Bitlis Eren Üniversitesi Fen Bilimleri Dergisi
BİTLİS EREN UNIVERSITY JOURNAL OF SCIENCE
ISSN: 2147-3129/e-ISSN: 2147-3188
VOLUME: 12 NO: 3 PAGE: 704-711 YEAR: 2023
DOI:10.17798/bitlisfen.1285270

Secure Handover Management Against False Base Station Attacks

Yerdos AMİRBEKOV[1], Elif BOZKAYA[2*]

[1]*National Defence University, Istanbul, Türkiye*
[2]*National Defence University Turkish Naval Academy, Istanbul, Türkiye*
(ORCID: 0000-0001-8117-3373) (ORCID: 0000-0001-6960-2585)

Keywords: False Base Stations, Measurement Report, Handover, 5G Networks, Man-in-the-Middle Attack.

Abstract
False Base Station attack raises concerns about data privacy during handover process in 5G networks. Broadcasting of measurement reports unveils the need for security assessment since a false base station can send a stronger signal to the User Equipment (UE) to establish a connection with itself. This may cause the leakage of information. Thus, a fundamental solution is to protect measurement reports with encryption algorithms. In this paper, we identify the security vulnerabilities of handover process and simulate a scenario, where a false base station is deployed and UEs can be connected to it during handover process. To prevent this, we propose a secure handover scheme to protect measurement reports by using two encryption algorithms; (i) Advanced Encryption Algorithm (AES)-256, and (ii) Rivest Cipher 4 (RC4) Algorithm. Then, we analyze the computation time and show the secure connection to a legitimate base station during the handover process.

1. Introduction

With the development of wireless networks, the traffic volume and the number of devices have been significantly increased. Consequently, new technologies, e.g., Software Defined Networks (SDN) [1], Network Function Virtualization (NFV) [2], edge computing [3], have become effective ways to meet the ever-increasing needs of mobile users. The radio communication Sector of ITU (ITU-R) has defined three usage scenarios for 2020 and beyond [4]: (i) Enhanced Mobile Broadband to focus on the increased data rates, a high number of users, and high traffic requests for hotspots (ii) Ultra Reliable and Low Latency Communications to meet Quality of Service (QoS) requirements such as latency, reliability, throughput, etc., and (iii) Massive Machine Type Communications to connect a large number of Internet of Things devices with low cost and long battery life.

To meet these stringent requirements of the new services and applications, 5G networks offer high QoS, higher data rates, and latency of less than one millisecond with the deployment of a large number of Access Points. In this case, one of the most important issues is the handover management for such ultra-dense networks due to user mobility. The handover procedure is the transfer of an ongoing service from one base station to another without interruption and with minimum delay. To facilitate this process, the Third Generation Partnership Project (3GPP) has proposed a measurement report containing frequency and power measurements to decide whether handover is necessary and which transmission is required [5]. Handover management is mainly based on the measurement report of the User Equipment (UE). The source base station triggers the handover procedure and sends it to the target base station. When the target base station receives and confirms the handover request, the source base station initiates the handover procedure. However, measurement reports are vulnerable to attacks, and the handover management is challenging due to the authentication complexity and requires high bandwidth.

Man-in-the-middle attack is one of the critical attacks that targets data confidentiality and integrity and can cause service interruption [6]. In this attack,

*Corresponding author: ebozkaya@dho.edu.tr
Received: 19.04.2023, Accepted: 18.09.2023

a false base station can enter between two base stations and force UEs to connect to themselves. To implement this, a false base station transmits more power than the legitimate base station, and service interruption can occur during the handover process.

False Base Station can perform passive and active attacks against the UEs over the Radio Access Networks (RAN). In 5G networks, base stations periodically broadcast information about the network. The UEs listen to these broadcast messages and select a suitable cell to connect. Due to practical difficulties, broadcast messages are not protected for confidentiality, authenticity, or integrity. Therefore, broadcast messages are prone to spoofing. 3GPP 5G Release also addresses the detection of false base stations [5]. Accordingly, the Received Signal Strength Indicator (RSSI) and location information in measurement reports can be used for detection. This can be accomplished by detecting inconsistency between the information on the broadcast information and the base station deployment information. The 5G system has already made significant improvements against false base stations such as mutual authentication, integrity protected signaling, and secure algorithm negotiations [7]. However, there are still challenges due to the computation complexity and requiring high bandwidth.

In this respect, we simulate a scenario, where a false base station is deployed and users can be connected to it during handover process. Then, we show the steps of how an attack can be prevented and, propose a solution to protect broadcast messages with two fundamental encryption algorithms; AES-256 Algorithm and RC4 Algorithm.

As a result, the main contributions of this paper are as follows:

- We describe the handover procedure in 5G networks and give a threat model.
- We simulate a false base station attack and analyze the security of the proposed system model.
- Then, we observe the handover procedure in different radio access technologies and propose to encrypt the measurement reports showing the computation time.

The rest of the paper is organized as follows. Section 2 reviews the most relevant studies related to the handover process and false base station attacks. Section 3 describes the system model during the handover process and gives our proposed solution in a simulation environment. Section 4 evaluates the performance of the proposed solution. Finally, we give our conclusions in Section 5.

2. Related Work

A false base station can collect user information or prevent users from accessing the service. Due to the difficulty of detecting false base stations, many researchers have investigated the handover procedure [8]. In this section, we give the security weakness of the handover process and false base station attacks.

In [9], the authors focus on estimating the location of false base stations and propose a network-based localization method. The proposed method is based on the analysis of Reference Signal Received Power (RSRP) and UE location information in the measurement reports. Measurement reports are used to check for any inconsistencies in the network topology since the reports contain information about both the false base station and the legitimate base stations. This method is based on estimating the UE locations where measurement reports are sent to identify the locations of false base stations. In [10], the authors consider the International Mobile Subscriber Identity (IMSI) catcher device to simulate a false base station. The IMSI catcher can obtain the IMSI number sent by the UEs within the coverage area and capture the data traffic [11]. It is emphasized that the IMSI catcher can eavesdrop on calls, intercept messages, and obtain UE locations. Thus, an IMSI catcher detection mechanism is proposed against the possible attacks and a location-based cell print algorithm is presented. However, both of these methods assume that the UEs are legitimate and already known and the measurement reports are not filtered for malicious traffic.

In addition, the authors in [12] investigate the false base station attack and propose location awareness-based methods since UE can receive multiple signals from the nearby base stations and a false base station can send the strongest signal to the UE to establish a connection with itself. In this regard, the received signal strength is checked according to the location of UE and legitimate base station. This method can effectively mitigate the false base station attack, but this process is time-consuming for a mobile network as malicious traffic can be generated for network congestion. In [13], the authors aim to detect false base stations and prevent denial of service attacks. To achieve this, the authors use automatic neighbor relations in self-organizing networks to prohibit UEs from establishing a connection with the false base station. The authors classify the base stations as false and legitimate according to the measurement reports and send each UE a list of false base stations. However, updating the list and sending it to each UE inevitably consumes resources (e.g. time, bandwidth). In [14], [15], the authors identify

the unique RF characteristics of the transmitter to distinguish legitimate base stations from false base stations. The authors only investigate the measurements of false base stations, but the measurements of legitimate base stations are also an important factor for detection criteria. In [16], the authors propose an identification protocol to verify the base stations and protect user privacy. The authors use the measurement reports of UEs in different positions so that they estimate the power and position of the real base stations. When a new base station is included in the topology, its position and power are verified by a cloud server. After the verification process, the UEs can be connected to the base stations. However, this method requires a database to check legitimate base stations, which may cause a change in the current LTE procedure.

Frequent handovers between base stations cause security vulnerabilities and potential threats. Although 3GPP has determined the new security functionalities [7], secure handover is still a critical issue, in particular, against false base station, and denial of service attacks. In [17], the authors propose a secure handover authentication protocol between neighbor base stations by using the Chinese remainder theory. It is aimed to enable mutual authentication between UE and the network so that after the UE has completed the authentication with the current base station, a handover process can happen. Then, mutual authentication is executed with the target base station. However, the attackers can implement more volumes of malicious traffic, and the handover procedure may be much more complicated and time consuming, especially in latency sensitive applications resulting in lower QoS. In [18], the authors investigate the challenges of the false base station, denial of service attack, and high network complexity and, then propose authentication and key agreement process for handover in 5G networks. However, this work does not take into consideration the characteristics of false base station attacks, and cannot be implemented for specific attack scenarios related to measurement reports.

In [19], the authors present an Elliptic curve cryptography-based authentication model to both confirm the validity of the node and design handover schemes. In the study, by using the cryptography-based solution, the main-in-the-middle attack is prevented. When the malicious node receives the user authentication request, the node needs to master the private key to confirm its identity, thus the malicious node cannot send back the legitimate response message. However, the proposed secure method can be challenging for UEs due to the limited storage and energy capabilities, and extensive computation. Thus, the solution should be a distributed security solution and constantly monitor the measurement reports to detect false base station attacks. Similarly, in [20], the authors present a secure handover authentication scheme based on the certificateless public-key cryptography technique. In this technique, a key generator center generates the partial public key and private key and the user obtains the complete public key and private key by combining the partial keys and a random number by itself. Thus, in the proposed model, privacy is preserved with an authentication scheme and three-handshake during handover in the mobility scenarios. In [21], the authors also address the problems of authentication mechanisms and introduce a robust handover authentication protocol for 5G heterogeneous networks. A mutual authentication with the key procedure is presented. Although certificateless public-key cryptography and key procedure method can support secure handover with reduced computation time, the complicated procedure associated with UEs is still concerning.

These approaches mainly consume a lot of resources of UEs leading to the decrease in application performance to detect false base stations. On the other hand, this work is motivated to provide a cryptography-based solution for the handover procedure by diminishing the overall computation time in addition to restricting the communication with measurement reports between UEs and base stations. This is important for the handover authentication procedure.

3. System Model and Proposed Solution

This section describes the 5G handover system model and threat model. As illustrated in Fig. 1, 5G networks basically consist of two components: Core Network (CN) and Radio Access Network (RAN). CN includes the Access and Mobility Function (AMF), User Plane Function, Session Management Function (SMF), and Authentication Server Function (AUSF). In the 5G RAN, there are g-Node BSs (gNBs) communicating with the UEs. If a UE requests to connect to the 5G CN, the AMF first offers the AUSF to perform mutual authentication with the UE.

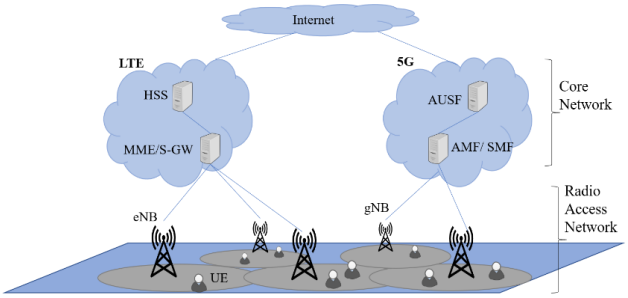

Figure 1. The illustration of handover for 5G networks.

In a cellular network, UE is configured to send the measurement reports to the gNBs to which it is connected. Measurement reports include power and frequency measurements collected from nearby gNBs. All information necessary for the UE to measure is available in the gNB's system information block (SIB) and main information block (MIB) broadcast messages. After receiving the messages, the serving gNB evaluates the measurement reports and decides whether a handover procedure is required. In particular, if the communication with the serving gNB deteriorates and/or another neighboring gNB at a different frequency becomes better than the serving gNB, then the handover procedure may be performed from the serving gNB to the neighbor gNB. In addition, the Reference Signal Received Power (RSRP), the Reference Signal Received Quality (RSRQ), and Signa

Interference and Noise Ratio (SINR) are considered when making the handover decision. The handover decision and these measurement reports are standardized by 3GPP [22].

3.1. Thread Model

In this paper, we simulate the Man-in-the-Middle attack through the scenario of eavesdropping, changing, and retransmitting messages. As seen in Fig. 2, we focus on a scenario, where an active attacker can deploy a false base station with the same capabilities as the legitimate base station. Specifically, a false base station could impersonate a legitimate base station, thereby forcing UE to connect itself. This may occur by broadcasting MIB and SIB messages of the false base station with a higher signal strength than the legitimate base station to which it is connected. We also assume that an attacker could intercept the MIB and SIB messages of legitimate BSs by listening to open channels.

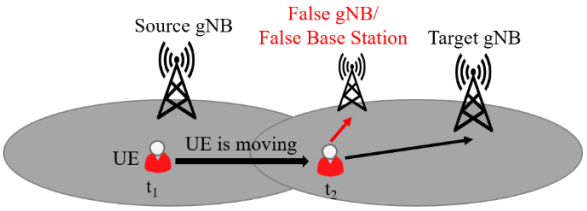

Figure 2. The illustration of the threat model.

3.2. Proposed Solution and Simulation Environment

In this subsection, we give our scenario to simulate a false base station with the presented threat model and analyze the security of the proposed model using discrete-event network simulator NS-3.

In our experiment, we simulate two scenarios, where a UE is in a Radio Resource Control (RRC)-connected state and transmits video data while interacting with the network. In the first scenario, the UE moves randomly choosing different directions. In the second scenario, the UE moves along a certain trajectory.

As shown in Fig. 3, our first scenario consists of a 4G/5G core network, two eNB/gNB representing the legitimate base station, a malicious/false eNB/gNB used for attacks, and several UEs. Two legitimate eNB/gNBs are connected to the core network via S1 in 5G and N2 in 4G. In addition, legitimate eNB/gNBs are interconnected via interface Xn in 5G and X2 in 4G, and their cellular interfaces are configured according to the NS3 documentation.

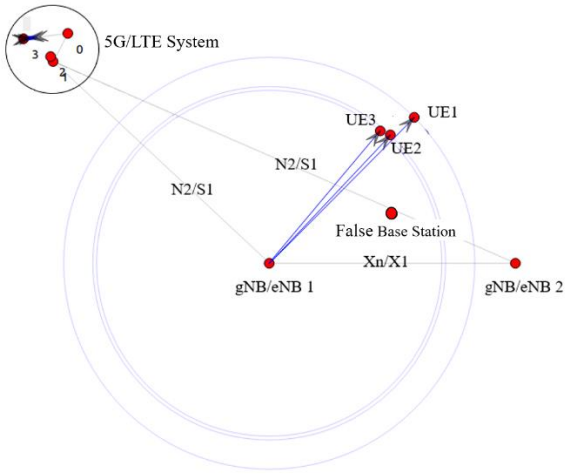

Figure 3. The implementation of scenario 1 in NS-3.

To simulate the handover procedure, we increase the signal strength of the false base station and reduce the signal strength of eNB_1/gNB_1. Unaware of cell 2's existence, the UE reports a strong signal from the false base station to cell 1 via

measurement report. Figs. 4 and 5 show examples of malicious measurement reports with false power measurements on LTE and 5G, respectively. The UE is eventually forced to disconnect from the legitimate base station and connect to the false base station.

```
Message: Measurement Report

Data:

{
  message c1: measurementReport: {
    criticalExtensions c1: measurementReport-r8: {
      measResults {
        measId 3,
        measResultPCell {
          rsrpResult 53,
          rsrqResult 33
        },
        measResultNeighCells measResultListEUTRA: {
          {
            physCellId 2,
            measResult {
              rsrpResult 59,
              rsrqResult 26
            }
          }
        }
      }
    }
  }
}
```

Figure 4. Malicious measurement report on LTE.

```
Message: Measurement report

Data:

{
  message c1: measurementReport: {
    criticalExtensions measurementReport: {
      measResults {
        measId 3,
        measResultServingMOList {
          {
            servCellId 0,
            measResultServingCell {
              physCellId 500,
              measResult {
                cellResults {
                  resultsSSB-Cell {
                    rsrp 39,
                    rsrq 61,
                    sinr 52
                  }
                }
              }
            }
          }
        },
        measResultNeighCells measResultListNR: {
          {
            physCellId 501,
            measResult {
              cellResults {
                resultsSSB-Cell {
                  rsrp 72,
                  rsrq 66,
                  sinr 71
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Figure 5. Malicious measurement report on 5G.

Then, we observe the handover procedure in different radio access technologies and evaluate the results of the handover between the 4G system and the 5G system. We consider that the UE is located at base station 1 and the UE is moving to the coverage area of base station 2, thus a handover is required between base stations 1 and 2. Here, in the simulation environment, BS_1 operates on 4G and BS_2 operates on 5G. At the same time, the attacker tries to abuse the handover by impersonating BS_2. In Fig. 6, eNB CellId 4 represents the malicious BS.

Figure 6. Handover Report.

In the second scenario, where the UE moves from point A to point B along a given path at a speed of 50 m/s, it connects to BS_1 and transmits data to the network as seen in Fig. 7. At initial 16 seconds of the simulation, the UE sends a measurement report to the serving BS_1, triggers the BS_2, but connects to malicious/false BS_3 as shown in Fig. 8. UE connecting to a malicious BS is under attack for 3 seconds. In the 19th second, it reestablishes the connection with the BS_2 and receives the available services from the network.

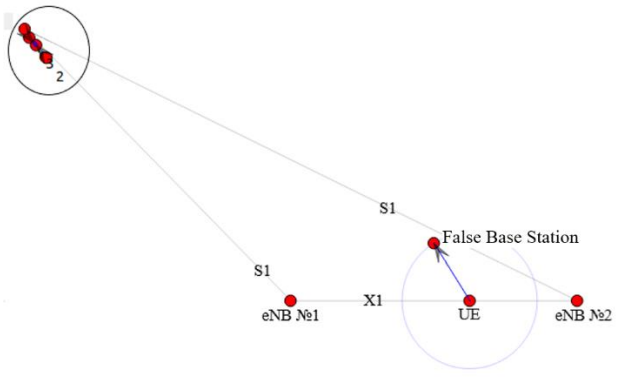

Figure 7. The implementation of scenario 2 in NS-3.

```
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] Best neighbour cellId 2
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] Trigger Handover to cellId 2
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] target cell RSRQ 31
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] serving cell RSRQ 14
+16.000001000s -1 A2A4RsrqHandoverAlgorithm:DoReportUeMeas(0x5644395dc6f0, 1, 2)
+16.000001000s -1 A2A4RsrqHandoverAlgorithm:UpdateNeighbourMeasurements(0x5644395dc6f0, 1, 3, 31)
+16.000001000s -1 A2A4RsrqHandoverAlgorithm:UpdateNeighbourMeasurements(0x5644395dc6f0, 1, 2, 18)
/NodeList/7/DeviceList/0/LteUeRrc/ConnectionEstablished UE IMSI 1: connected to CellId 3 with RNTI 1
/NodeList/6/DeviceList/0/LteEnbRrc/ConnectionEstablished eNB CellId 3: successful connection of UE with IMSI 1 RNTI 1
```

Figure 8. Handover to a Malicious BS.

4. Performance Evaluation

Traditional detection mechanisms such as mobile applications or network sniffers cannot prevent handover attacks because the UE cannot implement security measures against a false base station on its own and the attack will likely be detected after completion. Therefore, we propose to use the AES-256 and RC4 encryption algorithms to encrypt the identification number of the base stations to prevent false stations and, then we evaluate the performance of our cryptographic-based solution.

The cryptography-based methods have significantly improved secure communication, but it is still time-consuming for most applications. Similar to our work, in [20], the authors also propose a cryptography-based handover scheme for the mobile UEs in LTE-A networks. However, due to the mobility of UEs, a secure handover mechanism should be designed to make it available to the battery-limited UEs. Although the proposed method in [20] can support secure handover with reduced computation time, the complicated procedure associated with UEs is still concerning. This approach mainly consumes a lot of resources of UEs leading to the decrease in QoS [23]. Therefore, we simulate a false base station attack and analyze the security of the proposed solution in terms of computation overhead.

The cell ID is a 28-bit value that contains the ID of a base station. Initially, we assume that base station identifiers are encrypted and transmitted over broadcast channels. During the handover process, the source base station will decrypt the target base station ID received by measurement reports from the UE.

Fig. 9 shows the computation time to decrypt the base station identifier using the AES-256 and RC4 algorithms concerning the number of UEs. As seen in the figure, while the AES-256 algorithm provides higher security, it offers more computation time. On the other hand, the RC4 algorithm provides a less computation time, but a less reliable solution. Both AES-256 and RC4 algorithms are symmetric-key algorithms. In particular, as the number of UEs increases, more processing time is required for encryption and decryption for a more secure solution. While the RC4 algorithm encrypts data independently of each other, either bit by bit or byte by byte, and offers fast processing capability, the AES-256 algorithm encrypts data in 128-bit blocks using a 256-bit key and the latency is higher as the data is processed in blocks.

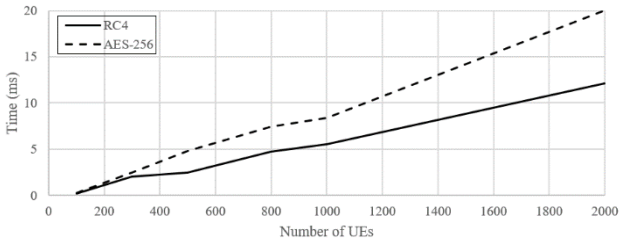

Figure 9. Computation time for AES and RC4 algorithms.

In Fig. 10, we show the secure handover solution after the cell ID of the base station is encrypted. As seen in the figure, according to the measurement reports, the UE is triggered for handover to cell ID number 2 since the Reference Signal Received Quality (RSRQ) from the target cell is better than the serving cell. Thereby, the UE connects to the legitimate base station by encrypting the cell ID.

```
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] Best neighbour cellId 2
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] Trigger Handover to cellId 2
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] target cell RSRQ 31
+15.920001000s -1 A2A4RsrqHandoverAlgorithm:EvaluateHandover(): [LOGIC] serving cell RSRQ 14
+16.000001000s -1 A2A4RsrqHandoverAlgorithm:DoReportUeMeas(0x5644395dc6f0, 1, 2)
+16.000001000s -1 A2A4RsrqHandoverAlgorithm:UpdateNeighbourMeasurements(0x5644395dc6f0, 1, 3, 31)
+16.000001000s -1 A2A4RsrqHandoverAlgorithm:UpdateNeighbourMeasurements(0x5644395dc6f0, 1, 2, 18)
/NodeList/7/DeviceList/0/LteUeRrc/ConnectionEstablished UE IMSI 1: connected to CellId 2 with RNTI 1
/NodeList/6/DeviceList/0/LteEnbRrc/ConnectionEstablished eNB CellId 2: successful connection of UE with IMSI 1 RNTI 1
```

Figure 10. Triggering the handover and connection to a legitimate base station.

As explained in the previous section, measurement reports include power and frequency measurements collected from nearby base stations. All information necessary for the UE is available in the SIB and MIB broadcast messages. In addition to encrypting the identity of a base station, we also consider increasing data size to be able to encrypt fields such as tracking area code, scheduling information list, and radio resource configuration in SIB messages for a more secure solution [24]. Thus, we set the number of UEs to 500, also consider the AES-128 algorithm, which uses a 128-bit key, and compare the computation time to observe the results more clearly. As seen in Table 1, the computation overhead increases as the data size increases. AES-128 and AES-256 algorithms have longer computation time but are still suitable for latency sensitive traffic in a 128-bit data size because according to the 5G and beyond 5G Key Performance Indicator (KPI), it is assumed that the end-to-end latency requirement should be under 5 ms [25].

Table 1. Computation time overhead for different data sizes

Data size:	28 bits	128 bits	160 bits
RC4 Algorithm	3.33 ms	3.72 ms	4.25 ms
AES-128 Algorithm	3.97 ms	4.65 ms	5.02 ms
AES-256 Algorithm	4.42 ms	4.97 ms	5.36 ms

5. Conclusion

In this paper, we proposed a secure handover process to prevent the Man-in-the-Middle attack, i.e., the false base station. We simulated a false base station and defined the security vulnerabilities in different radio access technologies. We also proposed to encrypt the cell ID of the base station, which is sent with the measurement reports. We demonstrated the steps of handover triggering and handover process in a simulation environment. It is shown that the computation time is acceptable and a secure connection can be established between UE and a legitimate base station.

Contributions of the authors

The system model and proposed solution were developed by Yerdos AMİRBEKOV and Elif BOZKAYA. Performance evaluation was carried out by Yerdos AMİRBEKOV and Elif BOZKAYA commented on the results obtained from the study. All authors contributed to the writing of the article.

Conflict of Interest Statement

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The study is complied with research and publication ethics.

References

[1] D. Kafetzis, S. Vassilaras, G. Vardoulias and I. Koutsopoulos, "Software-Defined Networking Meets Software-Defined Radio in Mobile ad hoc Networks: State of the Art and Future Directions", *in IEEE Access*, vol. 10, pp. 9989-10014, 2022, doi: 10.1109/ACCESS.2022.3144072.

[2] P. Xue and Z. Jiang, "SecRouting: Secure Routing for Network Functions Virtualization (NFV) Technology*", in IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 69, no. 3, pp. 1727-1731, March 2022, doi: 10.1109/TCSII.2021.3119938.

[3] D. Zhao, Z. Yan, M. Wang, P. Zhang, B. Song, "Is 5G Handover Secure and Private: A Survey", *IEEE Internet of Things Journal* vol. 8, no.16, pp. 12855–12879, 2021. doi:10.1109/JIOT.2021.3068463.

[4] IMT Vision-Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond, Recommendation ITU-R M.2083-0 (09/2015).

[5] 3GPP TS 33.501, "Security Architecture and Procedures for 5G System (version 15.4.0 release 15)", Technical specification (2019).

[6] M. Conti, N. Dragoni, V. Lesyk, "A Survey of Man in the Middle Attacks*", IEEE Communications Surveys & Tutorials* vol. 18, no. 3 pp. 2027–2051, 2016. doi:10.1109/COMST.2016.2548426.

[7] 3GPP TR 33.809 v0.20.0, "Study on 5G Security Enhancement Against False Base Stations (FBS) (Release 18)", Technical specification (2022).

[8] V. Sharma, I. You, F. Leu, M. Atiquzzaman, "Secure and Efficient Protocol for Fast Handover in 5G Mobile Xhaul Networks", *Journal of Network and Computer Applications*, vol.102, pp. 38-57, 2018.

[9] L. Karaçay, Z. Bilgin, A. B. Gündüz, P. Çomak, E. Tomur, E. U. Soykan, U. Gülen, F. Karakoç, "A Network-based Positioning Method to Locate False Base Stations", *IEEE Access* vol. 9, pp.111368–111382, 2021. doi:10.1109/ACCESS.2021.3103673.

[10] H. Alrashede and R. A. Shaikh, "IMSI Catcher Detection Method for Cellular Networks", i*n 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769507.

[11] S. Park, A. Shaik, R. Borgaonkar, and J. Seifert. "Anatomy of Commercial IMSI Catchers and Detectors", *in Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society (WPES'19).* Association for Computing Machinery, New York, NY, USA, pp. 74–86, 2019. https://doi.org/10.1145/3338498.3358649.

[12] K.-W. Huang, H.-M. Wang, "Identifying the Fake Base Station: A Location Based Approach", *IEEE Communications Letters* vol. 22, no. 8, pp. 1604–1607, 2018. doi:10.1109/LCOMM.2018.2843334.

[13] J. Shin, Y. Shin, J.-G. Park, "Network Detection of Fake Base Station Using Automatic Neighbour Relation in Self-organizing Networks", *in 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 2022, pp. 968–970. doi:10.1109/ICTC55196.2022.9952901.

[14] A. Ali, G. Fischer, "Symbol Based Statistical RF Fingerprinting for Fake Base Station Identification", *in 29th International Conference Radioelektronika (RADIOELEKTRONIKA)*, pp. 1–5, 2019. doi:10.1109/RADIOELEK.2019.8733585.

[15] A. Ali, G. Fischer, "The Phase Noise and Clock Synchronous Carrier Frequency Offset based RF Fingerprinting for the Fake Base Station Detection", *in IEEE 20th Wireless and Microwave Technology Conference (WAMICON)*, pp. 1–6, 2019. doi:10.1109/WAMICON.2019.8765471.

[16] A. Mazroa, M. Arozullah, "Detection and Remediation of Attack by Fake Base Stations in LTE Networks", *International Journal of Soft Computing and Engineering (IJSCE)*, vol.5, no. 2, 2015.

[17] X. Yan, M. Ma, "A Lightweight and Secure Handover Authentication Scheme for 5G Network Using Neighbour Base Stations", *Journal of Network and Computer Applications* vol. 193, p. 103204, 2021. https://doi.org/10.1016/j.jnca.2021.103204.

[18] A. Sharma, I. Sharma and A. Jain, "A Construction of Security Enhanced and Efficient Handover AKA Protocol in 5G Communication Network", *in 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, pp. 1-6, 2019. doi: 10.1109/ICCCNT45670.2019.8944569.

[19] J. Guo, Y. Du, Y. Zhang, M. Li, "A Provably Secure ECC-based Access and Handover Authentication Protocol for Space Information Networks", *Journal of Network and Computer Applications* vol. 193, 2021. 103183. https://doi.org/10.1016/j.jnca.2021.103183.

[20] R. Ma, J. Cao, D. Feng, H. Li, Y. Zhang, X. Lv, "PPSHA: Privacy Preserving Secure Handover Authentication Scheme for All Application Scenarios in LTE-A Networks", *Ad Hoc Networks* vol. 87, pp. 49–60, 2019. https://doi.org/10.1016/j.adhoc.2018.11.012.

[21] Y. Zhang, R. H. Deng, E. Bertino and D. Zheng, "Robust and Universal Seamless Handover Authentication in 5G HetNets," *in IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 858-874, 1 March-April 2021, doi: 10.1109/TDSC.2019.2927664.

[22] 3GPP TS 36.331 – "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol Specification (Release 8)", Technical Specification (2013).

[23] Y. Y. Deng, C. L. Chen, J. Shin and K. H. Wang, "Cryptanalysis of Yang et al.'s Handover Authentication Scheme for Mobile Network Environment," *in 2017 International Symposium on Computer Science and Intelligent Controls (ISCSIC)*, Budapest, Hungary, pp. 152-157, 2017. doi: 10.1109/ISCSIC.2017.43.

[24] V. A. Vasudevan, M. Tayyab, G. P. Koudouridis, X. Gelabert, and I. Politis, "An Integrated Approach for Energy Efficient Handover and Key Distribution Protocol for Secure NC-enabled Small Cells", *Computer Networks*, vol.206, 2022. https://doi.org/10.1016/j.comnet.2022.108806.

[25] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems", *in IEEE Network*, vol. 34, no. 3, pp. 134-142, May/June 2020, doi: 10.1109/MNET.001.1900287.