New techniques for high-fidelity modeling and simulation in 5G mobile network environments

Mr. Steven Kropac*[1]
CACI/LGS Innovations
Herndon, VA
steven.kropac@caci.com,

Dr. Jeff Weaver
SCALABLE Network Technologies
Culver City, CA
jweaver@scalable-networks.com

ABSTRACT

Innovative new techniques for Modeling and Simulation (M&S) of 4G and 5G mobile networks can enable effective proficiency training, cyber situational awareness, network analysis and mission rehearsal exercise support for cyber physical activities. This is important to the community because commercial mobile network environments are evolving and proliferating globally. M&S live, virtual, constructive (LVC) techniques must advance to accurately represent and be interoperable with the new frequencies available with 5G (e.g. mmWave and cmWave) Access Points (AP), smart buildings and homes, mobile-to-mobile, telematics, and sensor networks.

For this effort, we used a high-fidelity modeling and simulation platform to model wired and wireless communication networks that include cellular, enterprise, and battlefield networks and detailed propagation models of signal transmission with a comprehensive library of cyber-attack and defense models. This approach provides an interoperable simulation for network elements and physical elements such as trees, houses, cellular towers, people and weapons systems. The architecture has been instrumented to provide deep operational understanding of new 5G elements and their impact on cyber situational awareness, particularly in contested environments. For 4G LTE networks, the solution enables understanding network chokepoints and analyzes how a network is affected in scenarios where certain elements are perturbated or degraded through kinetic or non-kinetic effects. High fidelity 5G mobile network M&S platforms provide important training, cyber situational awareness and mission rehearsal as cyberspace operations become more integrated into the tactical mission space.

ABOUT THE AUTHORS

Mr. Steven Kropac is VP of the Internet and Cyber Research Department at CACI/LGS Innovations. He has over 20 years of experience as a subject matter expert on global carrier class network architecture, design and implementation. This includes several network and Network Element (NE) technologies including Optical Transport, IP routing and switching, traditional and next generation mobile network technology (3G, 4G, 5G, and beyond) as well as traditional and next generation public switched telephone networks. Over the last 15 plus years, Mr. Kropac has been building a team of Cyber Security and Network Assurance experts primarily focused on security analysis of networks and network elements. His team consists of engineers and scientists with a strong background in carrier class network technology, reverse engineering, software development, protocol analysis and system engineering. Mr. Kropac holds a Master's in Computer Engineering from Stevens Institute of Technology.

Dr. Jeffrey Weaver, is VP of Engineering at Scalable Network Technologies, Inc. He obtained his Ph.D. degree from Western University in London, Ontario. Dr. Weaver has held key technical and executive engineering roles in Fortune 50 companies including Bay Networks, where he performed switch design, network architecture development; and OPNET Technologies performing model and software architecture development as a Manager of Consulting Services. At SCALABLE, Dr. Weaver developed MUOS and other multi-beam satellite models, performed research into the Communication Effect Server (CES), led efforts to integrate ADSB and Mode 5 GNU Radio waveforms into QualNet, led commercial wireless modeling efforts in LTE and Wi-Fi, and directed the technology upgrades in the message passing architecture and Parallel Discrete Event Simulation (PDES) algorithms to take advantage of advances in operating systems, processors, and programming languages .

[1] LGS Innovations, a wholly owned subsidiary of CACI Federal

New Techniques for High-Fidelity Modeling and Simulation in 5G Mobile Network Environments

Steven Kropac*[2]
CACI/LGS Innovations LLC
Herndon, VA
steven.kropac@caci.com

Jeff Weaver
SCALABLE Network Technologies
Culver City, CA
jweaver@scalable-networks.com

INTRODUCTION

As global cellular networks evolve from current 3G and 4G systems to future 5G networks, they are enabling and proliferating a more ubiquitous all-things-connected world. Nations around the world desperately need an efficient, high-fidelity approach for understanding, evaluating, and ultimately protecting critical infrastructure from theoretical or actual kinetic and cyber threats. In this paper, we will present innovative, efficient, and high-fidelity approaches for proficiency training, cyber situational awareness, network analysis, and mission rehearsal. These approaches and results were achieved using the integrated LGS LiveRAN™ and SCALABLE Network Technologies EXata® Modeling and Simulation platform (referred to as the Platform). The following sections provide details on how a high-fidelity M&S platform can be used to efficiently model and exercise a broad range of cyber mission scenarios. The analysis results include documented results in a 4G environment as well as theoretical expectations for 5G environments. Future paper(s) will describe how the approaches evolve and results can be obtained for 5G environments.

BACKGROUND

Commercial mobile networks are complex. These networks are typically architected, designed, and deployed across large physical regions, and can span multiple countries. To help set the stage for how we have established and exercised new techniques for high-fidelity modeling and simulation in 5G mobile network environments, we will first describe relevant concepts and terminology that are central to 4G and 5G mobile networks. Next, we'll discuss briefly how software platforms can be used to model and simulate these complex networks. This forms the basis for designing and exercising new training, cyber situation awareness and mission rehearsal techniques in modern 4G/5G mobile networks.

Third Generation Partnership Project (3GPP)

All commercial networks operating today adhere to some standard for communications using well-defined interfaces and protocols. This ensures interoperability and enables seamless communications between connected systems. The mobile network is no exception. Since the early-90s, mobile network interfaces and protocols have been defined and standardized by the Third Generation Partnership Project (3GPP) (www.3gpp.org). This standardization group has provided the basis for interoperability among hardware and software vendors.

Modern networks in use today are on the fourth major iteration of mobile network standards. This is referred to as 4G Long Term Evolution (LTE). These networks are comprised of several different components enabling high-quality voice and data services to subscribers. The Network Elements (NEs) that compose a 4G LTE network are shown in the following diagram. This network depicts various mobile devices connected to an Evolved Packet Core (EPC) via a Radio Access Network (RAN).

[2] LGS Innovations LLC, a wholly owned subsidiary of CACI Federal

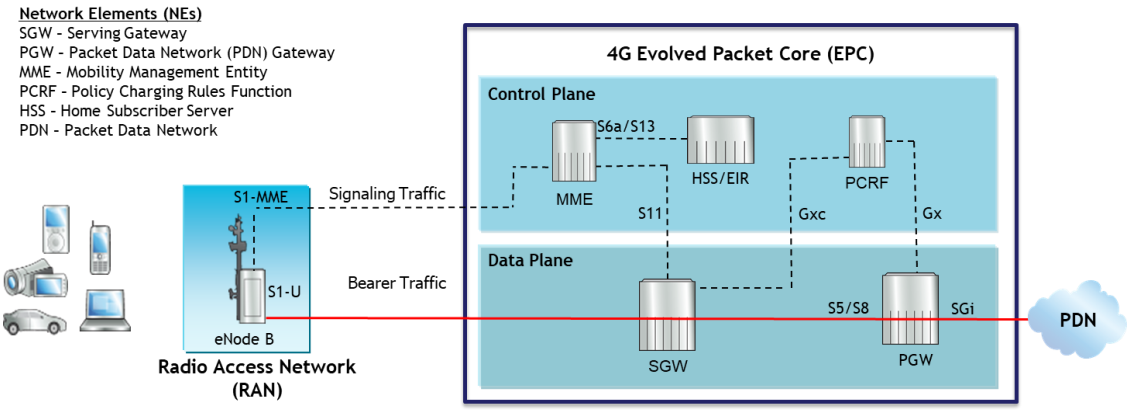


Figure 1: Logical view of a 4G EPC

Depending on the size and scope of the network being deployed, each one of the logical NE's shown in Figure 1 can be anywhere from the size of a pizza box to the size of several refrigerators and be load balanced across several physical instantiations. As networks have evolved today, several of these NEs are also deployed as virtualized instances that exist as software deployed within cloud computing centers. These fundamental attributes are important to note as we apply concepts for cyber situational understanding, network analytics, and mission rehearsal later in the paper.

5G Networks

From the late 2000s through today, 4G LTE and smart phones brought high-speed networking to people, enterprises and governments on the move. However, increased demand for bandwidth, low-latency, and ubiquitous connectivity requires an evolution towards the fifth generation of mobile networks. As shown in the diagram below, significant complexity has been added to support multi-function 5G networks. Many believe that 5G will be the first network architected to support massive amounts of Internet of Things (IoT) communicating on a machine to machine basis. 4G was all about connecting humans to data. 5G is going to be about ubiquitous communications globally and massive machine to machine communications. From the warfighter's perspective, this increases both the challenges in performing modeling and simulation as well as being able to understand how the network will perform when perturbated by kinetic or cyber effects.

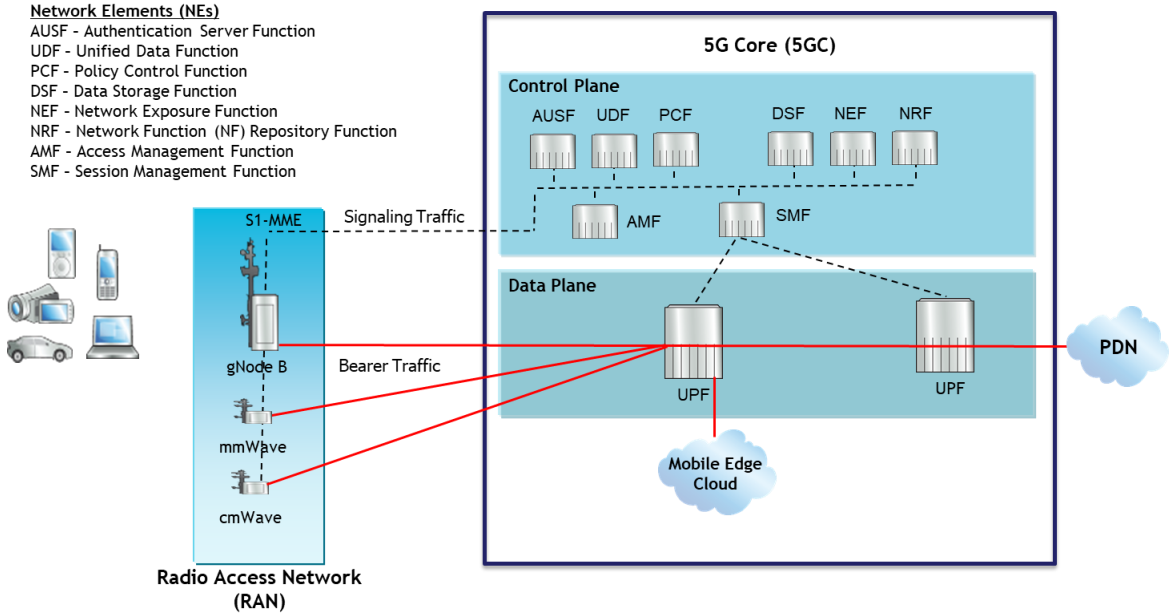


Figure 2: Logical view of a 5G Core

High Fidelity Modeling and Simulation of Mobile Networks

Modeling and simulation platforms for mobile networks are useful for many reasons: wired and wireless network planning, network analysis, and cyber threat analysis. For example; from a network planning perspective, understanding where to place a cell tower and optimizing that placement has significant impact on cost and operational effectiveness of the network. Operators and researchers continue to analyze networks to create new layouts that optimize cost and efficiency. Being able to first model these networks in a completely simulated domain to understand how radio frequency (RF) for these networks may theoretically perform based on terrain and environmental conditions controllable within the environment is important. The fidelity of these platforms can then be increased with the addition of hardware in the loop capabilities. This allows the user to understand down to the bit level how a system will react and perform under specific conditions. The following diagram provides a notional view of the split between Live, Virtual and Constructive (LVC) for modeling and simulation of mobile network environments.

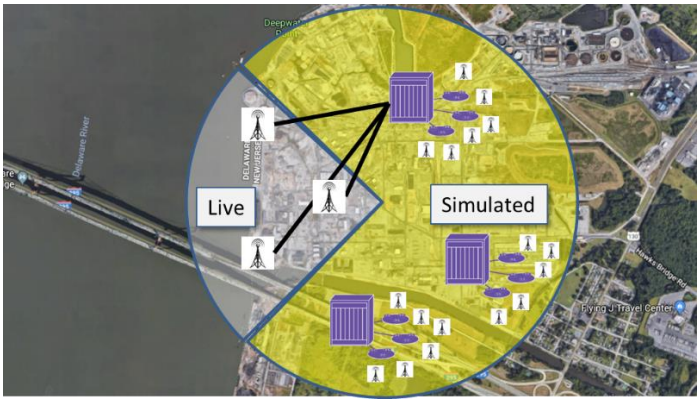


Figure 3: Notional View of a Modeling and Simulation Platform providing LVC capabilities

Modeling and simulation of 4G/5G systems are ideal for proficiency training, network analysis, cyber situational awareness, and mission rehearsal for the warfighter. Utilizing a M&S platform that can provide high fidelity hardware in the loop capability for focused areas of a network allows the warfighter to understand to a high fidelity, bit accurate traffic activity and system responses when the network is perturbated. In addition, the terrain map and configuration of each live, virtual or simulated NE can be quickly changed to meet scenario requirements. This approach provides a global scope view of the entire network, while also providing high-fidelity understanding of system operation for localized focus areas within the network.

NEW TECHNIQUES FOR MODELING AND SIMULATION IN 5G ENVIRONMENTS

This paper will explain new techniques that can prepare the warfighter with training, cyber situational awareness, network analysis and mission rehearsal. The objective of these new techniques is to provide enough knowledge gain for military service members to be as effective as possible when supporting mission operations. The remainder of this paper will describe the techniques and approaches we created to prepare the warfighter to rehearse and operate effectively across an interconnected warfighting domain including cyber and physical (land, sea, air). Increased depth of understanding is provided and available via bit-accurate representations of packet flows within the network protocols and application layer traffic including mobile application traffic.

Historically, training systems would use traffic generators to generate web, email or file transfer traffic. This is good for some of the networks' representative traffic, but today's network is dominated by mobile application traffic. Systems that can generate mobile application traffic equivalent to what an actual mobile application generates is ideal for mission preparation purposes. Understanding of current 4G networks and mobile application traffic is a necessary starting point, but the network is constantly evolving. Furthermore, being able to map these networks to a 3D terrain map specific to the Area of Responsibility (AOR) increases relevancy for situational awareness of RF propagation in urban and rural settings. As networks progress towards 5G and new IoT systems are added every day, the warfighter will need to more increasingly rely on modeling and simulation platforms as a training tool to accurately and precisely understand what is happening in the cyber domain. Platforms that can support high-fidelity, hardware in the loop (HIL) mix-and-match overlay of live components from numerous manufacturers with "generic" components that

emulate live elements, provide an ideal environment for training, understanding, and assessing networks, network attacks and failures.

Proficiency Training

Preparing the warfighter begins in the classroom. Aided by modeling and simulation systems, instructors can work with teams to provide hands-on training on the fundamentals of mobile networks and how cyber network attacks happen for mobile devices (handsets, IoT devices, telematics systems, Industrial Control Sensors (ICS) sensors). Modeling and simulation platforms provide the opportunity for hands-on understanding of network element functions and roles within the larger system of systems used to provide service to the mobile network user. It helps the warfighter understand that handsets and other customer equipment attach and operate on the network by communicating via signaling and data messages to the EPC and not just the cellular tower, otherwise known as the Radio Access Network (RAN). Furthermore, high-fidelity platforms can be used to train the operator on deeper insight into network attributes, such as:

- control plane and data plane separation
- local vs. global scope systems, and
- effects or impacts resulting from potential cyber or kinetic attacks.

Figure 4 and Figure 5, shown below, depict User Equipment (UE) attaching to the network with a breakout of key NE's that make up the EPC. This detail is what helps the trainee understand from a graphical perspective how NEs within a mobile network environment work together to authenticate and provide service to a user. The logical elements shown in Figure 1 are mapped to a physical terrain map shown in Figure 5. This graphical representation takes the trainee from logical diagrams shown in books and training manuals to the virtual physical world accurately mapped onto a 3D terrain map. Through this process, the trainee will gain a better understanding of control plane vs. data plane messaging.

As the Platform operates, it will show control plane and data plane messaging moving between the various nodes as shown in Figure 4. In this figure, the trainee learns that the UE begins the authentication process by initiating a sequence of attach messages starting with the eNodeB, and progressing through authentication via the Non-Access Stratum (NAS) with the MME. The MME utilizes the Home Subscriber Server (HSS) as the back-end database to authorize the UE and allow the appropriate data connection. Once that is completed, the network establishes a data-plane session for the UE through a series of create session and modify session requests with the Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW). By repeatedly going through hands on training exercises the trainee can best understand control plane messages sequences that allow a UE to attach and subsequently detach to/from the network.

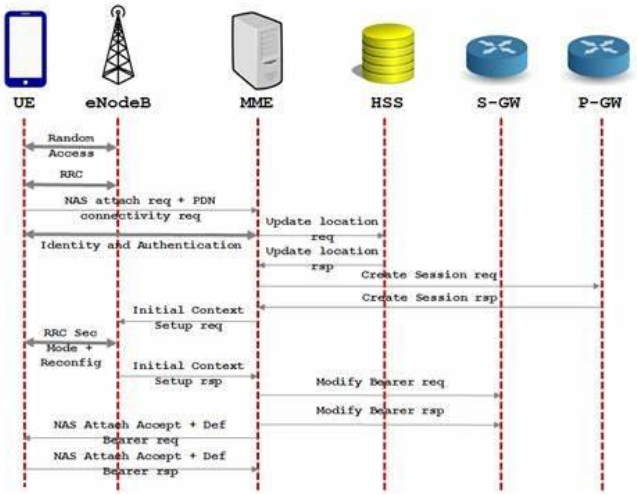


Figure 4: Control Plane and Data Plane Messaging Sequences

The repeated practice of monitoring control plane and data plan messages increases understanding and differences between control plane and data plane from both an operational perspective as well as from a cybersecurity perspective. Operationally, control plane messages are quantitatively less than data plane messages, but qualitatively, the control plane messages allow a mobile device onto the network and provide for mobility, as well as understanding of geolocation of the device. Data plane messages are used to send and retrieve content from the device. From a cybersecurity perspective, we can now begin to see where perturbations in this environment may cause degraded or lost capability for each of the attributes identified. In the mission rehearsal section of this paper, we'll talk about different cybersecurity concerns and potential effects.

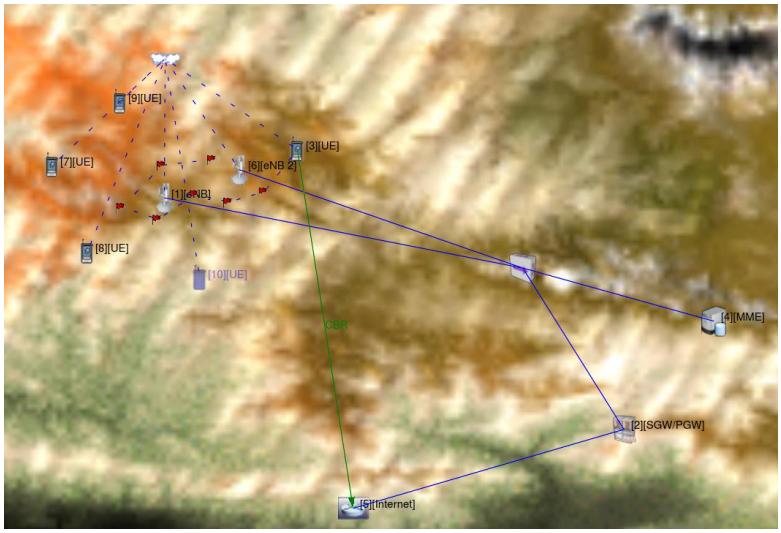


Figure 5: Mapping of 4G Logical Network Elements to the Physical Domain

In addition to the understanding of control plane and data plane messages, it is important to understand the local vs global scope system responsibilities and potential cyber effects. For example, a single 4G eNodeB access point within the RAN provides services to subscribers within range of that tower. However, if that eNodeB failed due to a kinetic or cyber effect, local users would experience loss of service, unless they are within range of another eNodeB. Some subscribers might be in range of another eNodeB because they are near the hand-over border between two nodes. However, all the other users would lose service. The impact is localized to the region covered by the eNodeB and thus considered local scope. Contrast this with control plane or data plane coverage provided by a MME or PGW, respectively. If either of these nodes failed due to a kinetic or cyber effect, the impact would be global. Several tens of thousands to millions of subscribers would lose service. To prevent this from happening carrier-grade service providers build in load-balancing and fail-over systems to support operations in these potential scenarios. In addition, when looking at the coverage heat maps depicted in Figure 6, one can see that the scope of local effect is much greater depending on configuration of the 4G access point. This same methodology will apply when comparing 4G to 5G. This is because 5G mmWave and cmWave systems will have a much smaller RF footprint. Analysis results like these help the trainee understand the scope of impact associated with a 4G vs. 5G outage at the access point. A more detailed explanation of how this is observed in a modeling and simulation environment is discussed later in the paper as part of performing mission rehearsal.

These same concepts apply in general for 5G networks, but several new concepts are introduced with this technology, which changes the landscape as far as understanding effects and confirmation of effects. 5G systems are similar in that they include control plane and data plane systems used to provide service to the user. However, a key difference is that 5G fully employs concepts like Software Defined Networking (SDN), Network Functions Virtualization (NFV), Mobile Edge Cloud (MEC), which further distributes computing resources across an underlay network of resources. These underlay resources allow for virtualizing what used to be big-iron resources into compute functions enumerated in Figure 2. For example, Unified Data Function is a software-only virtualized compute resource placed on a commercial off the shelf (COTS) hardware platform and can be readily executed in a number of physical locations determined by the SDN orchestrator. What this ultimately means is that the operator's SDN system can place physical resources close to the end user (i.e., MEC), to support the single digit latency requirement specified for 5G.

These resources can be brought into the modeling and simulation environment and be used to train the warfighter on how to identify attributes of a 5G system and where local effects vs. global effects may apply. 5G systems aren't only different based on the underlay. They are also different based on high-speed low latency access points, multi-connectivity and carrier aggregation technologies, which are key concepts from 5G.

Diversity of signals from RF space provides resiliency to the operator of the handset and this creates additional challenges to the warfighter looking to create local kinetic or non-kinetic effects in a contested environment. For 5G environments, simply taking out the cell tower in a region will likely not affect communications for users in the 5G area like it would in a 4G environment. In a 4G environment, users will lose service. In a 5G environment, because there are multiple access points, including new mmWave and cmWave, the user's equipment will merely receive service from a subset of access points. Similarly, global effects are mitigated at the 5G layer by nature of the virtualized and distributed nature of the systems. Ultimately, by training the warfighter to understand how data centers are used to provide compute resources for the mobile core (4G or 5G), they can develop and rehearse missions that meet mission requirements.

Cyber Situational Awareness and Network Analysis

Proficiency training provides the necessary background and fundamental understanding of relevant terms, network topology and system operation. This enables the warfighter to now leverage this understanding for greater cyber situational awareness and network analysis of various cyber-attacks.

The Platform can be used to model cyber-attacks within a cellular network. The tool provides the ability to jam the 4G/5G waveform using reactive jamming and an API to extend this to protocol-aware jamming. The cyber analysis and network analysis are integrated into a single emulation application to allow the user to measure the cyber resilience of a network while simultaneously demonstrating the effect of such attacks on the applications themselves.

Figure 6 shows a typical 4G small-cell laydown at 900 MHz and an equivalent laydown at 2600 MHz. Each figure is shown as a geographic distribution of received signal strength (dBm) versus location. This is developed by placing an isotropic antenna at each sample point in the generic urban terrain under consideration. The RAN is generated with high fidelity 4G models at one of two frequency bands. There is no single model under urban propagation models that covers frequency range from 700 MHz to 2600 MHz. The following models were considered depending on terrain type and frequency.

- Okumura-Hata has a frequency range of 150 MHz – 1000 MHz
- Cost 231-Hata has a frequency range of 1500 MHz – 2000 MHz
- Cost 231-WI has a frequency range of 900 MHz – 1800 MHz
- Irregular Terrain Model (non-urban) has a frequency range of 20 MHz – 20 GHz

In our initial experiment we considered 20 LTE UEs distributed in an urban environment and connected to a single eNodeB. The first is a 900 MHz 4G scenario in an urban environment using Okumura-Hata modeling. The radios are distributed in a 200m x 200m grid and the propagation results are shown below. The red and green regions are receiving good enough signal quality to be able to attach and use the network. The signal strength in the blue region is too poor to receive service.

Diversity of signals from RF space provides resiliency to the operator of the handset and this creates additional challenges to the warfighter looking to create local kinetic or non-kinetic effect in a contested environment. For 5G environments, simply taking out the cell tower in a region will likely not affect communications for users in the 5G area, like it would in a 4G environment. In a 4G environment, the base stations tend to be Macro cells or Metro cells that operate at much higher power levels and thus covers are larger range. There is also less overlap of cells within a 4G environment. As a result, 4G users will lose service. In a 5G environment, because there are multiple access points, with many of those access points overlaid, the user's equipment will merely receive service from a subset of access points. Similarly, global effects are mitigated at the 5G layer by nature of the virtualized and distributed nature of the

systems. However, by training the warfighter to understand how data centers are used to provide compute resources for the EPC, they can develop and rehearse missions that meet mission requirements.

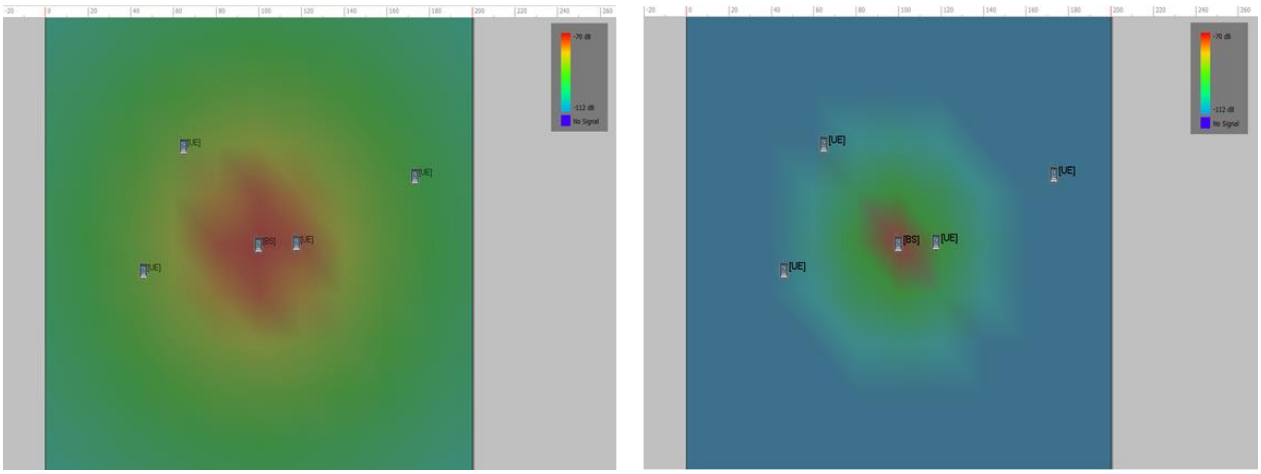


Figure 6: 4G heatmaps at 900 MHz and 2600MHz

The diagram on the left clearly shows that the two UEs near the center of the diagram and near the Base Station (BS) are well within range and receiving an excellent signal. The UE's on the edges of the diagram are receiving a signal in the -90 to -100db, but still able to obtain service. This demonstrates the broad coverage provided by a 4G BS operating at a lower frequency.

The figure on the right shows a similar UE laydown operating at 2600 MHz. While this is outside of the normal range of COST-231, we choose to extend the analysis slightly outside to demonstrate the greatest contrast between performance levels. In this scenario, the UE to the right of the BS receives good signal, but the outside UEs receive -112dB or lower signal levels. The UE on the right would likely not be able to establish a data session with the network. Network analysis at 5G potentially or probably involves digging down from the virtualized layer to where the physical fibers and connections are to drive towards choke points/critical nodes. A future paper is planned to provide details on 5G propagation results based on frequency and terrain settings similar to what is shown here.

Mission Rehearsal

Enabling efficient and informative mission rehearsal for the cyber warfighter can be achieved through the use of modeling and simulation platforms. The following scenario will describe a mission rehearsal progressing from monitoring normal system operation, to inserting an effect, and observing and confirming the effect. The specific mission scenario being planned is a cyber-kinetic mission (e.g., a bomb being dropped on one of our NEs). The end result is that it would likely keep any UEs from getting access to the Internet (i.e., no data plane traffic) and may cause mass panic. This scenario can be repeatedly tested and evaluated to ensure all team members understand potential side effects, metrics and areas for concern. For this scenario, the warfighter can setup the mission domain by instantiating all the NEs and UEs on an appropriate 3D terrain map as shown below:

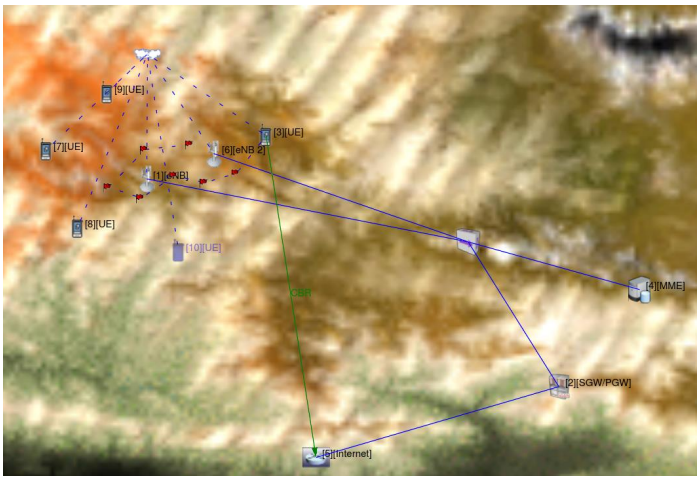
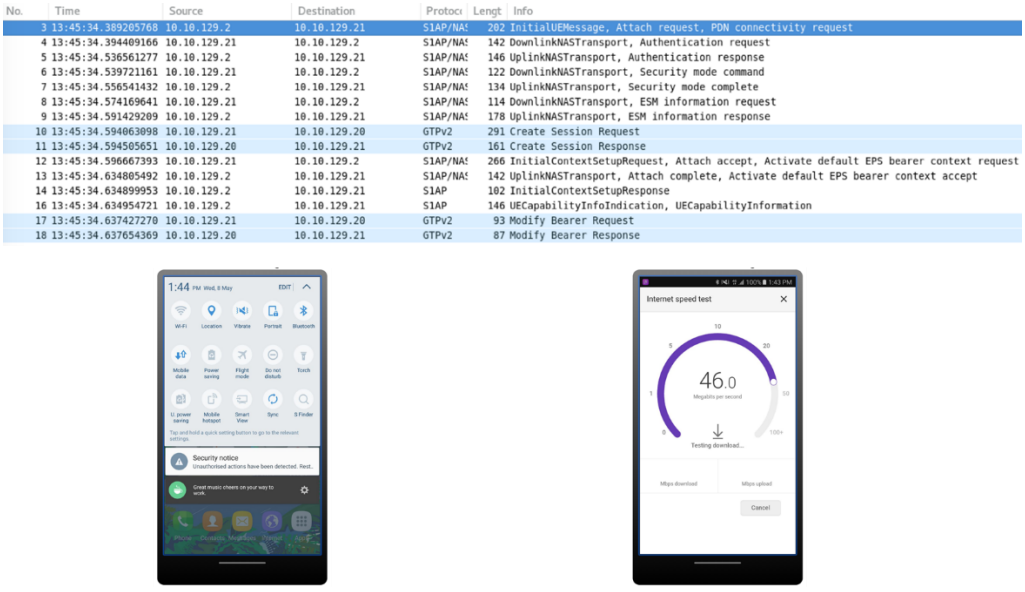


Figure 7: Mission Rehearsal (Scenario Preparation)

After the cyber-physical mission scenario is defined, the trainee can walk thru various cyber situational awareness and network analysis scenarios. This example scenario shows the trainee taking a virtualized UE that is operating in the target region out of airplane mode and observing the network attach control plane message sequences. Next, the trainee also runs an app to observe the data plane throughput being achieved by the UE. These mission rehearsal attributes appear in Figure 8. S1-AP UE attach message details are shown and available for review in the packet captures. The mobile app on the lower right depicts a the traffic application on the phone and shows that the UE is achieving 46Mbps of downlink traffic speeds. The messages observed in Figure 8 are bit-accurate and can be correlated with the proficiency training material provided in Figure 4. Scenario details like these provide unprecedented detail for analysis and understanding of cyber situational awareness as well as performance variation due to cyber effects. This is another example of taking the warfighter trainee from the classroom to the cyber-physical world. The Platform allows the trainee to repeat these exercises and select different NE configurations, switch to a different AOR, alter network architecture and ultimately re-play the exercise to observe and understand potential impacts.



No.	Time	Source	Destination	Protoc	Lengt	Info
3	13:45:34.389205768	10.10.129.2	10.10.129.21	S1AP/NA	202	InitialUEMessage, Attach request, PDN connectivity request
4	13:45:34.394409166	10.10.129.21	10.10.129.2	S1AP/NA	142	DownlinkNASTransport, Authentication request
5	13:45:34.536561277	10.10.129.2	10.10.129.21	S1AP/NA	146	UplinkNASTransport, Authentication response
6	13:45:34.539721161	10.10.129.21	10.10.129.2	S1AP/NA	122	DownlinkNASTransport, Security mode command
7	13:45:34.556541432	10.10.129.2	10.10.129.21	S1AP/NA	134	UplinkNASTransport, Security mode complete
8	13:45:34.574169641	10.10.129.21	10.10.129.2	S1AP/NA	114	DownlinkNASTransport, ESM information request
9	13:45:34.591429209	10.10.129.2	10.10.129.21	S1AP/NA	178	UplinkNASTransport, ESM information response
10	13:45:34.594063098	10.10.129.21	10.10.129.20	GTPv2	291	Create Session Request
11	13:45:34.594505651	10.10.129.20	10.10.129.21	GTPv2	161	Create Session Response
12	13:45:34.596667393	10.10.129.21	10.10.129.2	S1AP/NA	266	InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
13	13:45:34.634805492	10.10.129.2	10.10.129.21	S1AP/NA	142	UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
14	13:45:34.634899953	10.10.129.2	10.10.129.21	S1AP	102	InitialContextSetupResponse
16	13:45:34.634954721	10.10.129.2	10.10.129.21	S1AP	146	UECapabilityInfoIndication, UECapabilityInformation
17	13:45:34.637427270	10.10.129.21	10.10.129.20	GTPv2	93	Modify Bearer Request
18	13:45:34.637654369	10.10.129.20	10.10.129.21	GTPv2	87	Modify Bearer Response

Figure 8: Mission Rehearsal (Situational Awareness and Network Analysis)

After several exercises like these, trainees establish a familiarity with the network environment in various forms, having gone through several examples where they can observe signaling messages described in books and really see a UE that successfully attaches to the network. Trainees can now leverage their understanding of the network to choose where to deploy a kinetic effect. In our example, the trainee decides to experiment with taking out a data plane network element by dropping a kinetic bomb on it and observing the effects. The mission plan would be to observe what

happens if a kinetic bomb takes out a particular PGW residing on the terrain map. Prior to taking out the PGW, trainees will observe good traffic statistics for system users. The system is operating normally as shown in the following figure:

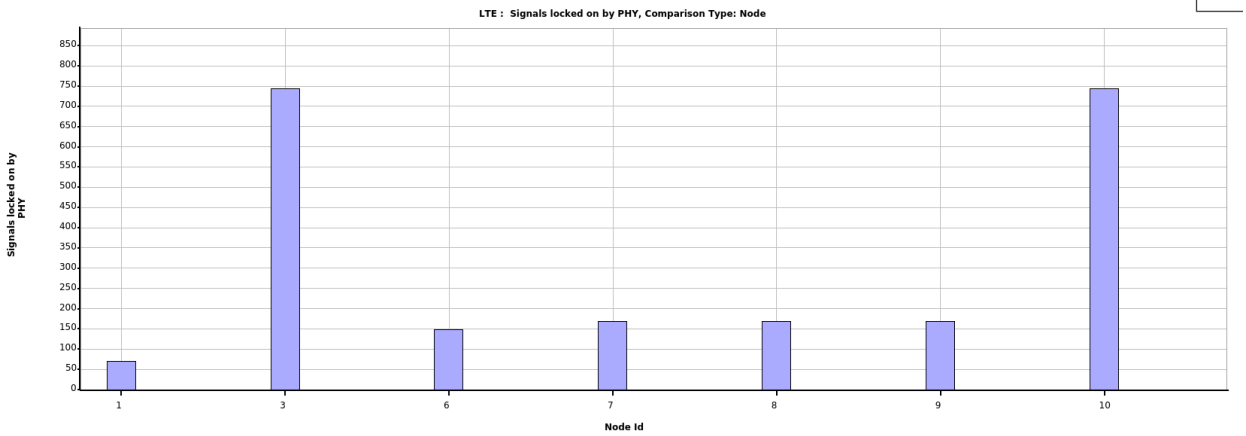


Figure 9: Mission Rehearsal (Statistics showing normal system operation)

Figure 9 shows that seven UEs are attached to the network and operating as normal. With this diagram, the trainee observes signal strength levels well above threshold. The trainee would likely first look at statistics like these from various points in the network to get a feel for the number of UEs attached and traffic statistics. The trainee can record this data to document normal system levels and statistics. Then the trainee can employ the chosen effect and observe results.

Upon deploying a theoretical kinetic effect to the PGW and effectively rendering it out of service, the trainee observes that the phones are now unable to transit/receive data plane messages. Confirmation of effects is shown in the following figure:

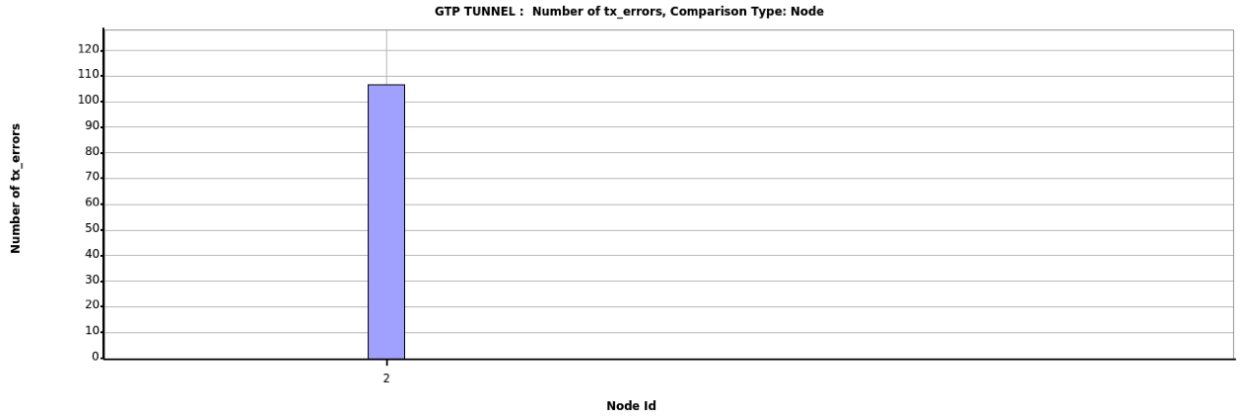


Figure 10: Mission Rehearsal (Confirmation of effects)

Once the effect is deployed, the trainee can observe that transmit (tx) errors begin to skyrocket on the data plane side. The control plane may still be allowing UEs to attach to the network, but the trainee can clearly observe that none of the UEs are receiving traffic. From here, the trainee can experiment with different network implementations or choose to fail different NEs to see how it effects the failure rates at different locations within the network.

These are just a few examples of how Modeling and Simulation can be utilized to better prepare the warfighter to operate in a cyber domain. Depending on objectives, the warfighter may choose to employ other services or capabilities to meet mission objectives. Regardless of approach, being able to test and evaluate each candidate course of action in a closed and repeatable environment with analysis of results is ideal. This enables the warfighter to understand effectiveness of candidate operations and define metrics for the percentage of users that would be expected to lose service.

CONCLUSIONS

Nations around the world desperately need an efficient, high-fidelity approach for understanding, evaluating, and ultimately protecting critical infrastructure from theoretical or actual kinetic and cyber threats. This paper described innovative, efficient, and high-fidelity approaches for proficiency training, cyber situational awareness, network analysis, and mission rehearsal. High-fidelity modeling and simulation platforms coupled with tangible real-world training scenarios will enable the U.S. warfighter and cyber community to maintain its technological advantage as mobile networks evolve to become a more important part of our everyday lives. With 5G networks, the increased diversity of signals from RF space provides resiliency to the operator and better protects the network from cyber-attack.

As described in the paper, simply taking out a cell tower will likely not affect communications for users in the 5G area like it would in a 4G environment. By creating a platform that can support high-fidelity, hardware in the loop (HIL) mix-and-match overlay of live components from numerous manufacturers with "generic" components that emulate UEs, Base Stations, and backhaul components, we can best train, understand, and assess networks, network attacks and failures on specific cellular network devices. Training the warfighter (across all of the services) using the approaches described in this paper will best enable them to understand the networks ever increasing complexity and how cyber effects may perturb the network.