Regular Paper

Communications of the CCISA
Vol. 27 No. 1 Feb. 2021

Overview of Cyberattacks Against Radio Access Networks in Long-term Evolution Mobile Networks and Defense Solutions

Ruei-Hau Hsu[1*], Onkar Mumbrekar[2]
Computer Science and Engineering, National Sun Yat-sen University
[1] rhhsu@mail.cse.nsysu.edu.tw, [2] onkar.mumbrekar@gmail.com

Abstract

Mobile communication standard has been extensively developed to introduce many more connected devices for the Internet of Things (IoT). However, the vulnerability of radio access network (RAN) in long-term evolution (LTE) would impact the security of IoT applications by LTE. RAN transmits/receives data over the air interface and is vulnerable to many active and passive attacks as RAN procedures typically occur before any security establishment. With the growth in devices connecting to the Internet, massive-scale attacks would be easier for the attackers to execute. This work practices those attacks against certain individual telecommunication service providers (TSPs) in Taiwan with various kinds of mobile devices. The potential solutions against the attacks in RAN are also introduced for the defense in this work.

Keywords: Long-Term Evolution, 5G, Radio Access Network, Model Checking, Intrusion Detection, Misuse Detection, Cyberattacks

* Ruei-Hau Hsu (Corresponding author.)

1. Introduction

1.1 Motivation

Cellular network security is critical for the nation's security as it affects everything from communication, businesses, transportation, healthcare and many more. Devices in these networks are increasing day by day. With the involvement of the Internet of Things (IoT) more devices will get attached to these networks. Such a network with devices of high computation capabilities creates the perfect environment for the attacker to exploit and take over.

With the advancement in technology, the tools used by these attackers are getting more affordable. Stingrays or cell-site simulators are one of them, which can identify the user's location or capture extremely critical data such as International mobile subscriber identity (IMSI) or any unencrypted data over this network, which can be misused by an attacker with malicious intent and resources to cause immense problems.

Some of the real-world examples include 2018's Hawaii fake broadcast where ballistic missile alert was issued via Emergency Alert System and Commercial Mobile Alert System over cellular networks [16]. This kind of fake alarms can cause huge chaos in people.

Here are some potential attack scenarios that can be caused by the attacker with resources such as stingrays and cell-site simulators:

- **Scenario 1:** IMSI is the permanent identity of a subscriber. It must be kept secret. To achieve this, LTE uses a Globally Unique Temporary Identifier (GUTI) which is used to identify subscribers. However, there are some situations like "TAU Request" where user discloses its IMSI. Disclosure of IMSI may cause the user to leak their location or other private information such as conversations. More strong attacks are also possible after retrieval of IMSI.
- **Scenario 2:** Location is considered private information of the user in the network. To give seamless and strong services to the user, mobile operators need to know the location of these users. An attacker can misuse the vulnerability to cause life-threatening consequences.
- **Scenario 3:** Attackers can execute jamming attacks because the radio network has a shared interface that is an air interface. The LTE network is vulnerable to "Radio Frequency jamming" in which an attacker prevents a legitimate user from making a network connection, "Spoofing" in which an attacker can imitate a real user, or "Sniffing" in which an attacker can obtain unencrypted data.
- **Scenario 4:** To manage radio resources efficiently and save the battery life of mobile devices, LTE allows reuse of the radio resources. Signaling messages which

are used for reassignment of the resources can be misused by an attacker to prevent legitimate users from connecting to the network.

- **Scenario 5:** Attacker can launch a series of attacks, such as location tracking, Denial of Service (DoS) or Man-in-the-middle attack using fake base stations created by affordable hardware or even personal base stations.

1.2 Contributions

This work focuses on the study of threats on the Radio Access Network (RAN). This work is looking at the main questions: what is the effect of RAN attacks on wireless networks and mobile devices? Why is it difficult to detect threats on mobile networks? How are we going to spot these attacks?

This work examined the effects of RAN attacks on various mobile devices and well-known Taiwanese cellular network operators. In order to examine the impact of these attacks, the author has carried out attacks on multiple devices and operators in order to assess the behavior of different operators and devices to the different attacks carried out. This work found that mobile devices have an influence on RAN attacks. This study carried out traditional radio network attacks using opensource LTE stacks and researched the impact of these attacks on different mobile devices and well-known Taiwanese cellular network operators.

1.3 Organization

The remainder of this study shall be organized in the following order. Section 2 will provide the reader with the background details required to understand this work. This background provides an overview of the cellular network, the types of intrusion detection, Model Checking, the methods used to detect attacks, and the open source software used to implement the device. Section 3 will set out the related work that has been done in this area. Section 4 will introduce the implementation of the famous attacks on LTE. Section 5 will present the proposed LTE attack detection system. The experimental findings will be analyzed in section 6 and, eventually, the paper will be concluded in section 7 with future directions.

2. Cellular Network

In December 2008, Long Term Evolution (LTE) was launched by Third Generation Partnership Project (3GPP) to provide a high rate of data and bandwidth, improved spectrum efficiency, and low latency compared to previous networks. LTE is often identified as the

Evolved Universal Terrestrial Access Network (E-UTRAN).

LTE came into existence due to a dramatic rise in cellular data consumption and the emergence of new services such as online video games and streaming media, which could not have been achieved by the previous Universal Mobile Terrestrial System (UMTS) technology. UMTS was indeed an enhancement of Global Mobile Communications System (GSM) and General Radio Service packet (GPRS) technologies

2.1 LTE Architecture

LTE network architecture is consisting of mainly three components: User Equipment (UE), evolved Node B (eNB), which is a core component of the radio access network or Evolved-Universal Terrestrial Radio Access Network (E-UTRAN) and Evolved Packet Core (EPC). These components, together known as the Evolved Packet System (EPS).

UE is a mobile device that consists of Universal Subscriber Identity Module (USIM), which stores International Mobile Subscriber Identity (IMSI), security algorithms, and other information such as home network identity. International Mobile Station Equipment Identity (IMEI) uniquely identifies UE.

E-UTRAN manages the radio communications between the UE and Evolved Packet Core (EPC). In LTE, the geographical area is divided into smaller hexagonal cells. Each cell is served by a single evolved base station, which is also called as evolved node B or eNodeB. Each eNodeB communicate with one or more UEs from one or more Cells.

EPC consist of the following components:

- The Home Subscriber Server (HSS) is a central database that contains UE's IMSI, IMEI, subscription data, and other relevant information such as cryptographic keys of all subscribers.
- The Packet Data Network Gateway (P-GW) communicates with the external network. Each package data network is identified by the access point name (APN).
- The Serving Gateway (S-GW) acts as a router that transmits data between the base station and the PDN gateway.
- Mobility Management Entities (MME) control advanced operations such as attach, paging, and detach of the UEs in a particular tracking area and also keeps track of locations of the UEs residing in its designated tracking area.
- The Policy Control and Charging Rules (PCRF) is responsible for policy control decisions and controls the flow-based charging.

2.2 Common LTE Procedures

The UE can first find a suitable cell by listening to message from nearby base stations, when it wants to connect with the network. If the UE identifies an appropriate cell, it initiates the Random Access (RA) procedure for obtaining info on the allocations and scheduling of uplink resources. The selected cell assigns the identifier to UE, known as the Temporary Cell Radio Network Temporary Identifier (C-RNTI). Using this temporary C-RNTI and uplink allocations, the UE seeks to create a Radio Resource Control (RRC) connection by transmitting the "RRC Connection Request". Upon receipt of the message, the eNB responds with the "RRC Connection Setup" including information on the distribution of radio resources and the significance of the C-RNTI to distinguish the UE for further coordination. Finally, the UE will complete the connection setup by sending the "RRC Connection Setup Complete" message.

1) **LTE Attach:** The UE must send the "Non-access Stratum (NAS) Attach request", through the "RRC Connection" to MME, after the UE is effectively attached to the nearby eNB. When this message is sent, the MME starts the process of Authentication and Key Agreement (AKA) by replying with an authentication vector created by HSS. By sending a "NAS authentication response" the UE authenticates MME. The MME picks encryption and integrity protection algorithms to be used in the key agreement, following mutual authentication, and transfers the "NAS Security Mode Command" to the UE to inform selected algorithms. The UE produces the security keys of the NAS layer when this message is sent. Finally, the MME may grant a Global Temporary Unique Identity (GUTI) to replace the IMSI permanent identity. Following exchange of optional NAS and RRC layer configurations, MME sends a message "NAS Attach Accept" with GUTI and other connection information. Finally, to complete the connection process, UE sends a "NAS Attach Complete" message.
2) **LTE Detach:** In certain cases, UE disconnect from the network after using services. In other situations, it may be disconnected by the network while still accessing services and may no longer be able to stay connected to the network. Once a UE is removed from the network, it needs to release all network / radio resources allocated to the EPS session and radio bearers. Both UE and Network can request detach. The detach triggered from the network is caused either by MME or HSS. UE or network expects detach accept message to complete the detach process.
3) **LTE Tracking Area Update:** The procedure for Tracking Area Update (TAU) may be normal, periodic, or combined. Normal TAU is started when the UE attaches itself to the cell in a different area of tracking. Periodic TAU is controlled

in the "NAS Attach Accept" message by tracking area update timer which the network sends to UE. When the UE connected to both the EPS and non-EPS systems detects a specific tracking area not included in the MME list of previously reported tracking areas, Combined TAU is initiated. The TAU procedure begins when UE initiates the "NAS Tracking Area Update Request" which contains existing GUTI or IMSI, and the last identifier of the tracking area visited. The network responds with "NAS Tracking Area Update Accept" after receiving this message which provides new GUTI. In some cases, the network also replies with "NAS Tracking Area Update Reject," which includes the network's cause for rejection.

2.3 Intrusion Detection System

Intrusion is any attempt to compromise the system, which includes both failed and successful attempts made to compromise a particular system [3].

An Intrusion Detection System (IDS) is a device or application that monitors a network or system logs for malicious activity or policy violations. Any malicious activity or rule violation leads to an alarm. Intrusion prevention systems (IPS) are extended versions of IDS, which also try to mitigate the attack.

An intrusion detection system (IDS) functions by monitoring all the activities on network or host, analyzing all events to find patterns based on known attacks or deviation from known behavior of the system. It differs from the traditional firewall as a firewall only tries to block the traffic based on a specified set of rules which allow or deny network connections. But on the other hand, IDS tends to alarm when malicious activity happened at the network or within the system itself.

Based on the source of information, IDS can be broadly classified into three categories: network-based, host-based, and hybrid IDS [12].

- Network intrusion detection systems (NIDS): NIDS is a system that monitors network traffic for possible malicious activity.
- Host-based intrusion detection systems (HIDS): HIDS is a system that monitors malicious activities within the host system.
- Hybrid intrusion detection systems (Hybrid-IDS): Hybrid IDS is a system that monitors malicious activities on both network and host.

The IDS may also be categorized as a Network Node Intrusion Detection System (NNIDS) or a Wireless IDS (WIDS) depending on the type of data source being handled by a specific IDS [1].

2.4 Types of Detection Methodology

There are mainly two detection methodologies that are followed by the IDS to detect an attack, which is the Misuse and Anomaly approach.

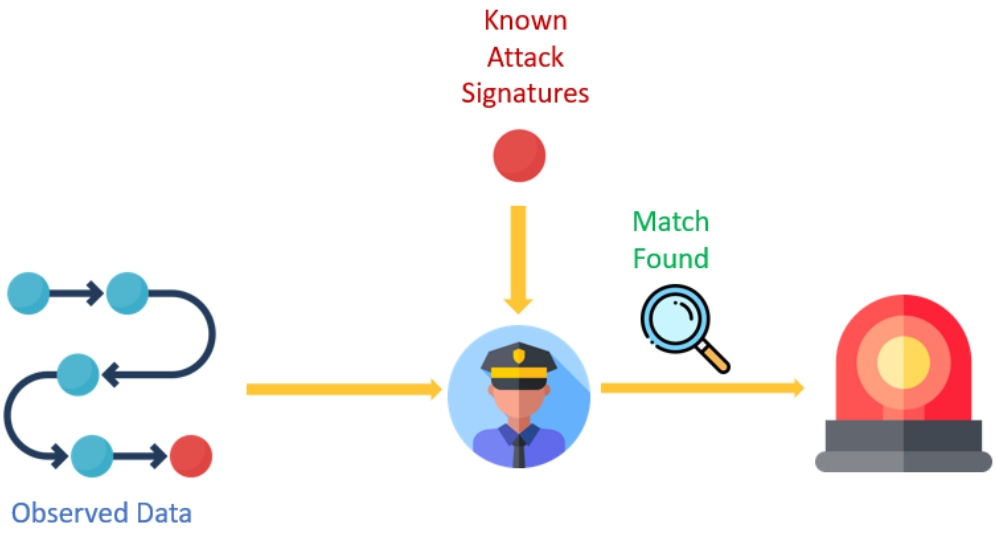

Figure 1: Misuse detection.

- **Misuse detection:** As mentioned in Figure 1, Misuse Detection approach utilizes knowledge of known attacks to detect the attack, which can be further classified as rule-based or signature-based. Rule-based misuse detection uses "if-then rules" to trigger the alarm; on the other hand, the signature-based method matches the known attack signature to the monitored event to detect the attack. Misuse detection has one flaw that it cannot detect unknown attacks, but it has very few false alarms

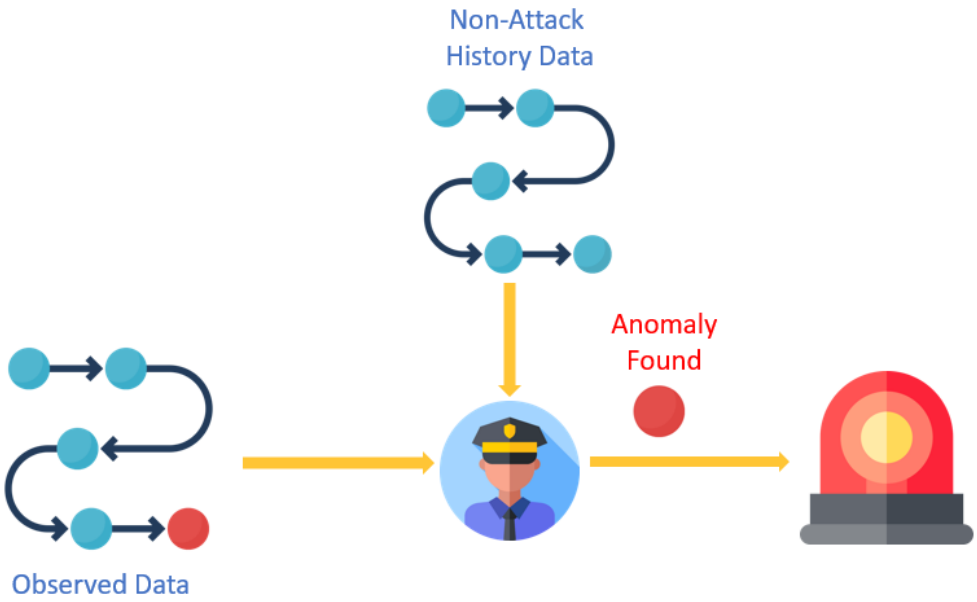

Figure 2: Anomaly Detection.

- **Anomaly Detection:** Anomaly-based IDS can be used to detect unknown attacks on the cost of a very high number of false alarms. As shown in Figure 2, Anomaly detection creates a generic behavior pattern called a trustworthy system profile, and any event that violates this system profile is classified as an attack. Anomaly detection needs a large amount of data and processing to correctly define a trustworthy system profile. These profiles can be created in various ways, such as by measuring certain variables, which is a statistical way, specifying rules for allowed behavior, which is the rule-based approach, or creating a model of trustworthy behavior, which is the model-based approach.

2.5 Discussion

As shown in the last module that there are many types of IDS. Before those IDS systems can be used to detect the attacks in RAN, one may need to figure out the actual steps of attacks that can be practiced against specified telecommunication operators. By the concrete steps, we can know further how the attacks can be captured.

3. Related Works

Further, this work introduces some pieces of literature which tried to analyze LTE

specification and performed adversarial testing to reveal multiple vulnerabilities. A Model based testing methodology [7] has been suggested to combine a NuSMV [18] Symbolic Model Checker and a Cryptographic Protocol Verifier to reveal weaknesses in the LTE specification. To incorporate with this method, the researcher has extensively researched the LTE requirements and developed a model utilizing a Tamarin Checker [23]. The author also uses this framework to show an attack scenario. The researcher evaluated these attack simulations on the open-source testbed [19]. The author was able to discover a reasonable amount of 19 attacks utilizing this method. While the author's contribution is intriguing, the author's method may not include real-time traffic because the author has carried out attacks identified via the model manually. The author's research focuses primarily on the detection of bugs by analyzing a malicious attacker model system.

Another work related to the testing of the LTE specification is proposed by Kim et al. [9]. In this work, the author has proposed a semi-automated testing tool [17] to dynamically test the LTE operational network. The researcher has deployed a method utilizing open-source LTE [22] tools to create and forward test cases to the target network. Further, user-side network traffic log is used to classify the problematic behavior.

To create test cases, the author used Victim UE control plane logs and performed alterations such as changing plain text, sending plain text instead of protected text, or replaying messages after a specified time to check the behavior of the network and the victim. The consequence of the attack is often to deny LTE services to legitimate customers, to spoof SMS or to monitor/modify user network traffic. The author has presented root cause analysis and possible countermeasures.

As per report published [5][14] IMSI Disclosure and Position Tracking attacks abuse false base station and a principal authentication and protocol (AKA). Rao et al. [11] designed an IMSI capturing technique in which an attacker could abuse the SMS procedure. An attacker must have a valid connection to the LTE network. IMSI can be obtained with the help of the Mobile Station International Subscriber Directory Number and Diameter Routing Agents address. The author also used this IMSI to identify the location of the device, where the attacker could act as the Home Subscriber Server (HSS) and send the Insert-Subscriber-Data-Request (IDR) to MME to request the UE EPS location information that contains Cell Identity (CI), Location Area Identity (LAI), and Service Area Identity (SAI). An attacker can also send the User-Data-Request (UDR) to HSS by acting as an IMS application to get the Location Area ID and Cell ID. Holtmanns et al. [6] have introduced a procedure in which IMSI can be captured using MSISDN. In this case, an attacker acts as a Short Message Service Center and sends commands to the victim's service provider with MSISDN. However, after signaling messages, the attackers can get the IMSI of the victim and track down the user. [4] IMSI Catchers have

also been used in mobile networks to identify and listen to phones. Shaik et al. [13] suggested the victim's IMSI could leak with the victim's phone number and paging protocol. Radio Frequency (RF) jamming, sniffing, and sniffing attacks surveyed in [5] indicated that synchronization signals such as the primary synchronization signal, as well as the secondary synchronization signal could be produced and transported regularly by attackers using a counterfeit cell to avoid UE from connecting to a valid cell. Other Physical Broadcast Channel (PBCH) and Physical Control Format Indicator Channel (PCFICH) can also be jammed as they provide useful information for more damaging attacks. An attacker can also use the Jam Physical Uplink Control Channel (PUCCH) as it is situated at the edge of the system bandwidth and can be used to disrupt the uplink channel so that PUCCH jamming is very useful and effortless. Most commonly attackers attack Physical Random-Access Channel (PRACH) by launching a counterfeit cell tower that pretends to be a legitimate cell tower prevents existing subscribers from communicating to the tower. The [5] Denial of Service (DoS) and Distributed DoS (DDOS) security threats are the most common and serious aimed at exhausting the network's Radio Resources. LTE resources are not only limited but also harmful to the user's battery if the connection status is maintained in the RRC. Its provision of services to all subscribers at the same time as LTE performs a reassignment of radio resources. To do this, it uses a radio carrier between user equipment and the core network to transfer data. LTE also uses signaling called random access to release and reassign resources to another UE. Numerous control signals are produced as part of the bearer setup as well as release process. Uncontrolled transmission of such control packets can lead to traffic congestion and cripple network services. Bassil et al. [2] explained that repeated setup and release messages from a group of malicious attackers could result in network resource depletion and network service degrading. The pieces mentioned above of literature focused solely on attacking the LTE system to find vulnerabilities. The countermeasures proposed have not been tested by the authors. In such a vulnerable environment, secure communication is need of the hour to ensure that sturdy intrusion detection and prevention system (IDPS) is required to recognize this type of attack and alarm or prevent such attacks by changing some parameters.

4. Implemented Attacks on Radio Access Network

4.1 Authentication Reject Attack AKA Numb Attack:

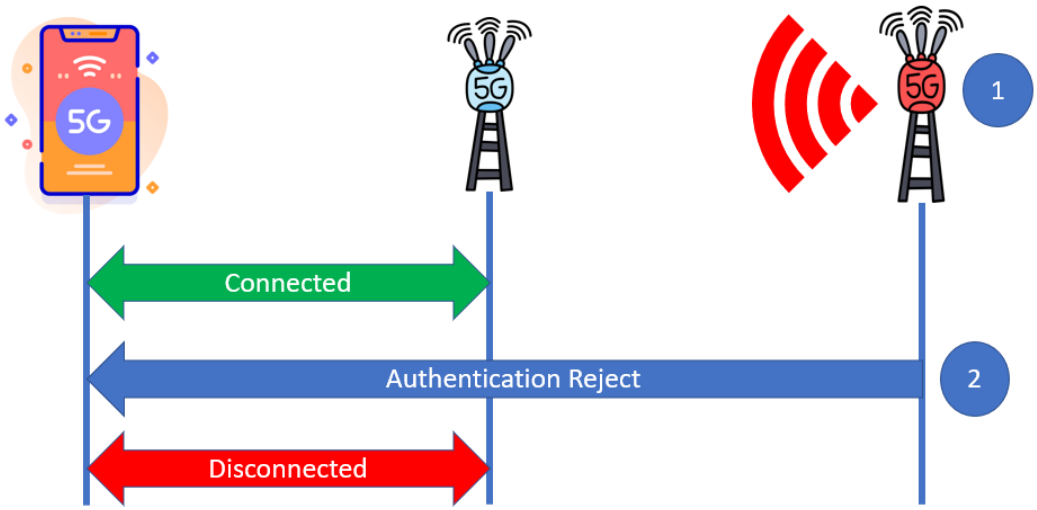

Figure 4: Numb attack

This attack as shown in Figure 4 was introduced in [7]. In this attack, the attacker injects out of sync "Authentication Reject" message using rogue eNodeB. Upon reception of "Authentication Reject" messages, UE aborts signaling procedure, and Enter in EMM-DEREGISTERED mode. UE also deletes any stored GUTI, TAI list [25]. This attack causes UE to detach from serving network completely, UE does not even try to reconnect with the network again only possible way to regain connection is to reinsert the sim card or toggle flight mode.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victim does not send Authentication_response to base station.
3) Victim Receives Authentication_reject.

This work obtains the atomic propositions for Authentication Reject Attack AKA Numb Attack in accordance with the principles and essential steps. LTL formula for Numb Attack based on temporal relations between the atomic actions is as follows:

$$\varphi Numb = Fakebasestation \wedge \neg send.authentication\_r\ \ esponse \wedge \bigcirc receive.authentication\_reject$$

In order to implement this attack, the author has used OpenLTE [20] as a rogue base station.

OpenLTE provides a state machine to manage responses from UE. OpenLTE also includes code for "Authentication Reject" message. The author has replaced attach state machine with a single response that is, "Authentication Reject" messages. Which causes a rogue base station to send "Authentication Reject" messages whenever UE sends attach request to the rogue base station.

4.2 AKA Bypass Attack:

In LTE Authentication and key Exchange (AKA) procedure is very important procedure as it satisfies a key role in verification of both parties in communication. After UE is successfully attached whenever UE sends "Service Request" network uses previous context to authenticate UE. However, if attacker bypass this procedure by sending "RRC Reconfiguration Request" as shown in Figure 5, then attacker can get all the messages in plaintext.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victim does not send Authentication_response to base station.
3) Victim Receives Authentication_reject.

The following LTL formula for AKAbypass can be given as follows, based on the concepts, critical steps and the temporal relationships between the atomic propositions:

$$\varphi AKABypass = Fakebasestation \wedge send.Service\_Request \wedge (receive.RRC\_Reconfiguration\_Request)$$

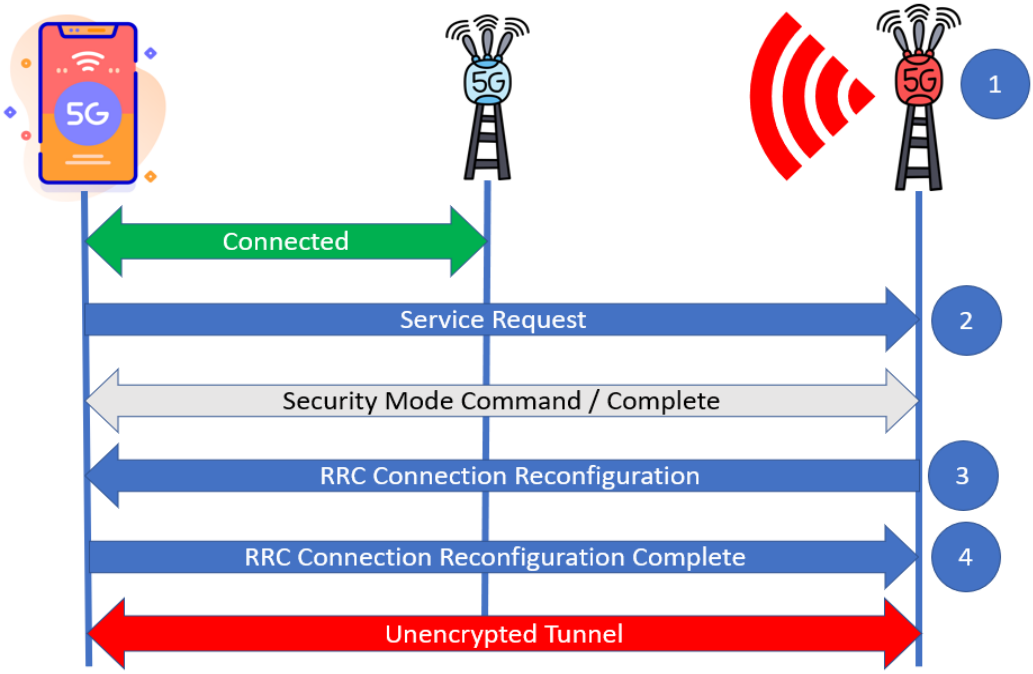

Figure 5: AKA Bypass

4.3 Tracking Area Update Reject:

This attack was mentioned in [13]. When UE moves to the different tracking area, UE initiates the "Tracking Area Update Request". On which network might respond with "Tracking Area Update Reject". This message is sent in plaintext, which can be misused by an attacker.

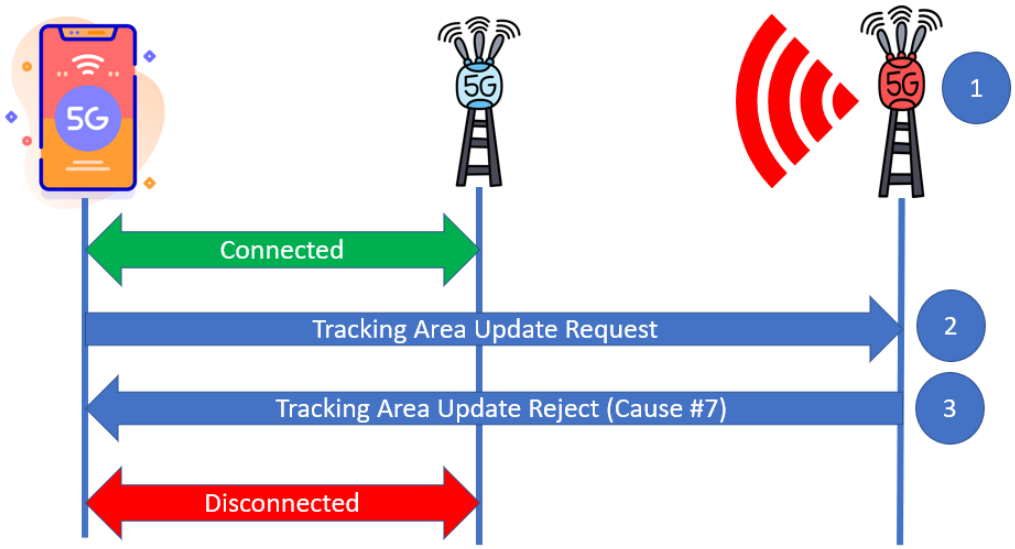

Figure 6: Tracking Area Update Reject

As shown in Figure 6, attacker setup rogue eNodeB with higher signal strength and same PLMN as serving eNodeB but with different Tracking area code. UE gets connected to rogue enb and initiates the "Tracking Area Update" procedure by sending the "Tracking Area Update Request" message. Upon reception of this message rogue base station immediately sends the "Tracking Area Update Reject" message. "Tracking Area Update Reject" allows the network to provide the cause of the rejection. Attackers misuse this field to deny EPS and non EPS services for the UE.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victim sends "TAU Request" to base station.
3) Victim Receives "TAU Reject" with following causes, \#7 "EPS services not allowed", \#8 "EPS services and non-EPS services not allowed", \#15 "No suitable cells In tracking area".

This work obtains the atomic propositions for TAU Reject attack in accordance with the principles and essential steps. LTL formula for TAU Reject attack based on temporal relations between the atomic actions is as follows:

$$\varphi TAUReject = Fake\ base\ station \wedge send.TAU\_Request \wedge \bigcirc (receive.TAU\_reject \wedge receive.cause.7 \vee receive.cause.8 \vee receive.cause.15)'$$

4.4 Attach Reject Attack:

This attack was mentioned in [13]. Like "Tracking Area Update Reject Attack", "Attach Reject" message also provides field which is used by network to provide cause of rejection. Attackers misuse this field to deny EPS and non-EPS services for the UE.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victim sends "TAU Request" to base station.
3) Victim receives "Attach Reject" with following causes, #7 "EPS services not allowed", #8 "EPS services and non-EPS services not allowed", #15 "No suitable cells in tracking area".

4.5 Service Reject Attack:

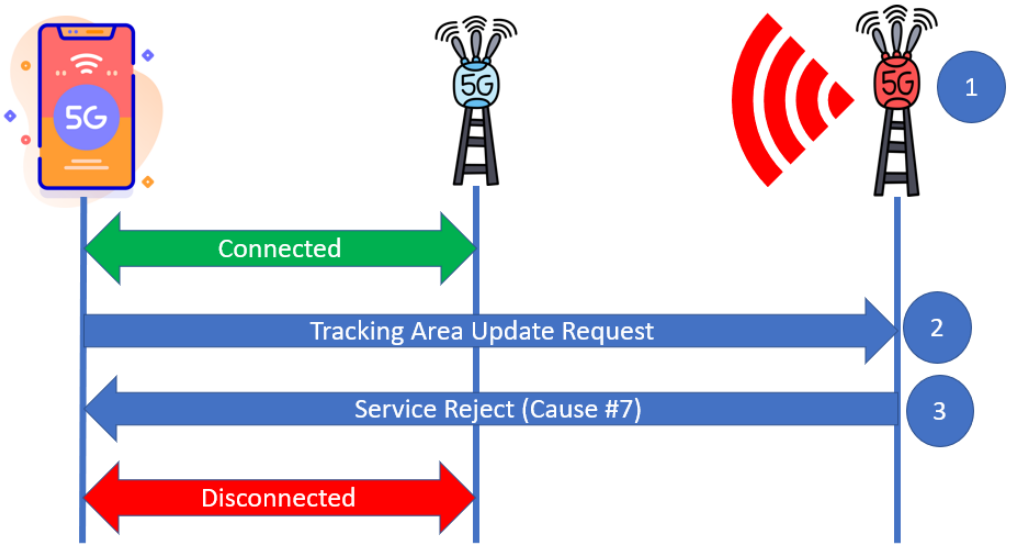

Figure 7: Service reject attack

This attack was mentioned in [13]. Like "Tracking Area Update Reject Attack", "Service Reject" message also provides field which is used by network to provide cause of rejection. Attackers misuse this field to deny EPS and non-EPS services for the UE.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victim sends "TAU Request" to base station.
3) Victim receives "Service Reject" with following causes, #7 "EPS services not allowed", #8 "EPS services and non-EPS services not allowed", #15 "No suitable cells in tracking area".

4.6 Detach Request Attack:

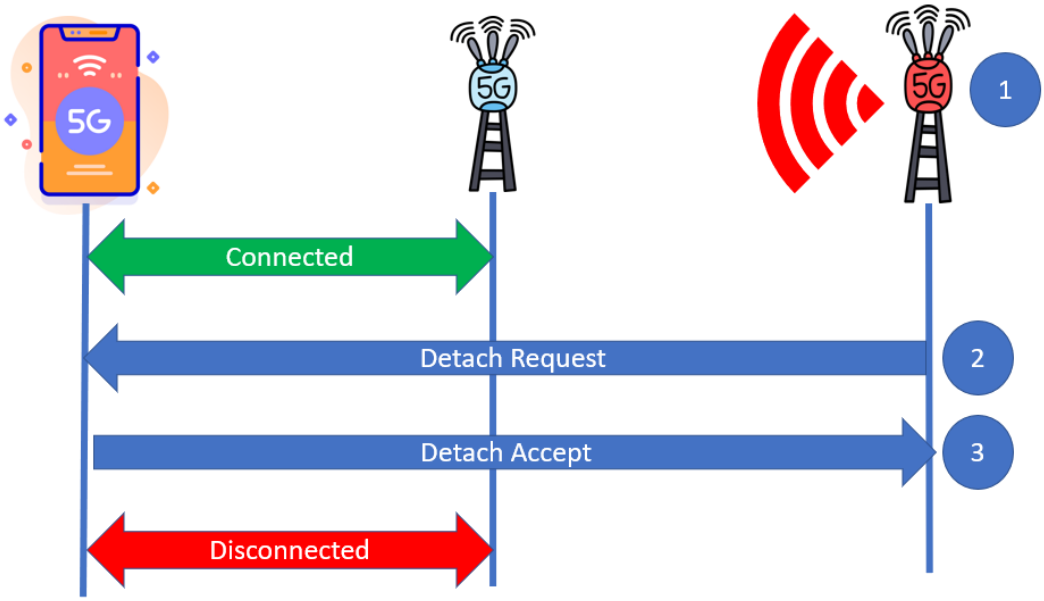

Figure 8: Detach request attack flow.

This attack as shown in Figure 8 was introduced in [7]. Both UE and network can initiate detach request. Further, if UE is detached from the network, it needs to release all the network resources. The attacker takes advantage of this consequence and as shown in Figure 8 sends the "Detach Request" message mimicking the serving network. After receiving this message, UE releases all the radio resources.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victim receives "Detach Request".

4.7 IMSI capture Attack:

This attack was mentioned in [13]. IMSI capture attack is the most straightforward attack to implement. In this attack, the attacker lures the UE to connect to it by using higher signal strength. When UE gets connected to the rogue base station, UE sends an "Attach Request" message. Upon reception of the "Attach Request" message, the rogue base station sends "Identity Request" message in plaintext. Upon reception of the identity request from the rogue base station, UE responds with an "Identity Response" message which contains the IMSI in plaintext.

Critical steps may be stated as follows:

1) Fake base station with higher signal strength.
2) Victims send "Attach Request".
3) Victim receives "Identity Request".

5. Conclusion

This work implemented famous attacks on LTE and tested on well-known mobile operators in Taiwan. Also, proposed detection system which combines machine learning and model checking to detect RAN attacks implemented in this study. The detailed steps of the attacks in RAN are also disclosed for the future study of detection technology.

Acknowledgment

This work was partially supported by the Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU), in part by the Ministry of Science and Technology of Taiwan under Grant MOST 108-2221-E-033, in part by the Information Security Research Center, National Sun Yat-sen University, Taiwan.

References

[1] K. A. Al-Enezi, I. F. Al-Shaikhli, A. R. Al-Kandari and L. Z. Al-Tayyar, “A Survey of Intrusion Detection System Using Case Study Kuwait Governments Entities,” 2014 3rd International Conference on Advanced Computer Science Applications and Technologies, Amman, 2014, pp. 37-43.

[2] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi, “Signaling oriented denial of service on

lte networks," Oct 2012 pp. 153–158.

[3] B. S. Bhati and C. S. Rai, "A Survey on Intrusion Detection Tools," 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2019, pp. 806-810.

[4] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," in Proceedings of the 30th Annual Computer Security Applications Conference, 2014, p. 246–255.

[5] L. He, Z. Yan and M. Atiquzzaman, "LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey," in IEEE Access, vol. 6, 2018 pp. 4220-4242.

[6] S. Holtmanns, S. P. Rao and I. Oliver, "User location tracking attacks for LTE networks using the interworking functionality," 2016 IFIP Networking Conference (IFIP Networking) and Workshops, Vienna, 2016, pp. 315-322.

[7] S. R. Hussain, O. Chowdhury, S. Mehnaz and E. Bertino. "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE." NDSS 2018.

[8] J. Jin, C. Lian, and M. Xu, "Rogue base station detection using a machine learning approach," Proceedings of 28th Wireless and Optical Communications Conference ,2019, pp. 1–5.

[9] H. Kim, J. Lee, E. Lee and Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane," 2019 IEEE Symposium on Security and Privacy, 2019, pp. 1153-1168.

[10] Z. Li, W. Wang, C. Wilson, J. J. Chen, C. Qian, T. Jung, L. C. Zhang, K. Liu, X. Li, and Y. Liu, "Fbs-radar: Uncovering fake base stations at scale in the wild," in NDSS, 2017.

[11] S. P. Rao, B. T. Kotte, and S. Holtmanns, "Privacy in LTE Networks," in Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, 2016, p. 176–183.

[12] F. Sabahi and A. Movaghar, "Intrusion Detection: A Survey," 2008 Third International Conference on Systems and Networks Communications, 2008, pp. 23-26.

[13] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," Jan 2016.

[14] K. Vachhani, "Security Threats Against LTE Networks", SSCC 2018, Jan 2019, pp. 242–256.

[15] DataLogger, https://github.com/STRCWearlab/DataLogger.

[16] Hawaii false missile alert, 2018, https://en.wikipedia.org/wiki/2018H awaiifalsemissilealert.

[17] LTEFuzz, https://www.sites.google.com/view/ltefuzz.

[18] NuSMV: a new symbolic model checker, http://nusmv.fbk.eu.
[19] OpenAirInterface, https://www.openairinterface.org.
[20] OpenLTE, https://sourceforge.net/projects/openlte.
[21] SCAT: Signaling Collection and Analysis Tool, https://github.com/fgsect/scat.
[22] srsLTE, https://www.srslte.com,
[23] Tamarin Prover, https://tamarin-prover.github.io.
[24] Wireshark, https://www.wireshark.org/download.html.
[25] https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1072