Securing the User Equipment (UE) in LTE Networks by Detecting Fake Base Stations

Alanoud Al Mazroa, Mohammed Arozullah

Abstract*— An LTE network attacker can set up rogue base station easily to make the victim user equipment (UE) connect to such base station. The privacy of the UE will be compromised. In this paper, we propose a protocol to identify fake base stations to protect user privacy. The basic idea is to synchronize to all base stations in range and collect the network IDs. Based on the fact that legitimate base stations have the same network ID that is different from fake ones, the UE can connect to the legitimate base station with the strongest power instead of any base station with the strongest power in traditional design. Our proposed protocol is a UE side solution and no base station modification is required. This property makes our protocol can be gradually deployed in the future. 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 always connect to the legitimate base station with the strongest power.

Keywords: LTE network attacker, NS3, UE, IDs, protocol,

I. INTRODUCTION

While most mobile phone users accept that the network operator can track their geographical movements, few would be happy if any arbitrary third part could do so. Such a possibility would enable all kinds of undesirable behaviors, ranging from criminal stalking to commercial and advertisement purposes. Such attacks are known to be fake base station attacks. It has been shown that cheap base stations can be produced by programming Universal Software Radio Peripheral (USRP) boards [1]. The increasing popularity of USRPs led for example to a cheap implementation of fake base station attacks. Shorter range base stations, available at affordable prices, have been targeted as well by open source developers and security researchers [3]. Such a fake base station can induce legitimate mobile users to connect to it. The objective is to access to sensitive information and/or create a Denial of Service (DoS). To remedy this situation, mutual authentication mechanism between UE and base station has been proposed [4]. In this way, the UE can identify fake base station from key exchanges. The drawback of this kind of mechanism is that both the UE and base station need to be changed, which makes it difficult for widely deployment. Another solution is to localize the base station physically [2]. First, a relative accurate localization algorithm is required to locate the femtocell or base station. Second, users may not be happy to physically check each base station they are going to connect. Third, even the user find the base station, s/he may still not be able to identify its legacy.

Manuscript Received on January 2015.

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

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

In this paper, we present a cross-layer design on UE side to identify fake base stations in early stage. The advantage of our solution is that only the UE needs to be modified, so that the new protocol can be deployed gradually. The basic idea of our protocol is to identify the network each base station belongs to. The UE tracks the parameters of surrounding base stations, e.g., the base station ID, the reference signals received power, and the network ID. Based on the fact that similar base stations should belong to the same network, the UE can identify which network each base station belongs to. The challenge is that the network ID is contained in System Information Block 1(SIB1) and not easy to get unless the UE synchronizes with the base station. To address this issue, the UE perform measurements on surrounding base stations and synchronizes to each base station in the range. After this procedure, the UE traverse all the base stations in the table and identify all the fake base stations from real ones. After identify the fake base stations, the UE connects to the real one with the maximum received power. To avoid base station eavesdropping the International Mobile Subscribe Identification (IMSI), the UE encrypts the IMSI by using standard encryption method. We implement our solution on Network Simulator 3 LTE module and evaluate it in various settings, our results show that the privacy of UE can be protected from fake base stations.

II. STATEMENT OF THE PROBLEM

An attack can use fake base station to forward call to premium rate numbers [5]. This is used for Bogus registration details of customer and that cannot be detected after computing any kind of theft. Using this attack it can also make roaming fraud for paying service. The intruder sends signaling and/or user data to the network, in an attempt to make the network believe they originate from the target user. The intruder can also eavesdrop signaling and data connections associated with other users. Or even worse, the intruder can send signaling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network. Therefore, fake base station attack is a privacy threat to UEs. We are exploring a low-cost cross-layer solution to this problem.

III. SOLUTION

In this section, we present the design of our protocol and how it is implemented in NS3 [6].

A. Introduction to the Solution Strategy

In the traditional design, UE RRC layer conducts measurement reporting (e.g., Base Station ID and received signal strength), adjust clock to

synchronize with base station and issue connection request to the base station etc. The drawback of traditional design is that the UE issues connection request to the base station with the strongest received signal strength and lacks of the functionality that identifying genuine base station and fake base station. In our design, the UE RRC layer maintains a base station lookup table, which periodically records the signal strength of base stations around. In order to identify fake and/or genuine base stations, the UE needs to request the network id of the base station and counts the number of base stations in each network. After collect all the information, the UE uses two strategies to identify genuine base stations, majority vote on the number of base stations in each network and selection on base station with strongest received signal strength when two genuine networks contain the same number of base stations.

B. Protocol

1) Protocol Diagram

The cross-layer design of UE is illustrated in Fig.1. The new features added to identify fake base stations are highlighted. Initially, the UE listens to the broadcast information from each base station. Once it collects all the base station ID and received power it tries to synchronize to each base station. Similarly to a OTDOA procedure, a E-CID procedure is initiated through the LTE Position Protocol (LPP) by the network, with a ECID-RequestLocationInformation request message. The UE performs and collects the necessary measurements, and reports them back using the ECID-ProvideLocationInformation. This message contains the base station ID of the base station, RSRP (reference signals received power) measurement, and RSRQ (reference signals received quality) measurement.

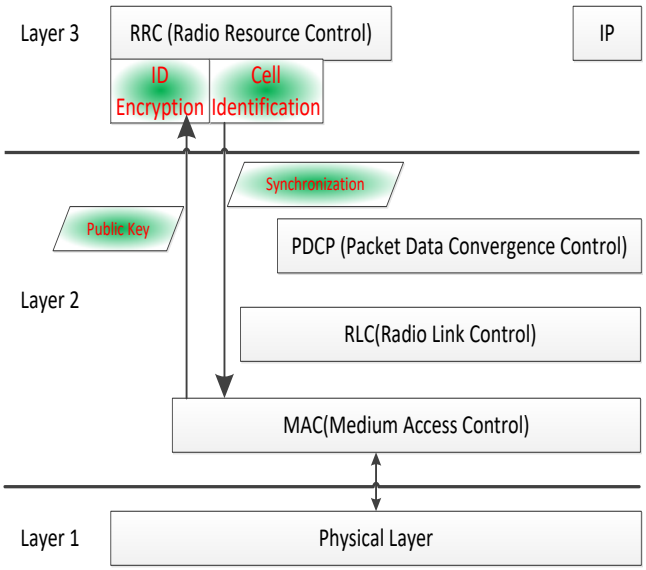

Figure 1: Cross-layer design on UE side.

To get further information, e.g., network ID from System Information Block 1(SIB1), the UE needs to synchronize with the base station. The UE maintains a table that records the base station id, the power and a zero network id by requesting location information message. After building up the table, the UE tries to synchronize to each unauthorized base station. After the synchronization, the UE can know the network id of the synchronized base station. After the UE is synchronized with all base stations, it calculates and removes the fake base station based on the network ID and power.

2) Protocol Description

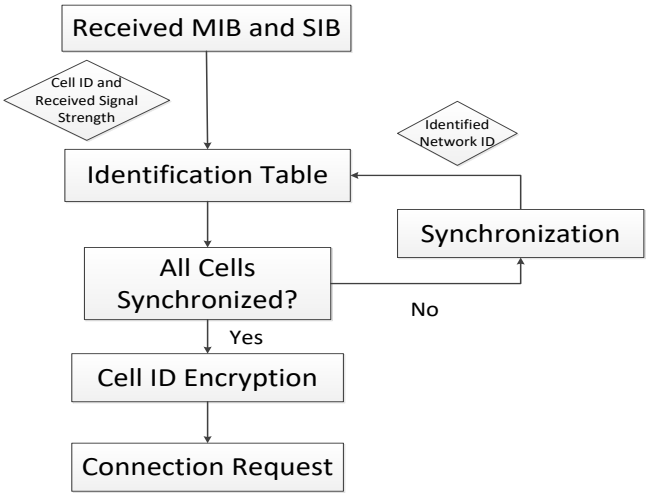

Figure 2: Control Flow.

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). To further request the network ID of a particular base station, UE needs to synchronize to that base station. All collect the entire base station ID and signal strength, the UE RRC layer put all the information into the identification table. Further, UE will try to synchronize each base station. After all the process done, we say that the identification is complete. The UE scans over the identification table to count the number of base stations belong to each network. 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. If there are two or more networks that have the same most number of base stations, the UE treats all of them as genuine base stations and it will send connection request to the one with the strongest signal strength. An illustration is shown in Fig. 2. 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, we use encryption and decryption technique to encrypt the UE ID on the UE side and decrypt the UE ID on the eNB side. The malicious attacker is not able to decode the UE ID as it has no access to the private key, which is being held by the eNB only. In this process, the eNB broadcasts the public key all the UEs who are going to send connection request. Public key is known to anyone, including the malicious attacker. Even if the attacker gets the public key; the attacker cannot decrypt the UE ID as it is not possible to derive the private key based on public key. Only the user holding the private key can decode the information encrypted by the paired public key. After receiving the public key from the eNB, the UE trusts the public key as it already identified all the base stations, and then it encrypts the public key with the UE ID. Instead of sending the UE in plain text, the UE sends the encrypted UE ID to the eNB. After receiving the encrypted UE ID, the eNB can decrypt the UE ID by the paired private key. The OpenSSL project is an Open Source toolkit implementing the Secure Sockets

Layer (SSL) and Transport Layer Security (TLS) protocol. We link the OpenSSL library into NS3 simulator so that NS3 can use OpenSSL library to conduct key generation, encryption and decryption operations etc. In the process of key generation, the function returns a pair of keys, the public key and private key. The eNB sends out the public key to the UE and keeps private key itself. After receiving the encrypted UE ID from the UE, the eNB decrypts the UE ID by the private key.

IV. EVALUATION BY SIMULATION

A. Abbreviations from LTE and NS3

We implement the proposed protocol on NS3 LTE module. NS3 is a 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 WiFi, WiMAX and LTE for layer 1, 2 and 3 and a variety of static or dynamic routing protocols. Our implementation falls in the LTE module. Specifically, the UE identification table is implemented in the RRC layer of LTE module UE component. The related modifications, e.g., sending the public key from physical layer to RRC layer, are happened in each layer that are delivering the packet data to RRC layer. We use OpenSSL to generate key pairs in LTE module eNB components.

B. Steps Involved in Implementation of the Simulation Model

In our evaluation, we set the real base stations into different networks. Usually there are several real base stations can be sensed by the UE from the same network. There is usually one fake base station due to deployment cost. We randomly set all the base stations into different coordinates in a grid topology. The base station will periodically broadcast master system information to nearby UEs. We use the default frequency band of LTE module of ns3 (we need to check the code if the specific frequency number matters). We set the UE to a random coordinate and start its attach process from the start of the simulation. The results show that the UE can always identify the fake base stations and send the IMSI in encrypted text to the best real base station.

V. RESULTS

A. Exercising the Simulation Model

An example log from NS3 when identifying fake base station is illustrated below.

Step 1: Add Networks and base stations
Add GenuineNetwork ID:1, base station/base station ID:1
Add GenuineNetwork ID:1, base station/base station ID:2
Add GenuineNetwork ID:1, base station/base station ID:3
Add GenuineNetwork ID:1, base station/base station ID:4
Add GenuineNetwork ID:2, base station/base station ID:5
Add GenuineNetwork ID:2, base station/base station ID:6
Add GenuineNetwork ID:2, base station/base station ID:7
Add GenuineNetwork ID:2, base station/base station ID:8
Add fake network ID:100, base station/base station ID:9
Add fake network ID:101, base station/base station ID:10
Step 2: Measure base station Power^A_a
LOG LteUeRrc::SaveUeMeasurement: measured base station 1, power in dbm -59.7603
LOG LteUeRrc::SaveUeMeasurement: measured base station 2, power in dbm -65.7809
LOG LteUeRrc::SaveUeMeasurement: measured base station 3, power in dbm -69.3027
LOG LteUeRrc::SaveUeMeasurement: measured base station 4, power in dbm -71.8015
LOG LteUeRrc::SaveUeMeasurement: measured base station 5, power in dbm -73.7397
LOG LteUeRrc::SaveUeMeasurement: measured base station 6, power in dbm -75.3233
LOG LteUeRrc::SaveUeMeasurement: measured base station 7, power in dbm -76.6623
LOG LteUeRrc::SaveUeMeasurement: measured base station 8, power in dbm -77.8221
LOG LteUeRrc::SaveUeMeasurement: measured base station 9, power in dbm -78.8452
LOG LteUeRrc::SaveUeMeasurement: measured base station 10, power in dbm -79.7603
Step 3: Synchronize to each base station to get network id
LOG LteUeRrc::SynchronizeToUnauthorizedCell: synchronize to unauthorized base station: 10
LOG LteUeRrc::DoRecvSystemInformationBlockTyp1: receive SIB1 from base station:10, network id:101
LOG LteUeRrc::SynchronizeToUnauthorizedCell: synchronize to unauthorized base station: 9
LOG LteUeRrc::DoRecvSystemInformationBlockTyp1: receive SIB1 from base station:9, network id:100
LOG LteUeRrc::SynchronizeToUnauthorizedCell: synchronize to unauthorized base station: 8
LOG LteUeRrc::DoRecvSystemInformationBlockTyp1: receive SIB1 from base station:8, network id:2
.....
Step 4: Select the best network and best base station
LOG LteUeRrc::SynchronizeToUnauthorizedCell: all base stations have been authorized
LOG LteUeRrc::RemoveFakeCells: Find the best network: 1 with 4 base stations
LOG LteUeRrc::DoRecvSystemInformationBlockTyp1: receive SIB1 from base station:1, network id:1
LOG LteUeRrc::EvaluateCellForSelection: base station:1 with network id:1 is the best to connect
Step 5: Send encrypted ID to connect
LOG UeMemberLteUeCmacSapUser::SetPublicKey: receive public key:
|{BEGIN PUBLIC KEY|{
MIIBIjANBgkqhkiG9w0BAQEF
AA

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

OCAQ8AMIIBCgKCAQEAy8Dbv8pr
pJa0kKhlGeJYozo2t60EG8L056
1g13R29LvMR5hyvGZlGJpmn65+
A4xHXInJYiPuKzrKUnApeLZ+vw
1HocOAZtWK0z3r26uA8kQYOKX9
QtdDbCdvsF9wF8gRK0ptx9M6R1
3NvBxvVQApfc9jB9nTzphOgM4J
iEYvlV8FLhg9yZovMYd6Wwf3ao
XK891VQxTrrkQYoq1Yp+68i6T4
nNq7NWC+UNVjQHxNQMQMzU6lWC
X8zyg3yH88OAQkUXIXKfQ+NkvY
Q1cxaMoVPpY72+eVthKzpMeyHk
Bn7ciumk5qgLTEJAfWZpe4f4eF
ZjrRc8Y8Jj2IS5kVPjUywQIDAQAB
|{END PUBLIC KEY|{
LOG LteUeRrc::DoNotifyRandomAccessSuccessful: send connection request to base station:1 real UE ID:1
LOG LteUeRrc::DoNotifyRandomAccessSuccessful: send connection request to base station:1, with encrypted UE ID: < some random characters>
Step 6: eNB receive the encrypted ID and decode
LOG UeManager::RecvRrcConnectionRequest: receive < some random characters>
LOG UeManager::RecvRrcConnectionRequest Decrypted ID =1

B. Various Attack Scenarios

We use different simulation set up to test the feasibility of our design. The results are shown in Table 1.
We vary the number of fake base stations (FBS). All the fake base stations can be successfully identified by our approach.

Table 1: Simulation Set Up

NO.	FBS	Real BS	All FBS identified
1	1	4	Yes
2	2	4	Yes
3	3	4	Yes
4	4	4	Yes

VI. 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 identifies fake base station in synchronization stage. There are several advantages for our solution. First, we identify fake base station in synchronization stage, which avoids the UE connection 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.

VII. RELATED WORK

A. Fake Base Station Attack

[11] reveals that IMSI catcher is an universal problem that the IMSI can be easily cached by a fake base station or man-in-the-middle attack. [1] makes use of formal symbolic analysis to discover some vulnerabilities in existing solutions. It also proposes to use encryption to protect IMSI. [5] illustrates how a fake base station can behave as repeater and can transmit some requests in the network. [7] propose a practical attack to build a rouge base station to gain full control over the victim's data communications. [10] shows that a fake base station can be built based on software radio.

B. Fake Base Station Detection

[2] estimates an approximate distance between a subscriber's device and the deployed femtocell. A subscriber can confirm whether or not the femtocell he connected with is physically-present. [9] detects rouge base station using Matlab. The basic idea is to scan all the SNR and sensitivities of frequencies over all base stations. [4] introduces two-way authentication and key agreement mechanism to protect subscriber privacy and security. [8] reviews mobility and security issues with the focus of key management in SAE/LTE and present possible solutions and analysis. Different existing approaches, our protocol identify the fake base stations in the synchronization stage and avoid two-way authentication, so that the protocol can be gradually deployed and the privacy of the user can be preserved.

REFERENCES

[1] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar. New privacy issues in mobile telephony: _x 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. Sun. Eliminating rouge femtocells based on distance bounding protocol and geographic information. Expert Systems with Applications, 2014.
[3] N. Golde, K. Redon, and R. Borgaonkar. Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In NDSS, 2012.
[4] 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.
[5] 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.
[6] N. L. module. http://www.nsnam.org/docs/models/html/lte.html.
[7] D. Perez and J. Pico. A practical attack against gprs/edge/umts/hspa mobile data communications.
[8] A. R. Prasad, J. Laganier, A. Zugenmaier, M. S. Bargh, B. Hulsebosch, H. Eertink, G. Heijenk, and J. Idserda. Mobility and key management in sae/lte. In Wireless Communications 2007 CNIT Thyrrenian Symposium. Springer, 2007.
[9] R. Singh and S. Singh. Detection of rogue base station using matlab. International journal of Soft Computing and Engineering, 2011.
[10] Y. Song, K. Zhou, and X. Chen. Fake bts attacks of gsm system on software radio platform. Journal of Networks, 2012.
[11] D. Strobel. Imsi catcher. 2007.