KAMPALA INTERNATIONAL UNIVERSITY
EXPLORING THE HEIGHTS

KIU
Journal of Science,
Engineering and Technology

KJSET Research Article

Detection and Prevention of SIP REGISTER Injection Attack on a VoLTE Network

U. H. Nakorji*[1], H. Bello-Salau[2], E. A. Adedokun[3], M. K. Mustafa [4], O. W. Salami [5]
[1, 2, 3,4,5] *Department of Computer Engineering, Ahmadu Bello University, Zaria Nigeria*

[1] *harry14ng@gmail.com,* [2]*bellosalau@abu.edu.ng* [3] *wale@abu.edu.ng,* [4]*mkmustafa@nda.edu.ng,* [5]*salamiow@gmail.com,*

Corresponding Author: harry14ng@gmail.com

Paper history:
Received 29 June 2022
Accepted in revised form 12 January 2023

Keywords
Machine Learning, Artificial Intelligence, Artificial Neural Network

Abstract

Recent technological advances have indicated widespread use of Voice Over Long-Term Evolution (VoLTE) networks based on developing 5G networks. Despite its ease of design and deployment, VoLTE is vulnerable to many sorts of attacks at the control plane's Session Initiation Protocol (SIP), which exchanges signaling messages for calls via starting call setups, management, and termination. These SIP attacks may take the form of modified SIP messages that force the SIP devices to restart, or they may take the form of flooding the SIP devices with invite messages, register requests that cause the device to run out of memory, and denying genuine users access to the device. These attacks are commonly known as Distributed Denial of Service (DDoS) attacks. The SIP register injection attack, which might be injected during the commencement step by SIP equipped devices (SIP smartphones), prior to setting up the Secured Internet Protocol (IPsec) tunnel for the remaining SIP sessions, is of particular relevance, due to its characteristics of exhausting the available bandwidth, memory, and CPU resources, resulting in SIP device failure. Consequently, there is a need to address this difficulty by building an SIP register injection attack detection and mitigation technique. Prior to being processed by the Proxy Call Session Control Function. The proposed scheme verifies each initial register request from User Equipment (UE) at the home network of Internet Protocol Multimedia Subsystems (IMS) and compares it to the incoming SIP register request pattern with those stored on the scheme's table (P-CSCF). The proposed technique detects and drops every SIP register request with an abnormal pattern that is associated with an attack. The method proved promising with detection accuracy of over 96.67 percent, which is a solid potential as a preliminary setup towards the creation of a robust Real-time SIP detection and mitigation scheme for 5G networks.

Nomenclature and units

Thalach	VoLTE
Trestbps	Injection Attack
Restecg	Session Initiation Protocol
Fbs	Modified Hidden Markov Model

1.0 Introduction

Voice over Long-Term Evolution (VoLTE) is the solution for voice, video, and multimedia over fourth generation (4G) mobile networks. When compared to the traditional circuit switch (CS) voice network, VoLTE has evolved to an all-IP packet switched (PS) voice network, allowing for more SIP devices to connect and have faster connectivity. VoLTE calls connect in around 0.25 seconds with HD voice quality and support for video conferencing, whereas CS calls connect in approximately 6 seconds. Because of these features, several telecommunications businesses are now transitioning to VoLTE (Lonkar and Reddy, 2022). According to Ericsson, by the end of 2019,

VoLTE will have reached 2.1 billion subscribers (Ericsson, 2020). VoLTE enables global voice and multimedia service interoperability over 4G and 5G networks.

Because the VoLTE network is entirely made up of IP network traffic, it has become a target for some of the vulnerabilities found in traditional IP networks, such as the SIP REGISTER injection attack (Chalakkal *et al.*, 2017). Voice and multimedia data is sent over the LTE Radio Access Network (RAN) and Evolved Packet Core (EPC), which are both components of the LTE network, to connect IP Multimedia Subsystems (IMS) (Shaik *et al.*, 2019). All call management and control activities are handled by IMS. The Proxy Call Session Control Function (P-CSCF), the Interrogating Call Session Control Function (I-CSCF), the Serving Call Session Control Function (S-CSCF), and the Telephony Application Servers (TAS) are all part of it. The SIP diameter protocol is used for all communications within the IMS (Li *et al.*, 2015). The Enterprise Packet Core (EPC) consists of the Mobility Management Entity (MME), S-Gateway (S-GW), Packet Data Network (P-GW), Home Subscriber Server (HSS), and Policy and Charging Rule Function (PCRF).

Before it can transmit data, the user equipment (UE) must first connect to the LTE network and execute Radio Resource Control (RRC). During the RRC attachment, MME not only authenticates the UE but also assigns it a default bearer (IP) for internet access. When a UE indicates that it wants to make a VoLTE call, the PCRF creates a default bearer that is only used for SIP communication with the IMS and nothing else. SIP signals from the UE are sent through the MME to the SGW, which then sends them to the PGW. The PGW is the first point of contact between the UE and the IMS, and it is this node that informs the UE of the available P-CSCF address for routing SIP signals. This request allows the VoLTE user to register its presence on the IMS network, and in some situations, a covert channel is constructed to protect transmission (Zhang *et al.*, 2018). The SIP REGISTER request is the initial SIP signal sent by the UE.

Prior to using the LTE network, a UE must be connected to the LTE network, which allows the UE to be assigned the default LTE Evolve Packet System (EPS) bearer with QoS Class Identifier value of 6-9 (QCI 6-9) for internet access, followed by the default EPS bearer with QCI 5 which is only used for SIP signaling between the UE and IMS, as the SIP protocol on its own is vulnerable to several security threats (El-Moussa *et al.*, 2010). The LTE network will just serve as a superhighway for the IMS SIP signal before establishing a dedicated EPS bearer with QCI 1 and QCI 2 for audio and video calls, respectively. This is illustrated in Figure 1.

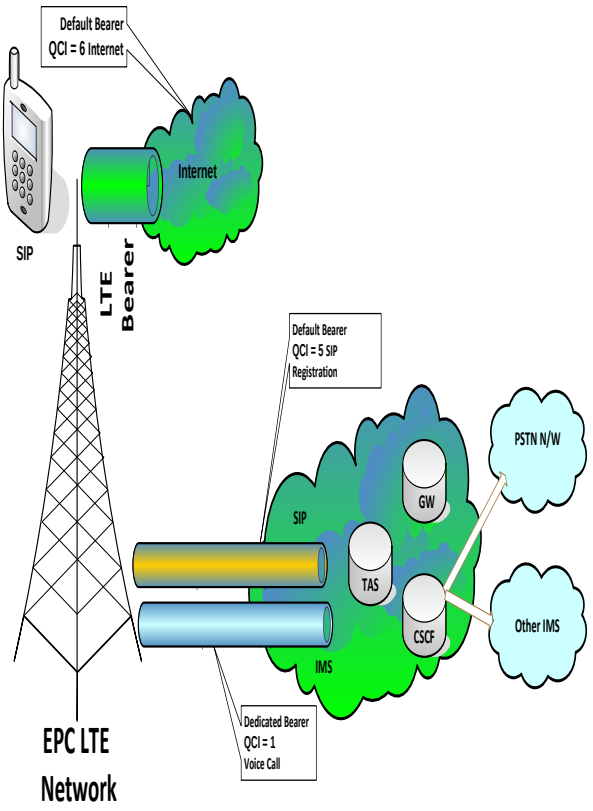

Figure 1: VoLTE Network.

The VoLTE SIP registration is done via the IP internet with the default EPS bearer for LTE and over the IP internet with the LAN RAN (Tóthfalusi and Varga, 2018). The SIP REGISTER request is initiated by the User Agent Client (UAC), and it is then transmitted via the LTE access network via the MME, then via the SGW to the PGW to the IMS network, with the P-CSCF serving as the first point of contact with the IMS network, as illustrated in Figure 1. After successfully establishing a default bearer with the IMS network, the UE attempts an initial unauthenticated registration with the IMS network; however, this unauthenticated SIP REGISTER request is refused by the IMS network's CSCFs. P-CSCF is attempting to contest the original SIP REGISTER attempt

by issuing an error 401 message (Zhang *et al.*, 2016). Despite the fact that it is being challenged, the first SIP REGISTER request contains the Internet Protocol User Identity (IMPU), the Private User Identity (IMPI), and the home network SIP User Resource Identifier (SIP URI). The P-CSCF encapsulates the request with a path header and sends it to the I-CSCF; once the I-CSCF receives the SIP REGISTER request, it sends it to the HSS, which uses the diameter User Authenticated Request (UAR) to obtain UE subscriber information and receives the answer via the User Authenticated Answer (UAA) (Majed *et al.*, 2017). The operation is complete after the HSS receives the authenticated parameters (Ashraf *et al.*, 2019). The I-CSCF performs IMS Authentication Key Agreement (AKA) security by forwarding the request to the next available S-CSCF, which contacts the HSS for multimedia authentication requests to collect the authentication vectors for completing IMS Authentication Key Agreement (AKA) security (Nakorji *et al.*, 2019). Finally, the S-CSCF sends a 401 Unauthorized to the UE via the I-CSCF to the P-CSCF, following which the UE sends a second SIP REGISTER attempt to authenticate itself using the AKA received with the 401 Unauthorized, and an IPSec connection is formed between the two networks. Finally, the CSCF responds with a 200 OK code, indicating that the UE has been registered successfully. This process is summarized as shown in Figures 2 and 3.

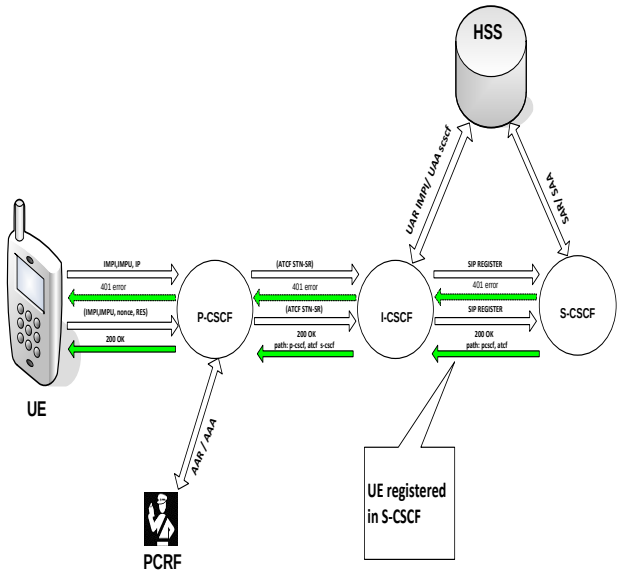

Figure 2: Complete UE SIP registration with IMS.

Even though the first SIP REGISTER request attempt is challenged by the CSCF before an IP Security (IPSec) connection is created, the initial SIP REGISTER request attempt, as seen in this research, goes through all of the IMS functional nodes. This means that an attacker can inject malicious code into the initial SIP REGISTER request to target the IMS core network in order to gain unauthorized access and perpetrate a distributed denial of service (DDoS) attack, spoofing other register users credentials from the HSS, or even bring down the entire IMS core network. Using a modified HMM model (mHMM) proposed in this study, SIP REGISTER injection attacks on VoLTE IMS UE registration were recognized and blocked (Nakorji *et al.*, 2019).

As a result, the paper's contribution is as follows:

1. Create a proxy tool for the VoLTE IMS core network's Proxy Call Session Control Function (P-CSCF) to detect and prevent SIP REGISTER injection attacks on the VoLTE network.
2. To use the Java programming language to simulate a VoLTE network and create a system that is 100% compatible with the VoLTE IMS network.
3. To create a proxy for the VoLTE IMS core network's Proxy Call Session Control Function (P-CSCF) to detect and prevent SIP Injection attack

The remainder of the paper is structured as follows: Section 2 2 describes the methodology, Section 3 provides the results and discussion, and Section 4 concludes the study.

2. Research Method

A VoLTE experimental network was simulated using JAVA. All the entire network functions were simulated, this comprises of the enodeB, Evolved Packet Core (MME, HSS, PCRF, SGW and PGW) with its IMS core network (P-CSCF, I-CSCF, S-CSCF and HSS) which are the main network functions responsible for UE SIP registration. The default bearers were equally mimicked with the QCI 5 to have a feel of the life VoLTE network speed. This was achieved by mimicking the SIP REGISTER request flow along the LTE control plane to CSCF of IMS and data was collated for computation of Detection Accuracy (D_A) of the proposed SIP REGISTER injection attack detection and prevention scheme. The system was developed from UE perspective. The experimental simulation was carried out on Windows 10pro, Intel(R) Core(TM) i5 – 3210M CPU @2.50GHz 2.50GHz with 12GB RAM.

Note that the simulated methodology was adopted because as at when this work was undertaken, no single telecommunication industry in Nigeria has deployed VoLTE services, they all relied on Circuit Switch fallback (CSFB) to make voice call, as such, there was no access to a life VoLTE network.

The scheme was developed using a two state modified Hidden Markov Model (mHMM), where each state of the mHMM model is made to observe each other which is not the case with a normal HMM model, this is to enable the incoming SIP REGISTER request to be compared with the legitimate (SR_L) stored in the mHMM tree. The illegitimate SIP REGISTER (injected SIP

REGISTER) requests messages were generated using a rooted UE with android version 8.1.0, precisely 213 SR_i were generated while legitimate SIP REGISTER request adopted for this work is the 3rd Generation Partnership Project (3GPP) IMS user equipment SIP REGISTER format. See figure 3.

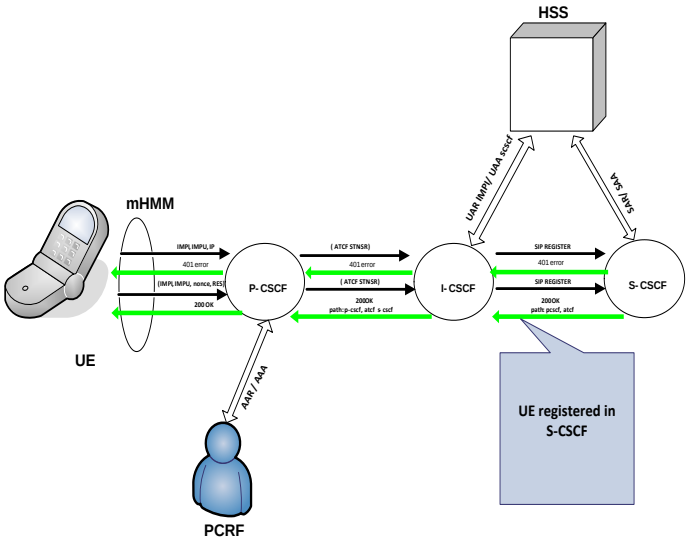

Figure 3: UE SIP Registration with mHMM Prevention and Detection Scheme.

The experimental set up consisted the UEs, UE_1 and UE_2, where UE_1 was used to generate legitimate SIP REGISTER request (SR_L), while UE_2 was used to generate illegitimate SIP REGISTER request (SR_i). The proposed scheme was then fed with the generated SIP REGISTER requests at random to ascertain the efficiency of the developed scheme. The experiment was conducted four times, with each experiment lasting for a period of 10 minutes to observe the efficiency of the scheme. The first experiment was conducted without the developed scheme with the illegitimate SIP REGISTER requests to ascertain the damage done to the IMS core network and the results were tabulated, a second experiment was conducted for legitimate SIP REGISTER request without the developed scheme and the results were tabulated, a third experiment was conducted with the developed scheme for illegitimate SIP REGISTER requests and the results were tabulated. A final experiment conducted with legitimate SIP REGISTER request with the developed scheme and the results were also collated for computing Detection Accuracy (D_A) and graphs were plotted.

The two mHMMs developed legitimate SIP REGISTER request (SR_L) and illegitimate SIP REGISTER request (SR_i) represented each. The two HMMs were modification in (U. Nakorji ***et al***, 2019) See figure 4.

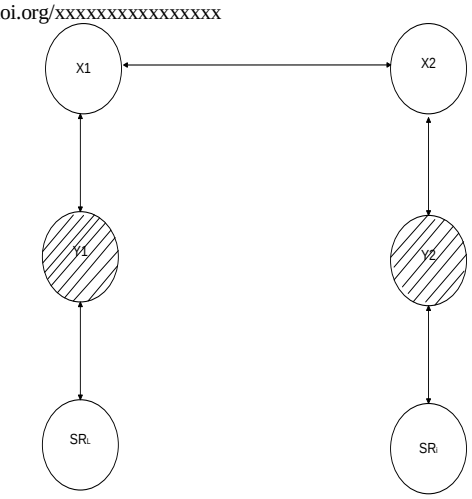

Figure 5: MODIFIED HMM MODEL FOR SIP REGISTER REQUEST FOR LEGITIMATE & ILLEGITIMATE USERS

Figure 4: Modified HMM Model SIP Register request of legitimate and Illegitimate call requests.

SR_L model has one observation state which contained all the standard features of 3GPP SIP REGISTER request, while SR_i has the features of malformed SIP REGISTER request with a single observation state. The mHMM act as a passive filter which is only active when SIP REGISTER request is observed, it only allows passage to P-CSCF when the SIP REGISTER request has a standard format as stored in the SR_L HMM model and drops any request contrary to that as represented.

The two HMMs is represented by equation (1);

$$\lambda_i = (A_i, B_i, \pi_i) \quad (1)$$

Where,

λ_i is the HMM model.

A_i is the transition state distribution

B_i is the observation state distribution

and π_i is the initial state distribution

The distribution variables of initial state distribution is determined by the percentage of the total numbers of initial SIP REGISTER requests sent to VoLTE IMS network, where 80% were SR_L and 20% were SR_i; this is presented in initial prior distribution state table in (2)

$$\pi_i = [x_1 \quad x_2] \times \begin{bmatrix} 0.8 \\ 0.2 \end{bmatrix} \quad (2)$$

The observation state distribution (B_i) is the modification made to the HMM model where the two HMMs (X_1 and X_2) were made to observe each other by making the summation of X_1 in the observation state equal to X_1 in the initial state distribution and likewise X_2. See table in (3)

$$B_i = [\mathrm{P}(X|Y)] \begin{bmatrix} 0.5 & 0.3 \\ 0.2 & 0.1 \end{bmatrix} \times \begin{bmatrix} Y_1 & Y_2 \\ X_1 & X_2 \end{bmatrix} \quad (3)$$

The transition state distribution (A_i) was computed with respect to time in the form of $P(X_t|Y_{t-1})$ which allows transition amongst the HMM states. The distribution state table is presented in (4)
Where,

$$A_i = [(\mathrm{Xt}|\mathrm{Yt}-1)] \begin{bmatrix} 0.7 & 0.3 \\ 0.9 & 0.1 \end{bmatrix} \times \begin{bmatrix} Y_1 & Y_2 \\ X_1 & X_2 \end{bmatrix} \quad (4)$$

The tucker condition for the modified HMM (mHMM) x_2 for dropping malicious SIP REGISTER request is given in (5).

$$f(x) = \begin{cases} x1, \ if \ 0.5 \geq y1 \leq 0.3 \\ x2, \ if \ 0.2 \geq y2 \leq 0.1 \end{cases} \quad (5)$$

3. Results and Discussion

This work was simulated adopting 3GPP VoLTE network architecture using JAVA, this is because as at when this work was undertaken there is no life VoLTE network deployed in Nigeria. The UEs were set to transmit SIP REGISTER requests at random to P-CSCF of the IMS with mHMM as its proxy. The mHMM work as a passive filter just for SIP REGISTER requests. Four scenarios were carried out, which are; sending an abnormal SIP REGISTER request to P-CSCF server without developed mHMM scheme, sending an abnormal SIP REGISTER request to P-CSCF with mHMM developed scheme, sending a normal SIP REGISTER request without the developed scheme and sending normal SIP REGISTER request with developed scheme. Each of the listed experimental scenarios lasted for 10 minutes, this is to enable observation of effectiveness of the developed scheme to prevention and detection of SIP REGISTER injection attack. At the first experiment, 120 illegitimate SIP REGISTER requests were sent to P-CSCF at interval without the developed mHMM scheme in place, before the 13th SIP REGISTER request was sent the IMS server was already taken down at about 1minute and 5 seconds (experimental time) by the illegitimate SIP REGISTER requests, this indicates that SIP REGISTER injection attack is quite harmful to VoLTE IMS network. For the second experiment, 120 illegitimate SIP REGISTER requests were sent to P-CSCF for registration only 3 made it through, 1 failed before it could not make it to P-CSCF for registration and 116 of the illegitimate requests were dropped by mHMM scheme, this implies that 96.67% of the illegitimate SIP REGISTER requests were detected and prevented from accessing the VoLTE IMS server for registration. When the third experiment was conducted with legitimate SIP REGISTER requests without the developed scheme it took less than 4 seconds (experimental time) for a UE SIP REGISTER request to complete its registration circle. The last experiment with mHMM scheme in place, it took UE with legitimate SIP REGISTER request about 5.7 seconds (experimental time) to complete its registration, this indicates that mHMM scheme poses a latency of 1.7 second (experimental time) which is negligible to the harm caused by SIP REGISTER injection attack.

3.1. Performance Evaluation

Detection Accuracy (D_A) was computed, and β_{dt} is the number of malicious SIP REGISTER requests correctly detected and prevented by mHMM scheme from harming VoLTE IMS network while α_{tl} is the total number of SIP REGISTER requests for the experiment. See equation (6)

$$D_A = \left\{\frac{\beta_{dt}}{\alpha_{tl}}\right\} X\ 100 \quad (6)$$

Latency (L_{tc}) due to mHMM scheme was computed using the duration ($£_t$) it takes a legitimate SIP REGISTER request to complete registration with the proposed scheme in place minus the duration (μ_t) it takes the same SIP REGISTER request without the proposed scheme in place using equation (7).

$$\text{Latency } (L_{tc}) = £_t - \mu_t \quad (7)$$

4. Conclusion

The results computed shows that without detection and prevention scheme as proxy to P-CSCF, when the VoLTE IMS network is attacked by SIP REGISTER injection attack, it takes less than 2 minutes (experimental time) to take down the entire IMS network and then gives the attacker the liberty to perform other attacks like DoS, spoofing user's identities from HSS server or eavesdropped on the VoLTE control traffic etc. When mHMM scheme was in place, 96.67% of the attacker's SIP REGISTER request was correctly detected and prevented from causing harm to the IMS network. However, a latency of 1.7 seconds (experimental time) was recorded, this latency can be negligible compared to damage caused by SIP REGISTER injection attack on VoLTE IMS network. Finally, further improvements can be made on mHMM scheme to improve the latency.

5 Acknowledgments

The Editorial team who took their time to critique this work to get this manuscript edited.

6 Notation

- β_{dt} : Number of illegitimate SIP REGISTER requests correctly detected.
- α_{tl} : Total number Illegitimate SIP REGISTER requests used.
- $£_t$: The time taken for SIP REGISTER request to complete registration with mHMM.
- μ_t : The time taken for SIP REGISTER request to complete registration without mHMM.

REFERENCES

Ashraf, H., Ullah, A., Tahira, S., & Sher, M. (2019). Efficient Certificate Based One-pass Authentication Protocol for IMS. *Journal of Internet Technology*, *20*(4), 1133-1143.

Chalakkal, S., Schmidt, H., & Park, S. (2017). Practical attacks on volte and vowifi. *ERNW Enno Rey Netzwerke, Tech. Rep*.

El-Moussa, F., Mudhar, P., & Jones, A. (2010). Overview of SIP attacks and countermeasures. Information Security and Digital Forensics: First International Conference, ISDF 2009, London, United Kingdom, September 7-9, 2009, Revised Selected Papers 1,

Ericsson. (2020). *VoLTE*. Retrieved May 15th 2020 from https://www.ericsson.com/en/volte

Li, C.-Y., Tu, G.-H., Peng, C., Yuan, Z., Li, Y., Lu, S., & Wang, X. (2015). Insecurity of voice solution VoLTE in LTE mobile networks. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security,

Lonkar, S. A., & Reddy, K. V. (2022). Analysis of audio and video quality of voice over LTE (VoLTE) call. *International Journal of Information Technology*, *14*(4), 1981-1994.

Majed, N., Ragot, S., Lagrange, X., & Blanc, A. (2017). Delay and quality metrics in Voice over LTE (VoLTE) networks: An end-terminal perspective. 2017 International Conference on Computing, Networking and Communications (ICNC),

Nakorji, U. H., Adedokun, E., Umoh, I., & Shettima, A. (2019). Mitigating coordinated call attacks on VoIP networks using hidden markov model. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 337-344.

Shaik, A., Borgaonkar, R., Park, S., & Seifert, J.-P. (2019). New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks,

Tóthfalusi, T., & Varga, P. (2018). Assembling SIP-based VoLTE Call Data Records based on network monitoring. *Telecommunication Systems*, *68*(3), 393-407.

Zhang, S., Zhou, L., Wu, M., Tang, Z., Ruan, N., & Zhu, H. (2016). Automatic detection of SIP-aware attacks on VoLTE device. 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall),

Zhang, X., Tan, Y.-A., Liang, C., Li, Y., & Li, J. (2018). A covert channel over volte via adjusting silence periods. *IEEE Access*, *6*, 9292-9302.