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

Authors: Cheng-Yeh Chen, Guo-Liang Hung, Hung-Yun Hsieh

National Taiwan University Mobile Networks and Wireless Communications (TONIC) Research Group

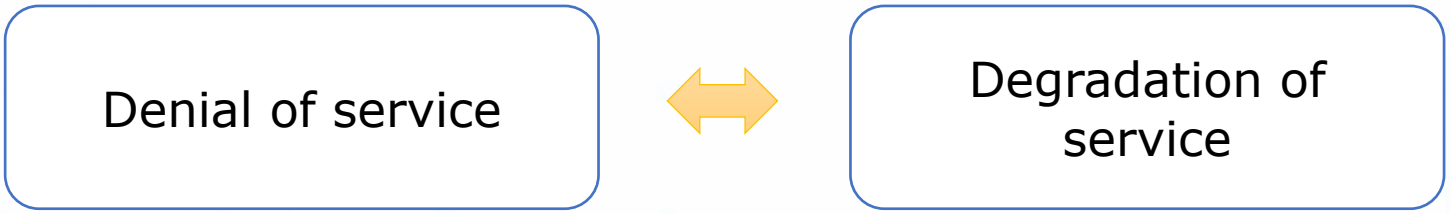
Jun 1, 2020

Summary

- In this paper, we focus on the ***eMBB/URLLC coexistence*** scenario in 5G.
- We discuss how the ***cancellation mechanism*** and ***high synchronization*** requirement could be used by the adversary.
- We investigate a ***low-volume highly-synchronized*** DDoS attack model.
- A ***standard-compliant*** simulator is developed and experimented to verify our model.

New DDoS attack against URLLC

- Conventional DDoS (or DoS) attack typically targets at completely blocking the service availability.
- For URLLC, the service is provisioned through strict guarantees on both latency and reliability. Denial of service can happen simply through degradation of service that leads to violation of the service guarantees.



The two enablers

- In our study, the new DDoS attack is enabled by the following two
  - **Cancellation mechanism** in the coexistence of URLLC and eMBB.
  - **High synchronization requirement** in the 5G synchronization architecture.

eMBB/URLLC coexistence

- 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)
  - ➢ URLLC: supports extremely low latency (0.5ms for both downlink and uplink) with high reliability (0.99999 for a 32-byte packet)
- Large amount of radio resource is needed to meet such stringent requirements on URLLC but URLLC is sporadic in most of use cases.
- 3GPP introduces the concepts of "cancellation" for multiplexing URLLC and eMBB traffic in uplink to enable URLLC while maintaining good spectral efficiency.
- Such coexistence mechanism, however, introduces potential vulnerabilities towards both eMBB and URLLC due to the design that URLLC is prioritized over eMBB.

Cancellation Mechanism

- A 5G NR base station (gNB) can cancel eMBB transmission if the resource is needed by any URLLC request.

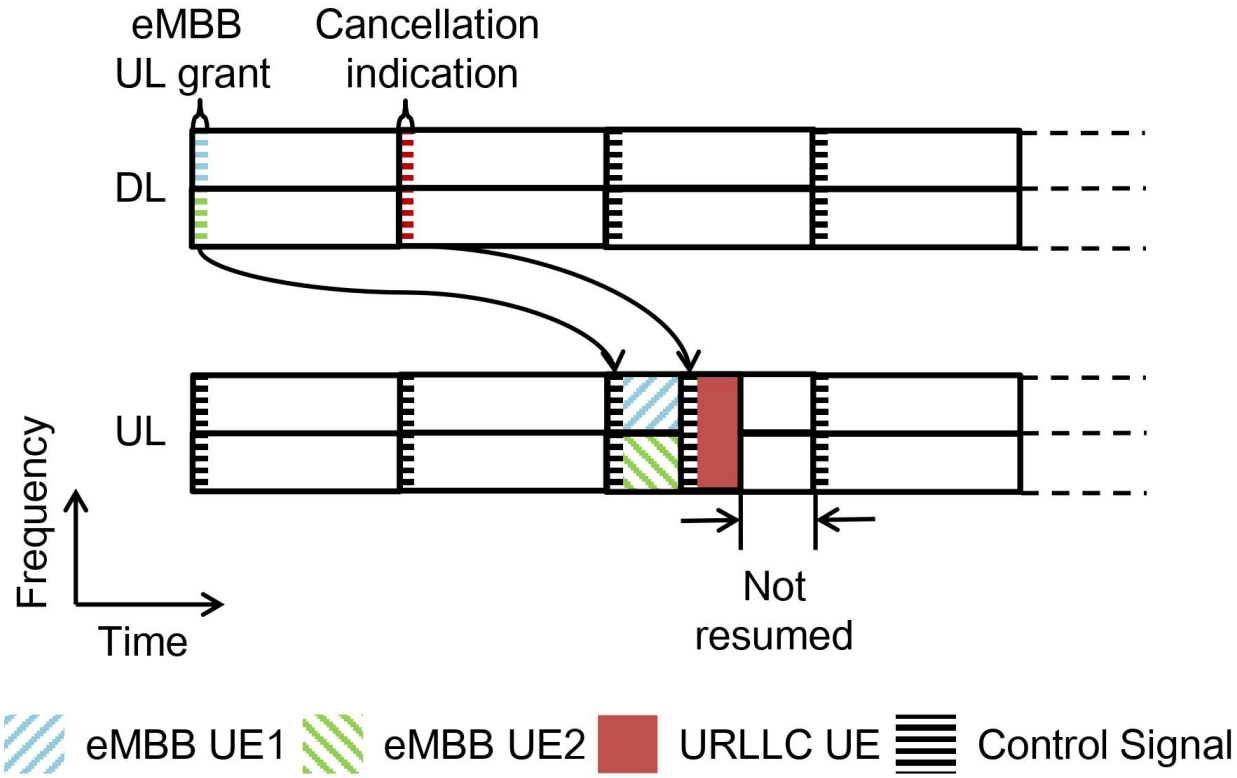


Illustration of UL cancellation indication and cancellation timeline for dynamic multiplexing between eMBB and URLLC.

High synchronization requirement

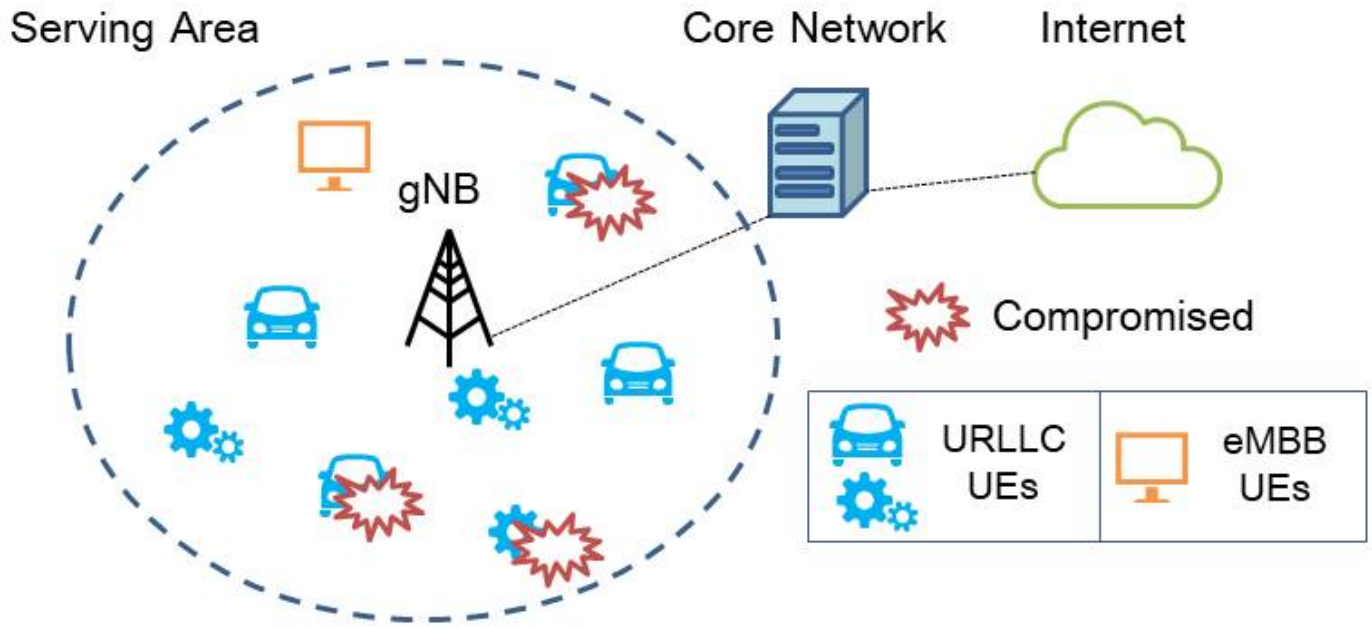
- The next-generation synchronization architecture in 3GPP is moving towards integration with the IEEE 802.1 time-sensitive networking (TSN), which specifies strict synchronization requirements of 1ms cycle time with 0.999999 reliability and 1μs jitter.

Possible vulnerabilities

- If one can compromised URLLC UEs and leverage their priority, aggressive attack could be launched.
- **Degradation on eMBB**
  - ➢Waste of transmission: The remaining resource within the slot after URLLC transmission left unused, and the data already transmitted before the URLLC allocation has to be re-transmitted.
  - ➢Grouped cancellation: 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.
- **Degradation on URLLC**
  - ➢High synchronization: The compromised URLLC could synchronized with each other in symbol level to increase the latency of normal URLLC.

Attack scenario

- A gNB
- 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



Synchronized attack model

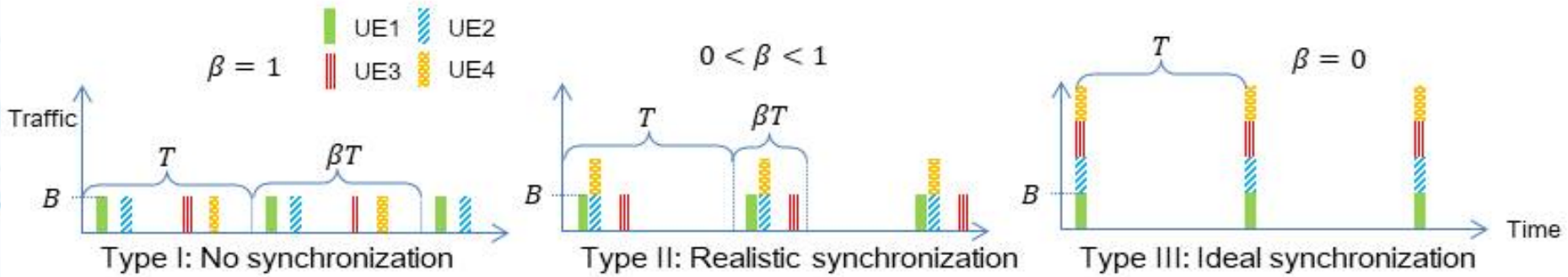
- We propose a low-volume and highly-synchronized DDoS model.
- Assume N compromised URLLC UEs named CUE_i for $i = 1,\ldots, N$ transmitting periodic traffic with T as the period in millisecond and B as the size of transmission in byte in each period.
- We define the first arrival time t_{CUE_i} of the i^{th} compromised UE in a period from time t to $t+T$ as

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

where $0 \le \beta \le 1$ denotes the degree of randomness, $1 - \beta$ denotes the degree of synchronization, and $rand(0,\beta)$ is a uniform random variable from 0 to β.

Synchronized attack model

- Such model allows us to characterize various degree of synchronization and evaluate how synchronization would affect the system level performance of URLLC and eMBB.
- Type I traffic ($\beta = 1$)
  - ➢Attack traffic is not synchronized at all and this is treated as a baseline attack.
- Type II traffic ($0 < \beta < 1$)
  - ➢Attack traffic is somehow synchronized, which is used to evaluate the feasibility of synchronization and effectiveness of attack.



URLLC reliability as a target

- To degrade URLLC reliability, the attack should as concentrated as possible.
- Apply equation (1) directly with tight synchronization (small β) to create periodic burst.

eMBB throughput as a target

- To leverage the cancellation mechanism to degrade the eMBB throughput, the attacker should synchronize infected UEs to
  - ➢scatter their requests across the entire period
  - ➢make their requests be aligned with the slot in NR numerology, which may have slot length of 2^{-n} ms for $n = 0,1,2,3,4$.
- The following equation describes the corresponding attack:

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

- If the attacker could synchronize all the infected UEs tightly, which is equation (2) with small β, each requests would cancel different eMBB transmission in different time slot and create the greatest leverage.

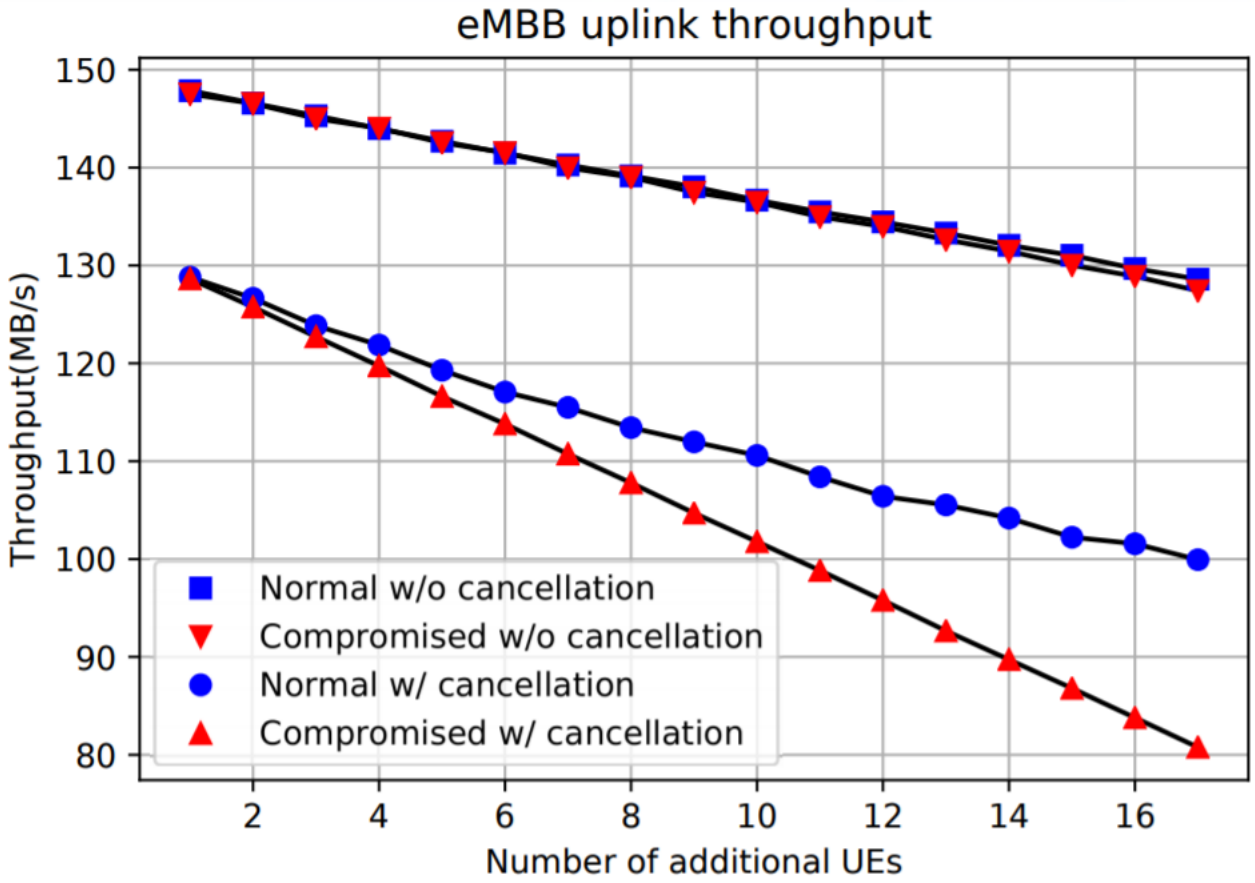
Simulation

- We develop our simulation platform on top of an end-to-end simulator, 5G LENA, which is an extension of ns-3.
- To simulate the resource cancellation mechanism in the uplink, we assign two levels of priority to URLLC and eMBB traffic.
- The scheduler does not allocate time frequency resource to eMBB request until all the URLLC request is fulfilled.

Simulation

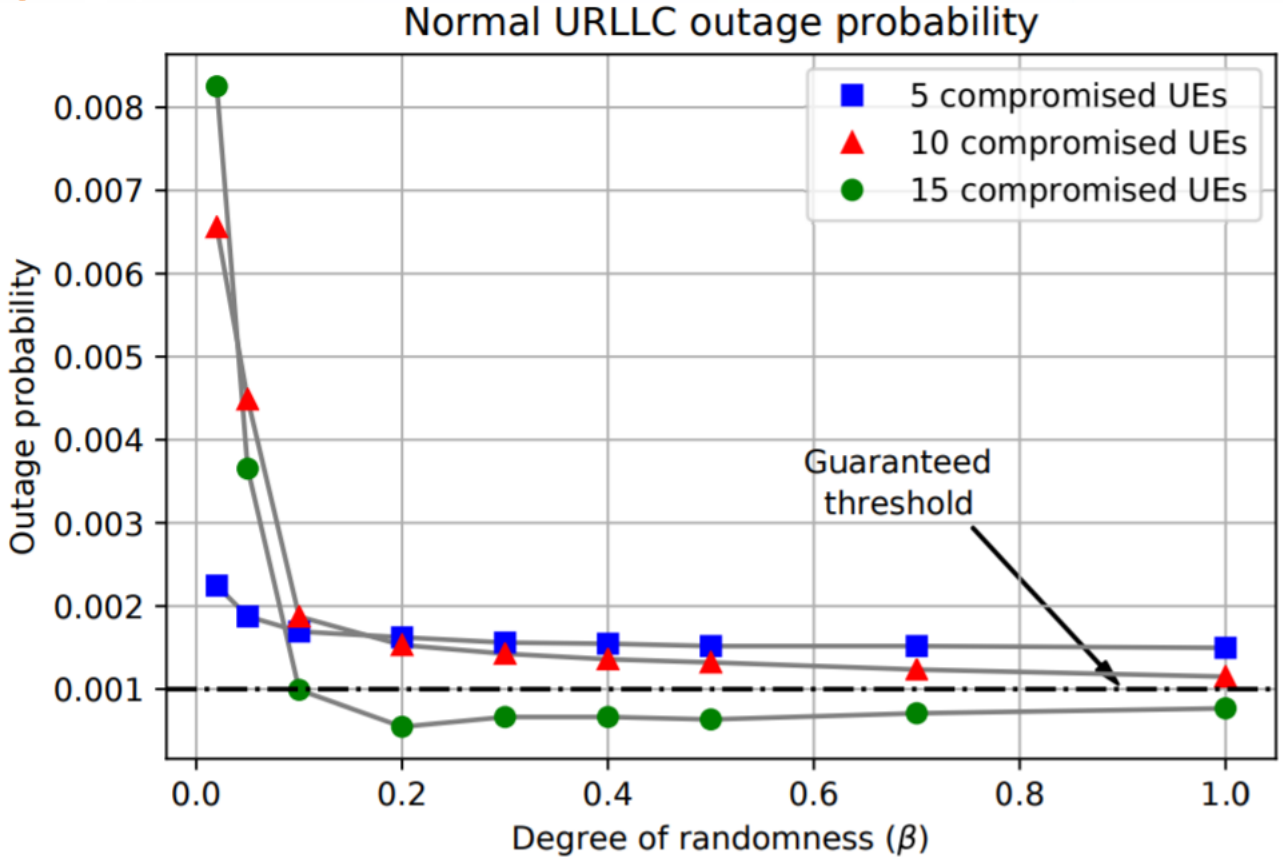
Parameter		Setting
Resource	Bandwidth	50MHz
	Carrier frequency	28GHz
	Sub-carrier spacing	60kHz
	Mini-slot	7 symbols for eMBB and 2 symbols for URLLC
	Duplex mode	TDD with alternating UL-DL
Network	Layout	Hexagonal grid
	UE distribution	Uniformly distributed
	gNB	1
	eMBB UE	1
	URLLC UE	10 to 27 in total 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

Result



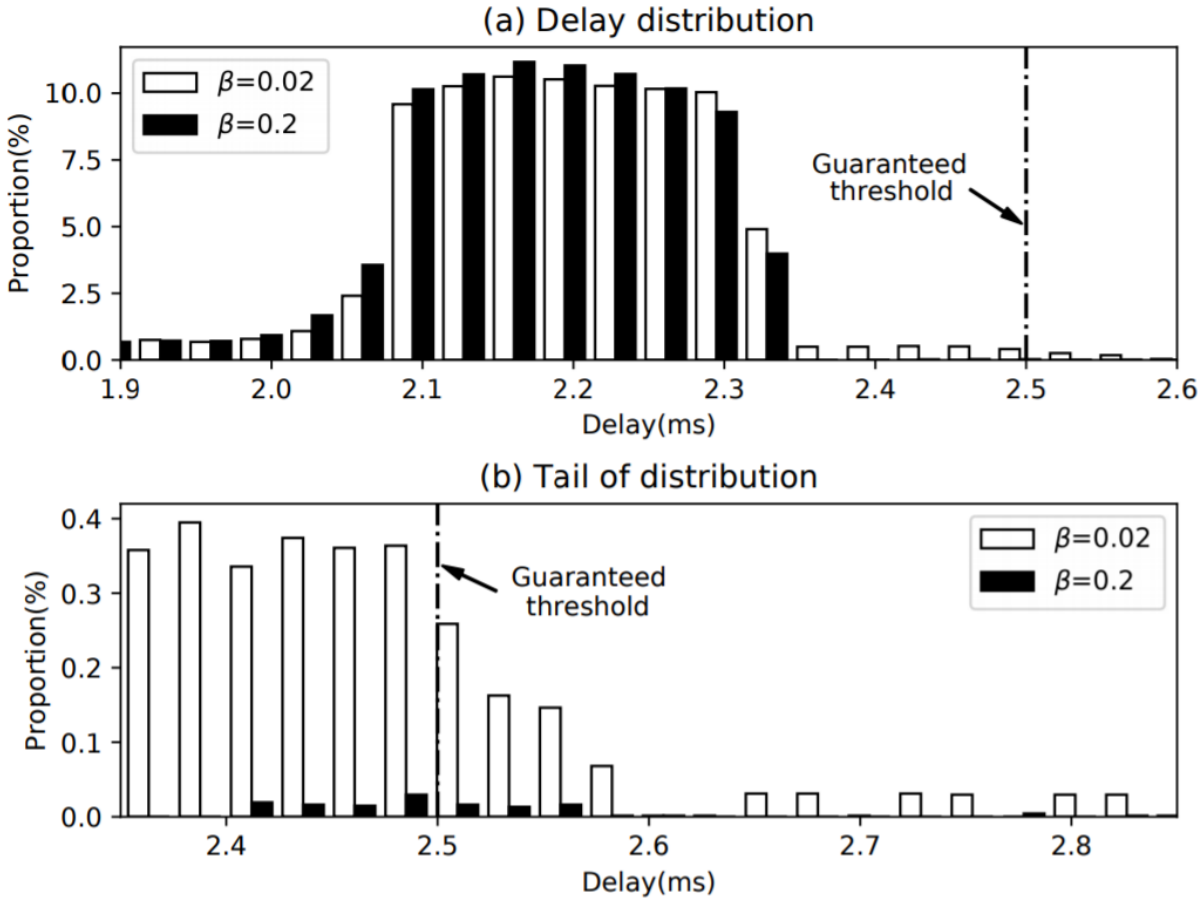
- Adding one compromised URLLC UE to participate can result in a degradation of 2.99 MB/s on eMBB throughput, which is 1.66 times of the degradation incurred by one normal URLLC UE

Result



- 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 (β = 0.02 with T = 8 ms), the outage probability would increase 10.73 times compared to an attack with no synchronization.

Result



- The long tail in latency could crash the whole system in fulfilling the service guarantee of URLLC UEs

Q&A

Jun 1, 2020