Abstract—LTE (Long Term Evolution) is the latest cellular communications standard to provide advanced mobile services that go beyond traditional voice and short messaging traffic. Mobility networks are experiencing a drastic evolution with the advent of Machine to Machine (M2M) systems and the Internet of Things (IoT), which is expected to result in billions of connected devices in the near future. In parallel, the security threat landscape against communication networks has rapidly evolved over the last few years, with major Distributed Denial of Service (DDoS) attacks and the substantial spread of mobile malware. In this paper we introduce Firecycle, a new modeling and simulation platform for next-generation LTE mobility network security research. This standards compliant platform is suitable for large-scale security analysis of threats against a real LTE mobile network. It is designed with the ability to be distributed over the cloud, with an arbitrary number of virtual machines running different portions of the network, thus allowing simulation and testing of a full-scale LTE mobility network with millions of connected devices. Moreover, the mobile traffic generated by the platform is modeled from real data traffic observations from one of the major tier-1 operators in the US.

I. INTRODUCTION

The Long Term Evolution (LTE) is the latest standard for mobile wireless communications. Such technology is rapidly being deployed by cellular network operators to provide capacity for advanced multimedia services. Mobility networks have become an essential element of our day-to-day lives, providing popular seamless services such as electronic mail, location-based applications, video streaming, and the like.

Hundreds of millions of people are connected to the Internet via smart phones and tablets [1]. In addition, communication networks are rapidly evolving, with connectivity reaching beyond user devices. The advent of the Internet of Things (IoT) and Machine to Machine (M2M) systems is pushing the number of network-enabled objects interacting with each other over mobile networks. The number of connected devices is expected to be in the range of billions within a few years [2], with the majority of these devices connecting over next-generation LTE access networks. In fact, the number of connected devices is expected to already outnumber the world’s population this year [3].

Although LTE presents tremendous capacity enhancements, in general, previous cellular networks are known to be vulnerable to certain security threats [4]. At the same time, the recent security attacks against communication networks have drastically changed the security ecosystem. The massive Distributed Denial of Service (DDoS) attacks against major banking institutions [5], the attack against Spamhaus that resulted in worldwide Internet service deterioration [6], and the surge of mobile malware [7] are good examples of the importance of securing communication networks.

Security research has been growing over the last few years, resulting in the successful identification and mitigation of many threats. However, the great majority of the work has focused exclusively on GSM (Global System for Mobile Communications) and UMTS (Universal Mobile Telecommunications System). This is perhaps due to the open source availability of platforms such as OpenBTS [8]. To this point there has not been much security research focused on LTE networks.

In this paper we introduce Firecycle, a test bed for security research in LTE and potential future mobility networks. Firecycle is designed to provide the means to implement, test, and analyze the impact of security attacks against an LTE mobility network. Based on a modular and flexible architecture, the proposed model allows for rapid prototyping, testing, and comparing of new cellular security architectures. As a result of its versatility and the abundant statistical information elicited from simulations run on Firecycle, the test bed is also a valuable resource for designing strong security architectures for future next-generation mobility networks. Implemented on the network simulation software OPNET [9], Firecycle is designed in order to be scalable. The network under analysis can be arbitrarily divided into portions that are individually run on separate virtual machines (VMs) in the cloud. The VMs intercommunicate over IP, effectively simulating an arbitrarily large network over multiple machines. This architecture, based on OPNET’s System-in-the-Loop (SITL) [10], provides a platform for security research over a full-scale LTE network with millions of simulated mobile terminals.

The remainder of the paper is organized as follows. Section II introduces the LTE security background of this project and discusses related work. Section III describes Firecycle in detail, along with a discussion on its motivation. Section IV presents initial results on the scalability of the simulation platform and potential applications. Section V explains Firecycle’s limitations and future work. Finally, Section VI concludes the paper.
II. LTE security

Wireless cellular networks provide connectivity to billions of users, electronic devices, and critical applications. Devices connect through a heterogeneous set of access networks, which range from the early 2G GSM networks to the more recent 3G UMTS networks and their Code Division Multiple Access (CDMA)-based counterparts, such as CDMA2000. These mobility networks have evolved over the recent years, enhancing capacity and throughput, defining both the Evolved High Speed Packet Access (HSPA+) and the Evolution Data Optimized (Ev-DO) and its revisions. All modern mobile networks, however, are converging towards one universal technology that will run the next-generation networks: LTE and its evolution, LTE-Advanced.

In addition to being the main wireless access network for billions of users, LTE is also planned to be used in certain critical applications with stringent security requirements. For example, LTE is the communication technology for the next-generation emergency response systems planned by the US Department of Homeland Security: the Nationwide Interoperable Public Safety Broadband Network [11]. LTE is also considered as the underlying technology for advanced military tactical networks [12].

Concurrent to the capital security requirements of LTE networks, the cyber security landscape has substantially evolved over the last few years. In the age of massive DDoS attacks, mobile malware and fraud, and the advent of the Advanced Persistent Threat, the importance of enhancing the security of LTE networks against security attacks is clear [13].

A. Related work

Over recent years, several researchers have proposed potential vulnerabilities and attacks against mobility networks.

The authors of [14] proposed a potential way to saturate a cellular core network. Based on signaling generated to transition UEs between RRC (Radio Resource Control) states, an attacker could potentially overload the network by forcing UEs (User Equipment) to constantly switch states. The negative impact of such a signaling spike has already been experienced in the wild due to inadequate legitimate applications that induce frequent RRC connections from many UEs [15] [16]. A similar attack was discovered in [17], aiming to saturate the network resources assigned to the paging mechanism. Further signaling-based attacks against a cellular network were introduced in [18].

A widespread malware infection or a botnet of mobile devices is often considered as a potential platform to launch such attacks. Along these lines, the authors of [19] discussed the feasibility of creating and operating a botnet of infected smart phones. The impact of such a botnet launching an attack against the UMTS Home Location Register (HLR) was theoretically analyzed in [20].

Security research in mobility networks, including the aforementioned works, has been often with a purely theoretical approach. Moreover, the open source availability of GSM platforms, such as OpenBTS [8], results in most of the hands-on security work focusing on GSM networks. Presently, the amount of security research concentrated exclusively on LTE is very small. One exception is the interesting recent work presented in [21], analyzing potential signaling attacks against LTE performed by UEs within the same cell.

The majority of the attacks against mobility networks proposed in the literature have been mainly theoretical and mostly focused on legacy 2G and 3G networks. Firecycle provides the means to analyze these known legacy vulnerabilities in a realistic environment and determine whether they also affect next-generation LTE networks, as well as identify potential new vulnerabilities.

There are some open access platforms available for security research. For example, the DETER project [22] provides means for large-scale security studies of IP (Internet Protocol)-based networks. Similarly, the ORBIT test bed is an impressive vehicle for testing and experimentation of next-generation Wireless Local Area Networks (WLANs) with up to hundreds of nodes [23]. The authors of [24] introduced another network modeling platform to study the impact of M2M traffic on the LTE physical layer (PHY). Although Firecycle and the model proposed in [24] both analyze the impact of M2M on LTE mobility networks, Firecycle is concerned with the LTE network at large whereas the other focuses exclusively on the wireless interface of an LTE single cell network. [25] presents an open source LTE simulator called LTE-Sim, although this tool is much simpler and less flexible than Firecycle, as it emphasizes only the physical layer and lacks the ability to deploy custom traffic models that are important for analysis of security attacks on the network. These two models can therefore be seen as complementary to Firecycle.

Firecycle is, to the best of our knowledge, the first custom standards-based LTE security research test bed. It provides unique means for rapid implementation and testing of security attacks against an LTE network as well as rapid prototyping and testing of security mitigation and attack detection strategies. Moreover, similar to the DETER test bed, this platform supports very large-scale security studies.

III. Model

This section introduces the main features of Firecycle, focusing on its capabilities and ability to scale up simulations and the model itself over multiple VMs in the cloud. The motivations behind this test bed are discussed as well.

Firecycle’s name is inspired by a concerto for 2 pianos, 5 conductors, and orchestra entitled Firecycle Beta by the contemporary English composer Brian Ferneyhough. The piece is characterized by complex multi-layered rhythms, where the performers are divided into small groups that are each simultaneously playing at different tempi. Firecycle executes similarly as it is scaled over the cloud; each simulation is an interplay of events that are independently generated by disjoint subsets of the model.
A. Motivation

The recent trend of DDoS attacks against communication networks, which impacted large banking organizations [5] and the overall Domain Name Service (DNS) [6], illustrate the importance of strengthening the reliability of mobility networks against security attacks. In order to guarantee full availability of communication systems against DDoS threats, security research is necessary to come up with both detection techniques as well as attack mitigation strategies [13].

Although mobile devices engage in IP communications over LTE, the specific characteristics of mobility networks, especially at the Medium Access Control (MAC) and RRC layers, make the network behavior and reaction to security threats very unique. For example, it is well known that the RRC strategies implemented in mobile networks can be theoretically exploited in a large-scale DDoS [14]. The abundant signaling traffic generated when a UE transitions from a connected state to an idle state and vice versa could saturate certain nodes or links in the core network. However, there is no simple way to test such an attack and quantify its impact against a network with millions of users.

No security research lab is sufficiently large to test a security attack that involves an extensive number of infected smart phones. Furthermore, no simulation platform is scalable enough to run a simulation of a full-scale mobile network with tens of millions of smart phones, tablets, and M2M devices operating in parallel.

Moreover, even in small-scale simulations of an LTE network, traffic is modeled following simple arbitrary probabilistic models. One such example is the random waypoint model [26]. Well known research has proven that such models are far from accurate as opposed to traffic models derived from real network traffic traces [27], [28]. The traffic modeled in Firecycle is based on analysis of fully anonymized real traces from one of the major tier-1 operators in the US.

B. Implementation

Firecycle has been designed, implemented, and coded from scratch using OPNET Modeler [9] as the underlying platform and simulation engine. All the nodes and elements of the model are custom coded and assemble together to run as a network simulation on OPNET. Finally, an original set of libraries and definition files provide the means to run the realistic traffic models.

Firecycle is designed and built as a standards-compliant test bed, closely following the specifications of the 3GPP LTE standards. Figure 1 (a) shows Firecycle’s architecture. The E-UTRAN (Evolved Universal Terrestrial Radio Access Network) is build as a set of eNodeBs (LTE base stations) that handle radio communication between UEs and the EPC (Evolved Packet Core). Our model can deploy any number of eNodeBs and UEs as well as establish the LTE X2 interface between interconnected eNodeBs.

The EPC model contains the Mobility Management Entity (MME), the Serving Gateway (SGW), the Home Subscriber Service (HSS), and the Packet Data Network Gateway (PGW). These are the main nodes required to establish connectivity and manage traffic flows to and from UEs [29]. The primary functions of the MME are control-plane signaling, SGW selection, authentication, and bearer management. The SGW routes and forwards traffic in addition to initiating the paging procedure when traffic arrives for a UE that is in idle state. The PGW handles UE IP address allocation and packet filtering. Furthermore, the HSS is a database that contains user identification, subscriber information and authentication information, as well as Quality of Service (QoS) assignments. Note that we have designed Firecycle to allow multiple SGWs, MMEs, and PGWs in order to study the impact of distributing traffic and signaling load across a larger network.

In the current implementation, UEs communicate by means of IP-based services with one or multiple external IP servers. UEs can send or receive different types of traffic to or from them. These servers connect to the LTE EPC through an IP cloud, which mimics the timing artifacts that packets experience as they travel through a network. Packet drop rates and reordering of packets could be produced as well.

Firecycle implements several 3GPP standards-based signaling procedures that are relevant to UE connection and utilization of network resources. In order for a UE that is currently not attached (off connection state) to transmit and receive IP data traffic, it must go through the initial attach procedure to reach the RRC connected state. During this sequence of signaling messages, the UE associates with a particular eNodeB, and the EPC allocates a collection of bearers which are used for the duration of the UE’s session [30], [31].

When a UE is inactive for a given period of time, the E-UTRAN and EPC release its resources, and the device is subsequently brought to the idle state. If traffic arrives at the SGW for a UE that is in idle state, the SGW sends a data notification message to the MME in order to initiate the paging procedure, leveraging the knowledge of the set of base stations with which the UE last associated [32]. Once the UE has received a page message, it will transition to connected. A UE in connected state possesses the ability to send and receive messages or data. Since in LTE both messages and data are IP traffic, we have implemented all traffic as IP packets, although the size and frequency of these packets are dependent on the traffic type.

Although Firecycle models all the relevant signaling procedures at the E-UTRAN and EPC, the actual cryptographic operations behind the HSS operation are modeled only as signaling exchanges. In the current implementation, Firecycle is not able to study vulnerabilities in the cryptographic operations behind, for example, the EEA2 confidentiality algorithm and the EIA2 integrity algorithm. It is our plan to include these operations as part of our future work.

OPNET models communications as a chronological sequence of events. Actions in each node, for example sending and receiving messages, determine the progression of states in the system. Each node is depicted as a finite state machine, where the next state depends on the type of event currently
being executed. For instance, while the MME is waiting for packets to arrive, it remains in the *ready* state. If it receives an authentication signaling message from an eNodeB, the MME will move to a new state that handles processing of eNodeB authentication packets. Once processing is complete, the MME will return to the *ready* state.

Each network node in Firecycle is implemented as a computing machine similar to those in a real production network. For example, the MME is essentially a combination of proprietary software and hardware from a given vendor. As such, each node has a limited processing speed and memory. Therefore, if a node, for example the HSS, is overloaded with authentication requests, it may get saturated, blocking or substantially delaying its processing and response packets. Such limitations are modeled in Firecycle in order to accurately quantify the impact of DDoS attacks against a mobility network. Moreover, by appropriately configuring each node, one can model the specific capacity of nodes from different vendors.

### C. Statistics

A significant motivation for our model is to assess the impact of a large-scale security attack against LTE. To serve this purpose, Firecycle captures a variety of statistical information from each simulation. This data can be classified into various categories.

Signaling statistics collect diverse information on the load, frequency, and time occurrence of LTE signaling events. Some examples are the communication between an eNodeB, the MME, and the SGW to establish a bearer and move a UE from *idle* to *connected* mode. For example, we can compute the ratio of signaling to actual data messages per each communication flow or track when each individual UE switches between RRC states. Statistics of this category are crucial for gauging the impact of an attack and are related to the QoS experienced by the UE. Load, frequency, and time occurrence statistics are additionally collected for user traffic.

Quantitative statistics track the total number of events associated with a particular type. The number of RRC state transitions, counting the number of data packets received at the SGW, and the prevalence of UEs entering *idle* state are a few examples. Such statistics can be informative when comparing the impact of multiple traffic types on particular EPC elements. Node limits statistics deal with capacities of individual nodes, including CPU and RAM usage, throughput, number of bearers, and number of UEs being handled. Similarly, link limits examine link throughput and utilization.

### D. Scalability

No known LTE network model can be easily scaled to research the impact of a large-scale security attack involving hundreds of millions of UEs. However, with the number of connected devices expected to grow substantially within the next decade, it is crucial that a model be flexible enough to handle an arbitrarily large number of UEs.

OPNET’s System-in-the-Loop (SITL) enables multiple pieces of a model to run on separate machines and communicate with each other over IP. Nodes within a single simulation piece correspond with each other via OPNET-based packets, while nodes across simulation pieces running on different machines communicate via real IP packets that contain simulation packets as payload. To distribute Firecycle over multiple VMs, subsets of the model’s nodes can be arbitrarily assigned to distinct simulation portions. Once the pieces are each assigned a unique IP address, they can interface over an IP connection by means of SITL gateways. Figure 1 (b) shows a screenshot of Firecycle with the EPC running on a VM and three instances of the E-UTRAN, each running on a separate VM.

When a node in one simulation portion needs to send a message to a node running in a different portion, the message, in the form of a simulation packet, is copied into the payload field of a real IP packet that is addressed to the corresponding remote VM. Since the SITL node operates at the data link
layer, the IP packet is further encapsulated into an Ethernet packet with the destination MAC address set to the MAC address of the destination machine’s network adapter.

The task of copying and encapsulating simulation packets into real network packets is performed in Firecycle’s gateway node. Correspondingly, once an Ethernet packet arrives at its destination simulation portion, the gateway node extracts the encapsulated simulation packet and injects it into the OPNET-based local simulation. Thus, the receiving node in the simulation is unaware of the existence of the SITL interfaces and is able to process each packet as if the entire model were running on a single machine.

E. Traffic

We analyzed anonymized IP and SMS communications in a US tier-1 cellular network to build traffic models of smart phones, tablets, and M2M devices. No personally identifiable information was gathered or used in conducting this analysis. We collected anonymized Call Detail Records (CDRs) that log communications handled by cell towers located in the greater New York City metropolitan area within one day in August 2013, examining the following fields: (i) timestamp of communication (send/receipt time of SMS or IP session connection time), (ii) fully anonymized transaction identifiers (integers uniquely determining originating and terminating numbers or addresses for SMS or IP flows), (iii) the number of bytes in uplink or downlink IP flows, and (iv) the first 8 digits of International Mobile Equipment Identity (IMEI).

The first segment of IMEI, Type Allocation Code (TAC), discloses the manufacturer and model of the wireless device and categorizes it as a smart phone, tablet, or M2M subcategory (medical, detention, smart grid, eBook, etc.). Timestamps were used to compute lengths of intervals between each pair of consecutive SMSs or IP data flows. We estimated distributions of the traffic parameters for each category and derived custom probability distributions. Based on the identifier fields, we calculated the total number of unique devices of a particular type communicating in a given area. For each device category, we modeled the total number of messages or traffic flows during the period of analysis as well as estimated distributions of the uplink and downlink flow sizes in bytes.

IV. RESULTS AND APPLICATIONS

Firecycle is designed to provide a platform to both analyze the impact of security attacks against LTE networks and test potential mitigation techniques. For example, from a security point of view, it is particularly important to understand the impact of signaling load on the HSS, since any impairment to the HSS could result in failure of the entire network. A similar approach could be considered for the MME.

Figure 2 plots two examples of the signaling link utilization between two pairs of essential EPC nodes, MME-HSS and MME-SGW, for different numbers of UEs. During the simulation the UEs complete an attach procedure and then exchange traffic with a server. Figure 2 (a) shows the results with traffic modeled from one of the M2M subcategories. In Figure 2 (b) the UEs and server generate arbitrary intermittent traffic in order to induce frequent RRC state transitions. Note that this type of traffic behavior, forcing constant RRC state transitions, has been proposed as a potential way to launch a signaling-based attack against the EPC. This is indeed one of the security test cases being studied with Firecycle.

Note that the capacity of the links has been set arbitrarily for this example in order to highlight the results. In a real network, the bandwidth of these links would be much higher and thus the utilization lower. Note also that the number of UEs is scaled exponentially. One of the goals of our future work is to test Firecycle with an arbitrarily large number of UEs that increases exponentially over the entire network. The results in Figure 2 are intended to exemplify the type of studies that can be performed with Firecycle.

In Figure 2 (a) one can observe the spike in signaling traffic for the attach procedure that all UEs perform at the beginning of the simulation. This procedure involves authentication and attach messages that are exchanged with the HSS. However, once the UEs have successfully attached with the network, the signaling traffic at the HSS dissipates. Based on this observation, Firecycle is being used to test, for example, the impact of a malware infection that forces a large percentage of smart phones to attach at the very same time.

Figure 2 (b) illustrates the signaling traffic load between the MME and the SGW resulting from UE attachment and shifting of RRC states. It can be seen that the messaging between the MME and the SGW to set up and release bearers as UEs transition between idle and connected states creates a substantial and sustained amount of load in the EPC. This insight is being used to investigate the effects of a very large number of UEs constantly transitioning between RRC states.

A. Scalability results

Table I summarizes the main results of the scalability experiments, where we ran a fixed scenario in four different configurations. The scenario consists of 625 mobile terminals communicating over the LTE network, with a traffic profile modeling the behavior of M2M remote medical appliances. In each run we simulated 30 minutes of traffic, configuring a full constant statistics collection to maximize the CPU load of the simulation. In the first configuration, Basic, the entire network is simulated in a single VM, while in Distributed (2 VMs) the E-UTRAN is simulated on a VM and the EPC runs on a second VM. Similarly, in Distributed (3 VMs), the EPC is run over 1 VM and the E-UTRAN is split over 2 VMs. Finally, in Distributed (4 VMs), the EPC runs over 1 VM and the E-UTRAN is distributed over 3 VMs.

As shown in the table, the simulation speed increases substantially, from an average of 6,950 events per second in the basic run on a single VM to a total average of 29,294 events per second when scaling the model over 2 VMs, 182,759 events per second with 3 VMs, and 206,785 events per second with 4 VMs. This represents simulation speed increase of over 2,975%, which results in a much shorter simulation time. The entire simulation finishes in 30 minutes when using 4
VMs as opposed to over 24 hours when using one single VM. Although there is a memory overhead incurred when initially scaling the simulation over multiple machines due to the necessary extra nodes and copying of packets, this cost is clearly compensated for as more VMs are added. As indicated in Table I, distributing the simulation over 4 VMs requires nearly half the memory than is needed when using a single VM.

It is important to note that the substantial performance improvement achieved by distributing a simulation is due to multiple factors. One of the key elements is a better memory utilization. The OPNET Modeler simulation engine stores all the statistics (i.e. “results”) in memory as the simulation runs. Therefore, in the case of a very large scenario that gathers a large number of statistics, the memory limits of a single machine can potentially slow down a simulation substantially. Although this negative effect could be alleviated by collecting fewer statistics and having a shorter simulation time, distributing the test bed over the cloud provides clear benefits while still collecting all the available results during a long simulation.

These results give an indication of the strong scalability property of Firecycle. Given enough cloud resources, this security test bed can perform rapid and efficient simulations of attacks against realistically large LTE networks.

V. LIMITATIONS AND FUTURE WORK

Despite the great potential for security research, Firecycle cannot be applied to every type of LTE security analysis. The wireless interface at the physical layer of an LTE mobile network is based on an Orthogonal Frequency-Division Multiple Access (OFDMA) method. The characteristics of this wireless access method are not implemented, modeling instead a simplified wireless link. While capacity, throughput, and latency are equivalent to a real LTE access network, the results obtained could substantially differ from a real network in some specific cases. For example, Firecycle will not accurately model a real network in the case of an unrealistically large number of active UEs per eNodeB. In this extreme case, the specific details of a full OFDMA system would not be accurately modeled. Firecycle has not been designed to test local wireless resource saturation or radio jamming attacks. Instead, it is designed to investigate the wider scope impact of widespread malware infections, botnets of mobile terminals, and large-scale signaling attacks against the EPC. However, a standards-based implementation of the PHY layer is part of our future work.

In its current form, Firecycle does not implement certain higher layer protocols, such as IMS (IP Multimedia Subsystem) and SIP (Session Initiation Protocol). However, the modularity and scalability of the model highly simplifies the implementation of these and other applications.

Firecycle is currently being used to assess the impact and
scalability of the IoT and M2M on LTE networks, with focus on the signaling and traffic load in the EPC. However, we are also utilizing it to quantify the impact of large-scale attacks against LTE. In this context, as part of the future work, Firecycle will leverage the features of SITL to be integrated with the hardware in our LTE security lab. Firecycle will also be tested with traffic generated by UE-eNodeB emulators.

As part of our ongoing work, Firecycle has been recently enhanced with new M2M and smart phone statistical traffic models and the implementation of the signaling procedures related to handover and mobility.

VI. CONCLUSIONS

This paper introduces Firecycle, a scalable test bed for LTE security research. This platform is designed and implemented to test and realistically quantify the impact of large-scale security attacks against LTE. Firecycle provides the means for rapid prototyping and testing of new attack mitigation strategies and alternative cellular network architectures for enhanced security. Offering the ability to compare the impact of attacks on multiple architectures, Firecycle can aid in the design of robust future next-generation mobility networks.

Firecycle realistically models the main nodes of an LTE mobility network. Special emphasis is given to Layer 2 protocols and signaling traffic. User traffic is accurately modeled based on real LTE network traffic traces from one of the main tier-1 operators in the US.

Firecycle is designed to be scaled over the cloud. The network under analysis can be divided into a number of portions, with each one running on a separate VM in the cloud. VMs intercommunicate over IP, enabling an arbitrarily large network that virtually behaves as though it were running over a single machine. Based on this scalability property, we are using this test bed to analyze and quantify large-scale security attacks against an LTE network originated from a botnet of UEs. We are also leveraging Firecycle to study the scalability of the IoT and M2M systems over LTE mobility networks and to prototype security mitigations and attack detection schemes, which are analyzed and compared against each other to improve the security of the design. The results of these independent studies will be presented in the near future.

REFERENCES