The benefits of Deceit: a Malicious client in a 5G Cellular Network

Jason J. Quinlan, Utz Roedig

Summary

Goal: Investigate the scheduling impact of a malicious device in a simulated 5G (mmwave) cellular network

Approach: Utilise real-time 4K ultra-high definition video delivery as an example of a high throughput demand application and compare the delivery rates of multiple devices in an Open-source 5G simulated NS-3 network

Contribution: Expose how existing trust-based client-side channel metrics, such as Channel Quality Indicator (CQI) can be modified to improve throughput or even negate the download rate of others

Malicious Opportunities

- An autonomous future: smart cities, connected vehicles and the avalanche of IoT devices
- Typically, cellular networks will be the backhaul and first/last hop for all traffic
- Base-station determines scheduling decisions based in part on client input
- Currently trust-based client-side cellular channel metrics, such as CQI
- Open-sourced communication systems, such as software- defined radio, give access to core network functionality
- 3G: 10% malicious clients - 2 sec VOIP delay
- 4G: 2 malicious clients causes DOS for all other users requesting TCP-based applications
- 5G: what happens in the next generation of cellular networks?

Attack Goals

By modifying performance data reported to the base station, a client can:

1. Gain a better allocation of bandwidth than would be assigned normally
2. Prevent other users from obtaining their fair bandwidth allocation
3. Prevent other users from using services at all (push bandwidth allocation modification towards DoS)

Use Case – DI5GUISE

Real-Time 4K UHD DASH Video Streaming:

- Four clients range between 25m and 35m in distance from a single base station
- Rural macro-channel scenario *(Rma)*
- 3GPP propagation loss model *(3GPPprop)*
- Transmission Time Interval *(TTI)* base station mac scheduler
- Stream five minutes of 4K adaptive video content to a number of video clients
- Clients adapt the quality of their streaming video clip depending on their scheduled throughput rate
- For the evaluation with a malicious client, we maximise the CQI value of Client 1.

Header	Description
Avg_quality	average view-able quality per segment in Kbps
Avg_del_rate	average download rate per segment in Kbps
Avg_del_time	average delivery time per segment in seconds
Num_stalls	number of stalls
Stall_Dur	total stall duration in seconds

TABLE II
5G CLIENT METRICS WITH NO MALICIOUS CLIENTS

Client	Avg_quality	Avg_del_rate	Avg_del_time	Num_stalls	Stall_Dur
1	11,508	20,091	2.435	0	0
2	8,934	16,589	2.147	1	3.337
3	13,477	22,141	2.738	2	5.22
4	11,636	20,618	2.568	3	3.395

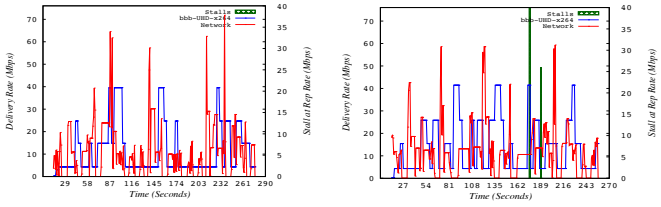
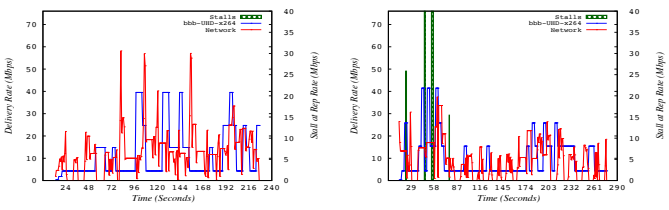


TABLE III
5G CLIENT METRICS WITH CLIENT 1 AS THE MALICIOUS CLIENT

Client	Avg_quality	Avg_del_rate	Avg_del_time	Num_stalls	Stall_Dur
1	11,997	20,221	2.706	0	0
2	7,246	14,823	2.064	0	0
3	9,865	17,318	2.433	4	10.422
4	8,144	16,030	2.221	0	0



Further information and build instructions for DI5GUISE are available at http://www.cs.ucc.ie/misl/research/software/di5guise/

{j.quinlan, u.roedig}@cs.ucc.ie,Computer Science & Information Technology, UCC, Ireland

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) under Grant Number 13/IA/1892