BOOK CHAPTER - PRE-PRINT AUTHOR VERSION

Security and impact of the IoT on LTE mobile networks

Book: Security and Privacy in the Internet of Things (IoT): Models, Algorithms, and Implementations

Taylor & Francis LLC, CRC Press

(To be published - Winter 2015)

Roger Piqueras Jover

Principal Member of Technical Staff

AT&T Security Research Center

New York NY

July 20, 2015

Chapter 1

Security and impact of the IoT on mobile networks

The ongoing evolution of wireless cellular networks is creating a new ecosystem with pervasive presence of a great variety of network-enabled objects which, based on unique addressing schemes, are able to interact with each other. Cellular connectivity is reaching beyond smartphones and tablets, providing access to data networks for connected home appliances, machinery and vehicles. The rapid evolution of mobile networking technologies and the transition towards IPv6 might drive this trend to an ecosystem where every single consumer item could be reachable through the cellular network. This convergence of the Internet and cellular mobility networks is breeding new Machine-to-Machine (M2M) communication systems, which are the enabling platform for the Internet of Things (IoT) [1].

Cellular-based IoT applications are experiencing a drastic growth backed up by the large investments from network operators [2]. Current studies forecast the cellular IoT to be 1000 times more profitable than mobile data and as lucrative for operators as the Short Messaging Service (SMS) [3]. This is an attractive new market for cellular operators, which are currently dealing with a heavily competitive market and declining revenues. Consequently, IoT applications are among the common denominator of some of the largest investments in mo-

bile and cellular technology innovation. Cellular operators are seeking valuable partnerships in markets such as connected cars [4] and remote health-care systems [5]. Indeed, forecasts preview the health industry as one of the main drivers of the IoT market over the next few years [6].

Consensus exists in the industry that great growth in mobile cellular connectivity from M2M and embedded mobile applications will be experienced. More than 50 billion non-personal data-only mobile devices are expected to join existing mobile networks, supporting this plethora of emerging applications [7]. Consequently, in order to provide ubiquitous broadband connectivity to the IoT, *massive device connectivity* (billions of connected devices) is one of the main goals for the design and planning of future 5G mobile systems [8].

The fourth generation of mobile networks, the Long Term Evolution (LTE), has been designed for greatly enhanced capacity in order to provide support to a large number of connected devices. As such, LTE introduces significant improvements at the Radio Access Network (RAN) and a more flexible IP-only (Internet Protocol) architecture at the Evolved Packet Core (EPC). Although a substantial percentage of current M2M systems operate over legacy second and third generation (2G and 3G) mobile networks, LTE is expected to be the main driver of the emergence of the IoT on cellular networks [9].

This massive deployment of IoT applications, and their underlying M2M devices, on mobile networks present a great challenge for network operators. The traffic characteristics of many IoT applications, substantially different than user traffic from smartphones and tablets, is known to result in network resource utilization inefficiencies [10]. There is an increasing concern about the potential impact the IoT could have on LTE mobility networks, specifically regarding the surge in both traffic and control plane load [11]. Moreover, known security vulnerabilities in legacy mobile networks have been exploited to eavesdrop communications between M2M embedded devices and reverse engineer IoT systems.

Fueled by the great challenges of securely deploying and scaling IoT systems over cellular networks, both the research and the standardization community are leading several efforts to enhance the security of the IoT in the context of mobile cellular networks.

1.1 Security threats against IoT embedded devices and systems

Security and privacy are two of the main challenges of the IoT, particularly due to the emerging threats embedded devices face due to their unique limitations in terms of connectivity, computational power and energy budget. Providing secure communications among M2M devices over cellular networks is an emerging research area, with different approaches being adopted. On one hand, efforts aim to secure the device itself [12] and, on the other hand, network/provider-based architectures that benefit from the existing authentication methods of a cellular telecom operator are being proposed [13]. In parallel, privacy is increasingly becoming one of the major concerns in these kinds of systems, specially given the surge of applications handling critical information. This is a particularly crucial area in certain IoT system categories, such as the case of network-enabled medical environments [14].

Despite the increasing focus on securing M2M communications, efforts still have to be made to design more effective security architectures and transfer them into actual system deployments. An alarming lack of basic security features in certain applications have allowed researchers to discover new vulnerabilities and attack vectors against IoT systems, such as allowing remote ignition of a car's engine [15] and getting root access on a home automation connectivity hub [16]. Other basic security flaws have been highlighted by the media, such as different types of connected devices being remotely accessible over the Internet with default or no access credentials [17].

IoT service providers often rely on the implicit wireless network encryption and authentication to protect the traffic from eavesdropping and Man in the Middle (MitM) attacks. Most deployments leverage legacy cellular 2G links, generally considered to be insecure and with outdated encryption schemes. This allows decryption and eavesdropping communications over the air [18]. For example, a recent study identified a popular geo-location platform that transmitted application information as plain-text in the body of text messages. This allowed security researchers to reverse engineer the entire M2M application [19].

Cellular M2M systems should be designed with the assumption that any attacker can eavesdrop the traffic over the air, so extra layers of encryption should be encouraged. Nev-

ertheless, certain low-power embedded devices with limited computing resources might not be capable of strong extra encryption. Overall, new M2M system implementations should be designed to leverage LTE mobile networks, with a state-of-the-art encryption and authentication scheme, preserving traffic privacy and security. Moreover, although studies have shown the feasibility of launching attacks and gaining control over network-enabled devices by means of deploying rogue base stations [20], this would not be possible over a mutually-authenticated LTE access link.

1.2 IoT security impacts against mobile networks

Aside from the security and privacy of IoT connected devices, the deployment of M2M systems on wireless mobile networks also has important security implications on the network itself. Resource allocation to millions of embedded devices is a big challenge for cellular network providers highly utilized mobile infrastructures [7]. Beyond the network operation challenge under such a large load of IoT traffic, M2M traffic is considered as one of the main factors within the overall LTE network security framework [21]. Industry and standardization forums defining the main security threats and requirements for mobile network security are indeed highlighting the IoT and its potential impact.

The traffic characteristics of many IoT applications, substantially different than user traffic generated by smartphones and tablets, are known to be a potential source for network resource utilization inefficiencies [10]. As a result, there is concern regarding the impact that M2M systems could have on the regular operation of LTE networks, which, if not architected properly, may be overwhelmed by the surge in both traffic and signaling load [11]. Given the number of threat vectors against embedded devices, there is also great interest in the potential impact of botnets of compromised devices and malicious signaling storms [22].

As mobile networks evolve and transition towards 5G, the capacity and throughput of the wireless interface is scaled up to tackle the goals of *massive device connectivity* and *1000 times more capacity*. To do so, researchers are already prototyping advanced systems at high milliliter wave frequencies and implementing massive MIMO systems. However, a common

topic of discussion at a major 5G industry forum was how it is not all about speed, but also about scalability [23]. The scalability of billions of embedded devices joining existing LTE and future 5G networks is one of the major availability challenges within the field of IoT security.

1.2.1 LTE network operation

LTE mobile networks were designed to provide IP connectivity between mobile devices and the Internet based on the architecture depicted in Figure 1.1. LTE mobile networks are divided into two separate sections: the Radio Access Network (RAN) and the core network, referred to as the Evolved Packet Core (EPC).

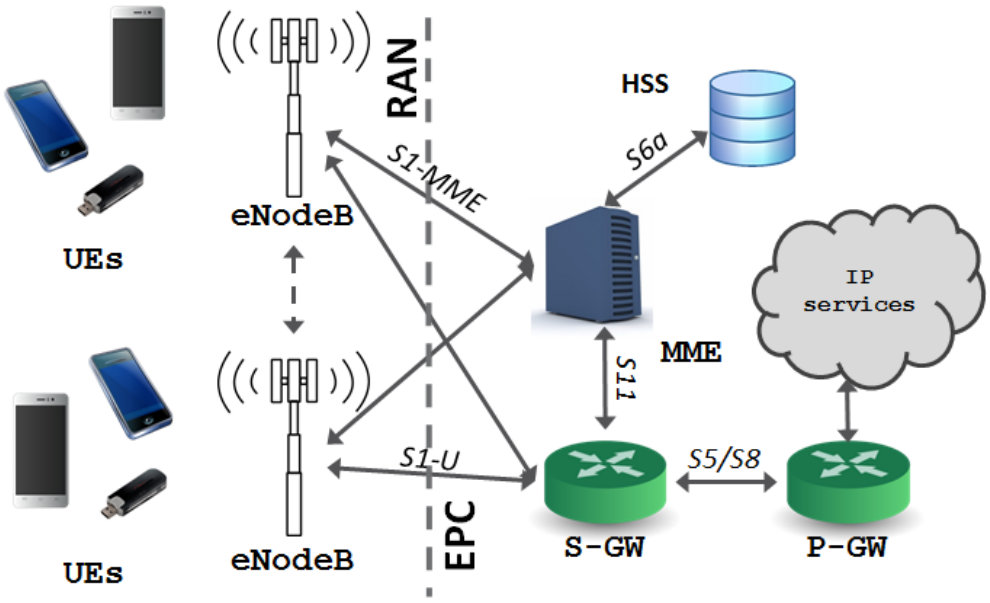


Figure 1.1: LTE network architecture

A number of User Equipment (UE) devices, or mobile terminals, and the eNodeBs, or LTE base stations, compose the RAN. This wireless access portion of an LTE network is in control of assigning radio resources to mobile terminals, managing their radio resource utilization, performing access control, and, in the case of the implementation of the X2 interface between eNodeBs, even manage mobility and handoffs independently of the EPC.

The EPC is the core in charge of establishing and managing the point-to-point IP connectivity between UEs and the Internet. Moreover, certain MAC (Medium Access Control) operations at the RAN are triggered or controlled by the core network. The EPC is composed of the following network nodes. The Serving Gateway (SGW) and the PDN Gateway (PGW) are the routing points that anchor a point-to-point connection, known as bearer, between a UE and the Internet. The Mobility Management Entity (MME) manages the control plane bearer logistics, mobility, and other network functions. In order to authenticate end users, the MME communicates with the Home Subscriber Server (HSS), which stores the authentication parameters and secret keys of all the UEs.

In order to operate the network and provide connectivity, LTE networks execute a series of signaling processes, known as Non Access Stratum (NAS) functions [24]. Such functions are coordinated and triggered by means of non-user data messages among the LTE network nodes, known as the *control plane signaling* traffic.

Upon being switched on, a series of steps and algorithms are executed in order to reach the connected state. At this stage, an IP default bearer is set up between the UE and the PGW and an IP address is assigned to the UE. The device executes the Cell Search procedure in order to acquire both time and frequency synchronization and, by means of the Random Access procedure, radio resources are assigned to the UE setting up a Radio Resource Control (RRC) connection between the device and the eNodeB. The NAS identity and authentication procedures are then executed between the UE and the MME, which in turn communicates with the HSS. At this point, the data traffic bearers through the SGW and PGW are set up, and the UE's RRC connection is reconfigured according to the type of IP service and Quality of Service (QoS) requested by the UE.

This entire NAS attach procedure is illustrated in Figure 1.2, which gives a clear visual intuition of the large number of messages exchanged among EPC elements in order to connect a mobile device [25]. Note that the Random Access procedure, the RRC connection establishment, and the NAS authentication and identity procedures involve a substantial number of messages not shown in the figure for simplicity.

Although all devices are assigned radio resources to communicate, there are not enough

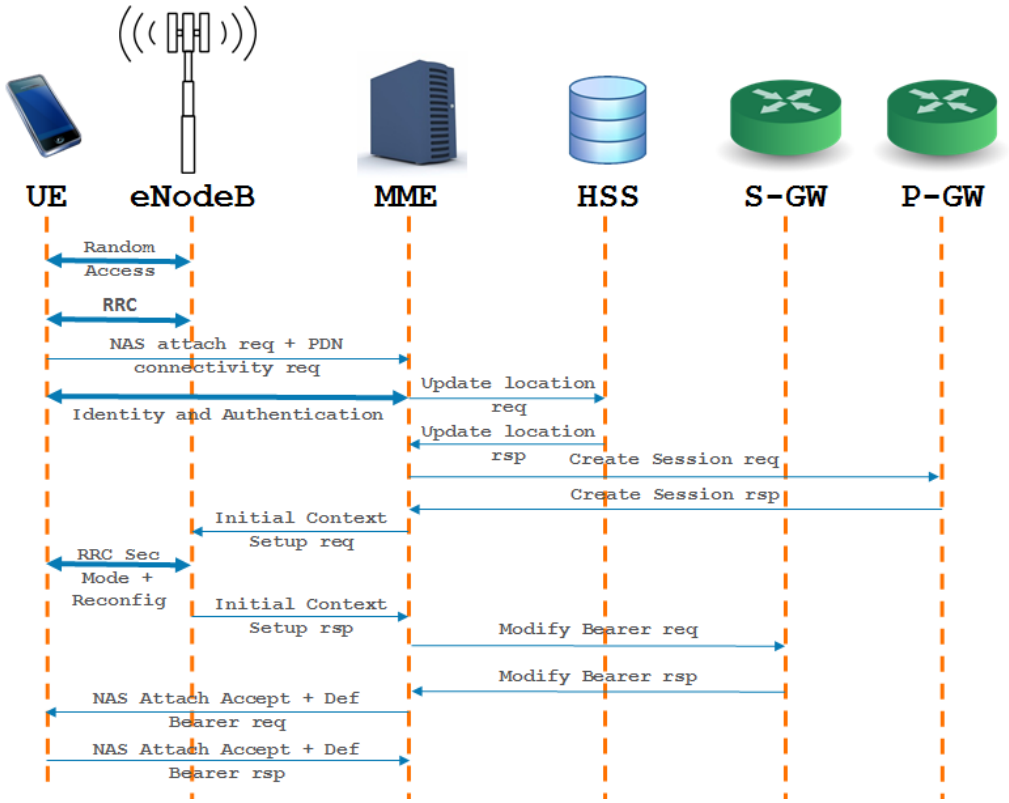


Figure 1.2: NAS Attach Signaling Procedure

resources for a simultaneous connection from/to all the UEs. As a result, in order to efficiently assign and manage the spectrum, strict resource management and re-utilization policies are implemented. Whenever a UE has been observed as idle by the eNodeB for more than a few seconds (often between 10 and 15 seconds), the RRC connection for this UE is released and its associated radio resources freed to be reused and assigned to another device, moving the UE to an idle state [26]. Although just one message from the eNodeB to the UE is sufficient to transition it down to an idle RRC state, this procedure still involves a series of messages among the EPC nodes in order to release the dedicated bearer. In parallel, a UE that is in idle state but needs to either transmit or receive data must be transitioned back to a connected state. To do so, a similar procedure to the NAS attach is executed. The main differences are that certain authentication and bearer operations are not required. For example, a UE transitioning from idle to connected state is not required to have a new IP assigned. Note that each time a UE transitions from idle to connected, the procedure must always start with a Random Access and an RRC connection.

The functionality of a mobile network involves further signaling procedures not listed here, such as paging and handoffs. The aforementioned network functionalities are described because they involve NAS signaling procedures that have been discussed in standardization bodies as a potential trigger for signaling storms in LTE mobile networks.

1.2.2 Control plane signaling storms

The spreading of IoT applications over mobile networks brings security implications to the LTE packet core. The operation of mobile networks must be considered before designing wireless embedded devices that leverage cellular connectivity to prevent network utilization inefficiencies and, potentially, larger network availability threats. As has been described, each transaction or traffic flow between the IoT devices and other mobile devices or the Internet results in control plane signaling at the EPC. Unnecessary connection establishment and release signaling could potentially overburden the core network and reduce the Quality of Service (QoS) of other devices [27].

The concept of mobile core overloading due to control plane signaling was introduced in [28], which described a theoretical signaling overload threat against cellular networks. A low-volume attack, consisting of small data packets addressed to a large number of mobile devices, would theoretically induce a large number of RRC state transitions and, theoretically, overload the packet core of a mobile network. In this context, certain categories of M2M devices are characterized by small and frequent communication bursts [10]. This traffic pattern differs from the typical smartphone or tablet usage patterns that LTE was designed to support. Such frequent traffic bursts could cause a large amount of signaling in the network as devices transition between idle and connected states.

This negative impact of control plane overloads has already been observed in the wild over the last couple of years in a series of signaling storms summarized in Table 1.2.2.

All the aforementioned signaling storm instances were caused by misbehaving mobile applications. However, security researchers argue that a signaling storm could potentially be triggered from within the network by means of a malicious botnet of compromised M2M

Cause	Event	Reference
Chatty app	IM app checking for new messages too frequently caused outage at US carrier	[29]
Signaling spike	Outage for 3 million users at the 6th largest operator in the world	[30]
Smartphone native apps	Native apps from one of the main mobile OSs causing signaling overloads to Japanese operator	[31]
Chatty apps	Operators at Open Mobile Summit discuss actions to mitigate signaling spikes from chatty apps	[32]
Adds in popular app	Signaling spikes caused by ads displayed in a popular mobile game	[33]
LTE-connected tablet	Connectivity from popular tablet increases control plane signaling substantially	[34]
Mobile cloud service	Frequent reconnect attempts to a cloud service under outage resulted in signaling spike	[35]

Table 1.1: Sample of known signaling overload events

devices [36]. The authors of [37] discussed feasible techniques and platforms to build and operate such a botnet, including potential command and control channels.

Additionally, certain M2M devices send or receive traffic at predefined time periods. For example, security cameras reporting a picture every few minutes or temperature sensors reporting a reading periodically. A large number of devices acting in this fashion could potentially generate peaks in both signaling and data traffic that could impact the core network. A similar situation could arise where an external event triggers a large number of devices to report or communicate, resulting in all the devices transitioning to an RRC connected state simultaneously. This is a specific use case of control plane signaling overload being discussed by standardization bodies [27].

In addition to M2M-related signaling overloads and network congestion, over the last few years, security researchers have theoretically proposed malicious ways to overload and congest LTE mobile networks. This congestion can occur in two different ways. Radio Access Network (RAN) congestion is the result of many simultaneous M2M connection requests, modifications, and releases to the same eNodeB [38]. Congestion in the core network can affect the Mobility Management Entity (MME), Serving Gateway (SGW), and Packet Data Gateway (PGW) when a large group of M2M devices attaches to different cells, transition

between Radio Resource Control (RRC) states, and move to different Tracking Areas [28]. Researchers have also theoreticized the potential impact of a signaling overload against the Home Subscriber Server (HSS) node in legacy 2G and 3G networks, known as Home Location Registry (HLR) [39].

1.2.3 Industry and security standardization work around M2M communications

Standardization bodies are actively working in proposing new security architectures to secure mobile M2M systems and the IoT. Certain industry forums are particularly engaged in proposing methods to alleviate potential signaling overloads and other security threats that could arise from the surge of IoT cellular systems.

The 3rd Generation Partnership Project (3GPP) is actively involved in defining a framework to mitigate control plane signaling spikes in cellular M2M systems [27], known as Machine Type Communications (MTC) in the context of 3GPP. This effort focuses on a series of threat scenarios that range from a sudden flood of attach signaling load after a node failure to a flood of mobile terminated events.

The major threat scenarios and proposed solutions proposed by this 3GPP task force are summarized in Table 1.2.3. Most of the solutions proposed by this effort provide the HSS with means to filter and, potentially, block its incoming signaling load. For example, a new feature is defined such that the HSS can notify the MME in the event of a spike in traffic. The MME, in turn, can then reject attach attempts from mobile devices without requiring a prior handshake with the HSS. Moreover, optimization on various HSS operations is proposed.

Beyond security architectures for the cellular IoT, 3GPP is also actively involved in proposing enhancements for MTC traffic over cellular networks [40]. Finally, there is also ongoing discussions at 3GPP in areas that, though not directly related to IoT security, would make a big impact. For example, new enhancements to reduce the amount of control plane signaling load during RRC state transitions are proposed [41].

The oneM2M organization, closely related to the European Telecommunications Stan-

Threat scenario	**Proposed solutions**
Overlaid RATs and failure of RAN node	Optimization of periodic TAU signalling
Flood of registrations	NAS reject solution
Flood of RRC resource allocation	HLR/HSS overload notification
Flood of Location Information reporting	Subscription data download optimization

Table 1.2: Main threat scenarios and solutions proposed by 3GPP to mitigate control plane signaling overloads at the HSS

dards Institute (ETSI), also has active projects defining the security architecture for IoT cellular deployments in the framework of the oneM2M Release 1 specifications [42]. This project is focused at providing security at the application layer of IoT services provided over mobile networks. Some of the threat scenarios under analysis range from the deletion of service encryption keys stored on the memory of embedded devices to handling malicious or corrupted software in the M2M core service provider network.

A series of recommendations are issued to ensure the confidentiality and availability of cellular M2M systems. These recommendations, which had already been defined in the previous releases of these specifications in [43], ensure that strong encryption is applied at the application layer, with encryption keys are stored in secure compartments. Note that, given the privacy threats of legacy 2G cellular links, it is not a good practice to rely solely on the wireless link encryption to secure M2M traffic.

This generalized interest in mitigating potential control plane traffic spikes in mobile networks is motivating certain industry players to develop appliances for mobile network infrastructure. These security solutions are designed as a control plane firewall, which sits between the RAN and the MME, and monitors for signaling spikes, mitigating the impact on the mobile core [44]. Mobile infrastructure manufacturers are also increasing their efforts to supply new tools to assist the packet core in optimizing the control plane, minimizing the risk for overloads [45].

1.2.4 IoT security research

Extensive research is aiming to design new network mechanisms to efficiently handle the surge of cellular traffic originated from the IoT. In [46], new congestion control techniques for M2M traffic over LTE are proposed. Other techniques are suggested in [47]. The authors of [48] introduce new adaptive radio resource management to efficiently handle M2M traffic, and [49] proposes enhancements to the Random Access Channel (RACH) of LTE systems to handle large numbers of embedded wireless devices.

1.3 Scalability of large deployments of cellular IoT systems

There is increasing interest among the telecommunications industry in understanding and, ideally, forecasting the scalability dynamics of IoT growth on LTE networks. Given the scale and device population expected, mobile network operators are expecting a large increase in both data and control plane traffic, to which network resources must adapt.

This necessity drives a substantial increase of research work in this area. For example, the authors of [10] introduced the first detailed study of the traffic characteristics of emergent M2M applications. The authors highlight radio resource and network resource inefficiencies of these communication systems as a challenge for mobile infrastructures. Other research projects have analyzed the characteristics of IoT traffic over LTE mobile networks [50], reaching similar conclusions: certain M2M applications send periodic small bursts of traffic which induce frequent RRC state transitions and, hence, are not efficient in terms of network resource utilization.

In order to be able to forecast and understand the scalability of the IoT over mobile networks, accurate modeling of the interaction of M2M systems with the cellular network is critical. The main goal of such modeling is to understand the non-linearity of control plane signaling traffic as it scales with the number of connected devices. The heterogeneous traffic patterns from different M2M device categories result in a great diversity of signaling traffic load statistics. Certain device types, reporting measurements periodically, generate very low

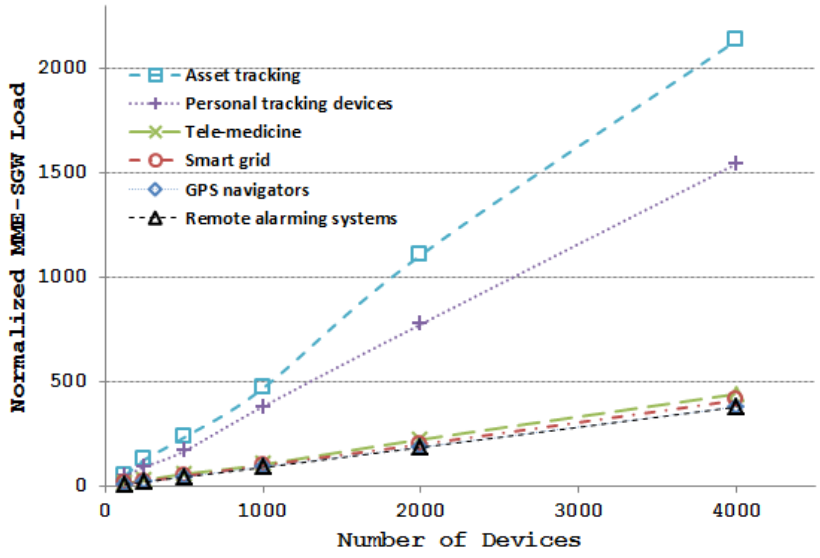
data loads (i.e. one 100kb measurement per hour), but induce a large number of RRC state transitions and, thus, control plane signaling load. In parallel, devices sending a large daily summary of readings at the end of the day (i.e. 100Mb) inject 1000 times more data traffic but have a marginal impact in terms of signaling load.

The study of the scalability of the IoT on LTE mobile networks requires a large-scale analysis. Lab testbeds are not sufficient to gauge the actual effects and implications of security threats involving the IoT. And, more importantly, lab-based research does not provide means for rapid prototyping and test of M2M security technologies at scale. The potential risk of signaling overload as well as mobile botnets of compromised embedded devices require a security analysis only possible on a simulation testbed.

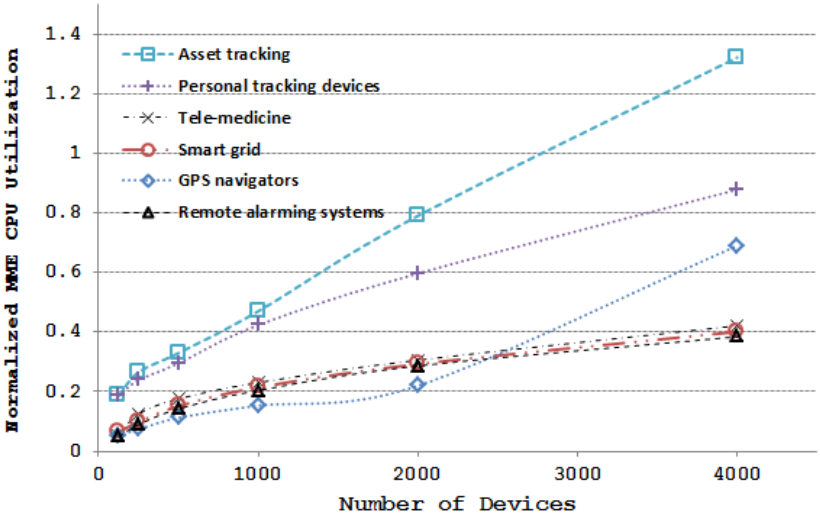
For example, a fully LTE standards-compliant security research testbed can be used [51]. The testbed is designed and implemented to be fully standards-compliant and can be scaled up over multiple virtual machines in order to simulate arbitrarily large scenarios. Moreover, the mobile devices simulated by this testbed run statistical traffic models derived from actual LTE mobile network traces, fully anonymized, from a tier-1 operator in the United States. Therefore, it can generate highly realistic results for smartphone traffic as well as several IoT device categories, such as smart grid, asset tracking, LTE-connected automobiles, telemedicine, remote alarming systems, security cameras, etc.

This testbed is leveraged to provide some insights on the scalability of IoT devices on mobile networks [52]. The experiments consist on deploying a simulated generic LTE network containing an instance of the EPC (MME, SGW, PGW, and HSS). IP communications occur between UEs and an external Internet server. The capacity of this server is assumed to be infinite as such to not interfere with the scalability impact at the EPC. A number of IoT devices, from different M2M categories (tele-medicine, asset tracking, smart grid, etc) are deployed on the network, with this device population being scaled up. As this occurs, multiple load metrics at the EPC are collected.

A generic experiment is summarized in Figures 1.3 (a) and (b), examining MME-SGW link load and MME CPU utilization in order to provide insights on the signaling impact of scaling M2M devices. It is intuitive that the M2M categories with the highest control



(a)



(b)

Figure 1.3: M2M scalability signaling impact: (a) normalized MME-SGW load and (b) normalized MME CPU utilization

plane signaling load impact (asset tracking and personal tracking devices in the case of the experiment in Figure 1.3) also result in the largest increase in MME CPU utilization. The load results in the figure are normalized.

The two device categories with the highest signaling load generate roughly the same load at the MME-SGW link for 125 devices. However, the load increases much more rapidly for asset tracking devices, with 2000 of these devices devices inducing 42.6% higher signaling

load than the same number of personal tracking devices. A similar trend can be observed with the MME CPU utilization. 125 personal tracking devices and 125 asset tracking devices induce roughly the same MME CPU utilization. However, 2000 asset tracking devices incur 32.5% higher load than the same number of personal tracking devices and, in the case of 4000 devices, 50.5% higher.

These results present important insights on the scalability dynamics of the IoT on LTE mobile networks. As expected, the control plane signaling load spikes as the number of connected devices increases. This increase is linear, which indicates that a, for example, exponential increase in load should not be expected. However, the largely heterogeneous scalability characteristics for different IoT categories present a challenge for network operators. This is due to the fact that the connectivity and resource utilization must be optimized for very diverse traffic dynamics, as opposed to current mobile networks mainly optimized for smartphone traffic.

The challenging of deploying and scaling up IoT systems over mobile networks is one of the main areas of discussion and work in standardization bodies and will be one of the main challenges in the design of 5G mobile systems. Although advanced technologies at the physical (PHY) layer will provide orders of magnitude more capacity and throughput than current wireless links, 5G systems must be designed so that the core network is not a capacity bottleneck due to control plane signaling issues.

1.3.1 New network enhancements for mobile IoT systems

Proactive efforts are being established by cellular operators to encourage and ensure proper network resource utilization by M2M nodes [53]. Among other guidelines, recommendations to hardware and system manufacturers are provided in order to avoid applications that repeatedly check with servers or send sporadic data traffic with little or no flow control. In other words, M2M applications should not behave in cellular networks the same way they do in wireless Local Area Networks (wLAN) or wired connections. It is essential that all network operators ensure proper implementation of such guidelines in order to minimize the

impact of the surge of M2M appliances connected to mobility networks.

Some solutions to the described threats have been proposed by the industry and standardization community [27, 54]. Although there is a certain amount of improvement that can be made from the application/device itself, network-centric solutions are known to be the most effective. Mitigations for the above scenarios are challenging and difficult to implement and test in order to understand their potential benefits. For example, extending the idle timeout period of User Equipments (UEs) has been proposed so that devices transition less frequently between RRC states [54]. This could potentially result in an increased cost, though, due to resources reserved for a longer time for an active device session, such as radio resources at the wireless link. The tradeoff between the security benefit and this cost is very difficult to determine. Other proposed solutions envision techniques to filter signaling load at, for example, the MME to protect the HSS from an overload [27].

In parallel, there is extensive work in the research community and standardization groups to propose new techniques to provide data links over cellular networks for IoT devices with minimal impact on the mobile core. An interesting proposal introduces a connection-less protocol to communicate with IoT devices over LTE cellular links with zero control plane signaling [55]. This technique, aimed to M2M device categories with periodic small bursts of traffic, is designed within the framework of the 3GPP standards, requiring no standards modification.

IoT connection-less communications leverage the LTE PHY layer channels used for the RACH procedure as described in Figure 1.2. This handshake between the UE and the eNodeB is executed every time a mobile device requires to communicate and transition to the RRC connected state. The first message in this handshake is also utilized to achieve UL synchronization with the eNodeB.

The transmission on the RACH channel is shared by all users within a cell or sector and follows the S-ALOHA/CDMA protocol so collisions might occur. A signature is randomly chosen out of 64 possible signatures and a preamble packet is sent over the RACH. Upon reception of a preamble, the eNodeB generates a reply message known as Random Access Response (RAR). This message contains 5 fields: the id of the time-frequency slot where

the preamble was received, the selected signature, a time-alignment instruction, an initial UL resource grant and a network temporary id for the UE (Radio Network Temporary identifier - RNTI). A real lab capture of a standard RACH procedure is shown in Figure 1.4, including the handshake between a smartphone and a commercial lab eNodeB. This capture was obtained with an off-the-shelf LTE traffic sniffer [56].

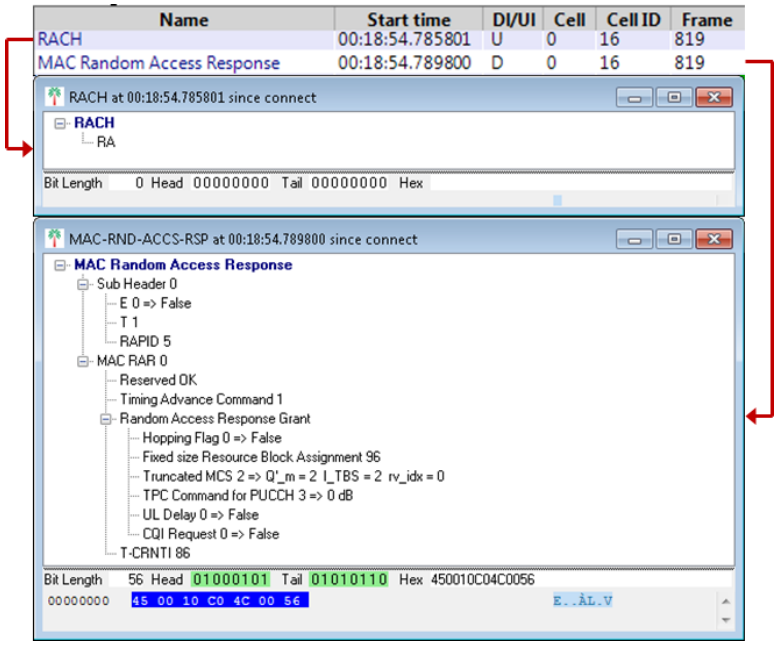


Figure 1.4: LTE Random Access procedure and capture from a real network

A connection-less link for IoT traffic over LTE networks encodes uplink traffic in the RACH preambles. 6 bits of information are encoded by the choice of a signature out of the 64 available. Given a number k of RACH resources per 10ms LTE frame, the total available throughput in a given cell would be of $\frac{k \cdot 6}{0.01}$ bits per second. Note that this throughput would be shared by all IoT devices within the cell and with the RACH traffic of regular smartphones and other mobile devices within the same cell. However, network measurements indicate the substantial under-utilization of the RACH channel in highly dense areas, leaving plenty of room for a connection-less link [55].

Given the possible configurations of the LTE RACH defined in the standards, k ranges from 1 to 10. The latter is the case of one RACH resource allocated in every slot [57]. Given a RACH collision probability of $p^{UE}_{collision} = 1\%$, including collisions and decoding

errors, $k = 10$ and 64 signatures, a connection-less link can support an uplink load of up to $R_{RACH}^{max} = -10 \cdot 64 \cdot \ln(1 - p_{collision}^{UE}) = 6.432$ preambles per frame. This results in a maximum throughput of $R_{UL}^{max} = \frac{6.432 \cdot 6}{0.01} = 3.86 kbps$.

In parallel, downlink traffic is encoded in the 16 bit RNTI field of the RAR, which is not necessary for a connection-less link. Assuming the same system configuration ($k = 10$), the maximum downlink throughput that can be delivered over a connection-less link is $\frac{10 \cdot (16+11)}{0.01} = 27 kbps$. This total raw capacity would also be shared by all the IoT devices within a given cell and the RAR messages sent to regular mobile devices and smartphones.

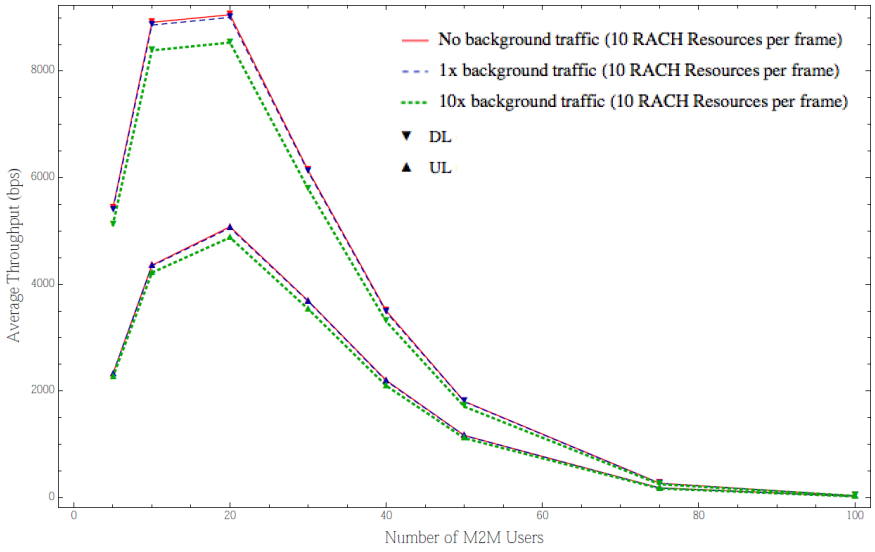


Figure 1.5: UL and DL connection-less throughput with background LTE RACH load

A mobile-initiated connection-less link is triggered by a series of preambles with a pre-defined pattern of signatures, while a network-initiated link is triggered by leveraging the 3 unused padding bits at the tail of the LTE paging message.

A system simulation of a connection-less link under a realistic load equivalent to that of a highly populated area is summarized in Figure 1.5. Results indicate that the RACH background load of one of a highly densely populated area would not impact the performance of the link. As a result, assuming a controlled M2M deployment and absence of adversarial UEs, the impact of the connection-less link on regular LTE communications would be almost null. This is a particularly positive result in the context of signaling overload threat mitiga-

tion and other large scale security threats that could be triggered by a swarm of misbehaving or infected IoT embedded devices.

Connection-less links are a viable solution to provide connectivity to IoT devices over mobile networks without expensive control plane signaling impact against the core network. This particular characteristics is necessary to protect the network from potential saturation attacks against the cellular core that could be triggered by, for example, a malicious botnet of IoT devices. In parallel, industry consortiums and research laboratories are working in further implementations to mitigate the impact of large M2M deployments on mobile networks, guaranteeing security and availability for both the IoT systems and the mobile network itself.

References

[1] A. Iera, C. Floerkemeier, J. Mitsugi, and G. Morabito, "Special Issue on the Internet of Things," in *IEEE Wireless Communications*, vol. 17, December 2010, pp. 8–9.

[2] K. Benedict, "M2M News Weekly," Sys-Con Media, December 2011, http://goo.gl/CI7T4D.

[3] T. Norman, "Machine-to-Machine traffic worldwide: forecasts and analysis 20112016," Analysys Mason, Technical Report, September 2011.

[4] "The Connected Car: Making Cars Smarter and Safer," AT&T, 2014, http://goo.gl/PJYp3g.

[5] A. Berg, "Gadgets: New Connected Devices Put Smartphones in the Middle," Wireless Week, January 2012, http://www.wirelessweek.com/articles/2012/01/gadgets-new-connected-devices-smartphones-in-the-middle/.

[6] "M2M News Weekly," Connected World Magazine, January 2012, http://goo.gl/H1hm6L.

[7] "More than 50 billion connected devices," Ericsson, Ericsson White Paper, February 2011, http://goo.gl/Xi7dE1.

[8] "5G Radio Access: Requirements, Concept and Technologies," NTT Docomo, 2014, http://goo.gl/L72689.

[9] D. Lewis, "Closing in on the Future With 4G LTE and M2M," Verizon Wireless News Center, September 2012, http://goo.gl/ZVf7Pd.

[10] M. Shafiq, L. Ji, A. Liu, J. Pang, and J. Wang, "Large-scale measurement and characterization of cellular machine-to-machine traffic," *Networking, IEEE/ACM Transactions on*, vol. 21, no. 6, pp. 1960–1973, December 2013.

[11] A. Prasad, "3GPP SAE-LTE Security," in *NIKSUN WWSMC*, July 2011.

[12] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for internet of things," in *Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on*, march 2011, pp. 1 –6.

[13] S. Agarwal, C. Peylo, R. Borgaonkar, and J. Seifert, "Operator-based over-the-air m2m wireless sensor network security," in *Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on*, oct. 2010, pp. 1 –5.

[14] A. Jara, M. Zamora, and A. Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments," in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*, jan. 2010, pp. 1 –5.

[15] C. Miller and C. Valasek, "A Survey of Remote Automotive Attack Surfaces," in *Blackhat USA*, 2014, http://goo.gl/k61KzN.

[16] C. Heres, A. Etemadieh, M. Baker, and H. Nielsen, "Hack All The Things: 20 Devices in 45 Minutes," in *In DefCon 22*, 2014, http://goo.gl/hU7a8G.

[17] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 97–106.

[18] K. Nohl and S. Munaut, "Wideband GSM sniffing," in *In 27th Chaos Communication Congress*, 2010, http://tinyurl.com/33ucl2g.

[19] D. Bailey, "War Texting: Weaponizing Machine to Machine," in *BlackHat USA*, 2011, http://www.isecpartners.com/storage/docs/presentations/isec_bh2011_war_texting.pdf.

[20] Hunz, "Machine-to-Machine (M2M) Security," in *Chaos Communication Conference Camp*, 2011, http://events.ccc.de/camp/2011/Fahrplan/attachments/1883_m2m.pdf.

[21] A. R. Prasad, "3GPP SAE/LTE Security," in *NIKSUN WWSMC*, July 2011, http://goo.gl/e0xAWQ.

[22] R. Piqueras Jover, "Security Attacks Against the Availability of LTE Mobility Networks: Overview and Research Directions," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, Atlantic City, NJ, June 2013, pp. 1–9.

[23] "2015 5G Brooklyn Summit," http://brooklyn5gsummit.com/.

[24] S. Sesia, M. Baker, and I. Toufik, *LTE, The UMTS Long Term Evolution: From Theory to Practice*. Wiley, 2009.

[25] S. Rao and G. Rambabu, "Protocol Signaling Procedures in LTE," Radisys, White Paper, 2011, http://goo.gl/eOObGs.

[26] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, "Evolved Universal Terrestrial Radio Access (E-UTRA) - Radio Resource Control (RRC) - Protocol Specification. 3GPP TS 36.331," vol. v8.20.0, 2012.

[27] 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects, "Study on Core Network Overload and Solutions. 3GPP TR 23.843," vol. v0.7.0, 2012.

[28] P. Lee, T. Bu, and T. Woo, "On the Detection of Signaling DoS Attacks on 3G Wireless Networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, May 2007.

[29] M. Dano, "The Android IM app that brought T-Mobile's network to its knees," Fierce Wireless, October 2010, http://goo.gl/O3qsG.

[30] "Signal storm caused Telenor outages," Norway News in English, June 2011, http://goo.gl/pQup8e.

[31] C. Gabriel, "DoCoMo demands Google's help with signalling storm," Rethink Wireless, January 2012, http://goo.gl/dpLwyW.

[32] M. Donegan, "Operators Urge Action Against Chatty Apps," Light Reading, September 2011, http://goo.gl/FeQs4R.

[33] S. Corner, "Angry Birds + Android + ads = network overload," iWire, June 2011, http://goo.gl/nCI0dX.

[34] E. Savitz, "How The New iPad Creates 'Signaling Storm' For Carriers," Forbes, March 2012, http://goo.gl/TzsNmc.

[35] S. Decius, "OTT service blackouts trigger signaling overload in mobile networks," Nokia

Networks, September 2013, http://goo.gl/rAfs96.

[36] J. Jermyn, G. Salles-Loustau, and S. Zonouz, "An analysis of dos attack strategies against the lte ran," *Journal of Cyber Security*, vol. 3, no. 2, pp. 159–180.

[37] C. Mulliner and J.-P. Seifert, "Rise of the iBots: 0wning a telco network," in *Proceedings of the 5th IEEE International Conference on Malicious and Unwanted Software (Malware)*, 2010.

[38] M. Khosroshahy, D. Qiu, M. Ali, and K. Mustafa, "Botnets in 4g cellular networks: Platforms to launch ddos attacks against the air interface," in *Mobile and Wireless Networking (MoWNeT), 2013 International Conference on Selected Topics in.* IEEE, 2013, pp. 30–35.

[39] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, "On cellular botnets: measuring the impact of malicious devices on a cellular network core," in *Proceedings of the 16th ACM conference on Computer and communications security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 223–234.

[40] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, "Machine-Type and other Mobile Data Applications Communications Enhancements. 3GPP TR 23.887," vol. v12.0.0, 2013.

[41] 3GPP work item description, "Signalling Reduction for Idle-Active Transitions. 3GPP RP-150426," March 2015.

[42] oneM2M R1, "Security solutions. ETSI TS 118 103," vol. v1.0.0, 2015.

[43] ETSI, "Machine-to-Machine Communications (M2M - Threat analysis and countermeasures to M2M service layer. ETSI TR 103 167," vol. v1.1.1, 2011.

[44] "Open Channel Traffic Optimization," Seven Networks, Tech. Rep., 2015, http://goo.gl/uz5YOH.

[45] "9471 Wireless Mobility Manager," Alcatel Lucent, Tech. Rep., 2015, http://goo.gl/0n2v8F.

[46] S. Duan, "Congestion control for M2M communications in LTE networks," *University of British Columbia*, 2013.

[47] S.-Y. Lien and K.-C. Chen, "Massive Access Management for QoS Guarantees in 3GPP Machine-to-Machine Communications," *Communications Letters, IEEE*, vol. 15, no. 3, pp. 311–313, March 2011.

[48] Y.-H. Hsu, K. Wang, and Y.-C. Tseng, "Enhanced cooperative access class barring and traffic adaptive radio resource management for M2M communications over LTE-A," in *Signal and Information Processing Association Annual Summit and Conference (APSIPA), 2013 Asia-Pacific*. IEEE, 2013, pp. 1–6.

[49] A. Laya, L. Alonso, and J. Alonso-Zarate, "Is the Random Access Channel of LTE and LTE-A Suitable for M2M Communications? A Survey of Alternatives," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 1, pp. 4–16, January 2014.

[50] C. Ide, B. Dusza, M. Putzke, C. Muller, and C. Wietfeld, "Influence of M2M communication on the physical resource utilization of LTE," in *Wireless Telecommunications Symposium (WTS), 2012*. IEEE, 2012, pp. 1–6.

[51] J. Jermyn, R. P. Jover, M. Istomin, and I. Murynets, "Firecycle: A scalable test bed for large-scale lte security research," in *Communications (ICC), 2014 IEEE International Conference on*. IEEE, 2014, pp. 907–913.

[52] J. Jermyn, R. P. Jover, I. Murynets, and M. Istomin, "Scalability of Machine to Machine systems and the Internet of Things on LTE mobile networks," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. IEEE, 2015.

[53] L. Iyengar, Y. Zhang, J. Jun, and Y. Li, "AT&T Network Ready Device Development Guidelines," AT&T Network Ready Lab, Tech. Rep., September 2011, http://goo.gl/nmUrSl.

[54] "System improvements for machine-type communications (mtc). 3gpp ts 23.888," vol. v11.0.0.0, 2012.

[55] R. P. Jover and I. Murynets, "Connection-less communication of IoT devices over LTE mobile networks," in *IEEE International Conference on Sensing, Communication and Networking (SECON)*. IEEE, 2015.

[56] Sanjole, "WaveJudge 4900A LTE analyzer," http://goo.gl/ZG6CCX.

[57] 3rd Generation Partnership Project; Technical Specification Group Radio Access Network, "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Physical channels and modulation. 3GPP TS 36.211," vol. v10.3.0, 2011.