a dedicated manner relying on the random-access channel (RACH) procedure [18]. As a result, an attacker gaining access to a number of victim machines can abuse and misuse this new on-demand SI acquisition procedure by sending a large volume of SI requests to disrupt the proper functioning of the gNB-CU in such a way that the system can no longer respond to legitimate requests.

In a nutshell, 5G promises to build ultra-lean designs for future mobile networks. This calls for new RRC protocol improvements including a centralized RRC function, an intermediate RRC inactive state and on-demand SIB transfer. However, the more functions are centralized, the more the burden on a single anchor point, i.e., the centralized unit, notably in case of massive access by a large number of devices with short transmitted packets within the 5G mMTC class. Further, the critical CU entity can be subject to fraudulent threats issued by billions of compromised internet of things (IoT) devices emulating legitimate on-demand requests. These threats are particularly difficult to be detected as they overload the control plane (i.e. RRC) while leaving the data plane mostly unaffected. This theoretical analysis will be corroborated by a rigorous performance evaluation of relevant system KPIs, as described in the following Sections 3 and 4.

3. Performance analysis of the new 5G RRC model

In this section, we will evaluate the signaling overhead and the radio resource utilization time characterizing the new 5G RRC state machine at the NG-RAN component level for different values of the inactivity timer (i.e. the timer that manages the idle-connected transition in 4G and its counterpart inactive-connected transition in 5G). It is worth noting that these two metrics are captured at the CU side as a direct result of the functional split feature of 5G systems. Since mMTC is among the three pillars of 5G networks, we will employ an mMTC traffic model for massive sensors connectivity introduced in [19]. The older 4G RRC two-state machine will be given as a reference scenario. These experiments are conducted using a discrete-event synthetic-traces simulator developed using Matlab and implementing the new 3GPP RRC features listed in the previous section.

Two performance indicators are quantitatively investigated, namely, the volume of mobile signaling (denoted as SL) that quantifies the RRC state transitions to the $RRC_{\mathrm{CONNECTED}}$ mode, and the resource occupation time (denoted as T_{RO}) referring to the period between the traffic end and the connection suspend or re-establishment during which the device remains in $RRC_{\mathrm{CONNECTED}}$ state.

3.1. Traffic modeling

In next generation 5G networks, mMTC services are expected to connect huge numbers of energy-constrained sensors and actuators largely exploited in verticals such as agriculture and energy. Such transmissions are usually modeled using the 3GPP bursty traffic FTP model 3 [19,20]. The latter considers bursty fixed-size packet downloads/uploads from/to a common source following a Poisson arrival process with rate λ, average packet inter-arrival time $\overline{f_{D,mMTC}(t)}$ and average packet size $\overline{f_{Y,mMTC}(t)}$. Both SL and T_{RO} performance indicators are computed for different (and realistic) inactivity timers $T_{5\mathrm{G}_{\mathrm{inac}}}$, ranging from 2 to 4 s. The $T_{4G_{inac}}$ value is often set to 5 s in existing 4G deployments. We consider N_{mMTC} devices spread over the area of interest and connected to the same CU, and T_{S} is the total simulation

Table 1
mMTC simulation parameters (3GPP FTP model 3)

N_{mMTC}	T_{S}	$T_{5\text{G}_{\text{inac}}}$	$f_{Y,mMTC}(t)$	$f_{D,mMTC}(t)$
1000	7200 s	2 s, 3 s and 4 s (5 s for $T_{4\text{G}_{\text{inac}}}$)	125 B	1 s

Algorithm 1 Signaling load for the mMTC traffic model

```
for a given execution period $T_{\text{S}}$ do
    for each mMTC devices $M \in \{1, \ldots, N_{\text{mMTC}}\}$ do
        Generate the data traffic for the device $M$ according to the 3GPP bursty traffic FTP model 3 [19,20].
        for each 5G inactivity timeout $T_{5\text{G}_{\text{inac}}} \in \{2\ \text{s}, 3\ \text{s}, 4\ \text{s}\}$ do
            Compare the inter-departure packets period $f_{D,mMTC}(t)$ with $T_{5\text{G}_{\text{inac}}}$
            if $f_{D,mMTC}(t) \geq T_{5\text{G}_{\text{inac}}}$ then
                Increment the signaling load $SL$ by the number of signaling messages exchanged during the state transition from $RRC_{\text{CONNECTED}}$ to $RRC_{\text{INACTIVE}}$.
            end if
        end for
    end for
end for
```

time. Using the traffic model parameters described in Table 1, we will simulate the mMTC traffic signaling load and the inherent resource occupation time for both 4G and 5G systems in accordance with the activity timers advised by real mobile rollouts.

3.2. Simulation results

As previously mentioned, the novel RRC_{INACTIVE} state has been introduced to optimize both latency and signaling load as well as prolonging device battery duration. The introduction of this new state has reduced the signaling load caused by the frequent device state promotions to the $RRC_{\text{CONNECTED}}$. More specifically, the lower- to the higher-power state promotion transition in 5G will occur mostly from the RRC inactive state through the resume procedure generating only three signaling messages (instead of seven as was the case for 4G) [21].

As depicted in Fig. 1 and despite the fact that the 5G signaling exchange generated by the RRC state transitions to the connected mode is reduced, the mMTC traffic pattern still generates a significant signaling overhead SL using the 5G RRC three-states model as compared to the worst-case scenario of the 4G RRC two-states model (i.e. $T_{4\text{G}_{\text{inac}}} = 5\text{s}$). This is due to the fact that 5G systems exploit shorter inactivity timers to move from the RRC_{INACTIVE} to $RRC_{\text{CONNECTED}}$ as a result of their tight latency requirements, whereas mobile operators set out typical inactivity timer values between 5 s and 20 s for 4G systems for transitioning from RRC_{IDLE} to $RRC_{\text{CONNECTED}}$. On the other hand, increasing the inactivity timer effectively reduces the involved control plane signaling, but according to Table 2 this comes at the cost of low efficiency in radio resource utilization (i.e. a high T_{RO} time) and accordingly high power consumption which negatively impacts the performance of battery-empowered IoT devices. It can be clearly seen that SL and T_{RO} are two conflicting metrics heavily dependent on the choice of inactivity timer value, so it may be advantageous to find the optimal timer value according to the target service class. This motivate the design of adaptive solutions embracing traffic patterns awareness to deal with timer settings under service diversity and avoid radio resources waste in 5G networks.

Given the earlier observations, performance evaluation of the novel 5G RRC state machine model has shown that the choice of the timer controlling radio resources release after a period of inactivity is of paramount importance to avoid heavy signaling load and unnecessary resource consumption in the normal course of network operations.

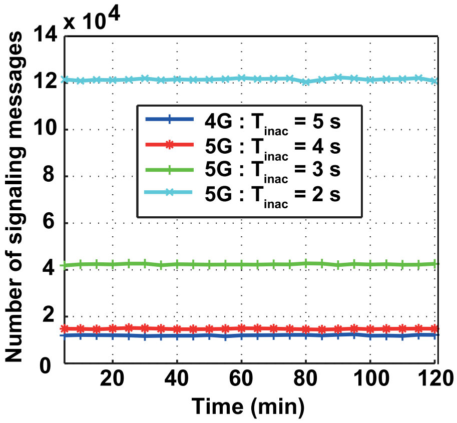


Fig. 1. New 5G RRC model vs 4G RRC model: Signaling load for the mMTC traffic model.

Table 2
mMTC resource occupation time for different 5G inactivity timers.

Inactivity timer (s)	2	3	4
T_{RO} (h)	1755	1912	1968

However, the situation can become even more detrimental if the network is under attack. Regarding the fragility of the air interface from the security perspective, such parameters can be intentionally intercepted and maliciously manipulated to overwhelm the 5G infrastructure. While this vulnerability is inherited from the previous mobile generations [11], we introduce a new possible attack that leads to network resource starvation through the injection of malicious software in a large number of vulnerable and buggy devices and subsequently trigger a massive number of simultaneous on-demand SIB requests. These two security flaws can jeopardize the availability of various network elements, and potentially open the door for further attack vectors against 5G infrastructure. The corresponding scenarios of both attacks will be illustrated in the next section.

4. Impact analysis of 5G RRC signaling threats

In this section, we will analyze the impact of two DoS signaling attacks exploiting the new enhancements brought to the RRC protocol in 5G systems. We start by analyzing a first attack that takes advantage of the new 5G RRC 3-states model (i.e. the new RRC_{INACTIVE} state) to launch a DoS attack aiming at overloading the 5G control plane. While this security flaw is not new and existed in early mobile generations [11], it can still be leveraged to degrade the safety of current 5G systems as we will successfully demonstrate hereafter.

4.1. 5G state dynamics-based DoS attack

DoS signaling attacks exploiting the inactivity timeout that manage the RRC state transitions have been emerged since 3G systems [5,7,9,10]. The primary objective of such attacks is to produce a heavy signaling load that can congest the control plane of mobile networks and likely lead to a global outage.

4.1.1. Attack scenario

Previous mobile generations (i.e. 2G/3G/4G) embrace specialized hardware equipment that are component-centric. Nowadays, however, 5G systems are shifting toward virtualized and software-based solutions making them easily remotely accessible and software controlled. Unfortunately, such features can be exploited by an unauthorized entity (endowed with sufficient resources) to gain access and maliciously monitor the network.

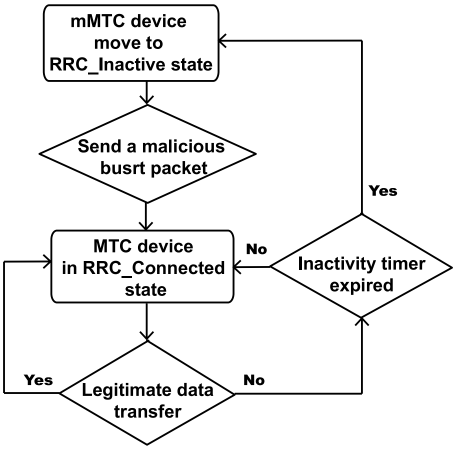

mMTC device move to RRC_Inactive state
Send a malicious busrt packet
MTC device in RRC_Connected state
Inactivity timer expired
Legitimate data transfer
Yes
No
Yes
No

Fig. 2. 5G State Dynamics-based DoS Attack scenario.

Table 3
Simulation parameters.

N_{mMTC}	T_{S}	$T_{5_{inac}}$	T_{Attack}	Ratio of infected devices
1000	7200 s	2 s, 3 s and 4 s	$\approx T_{5_{inac}}$	10%, 25% and 50%

For instance, an adversary can infiltrate the mobile traffic and control an important number of mMTC devices by either infecting their operating systems with a malware or through bypassing their authentication controls. Afterwards, the attacker will order them to send a burst of short packets regularly and immediately after the expiration of the inactivity timeout (i.e. $T_{5\text{G}_{\text{inac}}}$) to trigger frequent state transitions from RRC_{INACTIVE} to $RRC_{\text{CONNECTED}}$ and vice versa. These tremendous establishment and release messages can bring down the centralized unit, as the latter constitutes the termination point of the control plane. The periodicity of the attack (i.e. the frequency of injected packets sending) is denoted as T_{Attack}, and it is appropriately set by the attacker to be slightly larger than $T_{5\text{G}_{\text{inac}}}$ for a maximum impact. It is worth mentioning that traffic characteristics of mMTC services (i.e. short packet and massive access nature) make it very hard to detect such attacks using conventional intrusion detection tools (see Fig. 2).

4.1.2. Analysis and results

To evaluate the impact of the 5G DoS signaling attack described above, we will analyze the signaling load metric (i.e. SL) generated by the 5G NG-RAN infrastructure. Indeed, based on the same mMTC traffic model adopted in Section 3, we will simulate the signaling load SL maliciously produced by the induced RRC state transitions (promotions/demotions) for various portions of infected mMTC devices with respect to the total number of simulated devices N_{mMTC}, and with regard to different inactivity timers ranging from 2 to 4 s (see Table 3).

As depicted in Figs. 3(a), 3(b), and 3(c), the signaling load SL generated from the fraudulent state transitions (i.e. RRC_{INACTIVE} to $RRC_{\text{CONNECTED}}$) will increase the total signaling load up to 50% for an inactivity period of $T_{5G_{inac}} = 2$ s in case 500 mMTC devices are infected (i.e. half of overall connected users). In this case, the number of establishment + release messages attains 18.10^4. Bearing in mind that 5G networks and beyond are expected to handle ultra-high densities of connected devices (that can reach up to 1 million devices per kilometer square for 5G and much more for beyond 5G), the situation will be more disastrous by infecting larger sets of end-users, especially in case of smaller inactivity timers. In practice, critical mMTC services whose involved devices are machine-type and have tight delay constraints too (e.g. factory automation, early warning systems) are expected to flourish as a part of 5G and beyond, and accordingly can be the most susceptible to such attacks (see Fig. 3).

4.2. On-demand SI-based DoS attack

Little research effort has been devoted to designing and studying the concrete impact of DoS attacks on the 5G control plane. The technical paper [16] is a good attempt to enumerate potential attacks that can exploit the trust model of 5G networks, however these theoretical claims need to be corroborated with strong technical analysis to confirm the feasibility of such attacks (through providing concrete and practical attack scenarios) and the resulting performance loss.

Throughout this part, we will describe the second attack related to the newly introduced SI acquisition procedures. The attacker sends huge volumes of forged and fake on-demand SI requests in a short period of time. To the best of our knowledge, this attack has never been discussed in the previous literature, which make it a completely new 5G threat.

4.2.1. Attack scenario

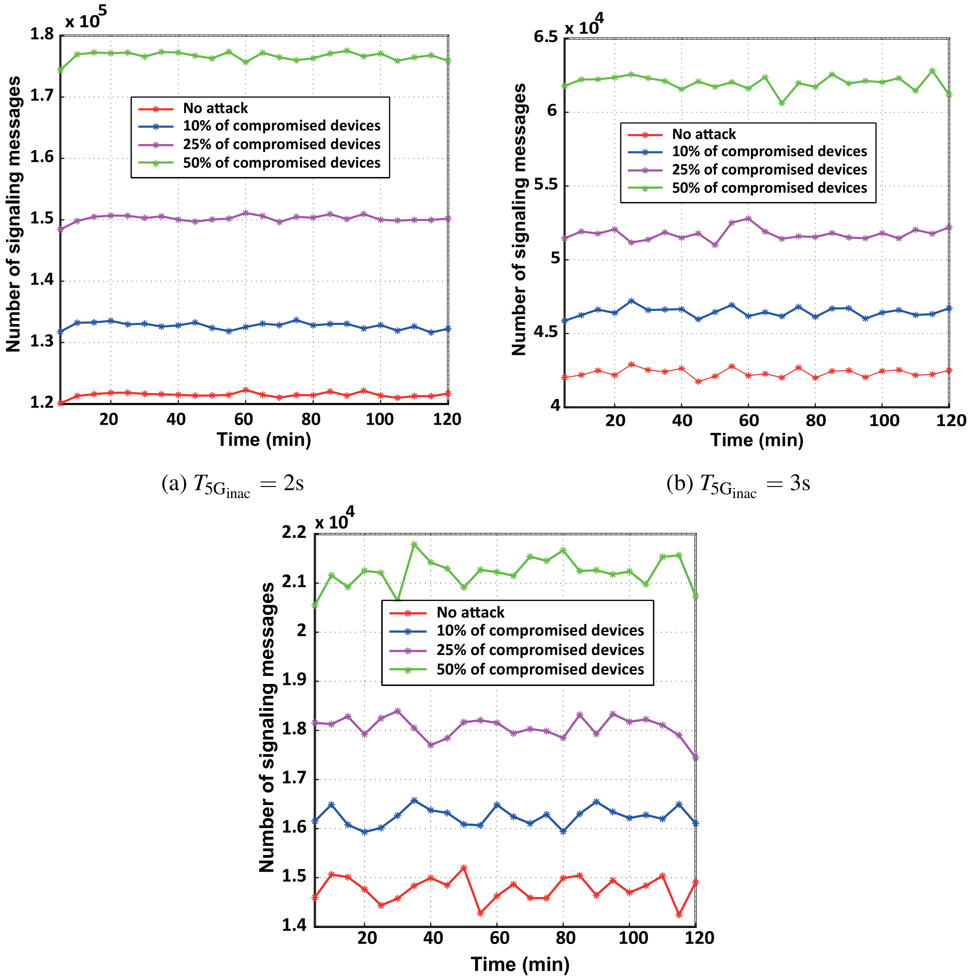
The SIBs are periodically broadcast to the end-users in LTE systems. This implies wasted energy especially when the cell is empty, and excessive signaling exchange due to the directional nature of millimeter communications envisioned for next generation wireless systems.

5G-NR implements two different classes of system information blocks. A first class referred to as **Minimum SI** transmitted periodically like in the conventional LTE case (i.e. MIB and SIB_1) and contains basic and critical information for UEs (e.g. initial cell selection and access), and a second class called **On-Demand SI** newly introduced and only transmitted upon explicit requests from UEs (i.e. SIB_2 to SIB_9).

We assume that the received SIB_1 indicates that the other SIBs are only provided on-demand, in which case SIB_1 needs to provide additional information regarding how the UEs can acquire their on-demand SIBs using a random access (RA) procedure.

A plethora of IoT services ranging from smart-homes and smart-grids to autonomous vehicles and smart-factories have profoundly affected our daily life. The mMTC class of 5G-NR is expected to support up to 1 million connections (at once) per square kilometer. This means that even a higher number of IoT devices or sensors can be concentrated in the same location. These devices are mostly designed with hard-coded authentication credentials to restrict the access to username/password information and also for an easier system administration at the first log-in. These default credentials, when left unchanged after the first application log-in, are easy to guess making it simple for attackers to bypass the authentication and have access and full control of these devices. Moreover, the lack of software upgrades in most sensors jeopardizes their security and privacy. Breaking down the authentication mechanism or exploiting the well-known vulnerabilities can both yield serious security flaws, making these devices exposed and easily manipulated by malicious third parties to launch different types of large-scale threats, including distributed denial of service (DDoS) attacks. Meanwhile, those devices are unfortunately used to silently spread malicious software and thus growing the group of compromised machines. In what follows, we assume an infected game app that contains a malware trying to make the user believe that it is frequently synchronizing the UE clock to avoid being rejected by the gaming server. This is a recurrent mechanism to prevent game cheating. The on-demand SIB_9 is responsible for such information related to Global Positioning System (GPS) time and Coordinated Universal Time (UTC).

After gaining control of a large number of infected 5G devices in either RRC_{IDLE} state or RRC_{INACTIVE} state, the hacker can use the malicious payload to remotely command these bots to send synchronized and coordinated on-demand SIB_9 requests each will trigger the RA procedure with the gNB-CU. A preamble is send by each infected UE to gNB over the physical RACH (PRACH) for each RA request. Similar to LTE, in 5G NR there are 64 preambles per cell. If more than 64 UEs make RA request simultaneously, more than one UE will select the same preamble leading to collision occurrences. The UEs whose preambles have been successfully acknowledged by the



(a) $T_{5G_{inac}} = 2s$

(b) $T_{5G_{inac}} = 3s$

(c) $T_{5G_{inac}} = 4s$

Fig. 3. New 5G RRC model Signaling overhead under a DoS signaling attack for different attack scenarios.

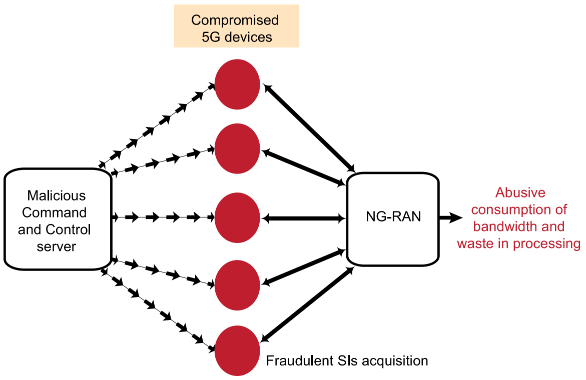

Compromised 5G devices
Malicious Command and Control server
NG-RAN
Abusive consumption of bandwidth and waste in processing
Fraudulent SIs acquisition

Fig. 4. On-demand SI DoS attack scenario.

gNB will normally continue the RA procedure. It is worth noting that the encoding process of the **Minimum SI** takes place in the gNB-DU, whereas the **On-Demand SI** are encoded by gNB-CU [22]. Therefore, the centralized unit is in charge of processing all the incoming SIB_9 requests from the malicious UEs thus putting a heavy burden on a single component and making it a single point of failure (see Fig. 4).

This procedure may be repeated multiple times until the maximum allowed number of preamble transmissions is exhausted, in which case the UEs may quit the RA procedure and fail to get access to the network. Even if a successful RA request is achieved within the upper limit of RA attempts, the access delay will considerably increase. Moreover, this problem is accentuated by the beam alignment constraint imposed by the directivity of the higher bands further complicating the whole RA mechanism.

The resulting congestion will block most of the RA attempts from legitimate collided UEs or at least will cause a long delay especially for trusted UEs performing initial uplink access and synchronization with their serving gNB. This leads to dropped calls and data connections, causing major network failure. The longer access duration is still intolerable and can become a serious impediment to the implementation of URLLC services, including connected vehicles frequently invoking handover procedures.

4.2.2. Impact evaluation

In this Section, we will evaluate the impact of the on-demand SI-based DoS attack that exploits the dedicated RRC signaling for SIB_9 provisioning to saturate system resources. This attack aims to deprive legitimate subscribers from accessing the 5G network leading to a huge number of delayed and/or failed connections and subsequently serious financial losses for the mobile operator. This can be achieved by disguising the corresponding malware as an innocent mobile application necessitating frequent time or GPS information updates which is a popular requirement in today's apps. To further increase the incident impact, We assume that the attacker will order the infected users to send their SIB_9 requests using the MSG_3-based scheme to ensure that the CU will respond through unicasting the SI to each individual device and consequently the number of SIB_9 deliveries is commensurate to the number of the victim devices.

Bearing in mind that RA procedure occasions are initiated according to a periodic cycle (usually set to 100 ms [18]), the unicasting delay denoted as T_b (which refers to the time needed to unicast the demanded SIB_9) is closely related to the repetitive RA cycle duration. Thereby, these attacks can be anticipated and scheduled in random time intervals immediately of the SI delivery causing a quick and hard-to-detect resource saturation.

In what follows, we assume that N_t refers to the total number of simulated devices, T_{MSG_j} and B_{MSG_j} define the transmission time and the data size respectively for the MSG_j, $\forall j \in \{1,2,3,4\}$. N_{mal} indicates the total number of compromised devices. To evaluate the impact of this new emerging DoS attack on the end-user performance, we consider two popular metrics. The collision probability P_c referring to the percentage of occurrences wherein two or more devices select the same RACH preamble to send a RA request with respect to the total number of available RACH preambles over the simulation period T_S, and the total transmission average delay $\overline{RA_{\text{delay}}}$ which denotes the time duration needed for each device to successfully access the network, in other words, the overall RA procedure time interval.

The above-cited metrics can be formulated as

$$P_c = \frac{\text{Number of preambles carrying two or more RA attempts (per second)}}{\text{Total number of available PRACHs (per second)}} \tag{1}$$

$$\overline{RA_{delay}} = \frac{\sum_{n=1}^{N_t} (T_{\text{MSG}_1} + T_{\text{MSG}_2} + T_{\text{MSG}_3} + T_{\text{MSG}_4} + T_w(n))}{N_t} \tag{2}$$

with

$$T_w(n) = \sum_{r=1}^{P} \mathbb{1}_{\{r\text{–th RACH procedure attempt}\}}(n) \cdot T_{\text{backoff}}$$

and

$$T_{\text{backoff}} = T_{\text{MSG}_2} + BI + RAR_{\text{win}}$$

where:

- T_w designates the MSG_1 waiting time for a successful preamble transmission.
- $\mathbb{1}_{\{r\text{–th RACH procedure attempt}\}}(n)$ an indicator function that indicates whether the device n succeeded the random access procedure on the rth retry or not. $T_w(n)$ can be viewed as an unit step function that monitors the end of the RA workflow for device n.
- P is the number of RACH attempts, the maximum allowed value for this parameter is set to ten.
- BI refers to the back-off indicator that indicates the time interval between two successive RACH procedures.
- RAR_{win} stands for the default RA response window.

On the other hand, to assess the impact of this attack on the CU, we will also evaluate the attack traffic load corresponding to the illegitimate bits generated by the malicious SI requests in both downlink BA_{down} and uplink BA_{up} directions for different attack periods, this is very useful to highlight the extra-processing time and capacity wasted by g-NB entity to encode and transmit the signaling messages exchanged during the malicious on-demand SI acquisition requests.

The SIB_9 message size B_{SIB_9} is about 56 bits. Mainly, the logical Broadcast Control Channel (BCCH) is used to transmit the SIs messages including MIB and SIBs. The SIBs messages are mapped into the downlink shared channel (DL-SCH) transport channel and then onto the Physical downlink shared channel (PDSCH).

Algorithm 2 SIB based DoS attack

```
for a given execution period $T_S$ do
    for $N_t$ simulated devices do
        Simulate the data traffic according to URLLC traffic pattern for 5% users among the total $N_t$ simulated devices.
        Simulate the data traffic according to non-URLLC traffic pattern for 95% users among the total $N_t$ simulated devices.
    end for
    Generate the RACH preamble malicious requests for $N_{mal} \in \{0,500,1000,1500,2000\}$ compromised devices.
    Compute the collision probability $P_c$ using Eq. (1).
    Compute the total transmission average delay $\overline{RA_{delay}}$ using Eq. (2).
    Compute the attack traffic load corresponding to the illegitimate bits generated by the malicious SI requests in both downlink $BA_{down}$ and uplink $BA_{up}$ directions according to Eqs. (3) and (4).
end for
```

Table 4
Simulation parameters [18,23].

T_S	T_{MSG_1}	T_{MSG_2}	T_{MSG_3}	T_{MSG_4}
3600 s	1 ms	3 ms	5 ms	5 ms
N_t	BI	RAR_{win}	URLLC traffic model	Non-URLLC traffic model
10000	Uniform (0,20) ms	5 ms	Beta arrival distribution (T = 10 s)	Uniform arrival distribution (T = 30 s)
B_{MSG_1}	B_{MSG_2}	B_{MSG_3}	B_{MSG_4}	B_{SIB_9}
64 bits	56 bits	48 bits	184 bits	56 bits

Accordingly, the quantities BA_{down} and BA_{up} read

$$BA_{\text{down}} = \sum_{n=1}^{N_t} \sum_{t=0}^{T_S} \mathbb{1}_{\{\text{malicious SI request occurrence}\}}(t) \cdot (B_{\text{MSG}_2} + B_{\text{MSG}_4} + B_{\text{SIB}_9}) \tag{3}$$

and

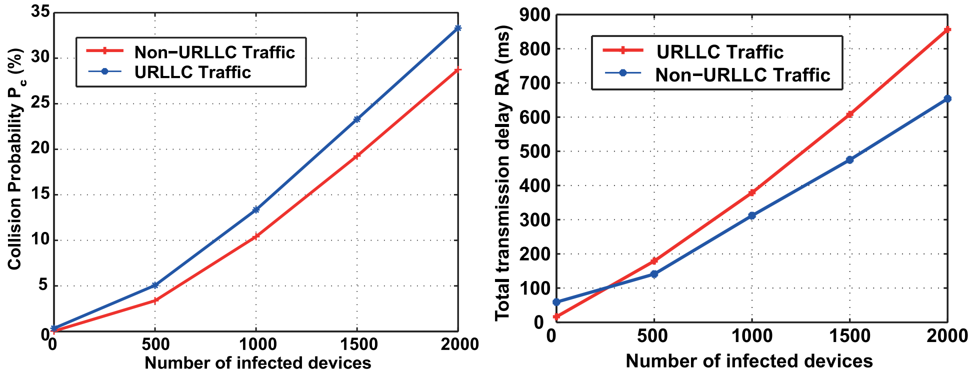
$$BA_{\text{up}} = \sum_{n=1}^{N_t} \sum_{t=0}^{T_S} \mathbb{1}_{\{\text{malicious SI request occurrence}\}}(t) \cdot (B_{\text{MSG}_1} + B_{\text{MSG}_3}) \tag{4}$$

4.2.3. Analysis and results

Combining 5% of URLLC and 95% of non-URLLC devices [18,23], we will simulate the collision probability P_c, the total transmission average delay $\overline{RA_{\text{delay}}}$, and the malicious traffic loads BA_{down} and BA_{up} using the parameters setting illustrated in Table 4.

As shown in Fig. 5(a), the on-demand SI DoS attack increases significantly the collision probability for both URLLC and non-URLLC traffic patterns, which may block a big number of legitimate RA attempts. It can be also noticed that the URLLC users experience higher collision probabilities compared to their non-URLLC counterparts, which will dramatically disrupt the responsiveness of such communications and substantially increase the corresponding access delay.

5G systems are designed to support low latency communications (i.e. URLLC), and the average end-to-end latency in 5G networks is around 10 ms. As illustrated in Fig. 5(b), the average total transmission delay will tremendously increase proportionally to the number of compromised devices. This delay will reach 850 ms for the URLLC traffic in the case of 2000 infected devices, incurring unacceptable delays for this type of services. Thus, this kind of on-demand SI-based DoS anomalies will lead to slow and interrupted connections causing a serious network breakdown (see Fig. 5).



(a) Collision probability P_c

(b) Average of total transmission delay $\overline{RA_{\text{delay}}}$

Fig. 5. Simulation results for different number of compromised devices.

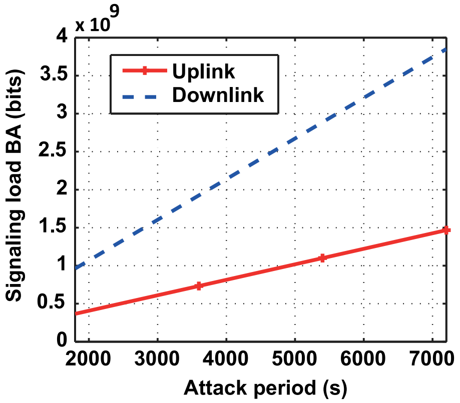


Fig. 6. SI attack signaling load BA for different attack periods and for $N_{\text{mal}} = 1000$.

As we can infer from the simulation results depicted in Fig. 6, the downlink signaling traffic caused by the malicious SI requests is significantly larger than its uplink counterpart. The malicious downlink traffic is handled by the g-NB entity, that encodes and transmits about $B_{\text{MSG}_2} + B_{\text{MSG}_4} + B_{\text{SIB}_9} = 296$ bits per each malicious SI request. For 1000 infected devices, the g-NB control plane needs to handle an extra-traffic of about 2 Gigabytes over one hour attack period. Taking into consideration the diversity of services to be served by the g-NB, this fraudulent traffic will constitute a supplementary computational burden that impacts the availability of the g-NB limited resources, namely, the BCCH logical channel. The availability of these scarce resources will be even more seriously affected if the number of infected devices increases.

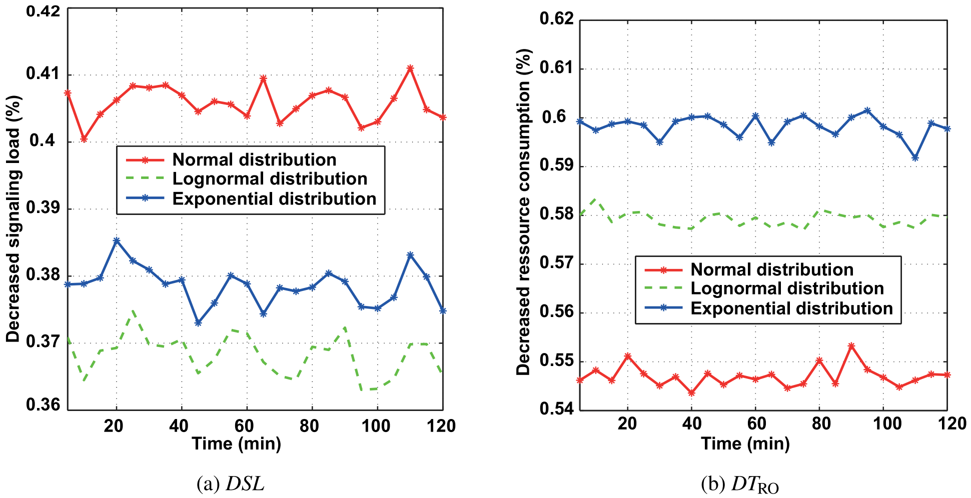
4.3. Security mechanisms for mitigating RRC-based DoS signaling attacks

4.3.1. Proposed solutions

Despite the security reinforcement and the network defenses brought by 3GPP (e.g. enhanced authentication methods [24]), securing the air interface is still a major concern in 5G designs largely due to the diversity of 5G use cases. For instance, we have deeply analyzed two emerging DoS attacks in the preceding Sections 4.1 and 4.2, and we have put into evidence their serious impact on the mMTC and URLLC service classes respectively.

Security consciousness should be integrated into the requirements specifications and standards development from early design stages. The lessons learned from older generations should provide guiding principles for designers and developers of future 5G and beyond systems. The protection of the 5G radio link along with devices should not be neglected in favor of more attractive features and novel capabilities. To this end, fundamental system information such as SIB messages should be communicated to 5G devices using an encrypted and integrity-protected radio channel. Furthermore, 5G devices should be regularly updated and endowed with basic and free anti-malware and anti-virus solutions to identify malicious applications. Modern security frameworks and tools should embrace a high degree of intelligence to operate in an autonomous and proactive fashion. In particular, artificial intelligence (AI)- and deep learning (DL)-based approaches are nowadays among the most promising techniques used to protect information systems and address several security issues including malware/software analysis, intrusion/fraud/botnet detection, and malicious activities prediction. For instance, authors in [25] proposed a malware detection framework relying on deep neural networks to distinguish whether a given software is benign or malicious for the 5G android devices. On the other hand, privileges and permissions should be carefully managed. For instance, authors of [26] proposed a three-phases cybersecurity framework able to identify malicious edge devices that misuses their granted privileges in IoT and fog computing environments. Privacy preservation is also a key requirement in recent and emerging services to avoid tracking users and emulating their behavior. For example, vehicular networks are nowadays an integral part of mobile networks but their high mobility and the large amounts of sensitive data being exchanged can lead to serious privacy concerns necessitating advanced location and trajectory privacy protection [27]. All the aforementioned frameworks can integrate ethical hacking and penetration tests to improve the robustness of attack detection and prevention. In fact, ethical hacking can be used to evaluate and identify security weaknesses and flaws in mobile applications and operating systems, and to pen-test the attack landscape to better defend against the emerging threats, including social engineering, advanced malware, out-of-date devices and data leakage. Further research efforts should be deployed to come up with innovative ways making all these supplemental security layers very lightweight in terms of energy and computation efficiency.

Advanced prevention and/or detection mechanisms should be integrated into the virtualized 5G components to face signaling threats. Among the most robust solutions, randomization of system parameters can be applied so that malicious third parties are unable to exploit their intercepted data or their prior knowledge about the system operating mode in a malicious fashion. This technique was proposed as a preventive solution to defend against DoS signaling attacks in 3G networks [9], and it can be also applied to meet the same issue in the context of 5G systems as illustrated in the next subsection. For the sake of simplicity and without loss of generality, we will limit our analysis to the first attack and we will assess the impact of randomizing the inactivity timer $T_{5_{\text{inac}}}$ as a mean to secure the 5G RRC state machine. In the same way, randomization can be leveraged to randomize the



(a) DSL (b) DT_{RO}

Fig. 7. Performance evaluation of randomization based detection framework for 50% of compromised mMTC devices and $T_{5G_{\mathrm{inac}}}$ = 2 s.

parameters involved in RRC signaling used in the request and delivery of the on-demand SI.

4.3.2. Analysis and results

The performance evaluation of the randomization-based detection framework within 5G systems is based on two major metrics that are the decreased signaling load DSL and the decreased time of resources occupation DT_{RO}. The DSL resulting from using the randomized method compared to the normal case (when no defense mechanisms are implemented) is the evaluated metric for the signaling efficiency. While for the resource consumption, the radio bearer occupancy time DT_{RO} during the randomized inactivity period compared to the static inactivity period (when no defense mechanisms are implemented) will be the second performance metric. Based on the mMTC massive sensors traffic pattern already described in sub Section 3.1, we will analyze the DSL and the DT_{RO} with respect to the new 5G RRC state handling under the DoS signaling attack discussed in sub Section 4.1, and regarding different statistical distributions, namely, Gaussian, Log-normal and Exponential distributions.

$$DSL = \frac{SL\{rnd = 0\} - SL\{rnd = 1\}}{SL\{rnd = 0\}} \tag{5}$$

$$DT_{\mathrm{RO}} = \frac{T_{\mathrm{RO}}\{rnd = 0\} - T_{\mathrm{RO}}\{rnd = 1\}}{T_{\mathrm{RO}}\{rnd = 0\}} \tag{6}$$

where:

$$\begin{cases} SL : \text{Signaling Load (in number of signaling messages.)} \\ T_{\mathrm{RO}} : \text{Resource Consumption Time.} \\ rnd : \text{A bit that indicates whether the randomization solution is} \\ \qquad \text{adopted } (rnd = 1\ ) \text{ or not.} \end{cases}$$

We have chosen the worst-case scenario to evaluate our detection mechanism using an inactivity timeout of $T_{5G_{\mathrm{inac}}}$ = 2 s and assuming half of total mMTC devices are compromised, in which case a huge volume of signaling load will be produced. As illustrated in Fig. 7, the three simulated distributions, namely Gaussian, Log-normal and Exponential functions reduce considerably the signaling load, while avoiding the unnecessary resource consumption. As highlighted in Table 5, by using randomization approach, we have arrived to mitigate efficiently the signaling load generated from malicious signaling attacks against 5G system while maintaining the resource consumption in a optimum level. Even more important, the randomization based Exponential technique, has shown better results in 5G context when compared to 3G context. Hence, the randomization approach remains very promising solution to be considered in mitigating the signaling threats in the new generations of mobile networks. First, this method offers a preventive framework that can avoid the occurrence of such attacks or at least mitigating their impact. Secondly and from a hardware perspective, the proposed randomized approach needs simply some low-complexity software updates in only some network entities such us g-NB.

Table 5
Randomization based detection framework: 5G vs 3G/4G performance comparison.

	Randomization based Distributions					
	Gaussian		Log-normal		Exponential	
	DSL (%)	DT_{RO} (%)	DSL (%)	DT_{RO} (%)	DSL (%)	DT_{RO} (%)
3G/4G	46.53	55.99	42.27	10.98	31.91	13.12
5G	40.58	54.70	36.82	57.92	37.86	59.82

5. Conclusion

In this work, we have outlined a number of security concerns threatening the 5G NG-RAN infrastructure. By analyzing the novel 5G RRC protocol features for high-frequency low-volume traffic patterns (e.g. mMTC), we have unveiled some security flaws that can be exploited by a fraudulent entity to launch DoS attacks against the g-NB entity. In particular, we dived deeper into two forms of such attacks. The first (second, resp) attack maliciously monitors the machine state transitions (the on-demand system information acquisition procedures, resp) to trigger excessive connection and release messages (random access attempts, resp). Both attacks can be easily engineered by simply recruiting an army of bots from any location, and are particularly dangerous as they can go unnoticed by network administrators and can lead to the whole system collapse. By emulating an mMTC traffic generator using Matlab, we have demonstrated the destructive power of both attacks in terms of service experience degradation (user side) and energy inefficiency (network side). We have then highlighted some recommendations to counter such emerging 5G threats. Notably, a randomization-based approach has been experimented to cope with the aforementioned kind of attacks. Compared to the attack-free scenario, the improvement in terms of signaling load and resource occupation time attains 37.86% and 59.82% respectively when the inactivity timer obeys an Exponential (instead of a static) distribution. Finally evolving the RRC protocol behavior (e.g. parameters and procedures) to be highly dynamic and adaptive with real-time service awareness capabilities through ubiquitous intelligence could be the way forward to strengthen the security of 5G systems and beyond, and will be the basis of our future works.

CRediT authorship contribution statement

Raja Ettiane: Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Abdelaali Chaoub:** Conception and design of study, Acquisition of data, Analysis and/or interpretation of data, Writing – original draft, Writing – review & editing. **Rachid Elkouch:** Conception and design of study, Writing – review & editing.

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.

Acknowledgment

All authors approved the version of the manuscript to be published.

References

[1] Series M. IMT vision–framework and overall objectives of the future development of IMT for 2020 and beyond. 2015, Recommendation ITU 2083.

[2] 3GPP. 3GPP TR 38.801 V14.0.0 (2017-03): Study on new radio access technology: Radio access architecture and interfaces. 2017.

[3] Da Silva IL, Mildh G, Säily M, Hailu S. A novel state model for 5G radio access networks. In: 2016 IEEE international conference on communications workshops. IEEE; 2016, p. 632–7.

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

[5] Signaling-oriented DoS attacks in UMTS networks.

[6] Pavloski M. Signalling attacks in mobile telephony. In: International ISCIS security workshop. Springer; 2018, p. 130–41.

[7] Abdelrahman OH, Gelenbe E. Signalling storms in 3G mobile networks. In: 2014 IEEE international conference on communications. IEEE; 2014, p. 1017–22.

[8] Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A. 5G security: Analysis of threats and solutions. In: 2017 IEEE conference on standards for communications and networking. IEEE; 2017, p. 193–9.

[9] Ettiane R, Chaoub A, Elkouch R. Enhanced traffic classification design through a randomized approach for more secure 3G mobile networks. In: 2016 International conference on wireless networks and mobile communications. IEEE; 2016, p. 116–21.

[10] Lee PP, Bu T, Woo T. On the detection of signaling DoS attacks on 3G wireless networks. In: IEEE INFOCOM 2007-26th IEEE international conference on computer communications. IEEE; 2007, p. 1289–97.

[11] Ettiane R, Chaoub A, Elkouch R. Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks. In: 2018 19th IEEE Mediterranean electrotechnical conference. IEEE; 2018, p. 62–7.

[12] Jover RP, Marojevic V. Security and protocol exploit analysis of the 5G specifications. IEEE Access 2019;7:24956–63.

[13] Khan R, Kumar P, Jayakody DNK, Liyanage M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. IEEE Commun Surv Tutor 2019;22(1):196–248.

[14] Singla A, Hussain SR, Chowdhury O, Bertino E, Li N. Protecting the 4G and 5G cellular paging protocols against security and privacy attacks. Proc Priv Enhanc Technol 2020;2020(1):126–42.

[15] Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M. Security for 5G and beyond. IEEE Commun Surv Tutor 2019;21(4):3682–722.

[16] Tao W, Mansour G. Security Analysis Of 5G Mobile Networks; A Technical Paper Prepared for SCTE.ISBE.

[17] 4G-5G Interworking RAN-Level and CN-Level Interworking White Paper, June 2017.

[18] Yang W-Y, Lin K-H, Wei H-Y. 5G on-demand SI acquisition framework and performance evaluation. IEEE Access 2019;7:163245–61.

[19] Maternia M, El Ayoubi SE, Fallgren M, Spapis P, Qi Y, Martín-Sacristán D, et al. 5G PPP use cases and performance evaluation models. Tech. rep., 5G-PPP; 2016.

[20] 3rd Generation Partnership Project. Technical Specification Group Radio Access Network; Study on Licensed-Assisted Access to Unlicensed Spectrum;(Release 13).

[21] Icaro LDS, Gunnar M, Paul S-B, Magnus S, Alexander V. Meeting 5G Latency Requirements with Inactive State (19 June 2019). Ericsson Technol. Rev. 2019.

[22] NG-RAN, F1 general aspects and principles (Release 15), 3GPP TS 38.470. 2018.

[23] Thota J, Aijaz A. On performance evaluation of random access enhancements for 5G uRLLC. In: 2019 IEEE wireless communications and networking conference. IEEE; 2019, p. 1–7.

[24] 3GPP security architecture and procedures for 5G system 3GPP TS33.501 Release 15. 2018.

[25] Lu N, Li D, Shi W, Vijayakumar P, Piccialli F, Chang V. An efficient combined deep neural network based malware detection framework in 5G environment. Comput Netw 2021;189:107932.

[26] Sohal AS, Sandhu R, Sood SK, Chang V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput Secur 2018;74:340–54.

[27] Liao D, Li H, Sun G, Zhang M, Chang V. Location and trajectory privacy preservation in 5G-enabled vehicle social network services. J Netw Comput Appl 2018;110:108–18.