A Study on a New Type of DDoS Attack against 5G Ultra-Reliable and Low-Latency Communications

Cheng-Yeh Chen*, Guo-Liang Hung†, and Hung-Yun Hsieh*†
*Graduate Institute of Communication Engineering
†Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan 106
Email: hungyun@ntu.edu.tw

***Abstract*—5G New Radio (NR) allows enhanced Mobile Broadband (eMBB) and Ultra-Reliable Low-Latency Communications (URLLC) to coexist in the physical layer for better resource utilization. To enable the coexistence while satisfying the QoS requirement of URLLC, 3GPP introduces the cancellation mechanism that allows a URLLC UE to preempt the transmission of eMBB UEs. In this paper, we show that the 3GPP design to provide stringent QoS guarantee for URLLC may become a threat to interfere both eMBB and URLLC via highly synchronized low-volume DDoS. We dissect potential vulnerability for both eMBB and URLLC UEs in the uplink from the 3GPP standards. An attack model is investigated and evaluated through system-level simulations. We find that synchronization among compromised URLLC UEs could be leveraged by the attacker to amplify the overall impact on both eMBB throughput and URLLC latency, even when the number of compromised UEs is small.**

***Index Terms*—URLLC, eMBB, coexistence, DDoS, time synchronization.**

I. Introduction

The third Generation Partnership Project (3GPP) has worked on the development and standardization of the 5G New Radio (NR) to support miscellaneous traffic types among manifold scenarios and applications specified in International Mobile Telecommunications 2020 (IMT-2020). Two main use cases in 5G NR are enhanced Mobile Broadband (eMBB) and Ultra-Reliable Low-Latency Communications (URLLC). eMBB supports high capability (peak rate of 20Gbps in downlink and 10Gbps in uplink) and high mobility (500km/h) with limited user-plane latency (4 ms) to enable high-throughput applications. On the other hand, URLLC supports extremely low latency (0.5ms for both downlink and uplink) with high reliability (0.99999 for a 32-byte packet) [1] to enable mission-critical transmissions that are intolerant to latency and loss in scenarios like factory automation, transport industry and electrical power distribution [2]. Although URLLC traffic is sporadic for most enabled scenarios, a large amount of radio resource is indeed needed to meet such stringent requirements on latency and reliability.

Various mechanisms to enable the coexistence of eMBB and URLLC using the same radio resource in the physical layer have been discussed in 3GPP. In particular, flexible numerologies and frame structures that can meet the requirements of URLLC while maintaining good spectral efficiency have been ratified in recent 3GPP documents [3], [4]. Such coexistence mechanisms, however, introduce potential vulnerabilities towards both eMBB and URLLC due to the design that *URLLC is prioritized over eMBB* to ensure its latency and reliability. Specifically, 3GPP introduces the concepts of "preemption" and "cancellation" for multiplexing URLLC and eMBB traffic in the downlink and uplink respectively, where a 5G base station (gNB) can interrupt previously allocated eMBB transmissions if any URLLC allocation is needed to meet its latency requirements. Coupled with the design that the URLLC's time resource (allocated in mini-slots) is shorter than eMBB's (usually allocated in slots), such cancellation mechanism can result in undesirable waste of radio resource and lends itself to potential exploitation by attackers.

In this paper, we focus on the eMBB/URLLC coexistence scenario in 5G and investigate a new type of DDoS attack against URLLC. Specifically, conventional DDoS (or DoS) attack typically targets at completely blocking the service availability through techniques such as jamming [5], [6] and flooding [7], [8] in cellular mobile networks. In some 5G scenarios, especially those related to URLLC, the service is provisioned through strict guarantees on both latency and reliability. In such scenarios, *denial of service can happen simply through degradation of service* that leads to violation of the service guarantees. The term "DoS attack" thus can have a new interpretation as one that results in *sufficient "degradation of service"* for URLLC traffic, rather than the conventional *complete "denial of service"* for best-effort traffic.

To the best of our knowledge, *this work is the first to propose the concept and substantiate the mechanism of DDoS attack against URLLC based on 3GPP Release 16.* We first dissect 3GPP standards on the coexistence mechanisms of eMBB and URLLC as well as synchronization requirements of UEs. We investigate the feasibility of a low-volume DDoS attack to degrade both eMBB and URLLC services through exploiting the vulnerability in the coexistence mechanism by a group of synchronized yet compromised URLLC UEs. In particular, we investigate a synchronized traffic model for compromised URLLC UEs and profile the impact of synchronization accuracy on the effectiveness of the attack. Although previous work on DDoS attack in mobile networks mainly focuses on the vulnerability of the control plane rather than

978-1-7281-4355-2/20/$31.00 ©2020 IEEE

the data plane, we show through system-level simulations that attacks in the data plane should not be ignored, at least under the current 3GPP releases for URLLC. Synchronization among compromised URLLC UEs could be leveraged by the attacker to amplify the overall impact on both eMBB throughput and URLLC latency, even when the number of compromised UEs is small.

The rest of the paper is organized as follows. Section II presents related work. Section III dissects and discusses potential vulnerabilities in cancellation and synchronization mechanisms. Attack scenario and a synchronization traffic model with different attack targets are proposed in IV. Section V conducts system-level simulation and analyzes how synchronization could amplify the damage of DDoS attack. Finally, Section VI concludes the paper.

II. Related Work

Different from conventional DoS or DDoS attacks proposed in [7] and [8] that block radio resource in the control plane, our work focuses on attacks in the user plane. Mission-critical services are often prioritized in various systems to meet their stringent latency and reliability requirements. They can therefore be potentially exploited by attackers. For example, in a cellular vehicle-to-everything (C-V2X) network, [9] proposed a resource reservation attack by requesting high priority services such as forward collision warning to deplete physical layer resource. Apart from mission-critical services, high bandwidth bearers with high priority in LTE have also been investigated to launch resource reservation attack by having a low Modulation and Coding Scheme (MCS) [10]. These research endeavors, however, focus on the use of QoS class identifications (QCI) for different priority levels while our work utilizes cancellation mechanism between URLLC and eMBB.

We note that low-volume DDoS attack has been investigated in recent work [11], where Very Short Intermittent DDoS (VSI-DDoS) attack is introduced in a different context. In [11], VSI-DDoS attack sends intermittent bursts of legitimate HTTP requests to the target website with the goal of degrading the QoS of the server. Feasibility to launch the VSI-DDoS attack in the application layer is challenged in [12] in view of the difficulty of achieving tight synchronization among Internet hosts. In the context of 5G communication systems, however, achieving tight synchronization among compromised URLLC UEs is in fact possible due to the 3GPP requirements in the 5G physical layer. Combined with the vulnerability residing in the 3GPP standards, even a small number of infected UEs could launch successful attack as we explain in the following.

III. Background

In this section, we first explain the uplink coexistence of eMBB and URLLC traffic specified in 3GPP documents [13], [14] and then explain the tight synchronization enabled in the 5G NR framework.

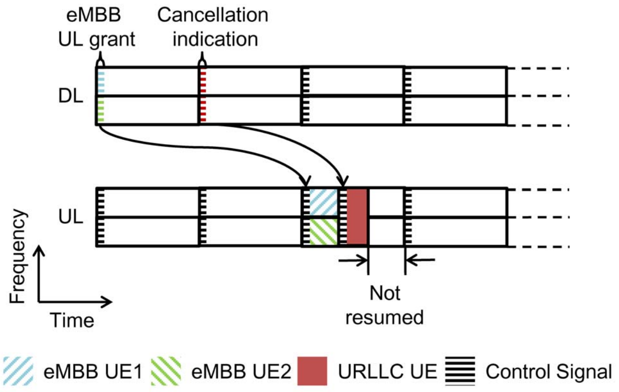


Fig. 1. Illustration of UL cancellation indication and cancellation timeline for dynamic multiplexing between eMBB and URLLC.

A. Coexistence of eMBB and URLLC

To meet the latency requirement of URLLC transmission for dynamic inter-UE multiplexing in the uplink, a 5G NR base station (gNB) can cancel eMBB transmission if the resource is needed by any URLLC request. As illustrated in Fig. 1, a gNB can send out a cancellation indication to eMBB UEs in advance while reserving sufficient processing time for relevant eMBB UEs to stop their transmissions in time. If the duration between the start symbol where a UE detects cancellation indication and the start symbol of cancellation is shorter than the minimum UE cancellation time, the UE is not expected to cancel its transmission. Notice that *multiple eMBB UEs may be cancelled simultaneously upon one URLLC request* since it is common for URLLC UEs to occupy large amount of frequency resource to ensure low latency and high reliability. In any case, the prioritized URLLC UE can interrupt the resource allocated to eMBB UEs.

Time allocation for URLLC UEs is in the unit of mini-slot, which may have a length of 2, 4, or 7 symbols. In contrast, eMBB UEs are usually granted one or more slot ($\geq$ 14 symbols). Note that the cancelled eMBB UE will not resume even if there is still remaining resource after the cancelling URLLC transmission due to the phase contiguity issue. As shown in Fig. 1, one uplink URLLC allocation can interfere *an entire slot* of the eMBB transmission. Not only is the remaining resource within the slot after URLLC transmission left unused, but the data already transmitted before the URLLC allocation has to be re-transmitted. While such interference on eMBB could be negligible under the normal scenario with sporadic URLLC traffic, the impact on eMBB throughput could be amplified if URLLC UEs are synchronized to deliberately scatter their requests to consecutive slots (e.g. at least one request per slot).

B. UE Synchronization Requirement

The next-generation synchronization architecture in 3GPP is moving towards integration with the IEEE 802.1 time-sensitive networking (TSN), which specifies strict synchronization requirements of 1ms cycle time with 0.999999 reliability and

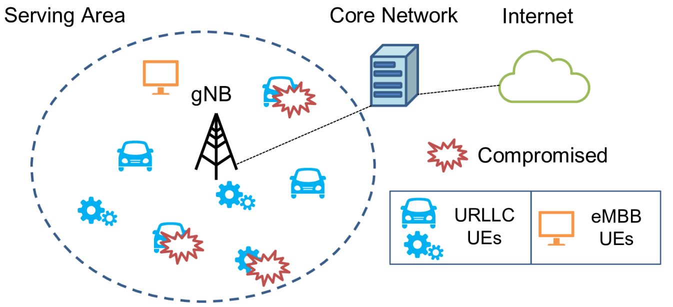


Fig. 2. Attack scenario with one gNB, one eMBB UE and a set of normal and compromised URLLC UEs.

1μs jitter [15]. Such strict requirements are enabled in 3GPP for time-critical machine-type communications, including industrial automation, power distribution, vehicular communication, and live audio/video production [16]. Further, 3GPP allows multiple time domains (i.e., universal time domain and working clock domain) to coexist and interact with each other [17]. The universal time domain synchronizes the whole system with precision from 1μs to 100μs. On the contrary, the working clock domain provides local synchronization in the order of 1μs. Combined with the fact that URLLC transmission could require a relatively wide frequency of resources, it is possible to deplete all available resources using a few (compromised) URLLC UEs in a very short period of time by exploiting such synchronization accuracy for URLLC. The increase in latency and decrease in reliability could result in degradation, and equivalently denial, of service for other (normal) URLLC UEs. We explain in the following such a new type of DDoS attack against URLLC.

IV. DDoS Attack Model

A. Attack Scenario

As illustrated in Fig. 2, we consider a scenario with one gNB and a set of UEs (eMBB and URLLC) in the serving area of the gNB. A subset of URLLC UEs are compromised and controlled by an attacker. All URLLC UEs connected to a gNB, being normal or compromised, are synchronized based on the 3GPP requirement. Hence, compromised URLLC UEs can leverage such synchronization to transmit small, simultaneous packets. This is a type of attack that can happen within one cell or among several neighboring cells (via synchronization among different gNBs). Note that the number of compromised UEs does not need to be large to launch the low-volume DDoS attack since *the enabler is the timing rather than the volume of the traffic*. With sufficient synchronization accuracy, the attacker could amplify the damage with limited number of compromised UEs over large radio resource as follows.

B. Synchronized Attack Model

To investigate the effectiveness of synchronization accuracy on the system performance, we investigate a periodic traffic model to simulate the very short intermittent attack traffic with configurable degree of synchronization. Unlike normal users with sporadic and random traffic, traffic from compromised UEs could exhibit a higher degree of periodicity (and intensity) such that the attack power of the compromised UE can be fully utilized. For sake of explanation, we assume in the following that each compromised URLLC UE sends attack traffic to the gNB with the same periodic. Denote T as the period in millisecond and B as the size of transmission in each period. Assume N URLLC UEs are compromised and each of them is denoted by CUE_i for $1 \leq i \leq N$. To quantify the degree of synchronization, we define the first arrival time t_{CUE_i} of the i^{th} compromised UE in a period from time t to $t+T$ as

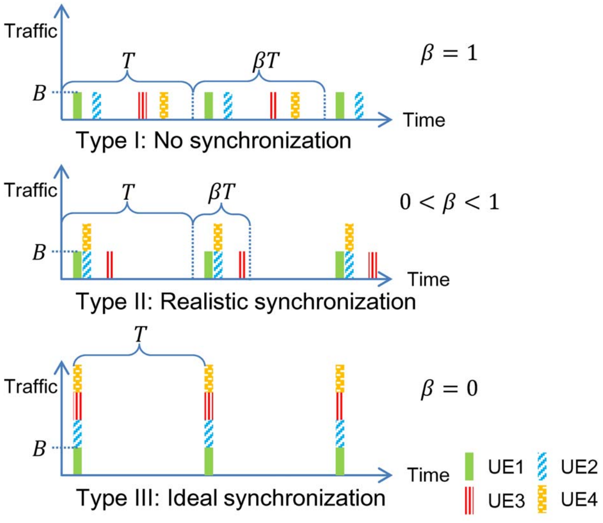

Traffic
T
βT
β = 1
B
Time
Type I: No synchronization
Traffic
T
βT
0 < β < 1
B
Time
Type II: Realistic synchronization
T
Traffic
β = 0
B
Time
UE1
UE2
UE3
UE4
Type III: Ideal synchronization

Fig. 3. Illustration of attack traffic with various degree of synchronization.

$$t_{CUE_i} = t + rand(0, \beta) * T, \quad (1)$$

where $0 \leq \beta \leq 1$ denotes the degree of randomness, $1 - \beta$ denotes the degree of synchronization, and $rand(0, \beta)$ is a uniform random variable between 0 and β. Under such a notation, the j^{th} arrival time of the i^{th} compromised UE can be denoted as $t_{CUE_i} + (j-1)T$. Fig. 3 illustrates three different degrees of of synchronization. If $\beta = 1$ (Type I traffic), the attack traffic is not synchronized at all and this is treated as a baseline attack. If $0 < \beta < 1$ (Type II traffic), the attack traffic is somehow synchronized, which is used to evaluate the feasibility of synchronization and effectiveness of attack.

C. DDoS Attack

With the synchronized attack model to be leveraged by the attacker, we now explain how the performance of eMBB and URLLC can be impacted.

1) eMBB throughput as a target: To degrade eMBB throughput using the minimal number of compromised URLLC UEs, the attacker can synchronize infected UEs to distribute their requests uniformly in the timeline. Note that one URLLC request alone is sufficient to cancel an entire slot of eMBB transmission. If another URLLC request comes immediately after the first detrimental URLLC request, the gNB can make use of the remaining resource of the cancelled eMBB transmission for URLLC. The timeline of the compromised URLLC UEs for this DDoS attack can be described by modifying Equation (1) as follows:

$$t_{CUE_i} = t + \left(rand(0, \beta) + \frac{1 + 2(i - 2^{\lfloor log_2 i \rfloor})}{2^{\lceil log_2 i \rceil}} \right) T. \quad (2)$$

Such modification allows compromised URLLC requests to scatter across the entire period and be aligned with the slot in NR numerology, which may have slot length of 2^{-n} ms for $n = 0, 1, 2, 3, 4$.

2) URLLC outage as a target: To break the guarantee on normal URLLC UEs for service outage, it is desired to launch concentrated attack and hence (1) can be applied directly. With tight synchronization, the attack traffic exhibits periodic bursts. During the burst, requests from normal URLLC UEs would be delayed such that their latency requirement could not be met. Notice that the degree of synchronization β should be limited since the compromised UEs themselves undergo the attack as well.

V. Performance Evaluation

A. Simulation Platform

We develop our simulation platform on top of an end-to-end simulator, 5G LENA [18], which is an extension of ns-3 [19]. 5G LENA is a Non-Standalone (NSA) NR simulator including the 4G Evolved Packet Core (EPC) and 5G Radio Access Network (RAN) with physical (PHY) and media access control (MAC) layer implementation compliant to 3GPP NR Release 15 specification. It reuses the variable transmission time interval (TTI) used in the mmWave module [20] to deal with flexible frame structure in the NR specification including the mini-slot for URLLC resource allocation. In this paper, we utilize the variable TTI implementation to realize the coexistence of URLLC and eMBB with different slot durations. Our modification and settings follow 3GPP meetings [14] and documents [1].

To simulate the resource cancellation mechanism in the uplink, we assign two levels of priority to URLLC and eMBB traffic. Refering to [21], higher priority is assigned to URLLC such that the scheduler does not allocate time-frequency resource to eMBB request until all the URLLC request is fulfilled. Scheduling for traffic within the same priority (be it URLLC or eMBB) follows the first-in first-out (FIFO) scheduling. Each URLLC allocation consists of 2 symbols and each eMBB allocation consists of 7 symbols. eMBB resource can only start from the first or the eighth symbol of a slot. If such condition cannot be met, the remaining symbols after URLLC allocation would be wasted. The scheduler allocates resource by taking the PHY/MAC processing delays into consideration in each slot [22]. The overhead of control signal is ignored since we concentrate merely on the resource allocation in the data plane.

TABLE I
Simulation Parameters

Parameter		Setting
Resource	Bandwidth	50MHz
	Carrier frequency	28GHz
	Sub-carrier spacing	60kHz
	Mini-slot	7 symbols for eMBB and 2 symbols for URLLC
	Duplex mode	TDD with alternating UL-DL
Network	Layout	Hexagonal grid
	UE distribution	Uniformly distributed
	gNB	1
	eMBB UE	1
	URLLC UE	10 to 27 in total with 0 to 17 being compromised
Traffic	Normal URLLC	Poisson process with arrival rate $\lambda = 125$ packets/s
	Compromised URLLC	Periodic traffic with period $T = 8$ ms and synchronization factor β from 0.02 to 1
	eMBB	Full-buffer
Scheduling	eMBB strategy	FIFO with lower priority
	URLLC strategy	FIFO with higher priority

B. Scenario and Simulation Settings

To evaluate the effectiveness of the DDoS attack, we use *Traffic Classification 3* in [23] as the QoS requirement for URLLC service. This class of traffic maps to a wide range of URLLC applications like immersive virtual reality (VR), automotive and Internet of drones. To further specify requirements on latency and reliability, we focus on audio in the application of Internet of drones with a typical air-latency of 2.5ms and reliability of 0.999 as the target service requirement. Note that the burst size thereof is 50-100 bytes and the rate is 10-1000 packets per second with periodic traffic. Such configuration can map well to the attack traffic pattern considered in this paper with slight modification since each single packet of a URLLC UE is fixed at 32 bytes.

Table I summarizes the simulation parameters used in this paper. The settings are compliant with the urban macro scenario for NR [1]. The carrier frequency is set to locate in 28GHz, which is within Frequency Range 2 (FR2), and the sub-carrier spacing is set to 60kHz. The duplex mode is alternating UL-DL, which is balanced in uplink and downlink. Resource is allocated in a mini-slot of 7 symbols length at most. The network layout is a hexagonal grid with an inter-site distance of 500m. UEs are distributed uniformly within cells. One eMBB UE with full-buffer traffic is deployed in coexistence with several URLLC UEs. We experiment different numbers of compromised UEs to evaluate the effectiveness of DDoS attack. For normal URLLC UEs, Poisson process is applied with an arrival rate λ of 125 packets per second per UE for baseline evaluation. Infected URLLC UEs share the same average arrival rate with periodic traffic of various degrees of synchronization accuracy. The size of each URLLC packet including normal and compromised UE is 32 bytes while the size of one eMBB packet is 1252 bytes.

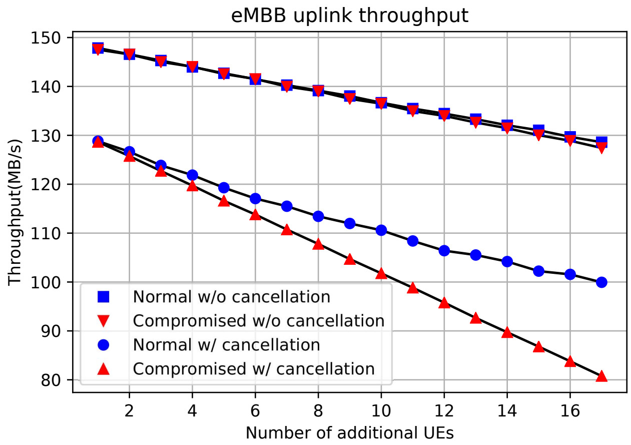


Fig. 4. eMBB throughput for additional URLLC UEs (compromised or normal) beyond 10 normal URLLC UEs with or without cancellation.

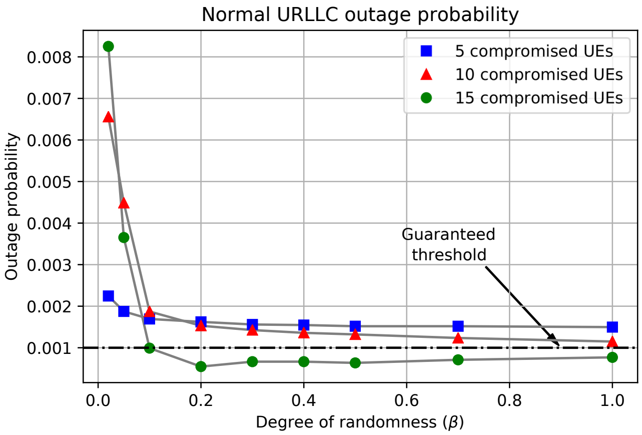


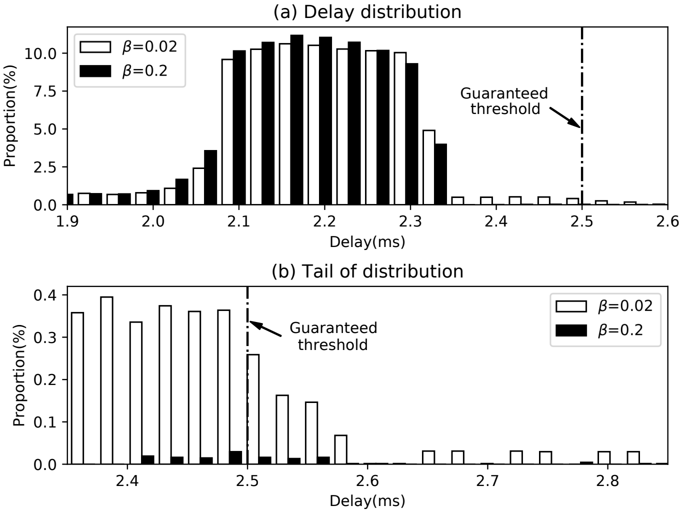
Fig. 5. Outage probability of normal URLLC UEs under attack from compromised URLLC UEs with various degrees of synchronization accuracy. The smaller the value of β is, the more accurate the synchronization is.

C. Simulation Results

We conduct simulations to evaluate the effectiveness of the synchronized low-volume DDoS attack against the vulnerability of the system. For DDoS attack targeting on eMBB throughput, (2) with $\beta = 0.02$ is applied to leverage the vulnerability of 3GPP specification. For DDoS attack targeting on normal URLLC outage, (1) with several different values of β is applied to saturate resource in a very short period with a few numbers of compromised URLLC UEs. Each configuration involves 3-second simulations run for 20 times. Since one URLLC UE transmits 125 packets per second, be it compromised or not, the outage probability measured from all the UEs corresponds to at least 75000 URLLC transmissions.

1) eMBB as a target: To evaluate the effectiveness of the synchronized DDoS attack, we place 10 normal URLLC UEs in the system as background traffic. The experiment is conducted for both systems with and without applying the cancellation mechanism against eMBB by URLLC request. (If no cancellation mechanism is applied, then URLLC serves only as a traffic class with higher priority than eMBB. No preemption on incumbent eMBB transmission is allowed.) For a baseline evaluation, we consider only normal URLLC traffic and compare eMBB throughput with or without the cancellation mechanism. As Fig. 4 shows, if cancellation is not allowed, adding one additional URLLC UE can degrade eMBB throughput of about 1.20 MB/s. On the other hand, with the 3GPP cancellation mechanism, one additional (benign) URLLC UE can result in 1.80 MB/s degradation on eMBB throughput, a 50% increase from the baseline value. It is interesting to observe from Fig. 4 that in a system without the cancellation mechanism (i.e. only prioritized sharing without preemption), synchronized requests from compromised URLLC UEs do not introduce further noticeable degradation on eMBB throughput. For the 3GPP design on eMBB/URLLC coexistence with the cancellation mechanism, however, adding one compromised URLLC UE to participate in synchronized requests can result in a degradation of 2.99 MB/s on eMBB throughput, which is 1.66 times of the degradation incurred by one normal URLLC UE. Therefore, such vulnerability does exist in the 3GPP specification that can be exploited by malicious attackers to degrade the eMBB throughput.

2) URLLC as a target: Recall that in the target application the service guarantee for URLLC is to incur latency no more than 2.5ms while providing a reliability of 0.999. Hence, we measure the latency and reliability experienced by normal URLLC UEs. We place 25 URLLC UEs in the system with 5, 10 or 15 of them being compromised. As we observe from Fig. 5, with weak synchronization (β close to 1) among URLLC UEs, a larger number of compromised UEs results in lower outage since the attack traffic, which is periodic, has lower variance in comparison with the normal traffic, which follows the Poisson process. However, the outage probability rises drastically when β is less than 0.1, meaning that all compromised URLLC requests arrive in an interval shorter than 0.8ms. The rise of the outage probability increases with the number of compromised UEs. Although the mean latency is kept invariant for all β values in our experiments, the *long tail* in the delay distribution as shown in Fig. 6 could result in the system failing to fulfill the service guarantee of URLLC UEs. For a system with 50MHz bandwidth, with merely 15 URLLC UEs being compromised, if an attacker could synchronize all the UEs to launch requests in a 0.16ms interval ($\beta = 0.02$ with $T = 8$ ms), the outage probability would increase 10.73 times compared to an attack with no synchronization. The resulting outage probability is 8.25 times of the guaranteed threshold. For a practical deployment scenario, attack from 15 infected UEs are feasible in consideration of the deployment density in future scenarios and the synchronization requirement set by the standards.


(a) Delay distribution

(b) Tail of distribution

Fig. 6. Delay distributions under different degrees of synchronization observed by normal URLLC UEs (β is set to 0.02 and 0.2 respectively). (a) demonstrates that the bulks of the distribution reveal slight variation for different degrees of synchronized attacks. (b) shows that the long tail of highly-synchronized attack.

VI. Conclusions

In this work, we investigate the cancellation and synchronization mechanisms in the 3GPP NR standards and reveal possible vulnerabilities therein. A synchronized attack traffic model is proposed with two configurations to attack eMBB and URLLC service respectively. Simulation results show that the proposed synchronized DDoS attack could amplify the degradation of eMBB throughput compared against the scenario with only normal URLLC UEs under the same traffic intensity. For URLLC services, the damage could be much more threatening. With only 15 compromised URLLC UEs that are synchronized based on 3GPP specification, URLLC services could be paralyzed due to the violation of latency requirement in the long tail.

Acknowledgment

This study is conducted under the “5G Cyber Security Detection and Protection System Project (1/1)” of the Institute for Information Industry (III), which is subsidized by the Ministry of Economic Affairs, Taiwan, ROC. This work is also supported in part by funds from the Ministry of Science and Technology and National Taiwan University under Grants MOST-108-2221-E-002-037 and MOST-108-2218-E-002-060.

References

[1] 3GPP TR 38.913, “Study on scenarios and requirements for next generation access technologies,” 2017.

[2] 3GPP RP-182089, “New SID on Physical Layer Enhancements for NR URLLC,” 2018.

[3] S. Lien, S. Shieh, Y. Huang, B. Su, Y. Hsu, and H. Wei, “5G New Radio: Waveform, Frame Structure, Multiple Access, and Initial Access,” *IEEE Communications Magazine*, vol. 55, no. 6, pp. 64–71, June 2017.

[4] J. Yeo, T. Kim, J. Oh, S. Park, Y. Kim, and J. Lee, “Advanced Data Transmission Framework for 5G Wireless Communications in the 3GPP New Radio Standard,” *IEEE Communications Standards Magazine*, vol. 3, no. 3, pp. 38–43, Sep. 2019.

[5] M. Lichtman, R. Rao, V. Marojevic, J. Reed, and R. P. Jover, “5G NR Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation,” in *Proceedings of IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018, pp. 1–6.

[6] M. Lichtman, J. H. Reed, T. C. Clancy, and M. Norton, “Vulnerability of LTE to hostile interference,” in *Proceedings of IEEE Global Conference on Signal and Information Processing*, Dec 2013, pp. 285–288.

[7] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, “Signaling Oriented Denial of Service on LTE Networks,” in *Proceedings of the 10th ACM International Symposium on Mobility Management and Wireless Access*, ser. MobiWac ’12. New York, NY, USA: Association for Computing Machinery, 2012, p. 153–158.

[8] F. Francois, O. H. Abdelrahman, and E. Gelenbe, “Impact of Signaling Storms on Energy Consumption and Latency of LTE User Equipment,” in *Proceedings of IEEE 7th International Symposium on Cyberspace Safety and Security*, Aug 2015, pp. 1248–1255.

[9] Y. Li, R. Hou, K. Lui, and H. Li, “An MEC-Based DoS Attack Detection Mechanism for C-V2X Networks,” in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, Dec 2018, pp. 1–6.

[10] R. Bassil, I. H. Elhajj, A. Chehab, and A. Kayssi, “A resource reservation attack against LTE networks,” in *Proceedings of the Third International Conference on Communications and Information Technology (ICCIT)*, June 2013, pp. 262–268.

[11] H. Shan, Q. Wang, and Q. Yan, “Very Short Intermittent DDoS Attacks in an Unsaturated System,” in *Proceedings of Security and Privacy in Communication Networks*, X. Lin, A. Ghorbani, K. Ren, S. Zhu, and A. Zhang, Eds. Cham: Springer International Publishing, 2018, pp. 45–66.

[12] J. Park, D. Nyang, and A. Mohaisen, “Timing is Almost Everything: Realistic Evaluation of the Very Short Intermittent DDoS Attacks,” in *Proceedings of the 16th Annual Conference on Privacy, Security and Trust (PST)*, Aug 2018, pp. 1–10.

[13] 3GPP TR 38.824 V16.0.0, “Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC),” Tech. Rep., Mar. 2019.

[14] 3GPP, “Meetings for Group R1,” Available at https://www.3gpp.org/dynareport/Meetings-R1.htm.

[15] A. Mahmood, M. I. Ashraf, M. Gidlund, and J. Torsner, “Over-the-Air Time Synchronization for URLLC: Requirements, Challenges and Possible Enablers,” in *Proceedings of the 15th International Symposium on Wireless Communication Systems (ISWCS)*, Aug 2018, pp. 1–6.

[16] A. Mahmood, M. I. Ashraf, M. Gidlund, J. Torsner, and J. Sachs, “Time Synchronization in 5G Wireless Edge: Requirements and Solutions for Critical-MTC,” *IEEE Communications Magazine*, vol. 57, no. 12, pp. 45–51, December 2019.

[17] T. Striffler, N. Michailow, and M. Bahr, “Time-Sensitive Networking in 5th Generation Cellular Networks - Current State and Open Topics,” in *Proceedings of IEEE 2nd 5G World Forum (5GWF)*, Sep. 2019, pp. 547–552.

[18] N. Patriciello, S. Lagen, B. Bojovic, and L. Giupponi, “An E2E simulator for 5G NR networks,” *Simulation Modelling Practice and Theory*, vol. 96, p. 101933, 2019.

[19] G. F. Riley and T. R. Henderson, *The ns-3 Network Simulator*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 15–34.

[20] M. Mezzavilla, M. Zhang, M. Polese, R. Ford, S. Dutta, S. Rangan, and M. Zorzi, “End-to-End Simulation of 5G mmWave Networks,” *IEEE Communications Surveys Tutorials*, vol. 20, no. 3, pp. 2237–2263, thirdquarter 2018.

[21] M. Mhedhbi, M. Morcos, A. Galindo-Serrano, and S. E. Elayoubi, “Performance Evaluation of 5G Radio Configurations for Industry 4.0,” in *Proceedings of International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct 2019, pp. 1–6.

[22] N. Patriciello, S. Lagen, L. Giupponi, and B. Bojovic, “The Impact of NR Scheduling Timings on End-to-End Delay for Uplink Traffic,” in *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, Dec 2019, pp. 1–6.

[23] K. S. Kim, D. K. Kim, C. Chae, S. Choi, Y. Ko, J. Kim, Y. Lim, M. Yang, S. Kim, B. Lim, K. Lee, and K. L. Ryu, “Ultrareliable and Low-Latency Communication Techniques for Tactile Internet Services,” *Proceedings of the IEEE*, vol. 107, no. 2, pp. 376–393, Feb 2019.