Mitigating Denial of Service Signaling Threats in 5G Mobile Networks

Raja Ettiane[1], Rachid EL Kouch[2]
National Institute of Posts and
Telecommunication

***Abstract*—With the advent of 5th generation (5G) technology, the mobile paradigm witnesses a tremendous evolution involving the development of a plethora of new applications and services. This enormous technological growth is accompanied with an huge signaling overhead among 5G network elements, especially with emergence of massive devices connectivity. This heavy signaling load will certainly be associated with an important security threats landscape, including denial of service (DoS) attacks against the 5G control plane. In this paper, we analyse the performance of a defense mechanism based randomization technique designed to mitigate the impact of DoS signaling attack in 5G system. Based on massive machine-type communications (mMTC) traffic pattern, the simulation results show that the proposed randomization mechanism decreases significantly the signaling data volume raised from the new 5G Radio Resource Control (RRC) model under normal and malicious operating conditions, which up to 70% while avoiding the unnecessary resource consumption.**

***Keywords*—5G New Radio (NR) network; Radio Resource Control (RRC) state model; Denial of Service (DoS); signaling threats; randomization**

I. Introduction

The emergence of the 5G standard was accompanied with a phenomenal rise in traffic volumes emanating from various new services and applications. To meet these new challenges, 5G technology has introduced three new classes of services, namely, the enhanced mobile broadband (eMBB), massive machine-type communications (mMTC) and ultra-reliable low latency communications (URLLC) [1]. While the eMBB services will ensure an enhanced throughput, the mMTC services will handle massive number of connected devices with stringent energy efficiency and battery autonomy constraints, and the URLLC use case will provide low latency and high reliability services [2]. These new 5G challenging requirements will certainly increase the complexity of the management procedures designed to handle the rising demand of mobile subscribers.

To reduce network signaling complexity and unnecessary control transmissions, ongoing research works are progressing in many fronts with the aim of optimizing the signaling load for a robust and ultra-lean 5G designs. Indeed, a novel radio resource control (RRC) inactive state $RRC_{INACTIVE}$ have been introduced for Next Generation of Radio Access Network (NG-RAN) [3] to enhance the energy efficiency, reduce the latency and optimize the signaling load through optimizing the idle-to-connected state transition. Even if the new 5G RRC model was developed to meet the huge signaling overhead handled by the cellular paradigm, the short inactivity timers joined to the tremendous number of connected devices will entail a number of security flaws, including the problem of Denial of Service (DoS) attacks against the next generation of radio access network (NG-RAN) signaling control plane, named signaling threats. The DoS signaling threats were first emerged in 3G system [4], [5], [6], [7], involving the signaling attack that exploits the Radio Access Bearer (RAB) allocation/ release procedures to overload 3G entities, specifically the Radio Network Controller (RNC) entity. By using the well known network parameter, named inactivity timer $T_{5G_{inac}}$, this attack could be also carried out against the 5G system to overload the signaling control plane, which can disturb the network functionality giving rise to a productivity loss for network operator.

Several research works have tackled the problem of signaling threats in 3G/4G mobile networks and have proposed detection and defense mechanisms to mitigate the impact of such attacks [4], [8], [10], but little research efforts have been dedicated to signaling-based threats in 5G context. A survey of the 5G security architecture related to the primary protocols of the control plane signalling was presented in [11], [12]. In [13], the authors have proposed a defence mechanism to protect the paging protocols against security and privacy attacks [14]. The proposed solution aims at securing the 4G/5G devices from unauthorized/fake paging messages by introducing a new identifier, named P-TMSI, randomizing the paging occasions, and conceiving a symmetric-key based broadcast authentication framework. In [15], the issue of DoS signaling attacks in different mobile network generations was outlined, including the post-5G technologies. This work provided also some security solutions to protect the 5G system against these threats, involving securing the data information exchange over the radio link and make the access more difficult for malicious parties.

Unfortunately, these few research works are still not enough to address the damaging 5G signaling threats, involving the DoS signaling attack tackled in this work. Hence, this paper extends our defense mechanism proposed in [10], as a preventive solution to defend against DoS signaling attack in 3G network, to meet also the problem of signaling threat in 5G system. Based on mMTC traffic model, the proposed mitigation mechanism based randomization technique has shown also promising results in decreasing the signaling load generated by the 5G infrastructure under signaling DoS attack while preventing the unnecessary use of the network resources.

The rest of the paper begins with a background section giving an overview of the new 5G RRC state model, and highlighting some security flaws of this novel RRC three-state model. The section three analyses the 5G DoS signaling attack detection mechanism based randomization technique. This section presents first an overview on related works, then, it outlines the traffic model used for the performance evaluation of the detection framework, which is introduced at a later stage. Still in the same section, the simulation results are carried out to evaluate the effectiveness of the randomization based detection solution in defending against DoS signaling attack in 5G mobile network. Finally, the section four concludes the paper.

II. Background

In cellular systems, wireless communications between the devices and the network are carried out using the RRC protocol that is responsible for allocating and releasing the necessary radio resources. The signaling load produced by these resource allocation and release procedures will increase tremendously, specifically with the great variety of applications based on burst traffic (e.g., mMTC use case), which could disturb the proper functioning of the mobile networks infrastructures. As depicted in Fig. 1, in 5G system, a new RRC state, named $RRC_{INACTIVE}$, is introduced to meet the challenge of signaling overhead, battery life and latency. This novel $RRC_{INACTIVE}$ state is designed to reduce the latency by minimizing the signaling exchange triggered by the transition to RRC connected state $RRC_{CONNECTED}$ among the 5G infrastructure, which would be relevant for many smartphone applications that transmit small data on a frequent basis. This new state will also allow devices to conserve their batteries life by reducing the signaling load generated by the idle-connected states transitions. Indeed, in the $RRC_{INACTIVE}$ state, the device stores the RRC context (Access Stratum (AS) context) and maintains the core network (CN) connection established, and any detected traffic activity will trigger the transition to $RRC_{CONNECTED}$ state through a resume procedure using only three signaling messages instead of seven messages used in the switching process from the idle state (RRC_{IDLE}) to the connected state in 4G system [16]. The transitions between $RRC_{CONNECTED}$ and $RRC_{INACTIVE}$ states occur transparently to the CN. indeed, the CN network may carry any downlink traffic to the RAN entity so that the state transition from $RRC_{INACTIVE}$ to $RRC_{CONNECTED}$ does not involve any CN signaling exchange. As illustrated in Fig. 1, the new 5G RRC state model involves three states, namely, RRC_{IDLE}, $RRC_{CONNECTED}$ and $RRC_{INACTIVE}$. In this RRC three-state model, the transition from RRC_{IDLE} to $RRC_{CONNECTED}$ will primarily occur during the first UE attaches to the network or as a fallback to a new RRC connection. Hence, this transition will hardly arise when compared to the transition from $RRC_{INACTIVE}$ to $RRC_{CONNECTED}$, and with the shorter inactivity timeouts managing this later transition [17], the signaling load remains important even if the number of exchanged signaling messages related to the 5G RRC three-state transitions is reduced by introducing the $RRC_{INACTIVE}$ state, specifically when the 5G NG-RAN network is under a DoS signaling attack. indeed, a malicious exploiting of this inactivity timeout will give arise to two DoS attack scenarios. The first scenario is similar to the signaling attack tackled in [20], which aims at affecting and compromising an important number of MTC devices, and forcing them to send periodic burst packets after the expiration of the inactivity timer to trigger frequent resource allocation and release procedures, thus causing a peak of signaling load that can not be properly sustained by the mobile infrastructure. Adversely, the second attack scenario aims to consume abusively the NG-RAN radio resources by maintaining a set of compromised devices in the $RRC_{CONNECTED}$ state for a considerable period of time leading to a network resource starvation. There are other security risks threatening the NG-RAN infrastructure, involving, the integration with the existing vulnerable systems, namely, Internet and 4G network, the immaturity of the 5G production process and maintenance procedures, and the overgrowth of the 5G components. These security flaws could amplify the risk of breaking down the confidentiality, integrity, and availability of network elements, and giving rise to more attack vectors against 5G system. Therefore, developing a robust a defense system that can protect the 5G system against such security threats, will be a serious challenge for mobile service providers.

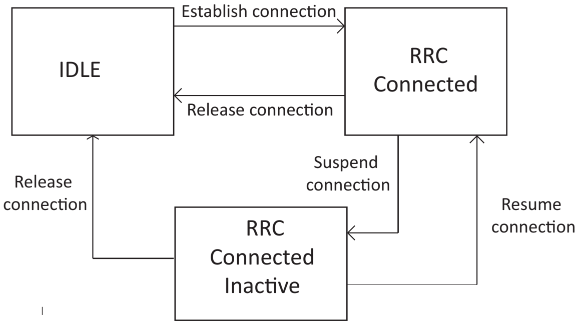

Fig. 1. 5G RRC State Machine Model.

III. 5G DoS Signaling Detection Mechanism based Randomization Technique

In this paper, we will evaluate the proposed detection mechanism based randomization approach regarding the DoS signaling attack exploiting the new 5G RRC three-state machine by analyzing the decreased signaling overhead ratio DSO_R and the network resource occupation time ratio ROT_R related to NG-RAN RRC handling process regarding different statistical distributions, namely, Gaussian, Log-normal and Exponential distributions. To carry out the performance evaluation of the proposed detection framework within 5G system, we will use the mMTC massive sensors traffic pattern [18] as 5G networks are expected to handle an significant amount of mMTC communications.

A. Related Works

To consolidate the security perimeter against signaling attacks in mobile networks, several protection mechanisms have been proposed in the literature review, specifically, for 3G and 4G networks. Among these defense solutions, a randomization method applied to some configuration parameters, like the channel inactivity timeout, has been proposed in [8], [9], [10], to increase the difficulty of hacking the value of such extremely vital network settings. According to [8], the randomization technique attributes the same random inactivity timeout to all UEs handled by the same 3G Radio Network Controller (RNC) regardless of the traffic volume handled by these UEs. The randomization approach proposed in [8] presented some drawbacks related to a rise in resource consumption due to system configuration that becomes dynamic and no longer optimal, leading to an unbalanced resource consumption among different traffic patterns. Hence, [10] has proposed an enhanced randomization based detection framework to cope with the DoS signaling attacks in 3G system while optimizing the resulting resource consumption as well. Indeed, this improved randomization technique deployed an additional concept of classifying the devices according to the traffic volume periodically received by the 3G control plane over the corresponding measurement reports. In 5G context, the randomization approach has been used to defend against paging message hijacking attack [13]. Indeed, this solution aims at randomizing the paging occasion, which consists on changing the paging occasion after every paging cycle regardless of whether the 5G device received any paging message in that paging cycle. Such an approach, however, depletes rapidly the available P-TMSI values, and requires that the device and the base-station should be accurately synchronized.

B. Traffic Modeling: mMTC use Case

mMTC communications connect a plenty of devices constrained by cost and energy considerations. mMTC can be used for monitoring and area-covering measurements through sensor and actuator deployments. This 5G traffic use case is usually modeled using the 3GPP bursty traffic FTP model 3 [18], which is based on Bursty traffic with a fixed-size packet following a Poisson arrival process with rate λ, packet inter-arrival time $f_{D,mMTC}(t)$ and packet size $f_{Y,mMTC}(t)$. According to [18], the number of mMTC devices is about 25000 per cell, in this paper, we will simulate the traffic pattern related to N_{mMTC} connected devices. Using the traffic model parameters described in Table I, we will first simulate the mMTC signaling load generated by the new 5G RRC state handling under a different DoS signaling attack scenarios in accordance with various $T_{5G_{inac}}$, namely, 1 s, 2 s and 3 s. Then, we will evaluate the DSO_R and ROT_R metrics to demonstrates the effectiveness of the proposed defense solution in mitigating the DoS signaling attack in 5G system.

TABLE I. MMTC SIMULATION PARAMETERS

N_{mMTC}	T_s	T_{inac}	$f_{Y,mMTC}(t)$	$f_{D,mMTC}(t)$
1000	7200 s	1 s, 2 s, and 3 s	125 B	1 s

C. Detection Framework

For the mMTC traffic model, we have a well known behaviour of devices, which transmit the same amount of data $f_{Y,mMTC}$ during a defined transmission time period $f_{D,mMTC}$, so the data traffic classification is meaningless in this case. To this end, we will use the randomisation techniques as follows:

For the Gaussian distributions, μ is set to $T_{5G_{inac}}$, and σ $=T_R$.

For the exponential case, we use a modified exponential distribution (weighted by a factor w), the λ are computed as:

$$\begin{cases}\frac{1}{\lambda}{=}T_{5G_inac}{\times}w; \quad w{=}\sqrt{\frac{{T_{5G_inac}}^2}{T_R}}\end{cases} \tag{1}$$

For the log-normal distribution, the μ and the σ are computed as follows:

$$\begin{cases}\mu{=}\log(\frac{{T_{5G_inac}}^2}{\sqrt{T_R{+}{T_{5G_inac}}^2}}) \\ \sigma{=}\sqrt{log(\frac{T_R}{{T_{5G_inac}}^2}+1)}\end{cases} \tag{2}$$

Where:

$$\{T_R{=}a * T_{5G_inac} \tag{3}$$

The weighted parameter a is set so that the available inactivity timers remain in the interval [1s 10s] defined for 5G standard.

D. Analysis and Results

To evaluate the performance of the proposed detection mechanism, we will analyze two metrics, namely, the DSO_R related to the promotion state transition to $RRC_{CONNECTED}$, and the ROT_R which refers to the ration of time period that device remains inactive in $RRC_{CONNECTED}$ state in normal case ($T_{5G_{inac}}$ is static) regarding the resource occupation time related to randomized $T_{5G_{inac}}$.

$$DSO_R = \frac{SL(N) - SL(R)}{SL(N)} \tag{4}$$

$$ROT_R = \frac{T_{\mathrm{RO}}(N) - T_{\mathrm{RO}}(R)}{T_{\mathrm{RO}}(N)} \tag{5}$$

Where:

$$\begin{cases}SL\text{: Signaling Load (in number of signaling messages)} \\ T_{\mathrm{RO}}\text{: Resource Consumption Time} \\ R\text{: Randomization} \\ N\text{: Normal case}\end{cases}$$

By periodically launching a DoS signaling attack using different numbers of compromised mMTC devices (10%, 25% and 50% of the total number of simulated devices N_{mMTC}) every $T_{5G_{inac}}$ (attack period), we will first evaluate the generated signaling load when no defense mechanism is implemented for different inactivity timeouts, namely, 1s, 2s and 3s. From the simulation results depicted in Fig.2, Fig. 3 and Fig. 4, we can infer that the mMTC traffic pattern gives rise to a larger signaling load for the smaller inactivity timers even in case when no DoS signaling attack is initiated. The high amount of signaling traffic for the small value of inactivity timer ($T_{5G_{inac}}$ =1s) can be justified by the fact that the mMTC traffic pattern is a Poisson distribution with a mean inter arrival rate λ_{mMTC} about one packet per second, thus, a higher $T_{5G_{inac}}$ (superior to 1s) means less state transitions between $RRC_{INACTIVE}$ and $RRC_{CONNECTED}$ states and then less signaling load.

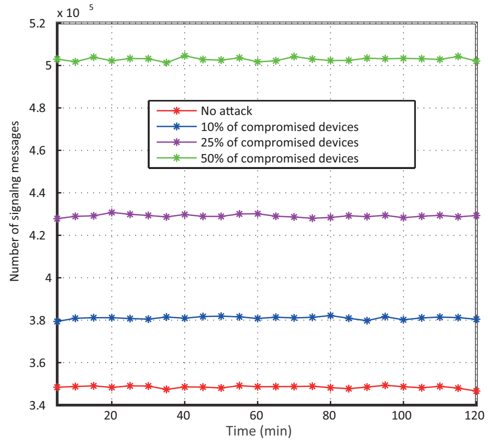

Fig. 2. New 5G RRC Model Signaling Overhead under a DoS Signaling Attack for $T_{5G_{inac}} = 1$s.

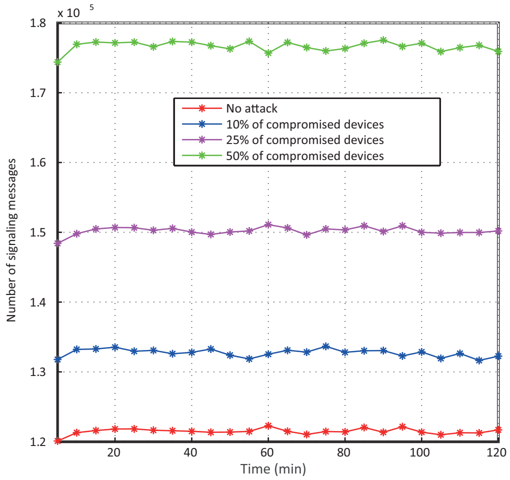

Fig. 3. New 5G RRC Model Signaling Overhead under a DoS Signaling Attack for $T_{5G_{inac}} = 2$s.

Regarding the two simulated metrics DSO_R and ROT_R, the performance evaluation of the randomisation based detection mechanism has shown promising results in mitigating the impact of DoS signaling attack against the novel 5G RRC three-state model. As illustrated in Fig. 5 and Fig. 6, the three simulated distributions, namely Gaussian, Log-normal and exponential functions reduce considerably the signaling overhead and the unnecessary resource consumption, which reach 70% and 65%, respectively for the exponential distribution with $T_{5G_{inac}} = 1$s and 50% of compromised mMTC devices. We have choose to evaluate our detection mechanism regarding the $T_{5G_{inac}} = 1$s, due to the large volume of signaling load generated by using this smaller inactivity timer, which constitute the most devastating attack scenario, specifically by compromising 50% of total mMTC devices.

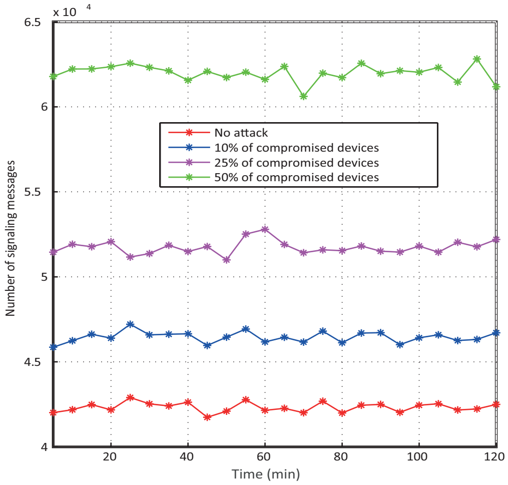

Fig. 4. New 5G RRC Model Signaling Overhead under a DoS Signaling Attack for $T_{5G_{inac}} = 3$s.

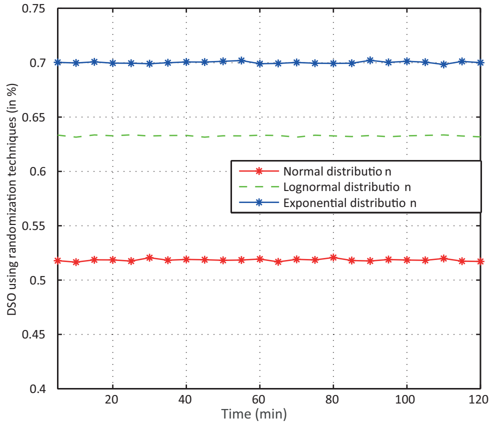

Fig. 5. Decreased Signaling Overhead using Randomization Techniques for 50% of Compromised mMTC Devices: $T_{5G_{inac}} = 1$s.

As outlined in Table II, the randomization technique has shown better results in 5G context when compared to 3G context, specifically for the Exponential and Log-normal distributions. Hence, the randomization approach remains very promising solution to be considered in mitigating the signaling threats in new mobile network generations. First, this technique offers a preventive framework that can avoid the occurrence of such attacks or at least mitigate their impact. Secondly and from a hardware perspective, the proposed randomized approach needs simply some low-complexity software updates in only some network entities.

IV. Conclusion

In this paper, we have extended our detection mechanism based randomization technique to defend against DoS signaling attack emerged in the new 5G RRC three-state model. The proposed solution has shown promising results in mitigating the impact of these signaling threats in 3G system, and we have demonstrated through simulation based on mMTC traffic pattern, the effectiveness of our detection framework regarding the 5G system as well. Indeed, for an inactivity timeout equal to 1 s and 50% of compromised mMTC device, the three simulated randomisation methods decrease significantly

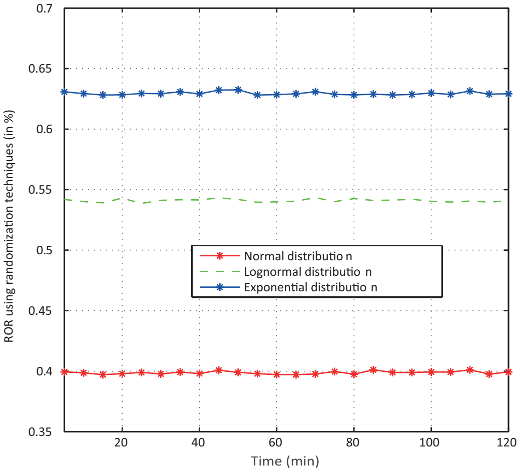

Fig. 6. Resource Consumption Ratio using Randomization Techniques for 50% of Compromised mMTC Devices: $T_{5G_{inac}} = 1$s.

TABLE II. RANDOMIZATION BASED DETECTION FRAMEWORK: 5G VS 3G PERFORMANCE COMPARISON

Randomization approach	3G system [10]		5G system	
	DSO_R (%)	ROT_R (%)	DSO_R (%)	ROT_R (%)
Gaussian distribution	46.53	55.99	52	40
log-normal distribution	42.27	10.98	64	54
Exponential distribution	31.91	13.12	70	64

the signaling load while avoiding the unnecessary network resource use. For the exponential distribution, the decreased signaling load is up to 70%, and the resource consumption ratio is around 65%, which constitutes an significant enhancement of network performances concerning the signaling overhead and the resource starvation raised from the new 5G designs, specifically when the network is under a DoS signaling attack. Our future work revolves around deeper analysis of new emerging signaling threats in the next generation (NG) of mobile systems, and new proposals to build a robust detection mechanisms to defend against the signaling attacks.

REFERENCES

[1] ITU-R, "IMT vision-framework and overall objectives of the future development of IMT for 2020 and beyond," Recommendation M.2083-0, September 2015.

[2] 3GPP, "3GPP TSG RAN WG1 Meeting 87," November 2016.

[3] Da Silva, I. L., Mildh, G., Säily, M., & Hailu, S. (2016, May). A novel state model for 5G radio access networks. In 2016 IEEE International Conference on Communications Workshops (ICC) (pp. 632-637). IEEE.

[4] Lee, P. P., Bu, T., & Woo, T. (2007, May). On the detection of signaling DoS attacks on 3G wireless networks. In IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications (pp. 1289-1297). IEEE.

[5] Kambourakis, G., Kolias, C., Gritzalis, S., & Hyuk-Park, J. (2009, June). Signaling-oriented DoS attacks in UMTS networks. In International Conference on Information Security and Assurance (pp. 280-289). Springer, Berlin, Heidelberg.

[6] Pavloski, M. (2018, February). Signalling attacks in mobile telephony. In International ISCIS Security Workshop (pp. 130-141). Springer, Cham.

[7] Abdelrahman, O. H., & Gelenbe, E. (2014, June). Signalling storms in 3G mobile networks. In 2014 IEEE international conference on communications (ICC) (pp. 1017-1022). IEEE.

[8] Wu, Z., Zhou, X., & Yang, F. (2010, September). Defending against DoS attacks on 3G cellular networks via randomization method. In 2010 International Conference on Educational and Information Technology (Vol. 1, pp. V1-504). IEEE.

[9] Chandra, M., Kumar, N., Gupta, R., Kumar, S., Chaurasia, V. K., & Srivastav, V. (2011, April). Protection from paging and signaling attack in 3G CDMA networks. In 2011 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC) (pp. 406-410). IEEE.

[10] Ettiane, R., Chaoub, A., & Elkouch, R. (2016, October). Enhanced traffic classification design through a randomized approach for more secure 3G mobile networks. In 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM) (pp. 116-121). IEEE.

[11] Jover, R. P., & Marojevic, V. (2019). Security and protocol exploit analysis of the 5G specifications. IEEE Access, (Vol.7, pp. 24956-24963).

[12] Khan, R., Kumar, P., Jayakody, D. N. K., & Liyanage, M. (2019). A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. IEEE Communications Surveys & Tutorials, 22,(Vol.1, pp. 196-248).

[13] Singla, A., Hussain, S. R., Chowdhury, O., Bertino, E., & Li, N. (2020). Protecting the 4G and 5G cellular paging protocols against security and privacy attacks. Proceedings on Privacy Enhancing Technologies, 2020, (Vol.1, pp.126-142).

[14] Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., & Bertino, E. (2019, February). Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. In NDSS (Vol. 19, pp. 24-27).

[15] Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. IEEE Communications Surveys & Tutorials, 21, (Vol.4, pp. 3682-3722)

[16] SILVA, D.,MILDH, G., PAUL, S-B., MAGNUS, S.,& ALEXANDER, V.(19 June 2019). Meeting 5G latency requirements WITH INACTIVE STATE. ERICSSON TECHNOLOGY REVIEW.

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

[18] 5G PPP use cases and performance evaluation models. White Paper, v1.0, 2016. [retrieved: 2017-07-28].[Online]. Available: https://5g-ppp.eu/wp- content/uploads/2014/02/5G-PPP- use-cases-and-performance- evaluation-modeling v1.0.pdf

[19] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on Licensed-Assisted Access to Unlicensed Spectrum;(Release 13)

[20] Ettiane, R., Chaoub, A., & Elkouch, R. (2018, May). Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks. In 2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON) (pp. 62-67). IEEE.