International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

System for Rogue VoIP Phone Detection and Managing VoIP Phone Mobility

Ilyas Khudhair Dubi, Ghiath Mageb Waheeb, Saif Ahmed Jabbar, Hasimi Sallehuddin, Nurhizam Safie Mohd Satar, Farashazillah Yahya, Nur Azaliah Abu Bakar

Abstract*: *The quickly propelling Voice over Internet Protocol (VoIP) innovation, is picking up customer fascination in the business today. Its uses, including IP communication frameworks, includes the transmission of voice as information bundles which after achieving the getting side, reassembles and deciphers according to necessity. This encourages open just as private IP frameworks. The real drawback, keeping numerous organizations off from utilizing VoIP advances is related to the security of this framework. This paper examines a strategy and the following framework that get to arrange data for approved system gadgets. The entrance insights and data empower to follow gadget development all through the system. In addition, it offers to recognize unapproved gadgets making false endeavors to get to the system, presenting to be an approved access gadget.

Index Terms*: *VoIP security threats, VoIP attacks.

I. INTRODUCTION

The VOIP is a strategy for correspondence, in a perfect world open if the need emerges, by using the quick web instead of settling on a customary phone line. VOIP offers spending neighbourly correspondence rates, due to which the business has moved over to this development generally in order to save time, money and be given trustworthy encryption. The past structure uses circuit switch orchestrate, yet it has been overhauled by the Internet Protocol-based group traded frameworks. VOIP structure contains telephones, control and door centre points and IP arrange. A one of a kind sort of media is used by the IP mastermind, for instance, Ethernet, fibre and remote for correspondence [1].

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Ilyas Khudhair Dubi*, Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia
Ghiath Mageb Waheeb, Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia
Saif Ahmed Jabbar, Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia
Hasimi Sallehuddin, Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia
Nurhizam Safie Mohd Satar, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Selangor, Malaysia
Farashazillah Yahya, Faculty of Computing & Informatics, Universiti Malaysia Sabah, Malaysia
Nur Azaliah Abu Bakar, Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia

This advancement has gotten the thought and energy of people in the business for quite a while now. A noteworthy number of Voice over Internet Protocol applications propose many open features on standard Private Branch exchange (PBX) plans. At the point when all is said in done, a suite of shows are used by the VOIP developments including hailing shows, for instance, SIP (Session Initiation Protocol), data control and trade shows, for instance, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Real-Time Transport Protocol (RTP), and Internet Protocol (IP). VOIP applications, for instance, IP correspondence systems, incorporate the transmission of voice as data groups which in the wake of accomplishing the tolerating side, reassembles and makes an interpretation of as indicated by essential. This empowers open similarly to private IP structures. One essential disadvantage is connected with the security of this structure, keeping various associations off from using VoIP headways. Encryption is always evaluated an essential bit of VoIP applications, expanding considerably more important stress in the business [2]. Customarily interlopers are known to be the general population who attempts getting unapproved access to PBX or telephone message structures while using free telephone calls by false controls. As demonstrated by a few researchers, such infringing undertakings occur in light of the way that the commuter is up for revenge, squeeze, mischief or some other individual interest. VoIP may in like present manner risks of call catch endeavour, breaking into someone's telephone message, or even check out the ordered discourses over IP frameworks. Another rising correspondence advancement, Voice over IP (VOIP), proposes different central focuses over Public Switched Telephone Network (PSTN) [1]. One of them is a by and large simple convenience of the VOIP phone. Customers can without a lot of a stretch move their phone beginning with one such port then onto the following in the basically like appending machines to an electrical fitting. Regardless, this transportability can make a cerebral agony for VoIP sort out director iterators. Exactly when customers are empowered full chance to move their phone, administrators can end up being altogether negligent concerning which phones are related with which switch port. Fail to screen phone territory suggests that correct phone position can't be given if there is a requesting from E911 structure. Likewise, it leaves the framework powerless to access by unapproved devices acting like endorsed devices.

A dissident phone can without a lot of a stretch tap into the framework and start unapproved organization or dispatch an attack on others One proposed response to the issue is to fix one change port to be committed for one VoIP phone just so a switch propels only the traffic started from the Media Access Control (MAC) address of that phone [3]. In this examination, Fix one change port to be given for one VoIP phone just so a switch propels only the traffic began from the Media

Access Control (MAC) address of that phone and rely upon a switch ' s customized channel set up. In this proposed plan the switch sets the essential MAC address, it sees as the primary endorsed contraption.

II. REVIEW

In February 1995, Vocaltec, Inc, an Israeli association, started VOIP. It incorporates the transference of voice-over quick framework, which is affordable when appeared differently in relation to PSTN and reachable wherever through the web by oddball made by Google with 4G LTE speed6.

A. *H.323*

H.323 is the first historically speaking sight and sound correspondence standard convention, distributed by ITU in February 1996. To join voice, video and information, it utilizes parcel arrange. It utilizes PSTN at the back by having characteristics of WWW. The fundamental pieces of H.323 design incorporate the terminal points, Multipoint Control Units (MCUs), Gateways, Gatekeepers, Peer and Border Elements. Each segment possesses its own element and usefulness like: Termination focuses are the terminals, for example end focuses. For instance; Soft telephones, Telephone and so forth.

- Conference calls can be made by utilizing the multipurpose MCUs.
- The Gateway interface alludes for correspondence between various conventions.
- Gatekeeper isn't a mandatory constituent, however it helps in the call affirmation and address goals. It can likewise make direct calls.
- Peer Elements switch the location data, and works inside the regulatory area [4].

This convention subtleties on how the voice, video or different components of the information, can be exchanged utilizing the IP built systems.

- Authentication: The accompanying kinds of confirmation exists i.e.:
- Symmetric encryption: no prerequisite of clients' pre-association
- Awry encryption: need of a mutual key before the correspondence
- Encryption: Encryption in VOIP is parcel based. It shifts with the amount of parcels, the rules and the principles.

B. *MGCP (Media gateway control convention)*

MGCP is an IETF VoIP expected for private doors, IP based telephones and huge trunks portals. It helps in correspondence between the various pieces of VOIP entryways. It is a relating convention to SIP and H.323. SGCP and IPDC set of conventions from which MGCP is determined. The convention structure contains a "call specialist" which is a server controlling calls and different administrations. Call specialist gives guidelines which are executed by this portal [6]. MGCP deals with a call control way. This convention parts they consider control from the employable unit and media passage control [5].

C. *SIP (Session Initiation Protocol)*

This content-based convention is not the same as H.323. It is utilized generally and is effectively open. Taste is conveyed by an assortment of conventions, for example, Transmission control convention and client datagram convention with low costs and improved effectiveness. It's organized as endpoints, an intermediary and area server, and a recorder. The area serves SIP productive [6]. It chips away at two-way correspondence design. At times it resembles HTTP. Being a flagging convention, SIP utilizes RTP for the exchange of media. The RTP convention contains start to finish encryption work. Taste is utilizing distinctive transport conventions which are TCP, UDP and SCTP. These simple to-utilize conventions have great highlights when contrasted with different conventions. UDP keeps up a dimension of execution, while TCP aids protected calls. Stream control transmission convention (SCTP) is essential in decreasing the DOS assaults [6].

III. VOIP SECURITY ISSUES

VoIP transmits the voice based on the information organized by means of various components including switches and switches that associate PSTN to the web. VoIP contains security issues for voice/video traffic which are normal in circuit switch organize, for example, tapping and fake assaults and other IP related issues. Security issues can be ordered into the following three kinds.FBI reviews, in the United States, revealed that various security occasions inside occupations submitted by present or previous workers, temporary workers, sellers with private information, lucky access or dependable inside affiliations. The response to "essential security prerequisites of VoIP" by [7] is as expressed: "An important state of any information the executive's framework suggests the insurance and unapproved exposure of private data, information and assets and unapproved or wrong adjustment, at the same time guaranteeing their comfort to certified clients." Three central security necessities, named secrecy, trustworthiness and accessibility, should be provided food to stay away from security dangers. In light of a couple of studies [5, 12], Table 1 condenses the bogus endeavours and connected dangers to security necessities in VoIP databases. Conceivable safety efforts are recommended in the accompanying sub-areas to handle every one of the security dangers.

Table I. Some Security Attacks And Threats In Voip

Threats	Confidentiality	Availability
Rogue sets	√	
Toll fraud		√
DHCP configuration		√

A. *Real-Time Issues*

VoIP utilized for various unlawful exercises, for example, hacking, and fear mongering and so on for as far back as a couple of decades. As of late in October 2014,

an occasion happened where telephone programmers broke into the telephone system of a firm and coordinated calls worth $166, 000 from the organization to finest rate phone numbers in Gambia, Maldives and Somalia. For right around 34 years, the organization would have escaped its phone charge charges.

B. *Network Related Issues*

Table 1 records the unlawful endeavours to nullify, square, uncover, change, take or accomplish unapproved access to data in VoIP organize pursued by various kinds of assaults.

C. *Voice Related Issues*

In view of voice traffic in VOIP structure, voice can be imitated by an assailant. A robot that dialogues and sings mimicking human vocalization, was made by M. Kitani, Kagawa University and is exposed to VoIP communication.

IV. VOIP ATTACKS

These segment subtleties various sorts of VoIP strikes.

A. *Physical Attacks*

Physical assault is done by the taking and breaking of system or by really controlling the gear/structure by getting unapproved access to districts containing unbelievable data. A few physical strikes combine dumpster skipping, gear key lumberjack and unequivocal access, and so on. It may be dismissed by maintaining the reports and account records safely inside the additional room and secret word to ensure all the hardware. At long last, security watchmen ought to be passed on outside at entering and leave focuses.

B. *ARP Spoofing*

Programming engineer spreads fake Address Resolution Protocol (ARP) circles VoIP sort out by changing ARP pad. Here, interloper ties guarantee structure MAC address with IP address of the demanded server which involves the traffic towards the aggressor. Programming planner may then take a gander at VOIP calls and answer or end them. ARP beating searched for after by surrendering affiliation dangers or spying, interruption or change perils which present senseless costs to the goal. In this way, Boosted ARP might relate to avoiding ARP deluding 11.

C. *IP Spoofing*

Assailant sneaks into the VoIP structure by getting the IP address of any admitted machine which makes him spread contemptuous note inside the framework. IP speaking to strengthens interloper to progress further ambushes, for instance, DoS attack, affiliations' robbery, toll dubiousness, etc. by reflecting affirmed have. All around, IP despising can be denied with most strange shots by arranging logically wide passage switch. In any case, change avoids pushing toward packs for endpoint address beginning from source address inside a structure. Second, change squares to control packs from close to structure to another. Y. Mother developed an inducing look for after course based way for precaution against IP dumbfounding and it is operated with reliable coterminous centers information.

D. *ICMP Flood*

One of the structures layers shows up, Internet Control Message Protocol (ICMP), transmit botch and arrangements messages sent by centre or end centre core interests. An intruder tries to wealth the recipient store by flooding the individual concentration with packs of ICMP. It demands that within point drop bundles until space gets free at the centre's extra. To set perfect concentrations for progressing toward traffic from different frameworks, switches are orchestrated. It will push the movements to not simply square inconsequential ICMP packages by dealing with ICMP requests yet in like manner slaughter bounty store. The undeniable VLAN must be composed by VOIP structures for firewall checked single framework packs. Brahui et al. have set up a framework that sees slip to see various sorts of ICMP attacks13. It incorporates two modules. Affirmation module bears witness to the beginning of ICMP groups, while Congestion check module isolates the usage of exchange speed information using the Simple Network Management Protocol (SNMP).

E. *TCP/UDP Floods*

In TCP flooding trap happens when maker produces gigantic SYN packs with atypical source IP passes on and exchanges to a beneficiary. Open focus doles out space in its Transmission Control Buffer (TCB) to each SYN demands. In answer to SYN packs, receptor sends SYN+ACK gatherings while keeping it together for ACK parties. The SYN+ACK packs pass on nonstandard IP passes on perceiving weakness to see ACK bunches which has recipient focus point to clear TCP SYN demands from assistance to flood later. Gatecrasher can use TCP flood event against VoIP hailing appear, for example, H.323 and SIP, both being association arranged appears. Harris et al. have winning to see TCP flood strike in correspondence by isolating payload and unusable zone of the HTTP appear [8]. In a UDP flood strike, a tremendous degree of UDP packs gets shaped with interesting source zones and port numbers. A short-range later, it is sent to the objective focus point. The receptor will check process keep running on those ports and locate a basic number of the ports blocked. As essentials are, recipient focus point makes an immense number of obstructed target packs. Updated number of ICMP packs surrender inside point and structure flood. The UDP flood strike stops genuine focus fixations to interconnect the sad disaster focus point. Gatecrasher can utilize UDP flood trap against VoIP transport appear, for example, connectionless shows RTP and RTCP. Bardas et al. predicted a relative gathering rate supposition framework to see UDP traffic for seeing false IP will with everything considered in charge of UDP flood attempts.

V. METHODOLOGY

Every one of these cases makes potential issues for the VoIP specialist co-op that may contrarily influence the administration to perform

mince as per one part of the creation a strategy and framework recognize telephone development on a VoIP arrange This empowers a director to monitor where the telephones are.

A maverick IP telephone additionally can be distinguished by marginally altering the methodology. As indicated by one exemplification the technique and framework examine each conceivable instance of a maverick telephone getting to the system pursued by broad methodologies to identify them in various cases. The unveiled epitome fabricates a database, called an Access Control List (ACL), which can be utilized for following telephone development, recognizing maverick gadgets, and/or physically finding a telephone for Extended - 911 (E911) use. In this manner, as per the creation a technique and framework can identify telephone development starting with one area then onto the next; uphold the telephone development by blocking administration for unapproved telephone move ; distinguish rebel IP telephone stopped to VIP arrange quickly, advise the IT staff of the interruption and square the calls began from the telephone find the IP telephone physically, whether it is real or not ; and furnish IT staffs with a way to empower and handicap a switch port [9].

VI. ROGUE SETS

Assaults are misleading with the end goal of access acquisitions to another person's assets. Computerized pantomime is accomplished by the assailants by including another arrangement of VoIP application to the encroached IP systems, when ID is tricking a focused accessible if the need arises member. At that point the noxious VoIP application can complete any action that may harm the IP framework enduring an onslaught. VoIP applications can complete a system lockdown to address such assaults. Just the overseers of a specific system can change sets of VOIP applications with a secret phrase known and subtleties are sent to the head after including new set. VoIP application will stop in the event of in excess of three wrong secret word sections. To put it plainly, maverick sets assaults present security dangers to protection on the grounds that the interlopers get unapproved access to an IP to arrange.

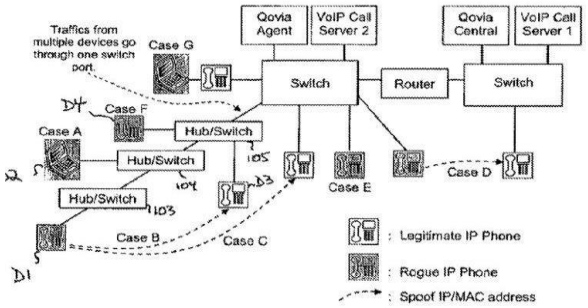

Figure 1

- *Case A:* Rogue Phone on Daisy – Chain: A rogue phone is connected to one hub/switch of a daisy-chained port and it is stealing an IP / MAC address of a phone that is hooked up to the switch directly via a different port Traffic generated from both phones travel through different switch ports of the same switch. Both phones cannot be online simultaneously as the MAC address collides. However, if the legitimate phone is off or unplugged the rogue phone can use the spoofed address for access.
- *Case B:* Rogue Phone on Switch Port Direct – A rogue phone is connected to a switch directly and it is stealing MAC address of a phone on a different subnet Traffic generated from both phones travel through different switch ports. Both phones may be online simultaneously if different IP addresses are used. The rogue phone will be able to make phone calls without any problem because VoIP call server identifies a phone by MAC address not by its IP address. But this scenario is possible when there is only one VoIP call server servicing the whole campus or university VoIP call server servicing the whole campus or university one thing that is not clear is the case when there are multiple VoIP call servers servicing different subnets. Say a legitimate phone is serviced by VoIP call server 1 and rogue phone by VoIP call server 2; the legitimate phone is registered on VoIP call server 1 and rogue phone is to be served by VoIP call server 2. Unless there is a database sharing or synchronization between the two VoIP call servers, the rogue phone won't be able to make a phone call.
- *Case C:* Rogue Phone on Switch Port Direct - The intruder introduces some arbitrary MAC address which is not registered on VoIP call server. It won't be able to make a legitimate call but could generate a malicious attack like a denial of service (DOS).

VII. DETECTING ROGUE OF IP PHONE

A key point in identifying a rogue IP phone is to track down the switch port to which the rogue phone is plugged. This port data can be compared with the port number of a connected legitimate phone, whose MAC address has been spoofed by the rogue phone. It is a rogue phone if MAC address matches but switch IP address or port number mismatch. The ACL, as was explained before, should be built to contain legitimate MAC addresses and a switch port that such addresses are authorized to plug into. Once the database is ready, a detection algorithm can be put into operation. Four different detection strategies are disclosed here. They can be deployed in combination depending on the network topology and enforcement policy.

A. *Detection by Traffic Monitoring Based on MAC Address.*

This process relies on an agent monitoring all the VoIP traffic from IP phones. It examines a MAC address of a VoIP packet originated from the subnet with which the agent is associated. It is assumed that all device MAC addresses are conveyed up to the agent's monitoring point. This technique may not work when a layer3 switch is used, where the device MAC address is usually stripped off while the frame crosses a subnet boundary. When a new phone is plugged to a port, the agent would query the switch and determine the port number to which it is connected. By comparing the discovered port number with the port number in ACL which it is supposed to be hooked up to this MAC address, we can detect if the new phone is a rogue one. A possible set of steps for performing this process are as follows:

- Agent constantly monitors MAC of all VoIP calls under its supervision.

- A rogue IP phone is plugged in with spoofed MAC address, called MAC_spoofed.
- SNMP trap (switch_IP, switch_port) generated, which triggers Agent to stay in alert mode keeping an eye on the port.
- Suppose a new call is initiated from a rogue phone.
- The agent detects a new call originated from MAC_spoofed.
- Agent queries all the switches under its supervision asking from which port the MAC_spoofed frames originated. Switch_IP and switch_port obtained at step 3 can be a cue for the search. Call the returned answers switch_IP_found and switch_port_found.
- Check the (switch_IP_found, switch_port_found, MAC_spoofed) against ACL.
- If MAC address matches, but switch_IP or switch_port does not.

B. *Alternative Detection Process Analyzes "Heartbeat" Messages.*

The purpose of generating a heartbeat message is to let the other end, such as a VoIP call server or phone, know a phone is present and "alive". It is sent out periodically to the phone's peer(s) and if such a signal is not detected or received within a period by the peer, the phone is regarded to be "dead" or malfunctioning by that peer. This method is adequate only if contents of heartbeat messages, exchanged between the IP phone and VoIP call server, can be decoded. It is assumed that the heartbeat messages contain IP and MAC addresses of the devices in the message payload, not in the header. The basic idea is to constantly monitor the heartbeats and keep track of new phones plugged in or removed. When a new call shows up, the switch is queried via SNMP, and the agent tries to find the MAC address and switch port number, given source IP address of the call. A possible set of steps for performing this process is as follows:

- Agent constantly monitors all the heartbeat messages exchanged between the VoIP call server and VoIP phones under its supervision.
- Decoding the heartbeat messages, the agent retrieves IP and MAC address of IP phone and maintains a list of active MAC and IP address.
- Check if any new IP/MAC address shows up against the active phone list.
- If new IP/MAC shows up while decoding the heartbeat, Agent queries via SNMP all the switches under its supervision asking from which switch port the IP/MAC address originated. The returned answers are referred to as switch_IP_found and switch_port_found.
- Check the (switch_IP_found, switch_port_found, MAC/IP) against ACL.
- If MAC address matches, but switch_IP or switch_port does not match, it is a rogue phone or a move one.

C. *Monitor all the VoIP traffic*

There can be cases where an agent cannot grab the device MAC address by any means because it is stripped off when a frame crosses a subnet boundary, or it is incorrect if layer 3 switch is involved in switching. This alternative detection process relies on an IP address rather than on MAC address. So, it is adequate regardless of whether the agent is located at a different subnet or the same subnet as the IP phone. It also works when the Layer3 switch is used. In the alternative, the basic idea is to monitor all the VoIP traffic and whenever a new call is discovered, the agent tries to find the MAC address and switch port number given source IP address of the call. It queries switch via SNMP. A possible set of steps for performing this process is as follows:

- Agent constantly monitors the IP address of all VoIP calls under its supervision.
- A rogue IP phone is plugged in with spoofed MAC address, called MAC_spoofed.
- SNMP trap (switch_IP, switch_port) generated, which triggers Agent to stay in alert mode keeping an eye on the port.
- A new call is initiated from a rogue phone.
- The agent detects a new call with IP_address originated from a could-be-rogue device.
- Agent queries via SNMP all the switches under its supervision asking from which port the IP_address packets originated and what is the MAC address of the device. Switch_IP and switch_port obtained at step 3 can be a cue for the search. Let's call the returned
- Answers switch_IP_found, switch_port_found and MAC_found.
- Check the (switch_IP_found, switch_port_found, MAC_found) against ACL.
- If MAC address matches, but switch_IP or switch_port does not match, it is a rogue phone or moved one.

D. *Traffic monitoring*

Yet another alternative detection process is available, but this method does not rely on traffic monitoring and takes some time to detect. As it depends upon SNMP trap which is not 100% reliable, it may be of more limited value if used as a sole measure. The basic idea in this alternative is to catch SNMP trap generated by a switch when a phone is plugged in and query the switch as to what is the port number the phone is plugged. A possible set of steps for performing this process is as follows:

- A rogue IP phone is plugged in with spoofed MAC address, called MAC_spoofed
- SNMP trap (switch_IP, switch_port) is generated.
- Agent issues SNMP query to switch_IP asking what the MAC address of devices plugged to switch_port are. It may take a couple of minutes for a switch to discover device MAC address. The MAC address found can be referred to as MAC_found.
- Check the (switch_IP, switch_port, MAC_found) against ACL

If MAC address matches, but switch_IP or switch_port does not match, it is a rogue phone or moved one.

VIII. CONCLUSION

We have summarized basic concepts on VoIP, and outlined all of its most important threats. As VoIP gains terrain in the world of telecommunications,

it seems that soon it will become one of the dominant technologies in telephony. Future work also includes software attacks prevention through solid security policies and their enforcement. Also, it is imperative to design intrusion detection systems capable of coping with emerging encrypted and polymorphic malicious code. Rogue sets represent protection from a constant threat which several systems have not yet been able to contain. The continuing adoption of VoIP in corporations has made more evident the urgency of efficient defence systems against these attacks.

ACKNOWLEDGMENT

We gratefully acknowledge that this research paper was funded by the National University of Malaysia Research Grant GGPM-2018-012 and Research Center for Software Technology and Management (SOFTAM), Faculty of Information Science & Technology (FTSM), UKM.

REFERENCES

1. Gavilanez, O., Gavilanez, F., & Rodriguez, G. (2017). Audit Analysis Models, Security Frameworks and Their Relevance for VoIP. arXiv preprint arXiv:1704.02440.
2. Shivankar, S. J., & Tembhurkar, M. P. (2015, February). Comparative analysis on security techniques in VoIP environment. In 2015 2nd International Conference
3. On Electronics and Communication Systems (ICECS) (pp. 1176-1180). IEEE.
4. Ghafarian, A., Seno, S. A. H., & Dehghani, M. (2016, July). An empirical study of security of VoIP system. In 2016 SAI Computing Conference (SAI) (pp. 1031-1036). IEEE.
5. Sadkhan, E. S. B., Al-Shukur, B. K., & Mattar, A. K. (2016, May). Survey of biometrie based key generation to enhance security of cryptosystems. In 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA) (pp. 1-6). IEEE.
6. Dermanilian, H. M., Saab, F., Elhajj, I. H., Kayssi, A., & Chehab, A. (2015). Energy-Efficient Security for Voice over IP. International Journal of Network Security, 17(1), 11-26.
7. Nogueira, T. A., Menezes, A. C., Admilson de Ribamar, L. R., & Ordonez, E. D. M. (2017). A Security Approach using SIP Protocol in Imbedded Systems. In WEBIST (pp. 352-355).
8. Safoine, R., Mounir, S., & Farchi, A. (2018, May). Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks. In 2018 6th International Conference on Multimedia Computing and Systems (ICMCS) (pp. 1-5). IEEE.
9. Miraz, M. H., Molvi, S. A., Ganie, M. A., Ali, M., & Hussein, A. H. (2017). Simulation and analysis of quality of service (QoS) parameters of voice over IP (VoIP) traffic through heterogeneous networks. arXiv preprint arXiv:1708.01572.
10. Shim, C. B., & Byun, J. (2017). U.S. Patent No. 9,749,337. Washington, DC: U.S. Patent and Trademark Office.

AUTHORS PROFILE

Ilyas Khudhair Dubi, Study Master in computer science **(**Network Technology) in Universiti Kebangsaan Malaysia.

Ghiath Mageb Waheeb, Study Master in computer science **(**Network Technology), Universiti Kebangsaan Malaysia.

Saif Ahmed Jabbar, Study Master in computer science **(**Network Technology), Universiti Kebangsaan Malaysia.

Hasimi Sallehuddin, is a senior lecturer at Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia. His research interest is in computer security and networks and also management information system

Nurhizam Safie, is a Professor Madya at Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia.

Farashazillah Yahya is a senior lecturer at Faculty of Computing & Informatics, Universiti Malaysia Sabah in Kota Kinabalu, Sabah Malaysia.

Nur Azaliah Abu Bakar is a Senior Lecturer at Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia.