Engineering Science & Technology
http://ojs.wiserpub.com/index.php/EST/

UNIVERSAL WISER
PUBLISHER

Letter

Automatic Mobile Network User Identification System: Idea and Tips

Amir Masoud Molaei[1*], **Mobina Ranjbar Malidareh**[2], **Seyed Hojjat Hosseini**[3]

[1]Centre for Wireless Innovation, Queen's University Belfast, BT3 9DT, Belfast, UK
[2]Electrical and Computer Engineering Faculty, Babol Noshirvani University of Technology, Babol, Iran
[3]Informatics Services Corporation, Tehran, Iran
E-mail: a.molaei@qub.ac.uk

Received: 30 July 2024; **Revised:** 23 December 2024; **Accepted:** 6 January 2025

Abstract: The purpose of designing an automatic system to identify mobile network users is to control the entry and exit of users at a specific location. The main idea is to set up a pseudo-base transceiver station (BTS) between the mobile phone and the nearest BTS. The mobile phone regularly reports its location to the nearest BTS. The key task is to search for the signal sent to the pseudo-BTS and extract the international mobile subscriber identity (IMSI) information. The proposed system will be able to communicate up to 12-30 meters. In addition, the system does not require a near-field communication tag, because the information is decoded by the communication protocols of the mobile network. Therefore, even the simplest and most basic mobile phones can be identified by the system. In this paper, in addition to presenting the main idea, the hardware and software structures of the system are also described.

***Keywords*:** IMSI, mobile network, pseudo-BTS, user identification

1. Introduction

Communicating between electronic devices for purposes such as money transfer, electronic business cards, identification, tracking, etc. is an issue that reputable electronic and telecommunications have been focusing on in recent years with their hardware and software technologies [1]. The near-field communication (NFC) system [2], for example, is a set of communication protocols for communication between two electronic devices (usually one of which is a portable device such as a smartphone) that are located close to each other. Today, this system is used in Europe and the United States to pay customers in supermarkets, to record driving violations by the police by reading the license plate tag, to provide e-business cards, and so on [3]. However, the main problem with this system is that, firstly, the distance between the two devices must be less than 4 to 10 cm, and secondly, non-smartphones and even some smartphones do not have such a system.

For instance, systems described by Onumadu et al. [4] and Markantonakis et al. [5] leverage NFC and radio frequency identification (RFID) for user identification but remain constrained by compatibility and range limitations. Despite advancements, the current body of research does not address the need for a system that:

- Functions seamlessly across all mobile devices, including basic phones without NFC capability.
- Operates over a broader range, extending its applicability beyond close-proximity use cases.
- Offers a cost-effective, hardware-agnostic solution for judicial/security purposes and consumer analytics.

DOI: https://doi.org/10.37256/est.6120255411

The purpose of proposing an automatic mobile network user identification system (AMNUIS) [6] is to control the entry and exit of mobile network users to a specific location. This place can be a chain store, school, university, airport, barracks, etc. By using such a system, it is possible to statistically obtain the number and time of visits of a particular subscriber. The extracted data can be used for marketing customers, mechanized recording of the time of entry and exit of staff and students to work and school, and so on. For example, if such a system is installed above the front door of a school or university classroom, it is easy to extract the time of attendance and leaving of a particular person from the recorded data. In security and judicial applications, recorded information can be used to prove a user's presence in a specific location. Also, recent advances in graph and network theory [7]-[9] provide valuable insights into optimizing communication systems and data flow, which can enhance the performance and design of AMNUIS.

The main idea and innovation of the plan is to set up a fake pseudo-base transceiver station (BTS) between the mobile phone and the nearest BTS. The mobile phone frequently announces its position to the nearest BTS, even when it has no call, this information is constantly updated on the home location register [10]. The key task is to detect the signal sent to the pseudo-BTS and then extract international mobile subscriber identity (IMSI) [11]. This fifteen-digit ID is unique to each subscriber identification module (SIM) card. Such a system can communicate up to a distance of 12 to 30 meters, so it is enough to install in the gate or the entrance and exit door of the desired location to detect any switched-on mobile phone that passes through that gate. In addition, the system does not require any NFC tag [12], because the information is decoded by the mobile network communication protocols. Therefore, even the simplest and most basic mobile phones will be identified by the system.

The rest of this paper is organized as follows. An overview of NFC technology is provided in Section 2. System design details and tips are provided in Section 3. Section 4 is devoted to a summary of the features of the system. In Section 5, potential malicious uses and mitigations are presented. Section 6 describes technical challenges and solutions in implementation. The conclusion, finally, is presented in Section 7.

2. An overview of NFC technology

NFC is the latest technology in the field of RFID cards [13]. This technology is employed by smartphone manufacturers such as Samsung, HTC, etc., and embedded in their mobile phones. Many mobile phones have NFC from 2011 onwards, which can be easily activated. The list of these mobile phones can be found in [14].

The core of the NFC module is the NXP PN532 chip [15], one of the most popular NFC technology chips. In this module, the input/output pins of NXP532 are spread on the module so that users can easily use it. The data connection is done by I2C [16] by default, but the user can also use protocols such as Universal Asynchronous Receiver Transmitter (UART) or Serial Peripheral Interface (SPI) [17] in this module according to their needs. This module can be connected to any type of microcontroller and the protocol can be set up and used. For instance, a reader for such a system can be found in [18].

3. System architecture

In this section, the hardware and software details of the AMNUIS are provided. This innovative idea is completely different from the NFC system. Besides, this system has scientific approval from the Iranian Research Organization for Science and Technology (IROST) with digital object identifier: 10.22104/IROST.1398.033.

This system consists of the following components:

- A UHV antenna at the receiver input.
- The first stage of the receiver includes an impedance matching circuit, low noise amplifier, microcontroller, bandpass filter, and variable gain amplifier.
- The Second (main) stage of the receiver includes the RTL2832U module [19].
- Tuner and digital down-converter (DDC).
- Analog-to-digital converter.
- Universal serial bus (USB) port for transferring data to the processor.
- A computer to process the received signals and extract the required data.

- Internal memory.
- A dedicated script for the intended application.

The technologies used in this system include electronic and telecommunication devices. Another important part of this system is the software and network component, in which the desired information is extracted and stored by functions in a dedicated script.

Each authorized network subscriber is assigned an IMSI that includes a mobile country code (MCC), a mobile network code (MNC), and a unique mobile subscription identification number (MSIN) in the public land mobile network [20]. Figure 1 shows the overall structure of the IMSI. IMSI is not a hardware feature; it is stored on a smart card for an authorized subscriber and serves as the only absolute feature that a subscriber has within the network. It contains MCC, followed by national mobile subscriber identity (NMSI), with a maximum of 15 digits.

Figure 2 shows the outline of the main idea. As can be seen, there is a fake pseudo-BTS between the mobile phone and the nearest BTS. The designed system, as an intermediate node, plays the role of an amplifier. In the detected signal, we are only looking for unique IMSI.

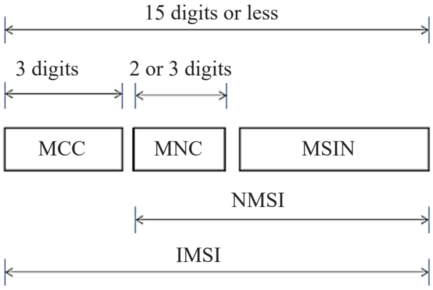

Figure 1. The overall structure of the IMSI [21]

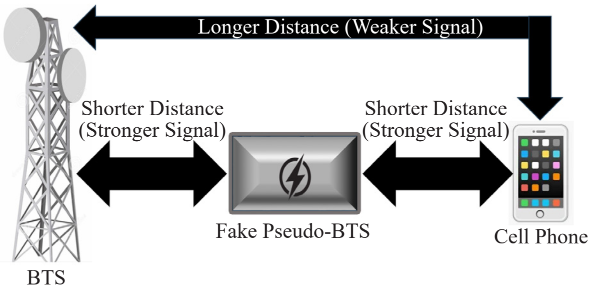
Longer Distance (Weaker Signal)
Shorter Distance (Stronger Signal)
Shorter Distance (Stronger Signal)
Fake Pseudo-BTS
Cell Phone
BTS

Figure 2. The outline of the main idea

The block diagram in [22] demonstrates the hardware schematic of the pseudo-BTS system to be implemented. To implement the circuit, we need a UHV antenna at the system input. The antenna output is connected to the low-noise amplifier (LNA) input via a matching circuit. The matching circuit is designed to maximize the power transfer from the antenna to the receiver. LNA is also used to amplify the signal without significant noise amplification. The output of the circuit is connected to a computer containing management software via a USB cable. One of the main modules of the above circuit is the RTL2832U processor. The RTL2832U is a high-performance coded orthogonal frequency division multiplexing (COFDM) demodulator [23] that supports the USB 2.0 interface. Modulation parameters, such as code rates and guard interval [24], are automatically detected. The RTL2832U supports tuners at an intermediate frequency (IF) of 36.125 MHz, low IF of 4.57 MHz, or zero-IF output using a 28.8 MHz crystal. It has an advanced analog-to-digital converter (ADC). A commercial model called the super stable 1 ppm TCXO R820T2 tuner RTL2832U RTL-SDR USB Stick-Version 3 is currently available for purchase at around £40 in 2024.

In the first step, we need to receive global system for mobile communications (GSM) information through the system. The system can hear up to 1,766 MHz, and with the use of DDC, it can also detect higher-frequency signals. Implementing it in many countries requires access to the 900 MHz band, which is the GSM frequency of their domestic operators.

IMSI numbers are registered through the common control channel (CCCH) [25] and the received information. CCCH is responsible for transferring control information between all mobile phones and BTS. This is essential for implementing processes such as call origination and call paging.

By using the software grgsm_livemon, the received waves can be viewed in the form of a graph. In fact, frequencies are displayed as diagrams. The user's received data is in the form of IP packets named GSMTAP. It is a pseudo-header format for encapsulating frames from the GSM Um interface into UDP/IP packets assigned to port 4,729.

The IMSI information consecrated to a SIM card is extracted from the information recorded by grgsm_livemon using a dedicated script, written in Python programming language. Next, each IMSI is saved as a file with the corresponding name.

Finally, using other functions in the dedicated script, if IMSI is repeated, its repetition and time are stored in the file.

Here is the general algorithm of the software part of the system:

- Define variables related to the temporary storage of signal data.
- Identify BTSs close to the device.
- Identify active and near-device operators.
- Identify the receivable frequencies of the mobile signal related to the physical location of the device.
- Activate the time switch to receive a signal from a receiver among active operators.
- Capture the signal information received on the found frequencies.
- Extract the required data (IMSI), using filtering.
- Decode the information in understandable language and save it into a file.
- Identify and control users by analyzing the file, and assign the appropriate output to the user.

Remark 1: To ensure compatibility with modern mobile communication standards, the proposed pseudo-BTS system has been designed to operate effectively within the frequency bands utilized by fourth-generation (4G) and 5G networks. Key modifications and enhancements include:

- Advanced Frequency Support: The pseudo-BTS must integrate tuners and DDCs capable of processing high-frequency signals up to 2.6 GHz for 4G and 3.5 GHz for 5G.
- Protocol Adaptation: Dedicated scripts and software modules need to be developed to decode IMSI data from the long-term evolution and new radio protocols used in 4G and 5G networks [26].
- Bandwidth Optimization: The system must employ advanced filtering and signal processing techniques to handle the wider bandwidths characteristic of 5G, ensuring efficient data extraction without compromising accuracy.
- Scalability for Network Generations: By incorporating software-defined radio (SDR) [27] capabilities, the pseudo-BTS can dynamically adapt to different network generations, supporting seamless integration and future upgrades.

These enhancements align the system with current and emerging telecommunications standards, making it suitable for real-world deployment in diverse operational environments.

Remark 2: Note that the system is intended for applications such as attendance tracking, security analytics, and judicial evidence gathering. Any implementation or production of the ideas presented in this paper requires obtaining the necessary permits from the competent authorities. Also, explicit consent and legal authorization must be obtained for any experiments and system validations before deployment.

Remark 3: According to Remark 2, to ensure compliance with applicable telecommunications and privacy laws, it is necessary to take legal authorization, regulatory alignment, impact assessment, and independent review steps [28], [29] before any practical implementation.

4. Summary of AMNUIS features

In the previous section, the details of designing a mechanized electronic system to record the presence of a mobile network user in a specific location were presented. The following is a summary of its features and tips:

- This system is a pseudo-BTS that receives mobile phone signals and extracts the desired information (IMSI only).

- A UHV antenna is used to receive signals. This system will be able to operate up to a radius of 12 to 30 meters. With the use of more powerful antennas, it is possible to upgrade the coverage radius up to 300 meters. The antenna is placed in the right position (it can be located above the entrance door of the place). The antenna is fake BTS input.

- The fake BTS apparently plays the role of an amplifier between the mobile device and the nearest actual BTS. Therefore, the signals of the mobile antenna that are sent to announce the position to the nearest BTS are received by the system antenna.

- After receiving the signals from the first and second stages of the receiver, the output signal is digitized by an ADC with the appropriate accuracy to be able to be processed and stored.

- By using digital information, IMSI is extracted from the raw data by a dedicated script and stored in internal memory.

- Classification of the files stored in the internal memory is done by the script automatically.

- Due to the focus on registering SIM cards incoming to the network's covered area, the speed of operation in the innovative device is high.

- By employing the tuner and DDC, the system can be used for second-, third-, and even fourth-generation telecommunications networks.

- Due to the specificity of the script, the system can include additional modules or plug-ins.

5. Potential malicious uses and mitigations

The proposed pseudo-BTS technology, while beneficial in controlled and authorized environments, poses potential risks for malicious exploitation. To address these concerns, the following safeguards and defensive applications are suggested in the system:

• Access Controls: The pseudo-BTS system must include secure authentication protocols to prevent unauthorized access or misuse. Only authorized personnel with specific credentials can operate the system.

• Signal Encryption: Communications between the pseudo-BTS and the processing unit must be encrypted to prevent interception and tampering by malicious actors.

• Monitoring and Logging: The system must continuously monitor and log its operations, enabling the identification of any suspicious activity or unauthorized usage attempts.

• Defensive Applications: The system may be developed to detect and counteract rogue BTS devices in sensitive areas, enhancing security by identifying unauthorized IMSI catchers.

• Public Awareness and Reporting: Deployment of the system should be accompanied by clear documentation and adherence to transparency practices, ensuring stakeholders and regulators are informed of its capabilities and limitations.

By embedding these safeguards and emphasizing defensive applications, the technology can be responsibly utilized while mitigating potential risks.

6. Technical challenges and solutions in implementation

The implementation of a pseudo-BTS for mobile network user identification involves several technical challenges that require solutions to ensure robust performance and compliance.

One of the primary challenges is signal interference caused by nearby legitimate BTS towers, which can disrupt the reception and processing of target signals. To address this, the system can incorporate advanced filtering techniques and adaptive frequency tuning, effectively isolating the desired signals.

Another significant challenge is managing transmission power. Overpowering the signal can lead to excessive interference, while underpowering can reduce the system's effectiveness. Dynamic power control algorithms that adjust the transmission strength based on environmental conditions and operational requirements may mitigate this issue.

Decoding IMSI data from modern 4G and 5G protocols presents additional complexity due to the advanced modulation schemes and encryption methods employed by these standards. The pseudo-BTS system can overcome this challenge by utilizing specialized scripts and SDR technology, enabling efficient data decoding and processing while maintaining compatibility with contemporary communication protocols.

Scalability and latency also pose challenges, especially in high-traffic environments where the system must handle a large number of connections without introducing delays. To ensure scalability, the system can employ a modular architecture combined with parallel processing techniques, enhancing its ability to accommodate increased loads without compromising performance.

Finally, compliance with legal and ethical standards is an overarching challenge in deploying a pseudo-BTS. As noted in Remarks 2 and 3, this issue can be addressed through comprehensive compliance frameworks, obtaining formal regulatory approvals, and adhering to stringent ethical guidelines.

By tackling these technical challenges with tailored solutions, the pseudo-BTS system is expected to achieve reliability and operational efficiency in real-world applications.

7. Conclusion

In this paper, the design of an innovative AMNUIS was presented. The original idea of the plan is to set up a pseudo-BTS, through which the main information, i.e., IMSI can be accessed. Among the applications of the system, in addition to the judicial and security fields, we can mention the mechanized registration of the presence of employees, students, customers, athletes, sports spectators, etc. in the workplace, school, chain store, club, and stadium.

The AMNUIS system offers several advantages over existing NFC and RFID technologies, including efficiency, cost, and user acceptance. NFC systems, while efficient for close-proximity transactions, are limited by their operational range of less than 10 cm and require specialized hardware that is not universally available on all mobile phones, particularly older or basic models. RFID systems, although capable of slightly greater ranges, also necessitate dedicated tags and readers, which add to the overall system cost and complexity.

In contrast, AMNUIS leverages existing mobile network infrastructure, eliminating the need for additional tags or specialized hardware. This significantly reduces the deployment cost, as it operates seamlessly with any mobile phone capable of connecting to a network. Furthermore, AMNUIS can identify users over a much greater range (12-30 meters or more), enhancing its efficiency for applications such as attendance tracking or security monitoring in large spaces.

User acceptance is another critical factor in which AMNUIS holds a distinct advantage. Since the system operates passively and does not require users to carry additional devices or interact directly with the system, it aligns more closely with user expectations of convenience and unobtrusiveness. This makes it particularly appealing for applications in public spaces or high-traffic environments where ease of use is paramount.

The adoption of AMNUIS could enhance security by improving surveillance and analytics, aiding in monitoring and investigations, especially in sensitive areas. However, these benefits raise privacy concerns, as misuse could lead to unauthorized tracking and erode trust in mobile networks. Strict regulations and transparency are essential to mitigate such risks. AMNUIS may also influence user behavior, with individuals possibly turning off devices in sensitive locations, prompting mobile manufacturers to develop privacy-preserving features.

Conflict of interest

The authors declare no competing financial interest.

References

[1] R. AlGhamdi, S. Drew, and W. Al-Ghaith, “Factors influencing e-commerce adoption by retailers in saudi arabia: A qualitative analysis,” *The Electronic Journal of Information Systems in Developing Countries*, vol. 47, no. 1, pp.

1-23, 2011.

[2] M. Fisher and R. Guha, "Mobile communication device near field communication (NFC) transactions," U. S. Patent 9,378,493, Google Patents, 2016.

[3] V. Potdar, C. Wu, and E. Chang, "Automated data capture technologies: Rfid," in *Ubiquitous and Pervasive Computing: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2010, pp. 82-111.

[4] P. Onumadu and H. Abroshan, "Near-field communication (NFC) cyber threats and mitigation solutions in payment transactions: A review," *Sensors*, vol. 24, no. 23, pp. 7423, 2024.

[5] K. Markantonakis, G. Arfaoui, S. A. Ghazalah, C. Shepherd, R. N. Akram, and D. Sauveron, "CO-TSM: A flexible model for secure embedded device ownership and management," *Smart Cities*, vol. 7, no. 5, pp. 2887-2909, 2024.

[6] M. Ranjbar Malidareh, A. M. Molaei, and S. H. Hosseini, "Automatic identification and registration system for entry and exit of mobile network user," Iran Patent 97071, H04L 9/00, 28 Oct., 2018.

[7] S. Cheng, J.-P. Argaud, B. Iooss, A. Ponçot, and D. Lucor, "A graph clustering approach to localization for adaptive covariance tuning in data assimilation based on state-observation mapping," *Mathematical Geosciences*, vol. 53, no. 8, pp. 1751-1780, 2021.

[8] M. Gueuning, S. Cheng, R. Lambiotte, and J.-C. Delvenne, "Rock-paper-scissors dynamics from random walks on temporal multiplex networks," *Journal of Complex Networks*, vol. 8, no. 2, pp. 1-10, 2020.

[9] D. Chen, S. Cheng, J. Hu, M. Kasoar, and R. Arcucci, "Explainable global wildfire prediction models using graph neural networks," *arXiv*. [Online]. 2024. Available: https://doi.org/10.48550/arXiv.2402.07152. [Accessed: December 22, 2024].

[10] A. Dabrowski, G. Petzl, and E. R. Weippl, "The messenger shoots back: Network operator based IMSI catcher detection," in *International Symposium on Research in Attacks, Intrusions, and Defenses*, 2016, pp. 279-302.

[11] S. K. Thodupunoori, S. R. Velu, and S. Muthuswamy, "Methods and apparatus for prefix filtering of international mobile subscriber identity (IMSI) wildcard application," U. S. Patent 8,965,362, 24 Feb., 2015.

[12] J. T. Griffin and S. H. Fyke, "System and associated NFC tag using plurality of NFC tags associated with location or devices to communicate with communications device," U. S. Patent 9,246,555, 26 Jan., 2016.

[13] N. A. Chattha, "NFC-Vulnerabilities and defense," 2014 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, 2014, pp. 35-38.

[14] *NFC phones: The definitive list*. Available: www.nfcworld.com/nfc-phones-list. [Accessed: July 29, 2024].

[15] A. Widiyanto, "Prototype of NFC reader as a attendance sign at the presence system," *Journal of Physics: Conference Series*, vol. 1196, no. 1, pp. 012042, 2019.

[16] R. S. S. Kumari and C. Gayathri, "Interfacing of MEMS motion sensor with FPGA using I2C protocol," 2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 1-5.

[17] P. S. Mutha and Y. M. Vaidya, "FPGA reconfiguration using UART and SPI flash," 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017, pp. 59-63.

[18] *Adafruit*. Available: www.adafruit.com/product/789. [Accessed: July 29, 2024].

[19] T. Shevgunov and E. Efimov, "Software implementation of spectral correlation density analyzer with RTL2832U SDR and Qt framework," Computer Science On-line Conference, 2019, pp. 164-173.

[20] J. Tagg and A. J. Campbell, "Identity management for mobile devices," U. S. Patent 9,253,630, 2 Feb., 2016.

[21] "IMSI Number," *Telecomedu.blogspot.com*. [Online]. 2013. Available: https://telecomedu.blogspot.com/2013/01/imsi-number.html. [Accessed: January 13, 2025].

[22] Imgur. *RTLSDR (with R82OT/T2 tuner) tentative block diagram*. Available: https://imgur.com/gallery/rtlsdr-with-r820t-t2-tuner-tentative-blockdiagram-la4YH. [Accessed: July 29, 2024].

[23] S. Obayya, A. M. Matarneh, and I. Robertson, "Coded orthogonal frequency division multiplexing (COFDM) transmission over graded-index multimode fiber," 2008 IEEE PhotonicsGlobal@ Singapore, 2008, pp. 1-4.

[24] J. Faezah and K. Sabira, "Adaptive modulation for OFDM systems," *International Journal of Communication Networks and Information Security*, vol. 1, no. 2, pp. 1, 2009.

[25] K. Aggrawal, M. Kamani, and K. Vachhani, "Analysis of GSM air interface using DVB-T receiver and GNU radio," 2017 International Conference on Trends in Electronics and Informatics (ICEI), 2017, pp. 635-640.

[26] T. Novlan, S. Akoum, A. Ghosh, and M. Majmundar, "Long-term evolution assisted new radio initial access and mobility for 5G or other next generation networks," U. S. Patent 10,536,981, 14 Jan., 2020.

[27] 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," *IEEE Access*, vol. 10, pp. 9989-10014, 2022.

[28] J. Srinivas, A. K. Das, and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” *Future Generation Computer Systems*, vol. 92, pp. 178-188, 2019.

[29] S. K. Shandilya, A. Datta, Y. Kartik, and A. Nagar, “Navigating the Regulatory Landscape,” in *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy*, 2024, pp. 127-240.