Shwetha H.K, Prof. D. Jayaramaiah / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.942-946

Study and Analysis of Security Issues in Next Generation Mobile Network

Shwetha H.K[1], Prof. D. Jayaramaiah[2]
[1]*PG Student, The Oxford College of Engineering, India*
[2]*Professor, HOD- Information Science & Engg, The Oxford College of Engineering, India*

Abstract

NGMN is a standard term describing the next level of evolution in wireless communication. Security is one of the important issue in next generation mobile network. The core infrastructure of NGMN network is packet based, all IP and heterogeneous where Long Term Evolution (LTE), WiMax & Wireless local area networks (WLAN) are examples of viable access technologies. By deploy femtocell it increasing demand for data rates , LTE is the mobile network technology for the next generation mobile communications as defined by the 3rd generation partnership project (3GPP). LTE has features such as increased data rates, lower latencies & better spectral efficiency. Goal here is to raise awareness about security issues in LTE & femtocell. In this paper we approach significant threats to security of femtocell enabled cellular networks (LTE). Approach Distributed Denial of Service (DDoS) defence scenario dynamics among service provider and mobile operator that is effective against malicious attacker. By considering parameters such as Internet traffic and femtocell subscriber shares, We propose novel approach could help service provider and mobile operators making strategic decisions.

Index Terms—Wireless Security, Cellular Mobile Networks, LTE, Femtocells

I. Introduction

In wireless communication networks cellular mobile networks are the most widely used and heavily deployed in the world. In the advent of digital technologies such as GSM the use of mobile devices has changed. Based on the subscriber's location users are able to browse the Internet and get the services such as ebanking, navigation, social networking and recommendations using modern smartphone. Femtocells, are low-power and low-range base stations for cellular networks installed by users at their own premises, are believed to meet the surge in data rates that these multimedia and interactive services require. They offload the macrocell network and provide backhaul connections to the cellular operators' networks through the users' residential broadband accesses [15].

Long Term Evolution (LTE) is the mobile network technology for the next generation mobile communications, as defined by the 3rd Generation Partnership Project (3GPP). The features such as increased data-rates, lower latencies and better spectral efficiency, and the IP core network architecture, known as Evolved Packet Core (EPC). The essential component of the Evolved Packet System (EPS, which includes the radio access, the core network and the handset) is give a importance for supporting the high-speed connections and a smooth handovers among LTE and other technologies such as GSM and WCDMA. LTE is expected to make extensive use of user-installed femtocells, very low-power and low-range base stations (femtocells), in order to achieve its goals of spectral efficiency and high-speed for a greater number of users.

Security in these networks is achieved by several levels. They concerns about the messages that are communicated over-the-air, the traffic routed by a mobile operator on its own internal network and the inter operator traffic. The main assumption underlying the security of the mobile networks cited so far is a high trust that each operator has in its own infrastructure and in other operators with whom it has a roaming contract. The main reasons behind such positive attitude are the following: (i) direct ownership and control of the network equipment, (ii) dedicated connections and protocols among network components and (iii) the highly hierarchical decision making process for providing network resources to mobile devices. Clearly, in case of a substantial change in the network architecture, such as evolving to a flat all-ip network, the trust relationships would need to be revisited.

The combination of LTE, all-ip network architecture and femtocells is stimulating the new security threats. A malicious user easily tamper with the femtocell, as it resides directly at the user's premises, or to disrupt the legitimate communications both at the femtocell and at the core network level, due to the openness of the IP networks. Moreover, as LTE is an evolution of the existing 2G-3G standards and is backward-compatible with them, it also inherits different vulnerabilities at the protocol level. Specifically, the privacy of the user's permanent identity and his/her geographic location is at risk both at the air interface (use of identifiers) and at the application layer (location based services).

In this report, we analyze security threat related to the all-ip and femtocell LTE network architectures. We analyze a scenario involving distributed denial of service (DDoS) attacks on the femtocell core network components, , and we present a novel game theoretic model to represent scenario between a mobile operator and different service provider.

II. RELATED WORK

On the security front, DDoS attacks are a well known phenomena for large companies hosting a multitude of web servers sparse around the globe, such as eBay, Amazon or Yahoo [6]. In order to deal with such attacks in a systematic way, Mirkovic [18] proposes a general classification of attacks and defense mechanisms, such that system developers and researchers can better observe and react to the inherently different attacks by exploiting their common traits. If the detection of ongoing DDoS attacks is best performed at the victim site, the suppression mechanisms are most effective near the source, as it is possible to filter the malicious traffic from the genuine connections and avoid the former to even reach and saturate the final link with the target. This idea has been investigated in several studies ([17], [5], [19], [16]) suggesting that a distributed solution is better suited against large-scale DDoS attacks than one localized only at the final link with the target. The requirement is that different ISPs are able and willing to cooperate in order to provide protection, and the authors agree that a failure to reach an agreement could jeopardize the effectiveness of their solutions. Only in more than one ISP is strictly required to implement the solution, otherwise even a single ISP would be able to ensure a partial level of protection.

One work that specifically aims at femtocells and mobile operators is [15], where femtocell gateways are the targets of DDoS attacks perpetrated with the intent to extort money from mobile operators. The authors manage to obtain real prices for such attacks but fail to illustrate any countermeasures that make use of the specific features of femtocell networks, such as the need for femtocells to be located in geographic regions where the mobile operator has the right to use the spectrum. Our DDoS defense scheme presents a model that leverages on incentives that cooperation among ISPs could bring both to them and to mobile operators.

III. LTE NETWORK ARCHITECTURES

In this section, we describe the network architecture of LTE (radio access and core network) that are related to the security issues discussed in this report. Figure 1 shows a basic network architecture for LTE[7], with a clear separation between the core network (CN) components and the radio access network (RAN). More information about the architecture and security of LTE RAN/CN can be found in following paper [13], [14], [21].

3.1 Radio Access Network

The RAN is responsible for all the radio interface related features of the network, and it is the point of entry to the mobile network for any compatible wireless device. In addition to encapsulating or decapsulating data, it performs radio channel and power management controls, handover procedures and over-the-air encryption/integrity for data and signalling traffic to and from the wireless devices (User Equipment, UE). Due to the broadcast nature of the wireless medium, the air interface is the most vulnerable to eavesdropping and traffic injection, and thus several measures have been taken in order to mitigate those risks. Eventhough it might be non trivial to break the algorithm and obtain the secret key, the user privacy is still at risk due to protocol flaws enabling a malicious user with a femtocell to track the where abouts of a subscriber.

In LTE and UMTS, all user and signaling traffic is encrypted and integrity protected against misuse by malicious entities on the air interface. The use of a shared secret key between the Universal Subscriber Identity Module (USIM) in the mobile device and the home network ensures that only authorized users and legitimate network operators can communicate and exchange information. There are, however, major differences in the way encryption and trust is managed in LTE and UMTS.

The UMTS the air interface encryption is terminated at the RNC, while in LTE it is terminated in the eNodeB (similar to GSM). UMTS uses encryption/integrity key pairs that are independent of the network that is currently serving the UE. Moreover, these keys must not be changed during a handover, if the UE is still served by the same SGSN. In LTE, on the contrary, the keys are not transfered as such from the home network to the eNodeBs but they are derived from layer to layer, depending on the particular serving network and the specific eNodeB that is used by the mobile device. As a consequence, LTE has already been developed with limited trust in network components and external partners from the beginning.

3.2. Femtocells

As defined by the Femto Forum [15] femtocells are low-power wireless access points that operate in licensed spectrum to connect standard mobile devices to a mobile operators network using residential DSL or cable broadband connections. The main differences with respect to traditional base stations, such as (e)NodeBs, are the following. Femtocells are installed by users at their own premises, without the involvement of authorized operator's technicians,

_ user-friendly and low-cost devices, connected to the operator's network through a public (insecure) connection, provided by a potentially different service provider.

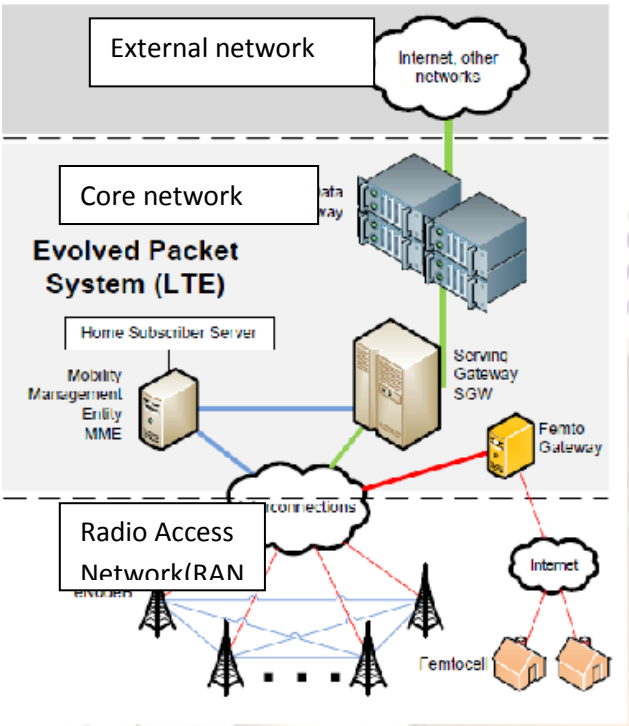

Figure 1. Basic architecture of LTE network

From a mobile device's point of view, being connected to a (e)NodeB or a femtocell is both are same, because the protocols and security standards used at the air interface are exactly the same. From a malicious user's point of view, it makes a substantial difference because for a malicious user it is much easier to tamper with a small and low-cost (£160 [15]) femtocell than it could be with a bigger device located on a rooftop. Moreover, as the traffic between the femtocell and core network goes through the Internet, so the attacker can easily attack through femtocell.

3.3 Core Network

The core network components of LTE, shown in Figure 1 (middle), are responsible for the storage of subscriber information, billing, mobility management, authentication /authorization and routing of user data to hits destination. Without this infrastructure, the calls and data services cannot be successfully established. Usually, the core network is protected from external access by firewalls located at its edges, and LTE have security measures in place to the malicious attacks on core components. Inside the core network, encryption is not specified for UMTS and not mandatory for LTE, although the IP interfaces in LTE can be protected by using IPSec secure connections among the RAN and CN components. As LTE supports interconnections with non-3GPP networks such as WiMax and WiFi, IPSec tunnels are used inside the core network to protect the confidentiality of information. Integrity, on the contrary, is not protected for performance reasons.

IV. SECURITY CHALLENGES

Figure 1 shows the threat model for a femtocell-enabled mobile network. The three vulnerable elements are indicated by arrows: (i) the air interface between the mobile device (User Equipment) and the femtocell (Home(e)NodeB), (ii) the femtocell itself and (iii) the public link between the femtocell and the security gateway (SecGW). Our intent is to focus on certain attacks on the aforementioned elements, which are achievable without breaking the cryptosystems or the protocols. A more exhaustive list of all possible attacks and countermeasures can be found in.

4.1 Attacks on the Femtocell

A mobile device, being connected to a regular base station, i.e., (e)NodeB, or a femtocell is both are same, because the protocols and security standards used at the air interface. From a malicious user's point of view, it makes a substantial difference because it is much easier for a malicious user to tamper with a small and inexpensive (£120 [15]) femtocell than it could be with a large and complicated device located on a rooftop. The physical size, material quality, lower cost components and the IP interface of the femtocell make it more suited for reverse engineering and tampering than a traditional, more expensive and business-grade (e)NodeB base station.

As the over-the-air user data encryption is terminated at the femtocell, hardware tampering with the device could expose the private information of the unsuspecting user. Moreover, attacks such as device impersonation, Internet protocol attacks on the network services, false location reporting or simply unauthorized reconfiguration of the onboard radio equipment could hinder the network operator from controlling interference and power management features. This could have severe consequences on the quality of service. To this end, femtocells should be equipped with trusted execution environments that render malicious manipulation of the onboard software and the on-the-wire sniffing very hard to achieve.

we develop a game-theoretic model to represent a possible security scenario for the femtocells and their core network components, the femtocell gateways. ISPs and mobile operators make decisions on the security demand/offer for the femtocell infrastructure by considering distributed denial of service (DDoS) attacks on femtocell gateways.

V. FEMTOCELL DDOS DEFENSE

One important security issue of current and next generation cellular networks will be related to the use of femtocells in order to provide better signal quality, service availability and data-rates to the subscribers. If, on one hand, this seems to be a very palatable solution for mobile operators as it avoids investments on the backbone connection, on the other hand the exposure to the public Internet has severe drawbacks. One of them is the public IP address that each femtocell gateway would be assigned, and to which tenths of thousands femtocells would connect to. DoS attacks are usually carried out against a service running on a specific IP address in order to deny access to legitimate users and cause damage to the service owner. A distributed DoS (DDoS) attack has the same goal but it is usually much more difficult to prevent, as it exploits a great number of zombie computers to generate apparently legitimate connections to the given IP address. It is clear that if the gateways were to suffer intense DDoS attacks, customers would not be able to connect to them anymore and would not get the service they are paying for. Ultimately, they could also change their mobile operator.

In this section, we develop a game theoretic model for the defense against DDoS attacks. The idea is based on the fact that femtocells are low power base station so attacker easily attack through the femtocell. In DDoS attack, attacker send many number of packets to the operate. As a consequence, The packet send from the attacker will not send to the SGW, ISP itself block all the packets which is received from the attacker. This way, the mobile operator can continue to serve legitimate users while avoiding to provide resources to malicious attackers.

We assume that an Service provider could either provide protection by cooperating with other service provider, on its own or not protect at all. If an service provider cooperates with others in order to provide protection, then it can lower its costs by sharing them with the other parties. In this case, it also gets only a share of the benefits (provided by the mobile operator) to compensate for the extra costs of setting up the protection mechanisms. If a service provider protects the mobile operator on its own, it gets all the benefits but has a greater cost as well, depending on its current Internet traffic share. If an service provider does not provide protection, it does not get any benefits but, at the same time, it does not bear any additional cost.

In game theoretic model We model the DDoS defense. The leader (mobile operator) chooses its strategy first and then the followers (ISPs), knowing the strategy of the leader, select their own strategies in order to maximize their payoffs. Once the leader has chosen its strategy, the followers play the game in a simultaneous fashion, i.e. all ISP select their strategies at the same time. Figure 2 illustrates the graph for the time to detect the attack and load on SGW.

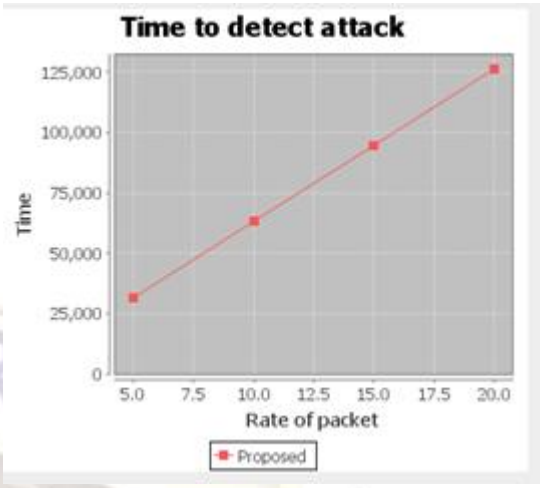

Figure 2a. Time to detect attack, x-axis is rate of packet in kilo bits and y-axis time in milisecond.

Figure 2b, Load on SGW, x-axis is time in second and y-axis is load on SGW. In this graph it shows the result of normal flow of data and the result of after lunch attack. Once the attack is lunch it drop out the load on SGW and constant for the next flow.

VI. CONCLUSION

The control over security in the next generation of mobile networks, such as LTE, is held by the core network. LTE and femtocells are combined together with an all-IP core architecture, they provide better service levels and data-rates than current 2G and 3G networks. In order to attach more users and to increase security, the research people (3GPP) has put more intelligence in the next generation base stations, enabling them to decide autonomously the radio channel characteristics (handover, power, channel assignment) for each user.

In this paper, we have approach some significant threats to security in femtocell-enabled

mobile networks. we suggested a novel approach towards the protection of the mobile network against internet-based DDoS attacks successful stimulating.

REFERENCES

[1] 3GPP LTE. Visited on 25.11.2009. [Online]. Available: http://www.3gpp.org/LTE
[2] Y. De Mulder, G. Danezis, L. Batina, and B. Preneel, "Identification via location-profiling in GSM networks," in Proceedings of the 7th AC workshop on Privacy in the electronic society. ACM New York, NY, USA, 2008, pp. 23–32.
[3] G. Koien and V. Oleshchuk, "Location Privacy for Cellular Systems; Analysis and Solution," Lecture Notes in Computer Science, vol. 3856, p. 40, 2006.
[4] L. Garber, "Denial-of-service attacks rip the Internet," Computer, vol. 33, no. 4, pp. 12–17, 2000.
[5] J. Mirkovic, "A taxonomy of DDoS attack and DDoS defense mechanisms," ACM SIGCOMM Computer Communication Review, vol. 34, no. 2, pp. 39–53, 2004
[6] Lee Garber, **"**Denial-of-Service Attacks Rip the Internet".
[7] Long Term Evolution (LTE) overview.
[8] LTE Simulator Documentation.
[9] Next Generation Mobile Network Beyond HSPA & EVDO, by the NGMN Alliance.
[10] Securing Next Generation Mobile Networks.
[11] Spectrum Requirements for the Next Generation of Mobile Networks.
[12] Anand R. Prasad, "3GPP SAE/LTE Security".
[13] 3GPP TS 23.401 v8.7.0. " General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Acceess Network access".
[14] 3GPP TS 33.401 v8.5.0, "3GPP System Architecture Evolution (SAE) Security Architecture".
[15] Femto Forum. http://www.femtoforum.org/femto/aboutfemtocells.php..
[16] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," ACM Computing Surveys (CSUR), vol. 39, no. 1, p. 3, 2007.
[17] S. Chen and Q. Song, "Perimeter-based defense against high bandwidth DDoS attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 16, no. 6, pp. 526–537, 2005.
[18] J. Mirkovic, M. Robinson, P. Reiher, and G. Oikonomou, "Distributed Defense Against DDOS Attacks," University of Delaware CIS Department Technical Report CIS-TR-2005, vol. 2, 2005.
[19] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan, "Cossack: Coordinated suppression of simultaneous attacks," in Proceedings of DISCEX III. Citeseer, 2003, pp. 2–13.
[20] GSM Association Market Data Summary Q2 2009. Visited on 24.11.2009. [Online]. Available: http://www.gsmworld.com/newsroom/market-data/ market data summary.html.
[21] 3GPP TS 33.401 v8.5.0, "3GPP System Architecture Evolution (SAE): Security architecture," . [Online]. Available: http://www.3gpp.org/ftp/Specs/Archive/33 series/33.401/33401-850.zip
[22] 3GPP TS 23.002 v4.8.0, "Network architecture," . [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/23 series/23.002/23002-480.zip