Generation of realistic signal strength measurements for a 5G Rogue Base Station attack scenario

Mohammad Saedi
School of Computing
Ulster University
Jordanstown, NI, UK
saedi-m@ulster.ac.uk

Adrian Moore
School of Computing
Ulster University
Jordanstown, NI, UK
aa.moore@ulster.ac.uk

Philip Perry
School of Computing
Ulster University
Jordanstown, NI, UK
p.perry@ulster.ac.uk

Mohammad Shojafar
5G Innovation Centre
University of Surrey
Guildford, UK
m.shojafar@surrey.ac.uk

Hanif Ullah
School of Computing
Ulster University
Jordanstown, NI, UK
h.ullah@ulster.ac.uk

Jonathan Synnott
School of Computing
Ulster University
Jordanstown, NI, UK
j.synnott@ulster.ac.uk

Ruth Brown
Applied Research
BT
Ipswich, UK
ruth.2.brown@bt.com

Ian Herwono
Applied Research
BT
Ipswich, UK
ian.herwono@bt.com

***Abstract*—The detection and prevention of cyber-attacks is one of the main challenges in Vehicle-to-Everything (V2X) autonomous platooning scenarios. A key tool in this activity is the measurement report that is generated by User Equipment (UE), containing received signal strength and location information. Such data is effective in techniques to detect Rogue Base Stations (RBS) or Subscription Permanent Identifier SUPI/5G-GUTI catchers. An undetected RBS could result in unwanted consequences such as Denial of Service (DoS) attacks and subscriber privacy attacks on the network and UE. Motivated by this, this paper presents the novel simulation of a 5G cellular system to generate a realistic dataset of signal strength measurements that can later be used in the development of techniques to identify and prevent RBS interventions. The results show that the tool can create a large dataset of realistic measurement reports which can be used to develop and validate RBS detection techniques.**

Keywords—5G, LTE, Rogue Base Station, Cyber Security, Vehicle Platooning, Privacy, Radio Access Network.

I. INTRODUCTION

The fifth generation of cellular telecommunications networks (5G) brings a significant increase in bandwidth and reduction of latency compared to previous standards [1]. The Next Generation Mobile Network (NGMN) Alliance defines 5G as an End-to-End (E2E) ecosystem supporting a movable connected society [2]. Nevertheless, 5G is not just a next step evolution from Long Term Evolution (LTE), which is currently the most widely adopted cellular communication standard but represents a paradigm shift [3]. Vehicle-to-Everything (V2X) services, one of the core applications enabled by 5G communication systems, enable data exchange between vehicles and other nodes. A remote V2X application server (AS) centralizes control and distribution of road and traffic information[4]. 5G could accelerate the adoption of a range of vertical markets, heterogeneous services, and use cases with their cybersecurity requirements (in wireless communication). It needs to support multiple access networks comprising General Packet Radio Service (GPRS), Universal Mobile Telecommunications Service (UMTS), and Long-Term Evolution (LTE). As a result, 5G implementations will be likely to inherit the security challenges of those access networks. The essential vulnerabilities and attacks on access networks are currently a key topic of research [5].

The many published threats at the 4G RAN layer include Rogue Base Stations (RBS) or International Mobile Subscriber Identity (IMSI) catchers to target IMSIs of User Equipment (UE) during the initial attachment process to the network, and paging threats using the IMSI paging feature. Once a subscriber's IMSI has been stolen, their privacy can be severely compromised. A Man in the Middle (MitM) attack is one of the most common attacks against a subscriber. In cellular networks, MitM uses an RBS, when the Base Station (BS) of a malicious third party masquerades as a genuine network's BS [6]. This study focuses on security considerations involving BSs.

A. Motivation

There is a significant body of research to develop accurate simulation models of 5G radio channels, mainly aimed at modeling both amplitude and phase variations across the bandwidth of the radio signal. Hence, they determine the performance of the signal processing algorithms that help to improve the performance of the radio link [7]. Such models are typically quite complex and require a high level of expertise to use them correctly. To fill such gaps, we propose a simulation model that can efficiently produce realistic signal strength metrics, using well-known radio propagation models. The model can be easily used by computer science researchers to quickly generate large datasets to train and test RBS detection methods. Moreover, to the best of our knowledge, there are no currently existing simulations of this nature that do not require expert radio knowledge. We consider that this solution will be beneficial to the wider 5G security research community.

B. Our Contribution

The scenario considered in this paper is an RBS attack on a platoon of vehicles to take control of the platoon and cause a

major traffic incident with significant potential danger to life. Such an attack could be executed as a MitM attack where the RBS mimics a legitimate BS and relays information between the platoon leader and the legitimate BS. Then, by modifying the content of the control messages, the platoon leader can be instructed to make a maneuver that results in a serious incident.

The work here assumes that it is possible to autonomously detect the presence of an RBS using received signal strength and the known location of the legitimate BSs and the position of the platoon leader. To develop Machine Learning (ML) techniques to perform this detection robustly, researchers require a method to generate realistic datasets of signals strength and associate locations. Obviously, one could use measured data from a UE in a vehicle driving through a 5G coverage area. However, it would be difficult to determine whether those observed datasets were typical or contained anomalous artifacts. To avoid generating abnormal radio data, or data that is in some way specific to the set of tests carried out, we have developed a simple simulation in MATLAB that can generate datasets for a wide range of scenarios in a fraction of the time required to acquire large datasets of measured data from a UE in a "drive test".

The remainder of the paper is organized as follows: Section II will discuss the related work and then Section III will provide the background. Section IV will present the proposed model. Section V will provide the results and discussion, while Section VI will conclude the paper.

II. Related Work

In recent years, the latest survey of the current technologies and open communication challenges focused on the 5G data transferring between BSs and V2X and their detection techniques [8]. The techniques of RBS detection can be summarized in three categories. The first involves the application of RBS detection methods from the previous generation of communications. The authors in [9] introduced an RBS detection method to avoid violations of received signal strength reports consistency in WiMax/802.16 wireless access networks. Their technique was not particularly robust for LTE and 5G technologies, and it did not support a DoS attack among BSs. Interestingly, our approach aims to provide a tool that can help to fill this gap. Moreover, in [10], the authors design a holistic solution to analyse the BSs and detect a rogue device in a network. To do so, they aim to scan mobile devices across the system, which includes predetermined criteria, executed by a processor. The idea is promising; however, they did not take account of various real-time interferences in the dedicated resources in the 5G network. In [11] the authors utilise a machine learning strategy to identify an RBS in the mobile network based on the key BS parameters and tested it on GSM/LTE features. The work suffers from a lack of deep appliance in 5G nodes considering the limited time and did not consider a platooning platform for IoT located in a 5G network, whilst our method will consider them. The authors in [12] designed and implemented a large-scale RBS detection and localisation system to detect and quarantine numerous spam and fraud SMS messages among UEs while having low resource requirements on end-user devices. The work is promising and reliable however, a practical implementation was not tested and did not check received signals against previously known information about the BS.

The second category of the research papers focuses on location-based methods which analyse the signals received from the BSs and then compare this with the known coverage pattern to identify an RBS in the network. For example, the authors in [13] designed two suspicious synchronization signal strength checking region criteria. Their method utilises shadow fading and small-scale fading effects to understand the cheating rates of the signals and locate the RBSs and claims that they could cover spoofing attacks in the LTE system. Also, the work presented in [14] monitors the imperfections of the transmitter on each BS using time-efficient symbol-based statistical RF fingerprinting techniques to understand the noise processes in the network to identify an RBS. Such works are computationally complicated when they are applied to higher modulation schemes under actual propagation conditions.

The third category of solutions considers some encryption strategies to preserve the privacy of the transferred data between the UE and BS. Such methods build certificates to conceal their identity and their detailed information to mitigate eavesdropping in an untrusted channel [15][16]. Such methods are unable to deal with real-time multi-cast cases in dealing with the RBS. The authors in [17] design an efficient tool named FBSleuth instantiated in BS devices that can identify RBS devices based on minor differences in the emitted signals caused by hardware imperfections. They tested their attack method by collecting signal traces from 6 real RBSs for 5 months and validated it under various settings. The work is a promising practical solution. However, FBSleuth is not applied to a 5G network.

III. Background

One of the aims of 5G communication networks is to provide very high bandwidth and more comprehensive coverage by dense deployment of Base Stations (BS) with enhanced capacity, significantly ultra-low latency, and better Quality of Service (QoS).

A. Radio Access Networks Threats

In the security architecture of cellular networks before 5G, mutual authentication between UE and core network (Evolved Packet Core in LTE), is considered to be one of the principal security features to preserve privacy. This uses the Authentication and Key Agreement (AKA) procedure to generate a ciphering key to protect data encryption and an integrity key to derive session keys for signaling integrity. Whilst this approach has demonstrated many benefits, it cannot completely eradicate the threats posed by RBS attacks [18][11].

5G exploits two mechanisms to enhance subscribers' privacy. The first mechanism involves the encryption of the long-term identifier to prevent IMSI catchers or stingrays [19]. Accordingly, 5G uses the Subscription Permanent Identifier (SUPI) instead of the IMSI and a Public Key Infrastructure (PKI), to encrypt the SUPI into the Subscription Concealed Identifier (SUCI) [20]. 5G networks also utilise frequent changes in subscribers' short-term identifiers. These two

techniques already considerably enhance resistance to RBS attacks in 5G networks compared to earlier generations.

B. Rogue Base Station Threat

The security architecture group in 3GPP (SA3) has identified that measurement reports received from mobile stations may contain fingerprints (cellprints) of RBSs [21]. SA3 outlined a framework based on the analysis of measurement reports, including information on the characteristics of the radio channel, to enable mobile networks to detect such RBSs. The framework supplements other techniques introduced in 5G and mentioned above to protect users against RBSs [22].

IV. Proposed Model

As mentioned in the literature, RBS detection is one of the major issues that needs to be addressed. In this paper, we propose a model where several legitimate BSs provide network coverage to an area of a city. The basic idea behind the model is to generate measurement reports which can be used to detect and identify RBSs in the upcoming cellular technologies.

In our proposed model, the cellular network's coverage area is divided into many tracking areas, each of which contains some BSs (gNodeBs) to serve the tracking area. Fig. 1 illustrates a scenario where (legitimate) BSs are providing 5G coverage to a particular area. The area includes a segment of an urban motorway along which platoons of autonomous vehicles regularly travel. The platoons are assumed to use some V2V communications system between vehicles and one of the vehicles is selected as the Platoon Leader which has a 5G connection to the 5G system.

In this example, mobile UEs are vehicles traveling at approximately 80 kilometers per hour. The platoon is controlled from the V2X application server in the 5G core, and the platoon leader exchanges messages with the application server periodically in the order of milliseconds [23]. In this model we focus on the communication between the platoon and BS based on Vehicle-to-Network (V2N) technology.

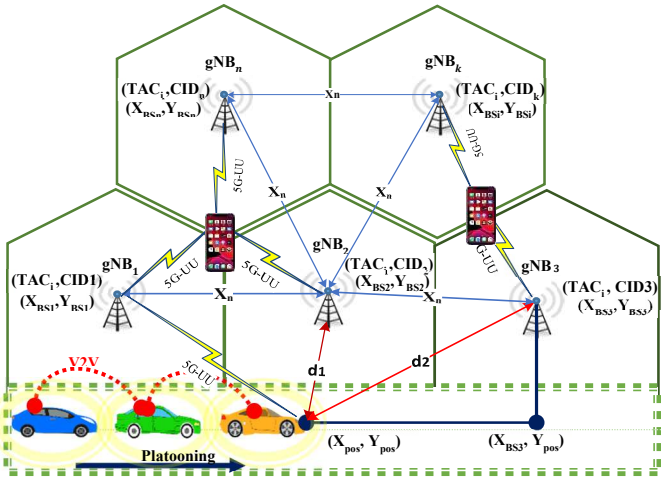

Fig. 1. Legitimate base station signal coverage. X_n: the connection between two gNB; TAC: Tracking Area Code; CID: Cell Identifier; (X_{pos}, Y_{pos}): location of Platoon's Leader; 5GUU: 5G uplink and downlink; *d*: distance between base station and Leader; and, gNB: gNodeB.

Vehicle platooning is one of the key V2X use cases in 5G by which a group of autonomous vehicles travel in close proximity to one another with the speed of the leader. The Vehicle-to-Vehicle (V2V) communication that provides the direct link between vehicles is part of Vehicular Ad-hoc Network (VANET) communication and is outside of the scope of this paper.

A. Mathematical Model

In free space (line of sight) communication, the electromagnetic wave propagates in a straight line and can be modeled by a version of Friis's free space equation [24]:

$$P_r = \frac{P_t G_t(\theta_t, \emptyset_t) G_r(\theta_r, \emptyset_r) \lambda^2}{(4\pi d)^2} \quad (1)$$

where P_r is the power (Watts) received by the UE, P_t is the power (Watts) fed into the BS antenna and G_t is the gain which is a function of the azimuth angle $\emptyset_t$ and elevation angle θ_t. G_r is the gain of the receive antenna which varies with $\emptyset_r$ and θ_r.

The variable d is the distance in meters between the transmitting antenna of the BS and the receiving antenna of the platoon leader, while λ is the wavelength (in meters) of the transmitted signal, given by:

$$\lambda = \frac{c}{f} \quad (2)$$

where c is the speed of light equal to 3×10^8 m/s. Substituting equation (2) in (1) results in:

$$P_r = P_t G_t(\theta_t, \emptyset_t) G_r(\theta_r, \emptyset_r) \left(\frac{c}{4\pi d f}\right)^2 \quad (3)$$

In our simulation, we calculate the location of the mobile stations every second and use that information to calculate the received power signal of each BS. From the geometry shown in Fig. 1 the distance between the BS and the vehicle is based on a triangular equation as follows:

$$d = \sqrt{(V * T - X_{BS_i})^2 + (Y_{BS_i} - Y_{pos})^2} \quad (4)$$

where V is the speed of the platoon (m/s), T is the simulation clock time in seconds and (X_{BSi}, Y_{BSi}) is the location of the BS_i, while (X_{pos}, Y_{pos}) is the position of the car. By substituting equation (4) into (3) we obtain the following equation:

$$P_r = \frac{P_t G_t(\theta_t, \emptyset_t) G_r(\theta_r, \emptyset_r)}{(V * T - X_{BS_i})^2 + \left(XY_{BS_i} - Y_{pos}\right)^2} \left(\frac{c}{4\pi f}\right)^2 \quad (5)$$

This calculation of the expected received power does not capture the variation in the path loss between the BS and the UE. The radio path will experience variations due to the presence of buildings or vehicles that can obstruct the line of sight path or highly variable reflective paths causing constructive or destructive interference at the receiver. Since the scenario here is a fast-moving vehicle, one would expect that the received power at the UE would vary significantly about this mean value. Based on a standard statistical model of radio propagation [25], we apply the variation and then convert the signal strength to dBm by the following equation:

$$Rxlev = 10log_{10}(P_r . x(t)) + 30 \quad (6)$$

where *x(t)* is a time-varying randomized variable that is bounded between zero and two [13]. Equation (6) can, therefore, be used to calculate the received power signal from each BS as the platoon moves along the roadway.

V. Results and Discussion

In this section, we will provide an overview of the results that we generated through simulation to validate our model. The simulation is carried out in MATLAB that is installed on a quad-core Dell machine equipped with 3.06 GHz Intel Xeon CPU and 12 GB of RAM. The entire simulation is based on the parameters listed in Table 1.

A detailed explanation of the figures generated from different scenarios through simulation is given in the following sub-sections. With regard to the accuracy of this simulation model, we assumed that the propagation is done while the mobile UE is within the antenna's coverage area, i.e. the platoon leader is within the range of BSs.

A. Legitimate Base Station Scenario and Results

The simulator is configured to emulate a 5G urban motorway scenario with three BSs with physical locations, as shown in Fig. 2. The transmission frequency used here is 3.8GHz, part of the 5G New Radio spectrum.

When the UE (in this example, the lead vehicle of a platoon) is within the range of the BSs, the received signal strength or RSRP (Reference Signal Received Power) is calculated once per second, producing the graph of received signal strength values shown in Fig. 3. Typically, the handover decision in 5G RAN is based on the data contained in the measurement report [26]. The UE measures the signal power of the surrounding cells based on the Synchronization Signal Block (SSB), which carries the Master Information Block (MIB) and synchronization signal without safety protection [27]. Moreover, as can be seen in Fig. 4, the UE handover from one BS to another occurs when the signal strength from the 2nd BS exceeds a specified threshold. In this simulation, the threshold difference to hand over is 7dB.

B. Attack Model Scenario and Results

In this section, we outline a potential RBS attack scenario. An attacker sets up an RBS in the vicinity of the road segment, indicated by the red dot in Fig. 2.

TABLE I. SIMULATION PARAMETERS FOR THE ATTACK MODEL

Parameter	Value	Parameter	Value
5G New Radio Frequency	3.8 GHz	Number of BS	3
Platoon Speed	80 Km/h	Road Width	300 m
RBS TX Power	0.5 (Watt)	Road Length	23000 m
BS TX Power	1 (Watt)	BS Gain	1 (dBm)
Number of RBS	1	RBS Gain	15 (dBm)

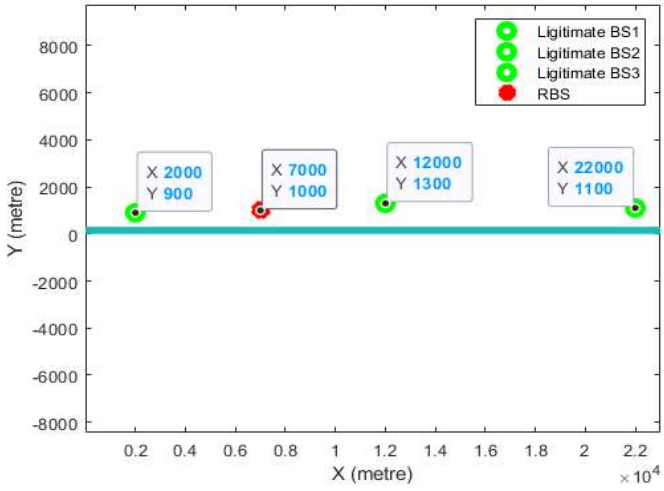

Fig. 2. The simulation geography, motorway width=300 metres, motorway length= 23000 metres

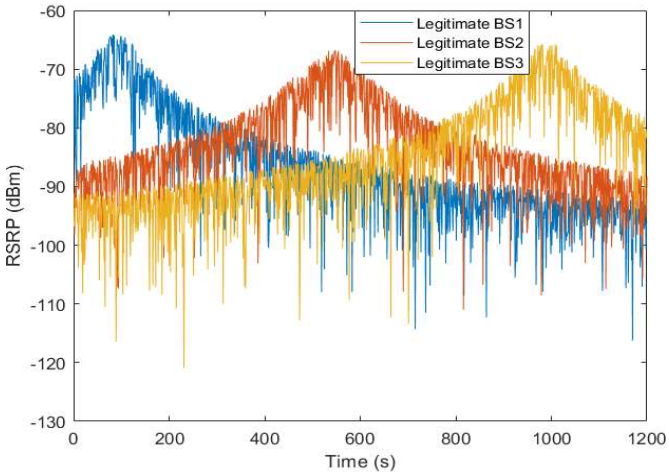

Fig. 3. Received signal strength for a mobile UE from several standalone legitimate base stations

This location enables the RBS to listen on the same channel as the legitimate BS for a sufficiently long time for it to be able to gather enough information to be able to mimic the legitimate BS. Then, when it detects the presence of a large platoon of autonomous vehicles, it begins to transmit using either a higher power transmission or a directional antenna. Thus, the platoon will see a substantially higher power signal from the rogue than it does from the legitimate BS. As a consequence of the handover protocol, the RBS requires the received power at the platoon to be more than 7 dB higher than the legitimate BS for the UE to switch to the RBS automatically. Once this threshold is reached, the handover takes place, and the rogue can now send commands to the platoon to make a sudden turn and cause a major road traffic incident. Fig. 5 illustrates an RBS with 2 beams – normally, they would use only one, but there are two included in our simulation to show how the direction in which the antenna is pointing could significantly impact the amount of road that is covered.

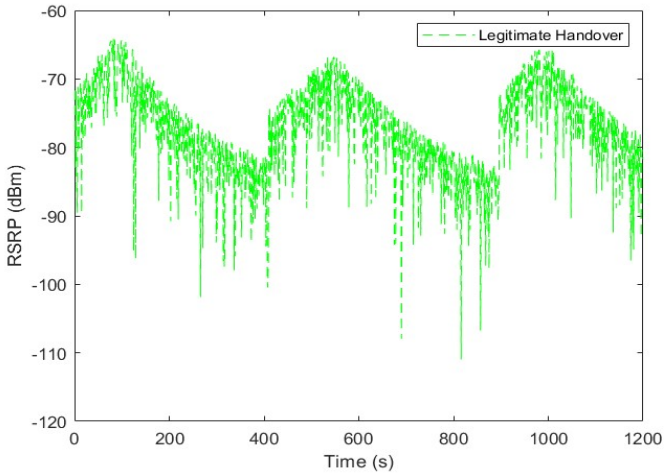

Fig. 4. Received signal strength for a mobile UE after the handover protocol

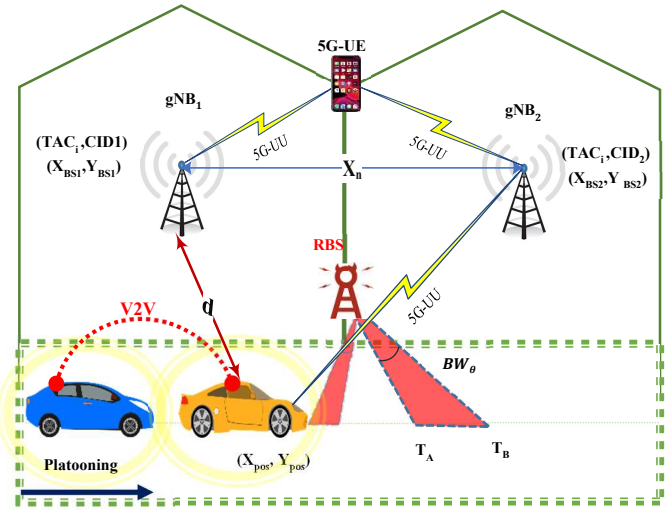

Fig. 5. RBS attack scenario, (X_{BS}, Y_{BS}): location of the base station; T_A, T_B: edges of narrow beams; BW_θ: beam width angles; V2V: Vehicle-to-Vehicle communications; TAC: Tracking Area Code; and, CID: Cell Identifier.

Implementing an RBS with high transmitting power is unlikely for adversaries because it is quite expensive and requires the installation of very large equipment. Typically, they set up an RBS consisting of a wireless transceiver, a laptop, and a cell phone, allowing passive and active attacks against UE subscribers over RANs. The transceiver broadcasts radio signals to impersonate genuine BSs.

In this study, an RBS has been simulated with less power but with an antenna with a narrow beam that covers part of the motorway with higher gain to deceive the user equipment and penetrate the network. Since the antenna concentrates power, it strengthens the transmission power in a single direction, while decreasing the power in other directions. Reducing the horizontal beam width, for example, strengthens the power in a narrower directional beam. The gain of an antenna is the ratio of the power flux density in a given direction to the power flux density that would be present from an isotropic radiator (i.e., an antenna that radiates equally in all directions). Therefore, the gain of the antenna is inversely proportional to the beam width [24][28]:

$$G(dB) = 10Log\left[\frac{APC}{BW_\theta BW_\Phi}\right] \quad (7)$$

In our model, the antenna pattern has been assumed as a rectangular area and the value APC (defined as the Antenna Pattern Constant) yields a constant of 41,253 when the beam width angles are expressed in degrees [12].

Within the simulation, it is assumed that the horizontal and vertical beam widths are equal. Thus, equation (7) is rearranged so that the beam width of the antenna is calculated from its specified gain. This is used with the location of the RBS to calculate when the UE is within the coverage of the RBS. This is then used to calculate the times when the UE is within the coverage of the RBS's narrow beams: T_A and T_B are these times indicated in Fig. 5. As can be seen in Fig. 6, the RBS produces a higher receive signal strength which can deceive the UE. As expected, there are two zones where the power from the RBS is higher since we are using two beams. The first beam is angled at 60 degrees to the roadway and hence we see a larger received power, but for a shorter duration, compared to the second beam which is angled at 30 degrees to the roadway.

Consequently, as shown in Fig. 7, the RBS masquerades as the second legitimate BS and forges its system information. As a result, the victim UE may camp to the RBS. In this scenario, the serving BS receives the UE measurement report which involves measurements from the RBS. The serving BS would assume that the information in the UE measurement report belongs to BS2 so may decide to handover the UE to the RBS instead of BS2.

As a consequence, the intended handover from BS1 to BS2 will fail. Instead, BS1 will hand-over the UE to the RBS which succeeds in gaining control of the communication link to the UE. Although the UE may only be captured for a few tens of seconds in such a scenario, this is sufficient for information to be stolen or for a traffic collision to be caused.

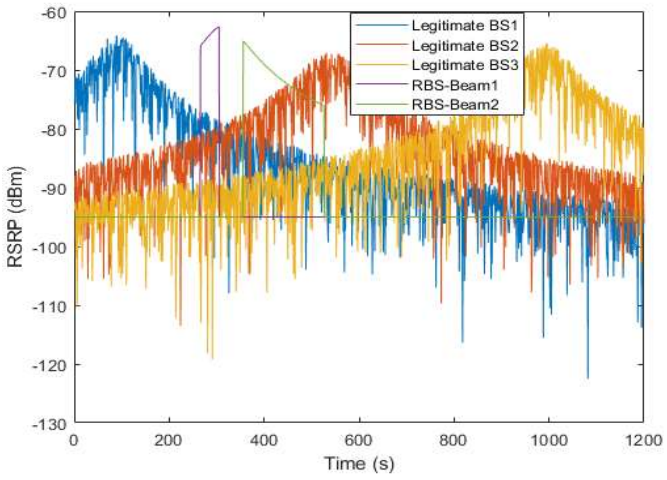

Fig. 6. Received signal strength for a mobile UE from a Rogue Base Station with two beams

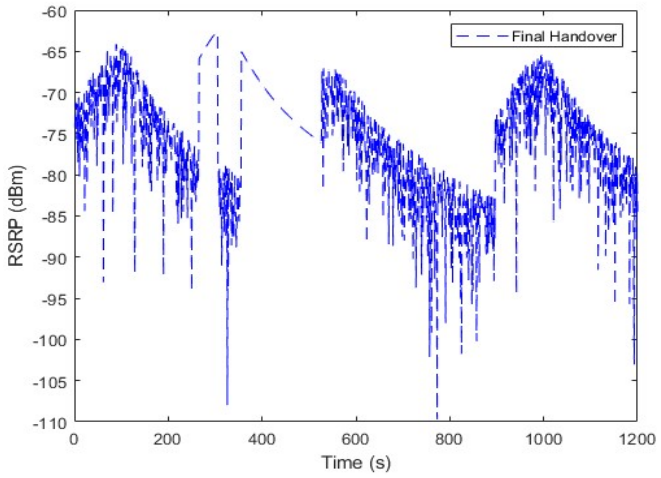

Fig. 7. Received signal strength for a mobile UE after the handover protocol in the attack model

Since the simulator described here is relatively simple and generates receive signal level reports calculated from a defined geographical arrangement of base stations and roadways, the essential parameters of a UE's measurement reports can be generated and used to devise new ways to prevent such RBS attacks.

VI. Conclusion

RBS attacks are a serious threat to cellular networks and users. The anticipated use of 5G systems to control critical systems such as vehicular platoons opens the possibility of catastrophic consequences. This paper describes the simulation of a platoon moving through a radio coverage area and calculating received signal strength. We build a tool generating a realistic dataset of radio information and signal strength measurements in an RBS scenario. The dataset is generated using well-known radio propagation models that can be easily used and do not attempt to be a highly accurate simulation of radio propagation. In summary, it is worthy to note that we can generate a dataset of 20 minute drive time in a 15 seconds simulation. This approach enables the researchers to create a range of geographical and radio scenarios and generate measurement report data in the absence of any anomalous radio propagation situations.

Since the broadcast channels of BSs in 5G and preceding systems must contain uncyphered information so that UEs can identify each BS and decide which one to attach to, it will always be possible for RBS attacks to be launched. However, by using the reported information in the measurement reports, the network can look for anomalous behavior to indicate that an RBS is attempting to capture a UE. Future work will use this simulator in a vehicular platooning scenario to design machine learning methods to detect RBS attacks and protect against them.

Acknowledgment

The authors would like to thank the BT Ireland Innovation Center (BTIIC) at Ulster University for supporting this work.

References

[1] A. S. Khan, Y. Javed, J. Abdullah, J. M. Nazim, and N. Khan, "Security Issues in 5G Device to Device Communication," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 17, no. 5, pp. 366–375, 2017.

[2] N. Alliance, "5G White Paper," *Next Generation Mobile Networks Alliance*, p. 124, 2015.

[3] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, Eds., *A Comprehensive Guide to 5G Security*. Chichester, UK: John Wiley & Sons, Ltd, 2018.

[4] C. Campolo, A. Molinaro, A. Iera, R. R. Fontes, and C. E. Rothenberg, "Towards 5G Network Slicing for the V2X Ecosystem," *2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft 2018*, pp. 303–307, 2018,

[5] 5G-Americas, "The Evolution of Security in 5G, A 'Slice' of Mobile Threats," *TAPPI Journal*, vol. 18, no. 7, 2019, doi: 10.32964/tj18.7.

[6] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," *Journal of Network and Computer Applications*, vol. 101, no. December, pp. 55–82, 2018, doi: 10.1016/j.jnca.2017.10.017.

[7] K. Haneda, J. Zhang, L. Tan, *et al.*, "5G 3GPP-like Channel Models for Outdoor Urban Microcellular and Macrocellular Environments," *IEEE Vehicular Technology Conference*, vol. 2016-July, 2016, doi: 10.1109/VTCSpring.2016.7503971.

[8] R. Lu, L. Zhang, J. Ni, and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 373–389, 2020, doi: 10.1109/JPROC.2019.2948302.

[9] M. Barbeau and J. M. Robert, "Rogue-Base Station Detection in WiMax/802.16 Wireless Access Networks," *Annales Des Telecommunications/Annals of Telecommunications*, vol. 61, no. 11–12, pp. 1300–1313, 2006, doi: 10.1007/BF03219898.

[10] J. L. Ryan, R. L. Justin, and K. A. Stone, "Rogue Base Station Router Detection with Statistical Algorithms." Google Patents, 02-May-2019.

[11] J. Jin, C. Lian, and M. Xu, "Rogue Base Station Detection Using a Machine Learning Approach," *2019 28th Wireless and Optical Communications Conference, WOCC 2019 - Proceedings*, no. Wocc, pp. 1–5, 2019, doi: 10.1109/WOCC.2019.8770554.

[12] Z. Li, W. Wang, C. Wilson, *et al.*, "FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild," no. March, 2017, doi: 10.14722/ndss.2017.23098.

[13] K. W. Huang and H. M. Wang, "Identifying the Fake Base Station: A Location Based Approach," *IEEE Communications Letters*, vol. 22, no. 8, pp. 1604–1607, 2018, doi: 10.1109/LCOMM.2018.2843334.

[14] A. Ali and G. Fischer, "Enabling Fake Base Station Detection through Sample-Based Higher Order Noise Statistics," *2019 42nd International Conference on Telecommunications and Signal Processing, TSP 2019*, pp. 695–700, 2019, doi: 10.1109/TSP.2019.8769046.

[15] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 1, pp. 228–255, 2015, doi: 10.1109/COMST.2014.2345420.

[16] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A Security Credential Management System for V2V Communications," *IEEE Vehicular Networking Conference, VNC*, no. December 2013, pp. 1–8, 2013, doi: 10.1109/VNC.2013.6737583.

[17] Z. Zhuang, X. Ji, T. Zhang, *et al.*, "FBSleuth: Fake Base Station Forensics via Radio Frequency Fingerprinting," *ASIACCS 2018 - Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security*, pp. 261–272, 2018, doi: 10.1145/3196494.3196521.

[18] D. Fang, Y. Qian, and R. Q. Hu, "Security Requirement and Standards for 4G and 5G Wireless Systems," *GetMobile: Mobile Computing and Communications*, vol. 22, no. 1, pp. 15–20, 2018.

[19] S. F. Mjolsnes and R. F. Olimid, "Private Identification of Subscribers in Mobile Networks: Status and Challenges," *IEEE Communications Magazine*, vol. 57, no. 9, pp. 138–144, 2019, doi:

10.1109/MCOM.2019.1800511.

[20] R. P. Jover, "The Current State of Affairs in 5G Security and the Main Remaining Security Challenges," vol. 1282, pp. 1–8, 2018.

[21] H. Alrashede and R. A. Shaikh, "IMSI Catcher Detection Method for Cellular Networks," *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019*, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769507.

[22] P. K. Nakarmi and K. Norrman, "Detecting False Base Stations in Mobile Networks," 2018. [Online]. Available: https://www.ericsson.com/en/blog/2018/6/detecting-false-base-stations-in-mobile-networks. [Accessed: 25-Jan-2020].

[23] S. S. Husain, A. Kunz, A. Prasad, E. Pateromichelakis, and K. Samdanis, "Ultra-High Reliable 5G V2X Communications," *IEEE Communications Standards Magazine*, vol. 3, no. 2, pp. 46–52, 2019, doi: 10.1109/MCOMSTD.2019.1900008.

[24] C. A. Balanis, *Antenna Theory: Analysis and Design, 3rd Edition*. 2005.

[25] J. B. Andersen, T. Rappaport, S. Yoshida, and T. S. Rappa-, "Models For," *IEEE Communications Magazine*, no. January, pp. 42–49, 1995.

[26] 3GPP Technical Specification TR 33.809, "Technical Specification Group Services and System Aspects; Study on 5G Security Enhancement against False Base Stations."

[27] 3GPP TS 38.331, "Technical Specification Group Radio Access Network; NR; Radio Resource Control (RRC); Protocol Specification," 2020.

[28] Naval Air Systems Command, "Electronic Warfare and Radar Systems Engineering Handbook," *Electronic Warefare and Radar Systems Engineering Handbook*, no. April 1997, p. 299, 1999.