Detection and Remediation of Attack by Fake Base Stations in LTE Networks

Alanoud Al Mazroa, Mohammed Arozullah

Abstract*— Rogue base station attack can compromise the privacy of user equipment (UE) in LTE networks. To address this issue, we propose a rogue base station identification protocol to protect UE privacy. Our protocol utilizes the mobile property of the UE and is designed based on the observation that rogue base station can only cover a small area. We use the measurements of UE in different locations to estimate the power and location of the base stations. The UE also tracks the signatures of each legitimate base station. If the base station is already verified by the detection protocol, then the UE connects to the base station according to LTE standard. For any new appearing base stations, it sends the power of the base station and the GPS location itself to a cloud server to verify the legitimacy of the base station. The cloud server maintains a database of real base stations. Our proposed protocol does not need to change existing LTE standard and no base station modification is required. Our protocol is implemented on NS3 LTE module and evaluated with various practical settings. The results indicate our protocol can ensure that the UE can successfully detect rogue base stations and avoid sending privacy data to rogue base station.

Keywords: user equipment (UE) in LTE networks, identification protocol to protect UE privacy, GPS, legitimacy, NS3 LTE module.

I. INTRODUCTION

Rogue base station attack is a well-known attack that can compromise user privacy by tracking their geographical movements, intercept user credit card information etc. According to [1], a cheap base station can be produced by programming Universal Software Radio Peripheral (USRP) boards. The increasing popularity of USRPs led for example to a cheap implementation of fake base station attacks. Such a short range fake base station is usually produced with affordable prices [4]. By inducing mobile users to connect to it, it can access to sensitive information.

There are some existing works that are trying to rem- eddy this situation. For example, a mutual authentication mechanism between has been proposed [5]. The basic idea of this approach is that the UE can identify fake base station from key exchanges. However, there is a drawback for this mechanism, i.e., both the UE and base station need to be changed as it is not the default LTE standard. This makes it difficult for widely deployment.

Our solution is inspired by a solution that enables UE to localize the base station physically [2]. We also localize the location of the base station, but we do not want the UE to physically check the presence of the base station. Our design decision is based on several reasons. First and foremost, users may not be happy to physically check each base station they are going to connect. Second, even the user find the base station, s/he may still not be able to identify its legacy. To address these issues, we use a cloud-assisted approach that maintains a database of real base stations. By contacting the cloud server first, the UE can ensure that they only send sensitive information through legal base station. An optimization is made by storing the real base stations locally, so that the user do not have to check the database every time they connect. For example, for the people have regular route every day, they only need to check the base station at the first time and free to connect in the future. The UE only have to check the legacy of the base station at the first time, and then store the id of the real base station locally to avoid future checking.

In our solution, a cloud server is used to calculate and maintain the locations of all the real base stations. The location of a base station is calculated based on several measurements from various UEs that connect to one base station. The location of each base station is determined by the GPS of each UEs and signal strength from each UE received. Based on the fact that a real base station usually have large area coverage, UEs in the same area should be able to receive the signal from the same base station. A fake base station utilizes a software radio can only cover a very small area and UEs in longer range cannot receive the signal. Based on this, the fake base station can be identified.

On the UE side, the UE device will send the measurements of surrounding base stations to the cloud server. This process is only being done once for each area.

For example, if the user measures the base stations at home and sends the signal strengths of base stations to the cloud server, it will not repeat this again next time it connects to the base station at home. Therefore, this is only a onetime cost. After contacting the cloud server, the UE can determine the legacy of each base station and connects to the best real base station. At the same time, the UE records the signal strength of the base station and record it as a real base station in the history log. Next time the UE sees the base station, it simply marks the base station as real.

II. COMPONENTS OF THE SYSTEM

In this section, we present our cloud-assisted approach to remedy fake base station problem. Our design consists of a cloud server, that crowdsourcing all the real base stations, and a UE, that probing the cloud server to identify the legacy of the base station and maintain a history log for all real base

Manuscript Received on March 2015.

Alanoud Al Mazroa, The Catholic University of America, Washington, D.C 20064.
Mohammed Arozullah, The Catholic University of America, Washington, D.C 20064.

stations detected at different locations.

A. UE Design

The UE connects to the cloud server by TCP/UDP connections. After the connection is established the UE sends the measured signals and base station IDs to the cloud server. After the UE verifies that which base stations are real, it records the ID and estimated location of the base station into a history log for future lookup. In our design, UE RRC layer collects the base station ID and received signal strength from Master Information Block (MIB) and System Information Block (SIB). The UE RRC layer put all the information into the identification table. After identify the legacy of the base station, UE will send connection request to the base station with the strongest signal strength from which network that has the most number of base stations. In the traditional UE protocol design, the UE sends the UE ID or International Mobile Subscriber Identify (IMSI) to the eNB in plain text. Therefore, a malicious attacker can easily decode the UE ID and copy it for illegal usage. The user privacy can be easily attacked in this design. To remedy this situation, the UE queries the legacy of the base station first before make any sensitive transactions with other sites, i.e., purchasing something.

B. Cloud Server

The cloud server consists of two parts. One part is to calculate the location of each base station based on the measured signal strengths from different UE devices. This is done by triangulation, geometry technic that localize a base station based on three known measurements from three different locations. The other part is a database that records the location of each real base station. Each base station is attached with a trust la- bel that refers to the number of UEs that sees this base station in different locations.

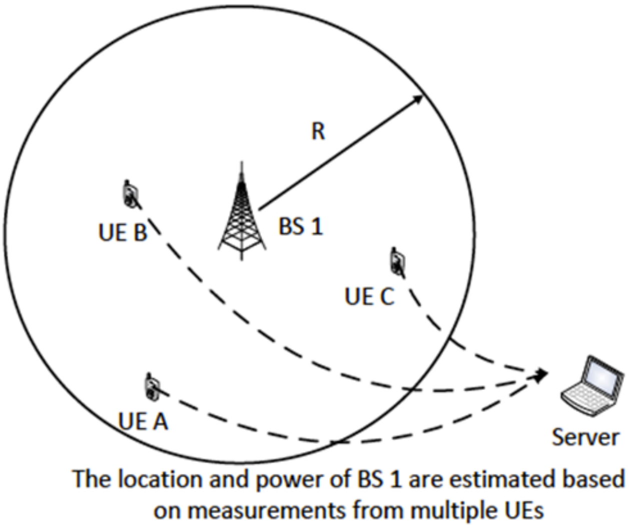
R
BS 1
UE B
UE C
UE A
Server
The location and power of BS 1 are estimated based on measurements from multiple UEs

Figure 1: Base station location and power estimation.

An example is given in Fig. 1. in this example, all three UEs (A, B and C) hears from base station with ID 1. All three will send the GPS location of itself, the measurement signal strength (or RSSI) and the base station ID to the cloud server. The cloud server calculates the location and power of the base station based on the information from the UEs and stores the information of base station 1 into database for future queries.

Because fake base station is usually implemented by simple hardware [1], so it generally has lower coverage range. As shown in Fig. 2, the coverage of real base station is around R, while the coverage of fake base station is around r, and we have r << R. After UE A sense the signal strength of the fake base station, it sends the information to cloud server. The cloud server finds that this base station has not been reported before. Also, according to a recent report from a nearby UE B, who does not sense the fake base station? According to all the information from crowdsourcing, the server can conclude the base station has a much smaller coverage, and therefore it is a fake base station. Another case is when UE B is also in the range of base station, but the cloud server can still estimate the location and power of the fake base station. Base on the power of base station, the cloud server can tell whether it is fake or not.

III. OPERATION OF THE SYSTEM

Long term evolution (LTE) is the next step forward in cellular 3G services. First, it is compatible to older cellular technologies, i.e., it is completely integrated into the existing cellular infrastructure for 2G and 3G. Second, it operates at higher rate than 3G, i.e., LTE is a way for cellular communications to operate at 100 Mbps or faster. Evolved Node B (abbreviated as eNB), also known as Base Station, is the element in E-UTRA of LTE that is the evolution of the element Node B in UTRA of UMTS. It is the hardware that is connected to the mobile phone network that communicates directly with user equipments (UEs), like a base station in GSM networks.

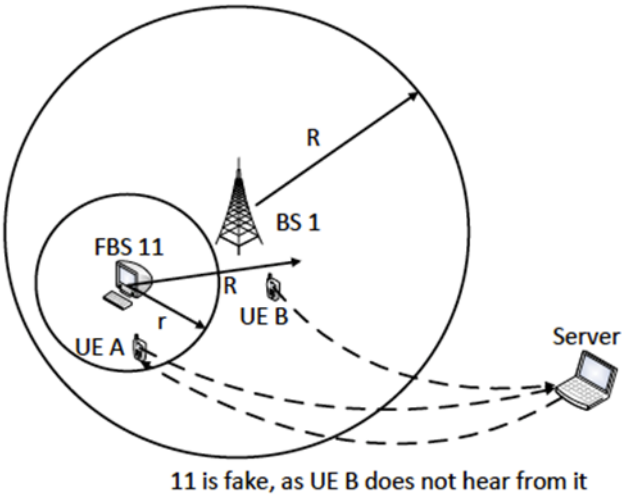

Figure 2: Fake base station identification.

IV. THE PROBLEM WITH THE SYSTEM

In LTE networks, UE has to connect with Base Station first to connect to the internet. Some attackers utilize this property to compromise user privacy by intercepting UEs' sensitive information. This is known as

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

rogue (or fake) base station attack. Such an attack usually conducted by a cheap base station with small range, e.g., produced by programming Universal Software Radio Peripheral (USRP) boards [1, 4]. By inducing mobile users to connect to it, it can access sensitive information. Such an attack is very effective because UE connects Base Station with the highest received signal strength and a fake Base Station can have high signal strength as it can be physically close to the UE.

A. Detection of Fake Base Station Attack

In our design, when UE starts to connect with a Base Station, it scans all the surrounding Base Stations and records their IDs and signal strengths received. The UE sends its own GPS location with these measurements to the cloud server. For easy understanding, we assume UE A measures the signal strength of Base Station 1. There are some other UEs, B and C, also measures the signal strength of Base Station 1, but in other different locations. The cloud server can estimate the location of Base Station A based on the three measurements and three different locations. Based on these estimation, the cloud server can has a power strength estimation on Base Station 1 and its coverage by signal attenuation model. If a new Base Station B measurements from UE A comes to the cloud server, and a nearby UE B does not send the measurement of Base Station 2 as it does not receive signal from Base Station 2. The cloud server assumes all real base station has a minimum power and coverage calculated based on the power. It does not receive any measurements from UE B, then Base Station 2 clearly has a shorter range and is identified as the fake Base Station.

V. SIMULATION OF THE PROTOCOL BY USING NS3

In this section, we discussed the implementation in NS3 platform. We implement the proposed protocol on NS3 LTE module. NS3 is a well-known discrete event network simulator for Internet systems. The ns-3 simulation core supports research on both IP and non- IP based networks. It involves wireless communication modules including Wi-Fi, WiMAX and LTE for layer 1, 2 and 3 and a variety of static or dynamic routing protocols. The UE connects to the cloud server by TCP connection. The cloud server stores the location of base stations into sqlite3, a light weight databases. The UE maintains a table to store the location of all real base stations detected.

VI. EVALUATION OF THE PROTOCOL

We use different simulation setup to test the feasibility of our design. The results are shown in Table 1. We vary the number of UEs and base stations. We test if the all the UEs can identify the legacy of the base station for each connection. All the fake base stations are successfully identified by our approach.

Table 1: Evaluation Setup

UE	FBS	Real BS	Privacy Preservation
2	1	10	Yes
4	2	10	Yes
6	3	10	Yes
8	4	10	Yes

VII. RESULTS

Step 1: Add base stations, UEs and Cloud Server

Add real base station ID:1

Add fake base station ID:11

Add UE: A Add UE: B Add UE: C

Add Cloud Server

Step 2: Measure Base Station Power

LOG LteUeRrc::SaveUeMeasurement: UE A measured base station 1, power in dbm -59.7603

LOG LteUeRrc::SaveUeMeasurement: UE B measured base station 1, power in dbm -65.7809

LOG LteUeRrc::SaveUeMeasurement: UE C measured base station 1, power in dbm -69.3027

LOG LteUeRrc::SaveUeMeasurement: UE A measoured base station 11, power in dBm -71.8015

Step 3: Send Information to Cloud Server

LOG UeManager::SendRrcConnectionRequest: UE A Send GPS (2, 2) and base station info to Cloud Server LOG UeManager::SendRrcConnectionRequest: UE B Send GPS (1, 9) and base station info to Cloud Server LOG UeManager::SendRrcConnectionRequest: UE a Send GPS (8, 8) and base station info to Cloud Server

Step 4: eNB Receive Information from UEs

LOG UeManager::RecvRrcConnectionRequest: Receive GPS and Measurement Info from UE A

LOG UeManager::RecvRrcConnectionRequest:Receive GPS and Measurement Info from UE B

LOG UeManager::RecvRrcConnectionRequest: Receive GPS and Measurement Info from UE C

Step 5: eNB Calculate BS Power and Range

LOG UeManager::CalculateBaseStationRange: Base Station 1 power in dbm 1dbm

LOG UeManager::CalculateBaseStationRange: Base Station 11 power in dbm -10dbm (fake detected)

VIII. CONCLUSTION

In this paper, we study the fake base station attack and a solution for it. The attacker can use fake base station to set up connection with UE. In this way the attack can explore user privacy. To address this issue, we use a UE side solution that identifying fake base station in synchronization stage. There are several ad- vantages for our solution. First, we identify fake base station in synchronization stage, which avoid the UE connects to the base station. Second, the solution is UE side solution so that can be gradually deployed.

We implement our solution on NS3 LTE module. The evaluation shows that our solution can identify fake base station in various attack settings.

IX. RELATED WORK

Fake base station attack is a well-known attack and many approaches have been proposed to address this issue. IMSI catcher is a universal problem that the IMSI can be easily cached by a fake base station or man-in- the-middle attack [9]. A fake base station can behave as repeater and can transmit illegal requests in the net- work [6]. Such a fake base station can be built based on software radio [8]. There is some authentication mechanism introduced in [5]. It introduces two-way authentication and key agreement mechanism to protect subscriber privacy and security. Similar work estimates an approximate distance be- tween a subscriber's device and the deployed femtocell [2]. A subscriber can confirm whether or not the femto cell he connected with is physically-present. Different from this approach, we do not need the user to physically identify the location of the femto cell. There are some work focus on localization in LTE networks [7, 3].

REFERENCES

1. M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar. New privacy issues in mobile telephony: fix and verification. In Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.
2. C.-M. Chen, Y.-H. Chen, Y.-H. Lin, and H.-M.
3. Sun. Eliminating rouge femto cells based on distance bounding protocol and geographic information. Expert Systems with Applications, 2014.
4. J. A. Del Peral-Rosado, J. A. Lopez-Salcedo, G. Seco-Granados, F. Zanier, and M. Crisci. Analysis of positioning capabilities of 3gpp lte. In Proceedings of the ION GNSS, pages 1–10, 2012.
5. N. Golde, K. Redon, and R. Borgaonkar.
6. Weaponizing femto cells: The effect of rogue devices on mobile telecommunications. In NDSS, 2012.
7. C.-K. Han, H.-K. Choi, and I.-H. Kim. Building femtocell more secure with improved proxy signature. In Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE. IEEE, 2009.
8. N. K. M. Mishra Sandip D. False base station attack in gsm network environment. In International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 2014.
9. D. Peral-Rosado, J. A. Lopez-Salcedo,
10. G. Seco-Granados, F. Zanier, M. Crisci, et al. Achievable localization accuracy of the positioning reference signal of 3gpp lte. In Localization and GNSS (ICL-GNSS), 2012 International Conference on, pages 1–6. IEEE, 2012.
11. Y. Song, K. Zhou, and X. Chen. Fake bts attacks of gsm system on software radio platform. Journal of Networks, 2012.
12. D. Strobel. Imsi catcher. 2007.