Reference Phone Number: A Secure and QoS-Improved SIP-Based Phone System

WenBin Hsieh *

Posted Date: 27 January 2025

doi: 10.20944/preprints202501.1897.v1

Keywords: SIP; RTP; ECMQV; Reference Number; Security

Article

Reference Phone Number : A Secure and QoS-Improved SIP-Based Phone System

WenBin Hsieh

Department of Green Energy and Information Technology, National Taitung University, Taitung, 950309, Taiwan; d9802106@gmail.com or wbhsieh@nttu.edu.tw

Abstract: With the improvement of the internet and the widespread adoption of digital communication devices such as smartphones, VoIP has largely replaced traditional telephone systems. Many companies are deploying VoIP systems due to their scalability and low cost. In this paper, address the issue of remote clients or traveling employees being unable to contact business partners due to specific phone numbers. We propose a reference phone number mechanism that combines a set of related business partners' phone numbers to enhance call availability. To ensure the confidentiality of calls, we also designed an algorithm to integrate key exchange protocols into the proposed mechanism. The mechanism can flexibly customize the required security protocols. A performance analysis is conducted by deploying the proposed mechanism in a medium-sized company. The results prove that the mechanism is feasible and the effect is satisfactory.

Keywords: SIP; RTP; ECMQV; Reference Number; Security

1. Introduction

With the widespread deployment of optical fiber lines in wired networks and the vigorous development of 4G/5G mobile networks, the bandwidth of the network has increased significantly. Voice over Internet Protocol (VoIP) has almost replaced the traditional phone systems such as the analog PBX phone system. People who own smartphones have mobile numbers, but in order to save communication costs, they still prefer to communicate through VoIP applications installed in their smartphones. Many companies have also deployed VoIP systems to reduce operating costs, especially for multinational companies that require overseas phone calls or video conferencing. Moreover, VoIP also provides scalability, allowing growing businesses to expand their branches and employees. The portability of virtual phone numbers like VoIP also brings convenience to employees who frequently travel. In order to provide a stable and versatile method to perform VoIP, many protocols have been invented to support VoIP services, such as H.323 [27], Media Gateway Control Protocol (MGCP) [28] and SIP. Among all these protocols, 3GPP defines SIP as one of the most important signaling protocols for VoIP, because SIP has many advantages such as ease to implement, support for multimedia communications, modularity, and Extensibility. SIP has user-friendly syntax and operations similar to HTTP, making it rapid to understand and deploy. SIP supports multimedia communication sessions, including voice, video, instant messaging, and presence. The modular architecture of SIP allows the addition of new features and functionalities through extensions and adjustments.

2. Background and Motivation

There has been a long-standing demand for secure VoIP communication between private companies and public institutions. Therefore, numerous encryption mechanisms have been designed and adopted to protect end-to-end communication. These encryption mechanisms require the establishment of a session between two user agents, in which the two user agents exchange certificates containing their public keys. That is, callers must remember the callee's phone number to

 doi:10.20944/preprints202501.1897.v1

initiate a dial-up call. This presents a significant inconvenience for users who must communicate with a large number of customers or colleagues, as well as for engineers who are traveling or working remotely and need to temporarily reach out to operators in the data center. To offer users more convenient VoIP services, the need for virtual reference phone numbers arises. Figure 1 illustrates the demand structure. The reference phone numbers are virtual, meaning corresponding physical certificates cannot be exchanged to negotiate session keys. Therefore, to address this need, this article makes the following contributions:

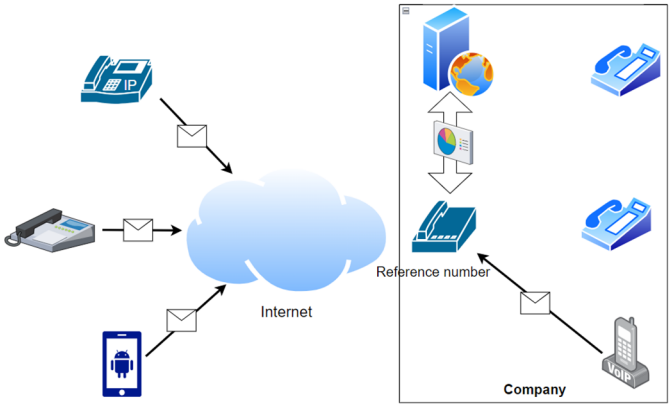

Figure 1. A virtual reference phone number to physical VoIP numbers.

1. We proposed a mechanism for converting reference phone numbers to physical phone numbers and demonstrated its feasibility by implementing the mechanism.
2. After deployment and application, as well as the statistical data analysis in this paper, the call success rate proves to be efficient and meets users' expectations.
3. The proposed mechanism is universal, meaning users have the flexibility to replace the key agreement algorithm or VoIP protocol with their preferred choices.

The structure of this article is as follows. Section III describes the necessary knowledge and related work. In Section IV, we propose architecture employing algorithmic reference phone numbers. The performance of the proposed approach is shown in Section V, along with a discussion of its benefits and drawbacks. Section VI concludes the work as well as some ideas for future research.

3. Preliminary and Related Work

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental conclusions that can be drawn.

3.1. SIP Overview

There are two types of entities defined in SIP, which are user agents (UAs) and servers. UAs stands for SIP endpoints. A SIP server consists of a registration server for location management and a proxy server for message forwarding. SIP messages can be classified into requests, such as INVITE and BYE for establishing and terminating SIP sessions respectively, and responses, such as 200 OK to confirm session settings. A SIP transaction refers to a set of messages comprising a request and its associated response.

SIP message forwarding (called proxying) is a key feature of the SIP infrastructure. This forwarding process is provided by the proxy server and can be stateless or stateful. Stateless proxies do not maintain state information about SIP sessions and therefore tend to be more scalable. However, many standard application features, such as authentication, authorization, accounting, and call forking, require the proxy server to operate in a stateful mode by retaining different levels of session state information.

 doi:10.20944/preprints202501.1897.v1

A typical message flow for a SIP proxy state with authentication enabled is shown in Figure 2. Two SIP user agents, designated as User Agent Client (UAC) and User Agent Server (UAS), represent the roles of caller and callee in a multimedia session. In this example [1, 2], the UAC wants to establish a with the UAS and send an INVITE message to the agent. The proxy server responds with a 407 Proxy Authentication required session message to enforce proxy authentication, requiring the UAC to provide credentials to verify its claimed identity (e.g., based on the MD5 [3] digest algorithm). The UAC then retransmits the INVITE message and includes the generated credential in the Authorization header. After the proxy receives and verifies the UAC credential, it will send a 100 TRYING message to notify the UAC that the message has been received, and there is no need to worry about hop-by-hop retransmission. The proxy then looks for the contact address of the UAS's SIP URI and, if available, forwards the message. In turn, the UAS acknowledges receipt of the INVITE message with a 180 RINGING message and causes the callee's phone to ring. When the called party actually picks up the phone, the UAS returns 200 OK. Both the 180 RINGING and 200 OK messages are sent back to UAC through the proxy.

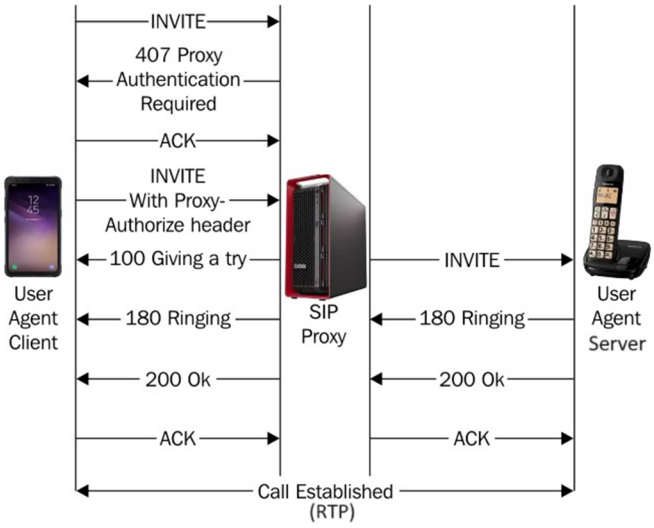

Figure 2. SIP stateful proxy for authentication.

The UAC then acknowledges the 200 OK message with an ACK message. After establishing a session, the two endpoints communicate directly point-to-point using media protocols such as RTP [4].

SIP proxy authentication is optional and usually occurs between the UA and its first-hop SIP proxy server. While the example above depicts a single SIP proxy on the path, in reality, multiple proxy servers often exist in the signal path. The message flow for multi-proxy servers are similar, except that proxy authentication usually only applies to the first hop.

3.2. RTP Overview

The Real-Time Transport Protocol (RTP) [2, 5] defines a standardized packet format for transmitting audio and video over IP networks. RTP is widely used in communications and entertainment systems involving streaming media, such as telephones, video conferencing applications, television services, and web-based push-to-talk capabilities (Figure 1). Applications often run RTP on top of UDP to take advantage of its multiplexing and checksum services; both protocols contribute part of the functionality of the transport protocol.

In addition, RTP is also used in conjunction with the RTP Control Protocol (RTCP). RTP carries media streams, while RTCP is used to monitor transmission statistics and quality of service (QoS), and assist in the synchronization of multiple streams. RTP is initiated and received on even port numbers, and associated RTCP communications use the next higher odd port number. The RTP

 doi:10.20944/preprints202501.1897.v1

header has the minimum size of 12 bytes that can be increased with optional fields. The RTP header specification is shown in Figure 3 below.

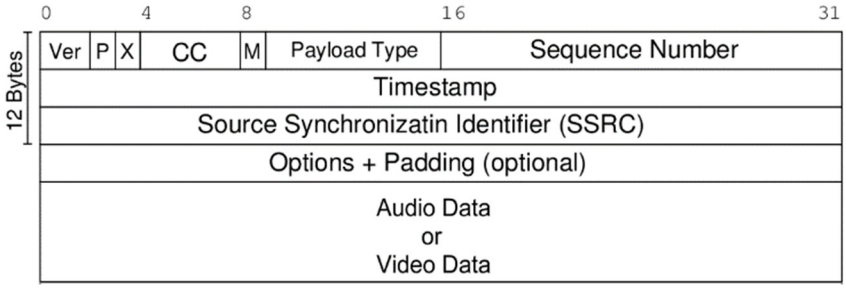

Figure 3. Location of RTP/RTCP in the protocol stack.

The payload type (PT) is a 7-bit field that indicates the format of the payload and determines its interpretation by applications. For example, when the value is assigned to 18, the audio codec uses G.729, and when the value is assigned to 34, the media codec uses H.323. In order to meet the diverse encoding algorithms, it now also supports dynamic binding of PT to media encoding. This means that before the establishment of an RTP session, the PT value used and its corresponding encoding format are specified. The audio/video data payload carries audio samples or compressed video data for playing audio and video services.

3.3. Related Work

Since SIP plays an important role in VoIP communications, the security of its application has also attracted the attention of researchers. To protect privacy and confidentiality, many studies have been proposed to validate UAS/UAC and encrypted RTP payloads.

In 2016, Zhang et al. [6] introduce an authentication protocol for SIP using smartcards and elliptic curve cryptography. This protocol eliminates the need for the SIP server to store passwords or verification tables, reducing energy consumption. Azrour et al. [7] used chaotic maps and smartcards to propose an efficient SIP authentication and key agreement protocol. However, modern communication devices no longer include smart cards. Meanwhile, Chaudhry et al. developed a lightweight privacy preserving authentication and key agreement protocol [8] for SIP. Elliptic curve cryptography is utilized in their protocol to provide mutual authentication as well as protect all known attacks, such as server impersonation attack. Nikooghadam et al. [9] later performed a cryptanalysis of Chaudry et al.'s protocol and pointed out its weaknesses against offline password guessing attacks. An improved lightweight authentication protocol was proposed to overcome these weaknesses of Chaudry et al. They also used BAN logic [10] to prove the correctness of the proposed protocol. But in 2019 Ravanbakhsh et al. [11] found that the protocol proposed by Nikooghadam et al. was insecure due to the lack of perfect forward secrecy [12]. Therefore, they presented an efficient two-factor authentication and key agreement protocol and used the AVISPA tool [13] to prove that it can defend against various active and passive attacks. Nevertheless, Nikooghadam et al. [14] proved that Ravanbakhsh et al.'s protocol did not provide perfect forward secrecy. Next, they proposed a secure two-factor authentication and key agreement scheme based on elliptic curve cryptography. They used the Scyther tool [15] to simulate and analyze the protocol to formally prove its robustness and security. In 2020, an advancement of an authenticated key agreement protocol for SIP, based on Dongqing et al.'s scheme [16], was introduced by Mahamood et al. [17] Mahamood et al.'s scheme supports running over a WLAN or WAN, but was found to be vulneable to privileged insider attacks and secret disclosure. Furthermore, strict time synchronization is impractical in the real world.

However, the aforementioned protocols have all been analyzed for their security and performance theoretically, without being put into practice or applied in the real world. VOCAL Technologies, Ltd. [18] adheres to the standards outlined in RFC 3261 [19] and RFC 3329 [20] to implement SIP-based VoIP services over TLS. SIPTRUNK [21] not only provides TLS security but

 doi:10.20944/preprints202501.1897.v1

also uses Real-Time Protocol (SRTP) [22] to secure the media sent during the connection. Leu et al. [23] establishes secure VoIP communication via SIP across wireless networks. Their protocol employs ECMQV for generating session keys to safeguard media packets and utilizes TLS to secure SIP signals. Despite that, none of these solutions provide the functionality mentioned in section 2, providing convenient services. Therefore, in this study, we propose a mechanism that not only resolves this issue but also enhances the user-friendly aspect of VoIP services.

4. Proposed Method

4.1. The Architecture

We implemented a realistic framework, as shown in Figure 4, to verify the practicality of the proposed mechanism and analyze its performance. The fundamental idea is

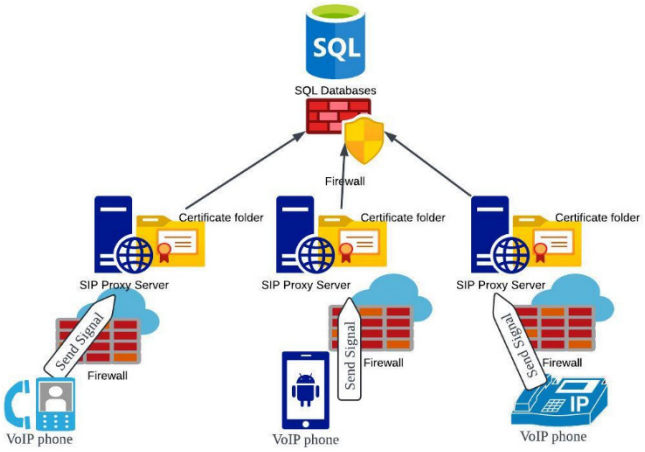

Figure 4. A realistic operational framework.

comparable to that of a SIP proxy server that is commonly deployed. In order to establish a call session, each SIP proxy server provides authentication, grants access, and routes call setup signals to other servers where the callee is registered. Additionally, each SIP proxy server contains a directory that houses all user certificates, including the public key. The database containing information on SIP servers, agents, and related data is protected by a firewall. Communication ports have been modified to help prevent attacks targeted to compromise standard SQL and SIP settings. VoIP end devices register with the SIP proxy server over the Internet and set up a Transport Layer Security (TLS) tunnel before sending SIP signals. Additionally, each VoIP end device has a private key stored in secure memory.

4.2. Algorithms

In order to protect the confidentiality of the session, we refer to [23] and adopt the ECMQV algorithm to be integrated into the SIP protocol. Symbols, algorithm, and integrated protocol are illustrated in Table 1, Algorithm 1, and Figure 5, respectively.

Table 1. Domain parameters in Elliptic curve cryptography.

Symbol	Meaning
G	The base point consists of (x, y) coordinate.
SEED	If the elliptic curve was produced randomly in a verifiable manner, an optional bit string is added.

 doi:10.20944/preprints202501.1897.v1

q	The size of a field, which is a number p or 2^m where p and m are primes.
FR	A basis indication.
a, b	Two field variables that establish the curve's equation.
n	The point G's order
h	The cofactor that results from dividing the curve's order by n.

As shown in Figure 5, the caller sends a SIP invite message containing his/her ephemeral public key cG. A SIP proxy server checks its database and the directory containing public keys. If the callee exists, the SIP proxy server will respond to the caller with the callee's static public key (bG) and forward the INVITE message to the callee. After receiving the INVITE message, the callee will reply with a SIP 200 OK message including his/her ephemeral public key dG. The SIP proxy server will return the caller's static public key (aG) to the callee and transfer the 200 OK message to the caller. The caller uses the callee's temporary and static public key received from the SIP proxy server paired with its own long- and short-term private key to calculate the Q-point. The session key K is then generated by hashing the extracted x-coordinate of the Q point. Finally, the caller sends the message authentication code of the session key MAC(K) which is produced by encrypting 16 bytes of zeros. The callee verifies the MAC by calculating the common session key.

Next, the pseudocode proposed in Algorithm 2 is used to solve the virtual reference phone number that does not have a corresponding public key. When a caller dials a reference phone number, the SIP proxy server searches for the group it represents. For example, a reference phone number 77777 may represent a group of numbers (70001, 70002, 70003, 70004) with related services. If the SIP proxy server cannot find its group, the number may be wrong and the algorithm 2 returns 0 which will be converted into a SIP 404 Not Found message to the caller. If the group exists, the algorithm checks the status of the numbers in the group one by one. When the algorithm finds an available number, then it searches the directory for the corresponding certificate. If the certificate is not found, -1 is returned, which is converted into a SIP 403 Forbidden message. If all the conditions are met, the number is passed back to the SIP proxy server; otherwise, the SIP proxy server will obtain 1 and interpret it as a SIP 486 Busy message. As a result, when the SIP proxy server gets an available number n, it will send the static public key of n to the caller and proceed the process as illustrated in Figure 5.

Algorithm 1: ECMQV algorithm

Input: A set of domain parameters ($\#E(F_p)$, q, h, G),
private keys (a, c), and
public keys (aG, cG, bG, dG)

Output: A session key K

1. $\lceil log_2 \#E(F_q) \rceil / 2 \rightarrow n$
2. $\left(x(cG)(mod\ 2^n)\right) + 2^n \rightarrow u$
   #The x coordinate of the public key (cG) is converted to an integer
3. $c + ua\ (mod\ q) \rightarrow s$
4. $\left(x(dG)(mod\ 2^n)\right) + 2^n \rightarrow v$
   #The x coordinate of the public key (dG) is converted to an integer

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 January 2025 doi:10.20944/preprints202501.1897.v1

5. $s(dG + v(bG)) \rightarrow Q$
6. return $K = Hash(Q_x)$

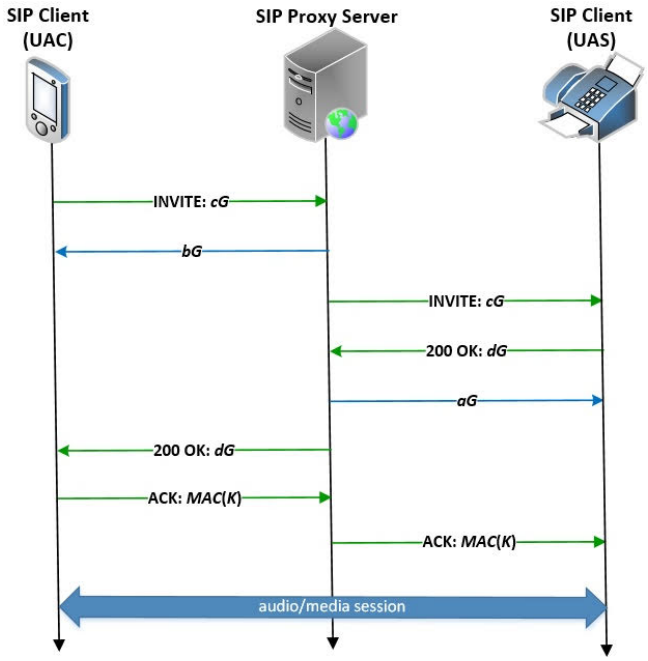

Figure 5. The standard SIP protocol integrates ECMQV algorithm.

5. Result and Analysis

The experimental environment is set up with the following. A hypervisor VMware ESXi 6.5 is installed and configured on a 1U rack Dell PowerEdge R450 server with DDR4-2400 64GB Memory and Intel Xeon Silver 4210 2.20GHz, 10 cores. Then we created and configured five virtual machines on the ESXi management console, including four SIP proxy servers and one RTP relay server running on the Ubuntu 18.04 operating system. The SIP proxy server is developed and modified from the free open source framework - Asterisk. A MySQL database virtual machine was created using a 1U rack Dell PowerEdge R350 server with Intel Xeon E-2300 3.1G 8 cores and DDR4-3200 16GB, and the virtual machine hypervisor VMware ESXi 6.5 installed.

Algorithm 2: Reference Phone Number algorithm

Input: A reference phone number R
Output: A real number n or 1 or 0

1. $Search\_Group(R) \rightarrow N$
2. $if\ N\ exists$
3. $\quad for\ n\ in\ N$
4. $\quad\quad Check\_Status(n) \rightarrow s$
5. $\quad\quad if\ s\ \neq busy$
6. $\quad\quad\quad if\ file\_exist(search\_cert(n))$
7. $\quad\quad\quad\quad return\ n$
8. $\quad\quad\quad else$
9. $\quad\quad\quad\quad return\ -1$
10. $\quad return\ 1$
11. $else$
12. $return\ \ 0$

 doi:10.20944/preprints202501.1897.v1

The deployment of terminal devices has become complex due to the presence of wired and wireless (mobile) equipment. The smartphone model is the HTC U20, equipped with a MicroSD card that has encryption capabilities, and installed a customized VoIP application designed by us. The conceptual diagram is illustrated as Figure 6.

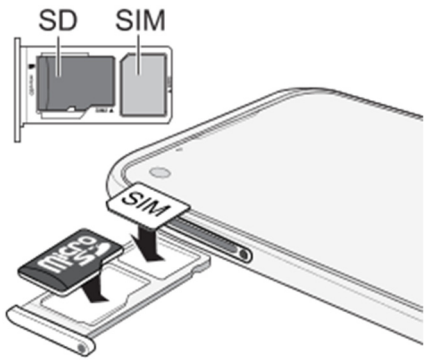

Figure 6. [25]: The smartphone is equipped with a MicroSD card that has encryption capabilities.

A wired desk phone connects to a custom VoIP gateway equipped with a Hardware Security Module (HSM) for key exchange and encryption. The conceptual diagram is shown in Figure 7.

Figure 7. [26]. This schematic illustrates a VoIP phone connecting to a VoIP gateway equipped with HSM.

The proposed system is deployed in an organization with 200 employees. The statistical results of call establishment success are presented in Table 2. The author divides the status of calls into 12 categories. "**Successful Call Setup**" means that the communicating parties successfully conducted a conversation. "**Missed Call**" means the called party did not answer the call. "**Line Busy**" indicates that the callee's line is currently in use or occupied. "**Offline**" means that the callee is not registered to the SIP proxy server. "**Callee No Response**" means that the SIP proxy server forwarded the INVITE signal to the callee, but the callee did not respond for some unknown reason. "**Wrong Number**" means the caller dialed a phone number that does not exist. "**Call Rejected**" means the callee hangs up the phone directly. "**Call Forbidden**" means the callee's account is illegal or the callee's certificate does not exist. "**System Service Abnormality**" means that the SIP proxy server cannot process SIP signals normally. "**ACK timeout**" refers to the situation where, after receiving a SIP 200 OK response, the system waits for the final SIP ACK signal for a duration that exceeds the specified time limit. "**Unstable Network, Msg Lost**" indicates that the SIP signal is lost or cannot be successfully delivered due to unstable network conditions. All remaining cases are classified as "**Other**" status. The statistical data collection period is from January 15th to 19th. In order to evaluate the trend changes, the "**Connection Success Rate**" is defined as the following equation,

$$\frac{\left(\begin{array}{c}\textbf{Successful Call Setup} + \textbf{Missed Call} + \textbf{Line Busy} + \\ \textbf{Wrong Number} + \textbf{Call Rejected}\end{array}\right)}{\textbf{total calls}}$$

 doi:10.20944/preprints202501.1897.v1

, and the equation for "**Call Setup Rate**" is defined as follows.

$$\frac{(\textbf{Callee No Response} + \textbf{Line Busy})}{\textbf{total calls}}$$

And the equation of "System **Abnormality Rate**" is defined as the below.

$$\frac{\left(\begin{array}{c}\textbf{Successful Call Setup} + \textbf{Call Forbidden} + \\ \textbf{System Service Abnormality} + \textbf{Unstable Network, Msg Lost}\end{array}\right)}{\textbf{total calls}}$$

The trend of call success rate is shown in Figure 8, the call connection success rate is as high as over 95%, which means users can smoothly access services and initiate calls. As we can see, the call is not dialed to a specific callee, but to a reference phone number that multiple callees can respond to. As a result, callers will experience fewer busy lines. However, an idle number does not guarantee that the callee is necessarily available at their seat, so there is still a possibility of missed calls happened. Since the caller may be in an unstable or poor network environment, SIP signals may sometimes be lost. States 4 and 10 can be classified as the aforementioned situations. Definitely, even with a reference phone number, callers may still dial the wrong number. Overall, the probability that users were able to find the callee and establish a call is about 80%, indicating that customers or employees traveling abroad can usually reach a business partner when making a phone call, thereby improving service satisfaction.

Table 2. Statistics of call status.

Date / Status	'24/01/15	'24/01/16	'24/01/17	'24/01/18	'24/01/19
Successful Call Setup*1	300	256	255	199	181
Missed Call*2	48	34	41	20	38
Line Busy*3	24	16	7	3	7
Offline	5	10	14	0	7
Callee No Response*4	5	2	0	0	2
Wrong Number*5	6	4	3	11	2
Call Rejected*6	0	0	0	0	0
Call Forbidden*7	0	0	0	0	0
System Service Abnormality*8	0	0	0	0	0
ACK timeout*9	0	0	0	0	0
Unstable Network, Msg Lost*10	1	5	3	1	1
Other*11	1	0	0	0	0

*1. Connection Success Rate = (1 + 2 + 3 + 5 + 6)/Total. *2. Call Setup Rate = (1 + 3)/Total. *3. System Abnormality Rate = (4+7+8+10)/Total.

 doi:10.20944/preprints202501.1897.v1

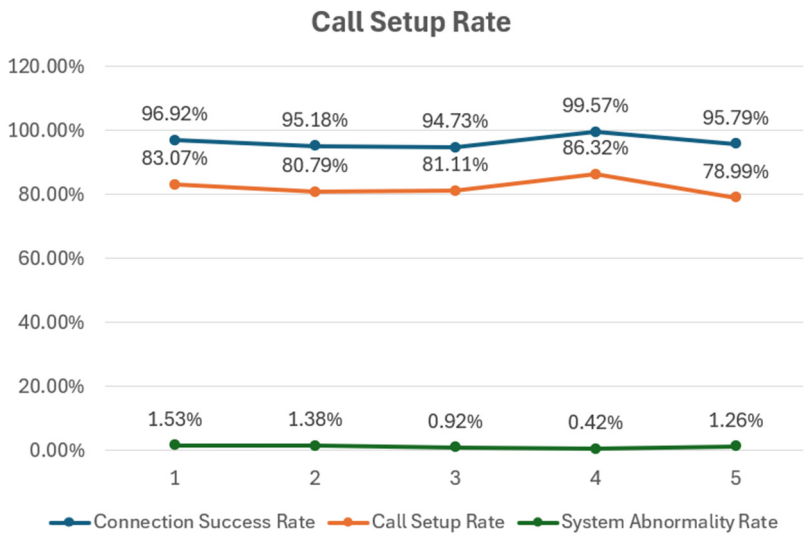

Figure 8. Statistical trend line chart.

6. Conclusions

In order to solve the issue of not being able to reach the relevant business personnel by phone while other personnel are available to answer the call, this study presents a practical VoIP service that improves call availability by utilizing reference phone numbers. The system can be built on the traditional SIP VoIP framework. By incorporating the proposed algorithms into existing servers and terminals, upgrading services can be seamlessly integrated. We also analyzed the performance of the reference phone number mechanism through actual deployment, and the mechanism showed satisfactory results, proving its practicality. As future work, research will be conducted on transferring calls from landline numbers to mobile numbers while implementing the corresponding key exchange mechanisms to ensure call security.

Author Contributions: The research contribution is as following statements. WenBin Hsieh is responsible for Conceptualization, methodology, software, validation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, supervision, and project administration. All authors have read and agreed to the published version of the manuscript.

Funding: There is no funding for this research.

Data Availability Statement: All research data is included within the content of the research.

Acknowledgments: We acknowledge the support provided to all users of this system.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. C. Shen, E. Nahum, H. Schulzrinne, and C. Wright, "The impact of TLS on SIP server performance," in Principles, Systems and Applications of IP Telecommunications (IPTComm '10), New York, NY, USA, 2010, pp. 59–70.
2. T. Zourzouvillys and E. Rescorla, "An Introduction to Standards-Based VoIP: SIP, RTP, and Friends," in IEEE Internet Computing, vol. 14, no. 2, pp. 69-73.
3. R. Rivest. The MD5 Message-Digest Algorithm. RFC 1321, April 1992.
4. H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RTP: A Transport Protocol for Real-Time Applications. RFC 3550, July 2003.
5. S. Paul, "Real-Time Transport Protocol (RTP)," in Multicasting on the Internet and its Applications, Boston, MA: Springer, 1998, pp. 193-201.

6. Z. Liping, T. Shanyu, Z. Shaohui, "An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks, " Journal of Network and Computer Applications, Volume 59, 2016, pp. 126-133.
7. [7] M. Azrour, M. Ouanan, and Y. Farhaoui, "A New Efficient SIP Authentication and Key Agreement Protocol Based on Chaotic Maps and Using Smart Card," In Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems (ICCWCS'17), NY, USA, Article 70, 2017, pp. 1–8.
8. S.A. Chaudhry, H. Naqvi, M. Sher, M.S. Farash, M.U. Hassan, "An improved and provably secure privacy preserving authentication protocol for SIP," Peer-Peer Netw. Appl., 10, 2017, pp. 1–15.
9. M. Nikooghadam, R. Jahantigh, H. Arshad, "A lightweight authentication and key agreement protocol preserving user anonymity," Multimed. Tools Appl., 76, 2017, pp.13401–13423.
10. M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Trans. Computer Systems, vol. 8, no. 1, 1990, pp. 18-36.
11. N. Ravanbakhsh, M. Mohammadi, M. Nikooghadam, "Perfect forward secrecy in VoIP networks through design a lightweight and secure authenticated communication scheme," Multimed. Tools Appl., 78, 2019, pp. 11129–11153.
12. W. Diffie, P.C. Van Oorschot, and M.J. Wiener, "Authentication and authenticated key exchanges," Des Codes Crypt, vol. 2, 1992, pp. 107–125.
13. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P.H. Drielsma, P.C. Héam, O. Kouchnarenko, J. Mantovani, "The AVISPA tool for the automated validation of internet security protocols and applications," In: International Conference on Computer Aided Verification. Springer, 2005, pp 281–285.
14. M. Nikooghadam, H. Amintoosi, "Perfect forward secrecy via an ECC-based authentication scheme for SIP in VoIP," J. Supercomput., 76, 2020, pp. 3086–3104.
15. C. Cremers, "Scyther, Semantics and Verifcation of Security Protocols," Ph.D. dissertation, Eindhoven University of Technology, 2006.
16. D. Xu, S. Zhang, J. Chen, and M. Ma, "A provably secure anonymous mutual authentication scheme with key agreement for SIP using ECC," Peer-to-Peer Networking and Applications, vol. 11, pp. 837–847, Sep. 2018.
17. M. Ul Hassan, S. Chaudhry, and A. Irshad, "An improved SIP authenticated key agreement based on Dongqing et al.," Wireless Personal Communications, vol. 110, pp. [page numbers], Feb. 2020.
18. Vocal Technologies Ltd., "Secure SIP," Vocal Technologies, [Online]. Available: https://vocal.com/sip/secure-sip/. [Accessed: March 20, 2024].
19. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "SIP: Session Initiation Protocol," RFC 3261, Internet Engineering Task Force, June 2002.
20. A. B. Roach, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)," RFC 3329, Internet Engineering Task Force, January 2003.
21. SIPTRUNK, "A Brief Guide to SIP Security," SIPTRUNK, [Online]. Available: https://www.siptrunk.com/2019/08/a-brief-guide-to-sip-security/. [Accessed: March 23, 2024].
22. T. T. Carrara, R. Housley, C. J. Kalt, and J. C. R. Lazzaro, "The Secure Real-time Transport Protocol (SRTP)," RFC 3711, Internet Engineering Task Force, March 2004.
23. W.-B. Hsieh and J.-S. Leu, "Implementing a secure VoIP communication over SIP-based networks," Wireless Networks (WINET), vol. 24, no. 8, pp. 2915-2926, Nov. 2018.
24. I. Blake, G. Seroussi, and N. Smart, "Advances in elliptic curve cryptography," London Mathematical Society Lecture Note Series, vol. 317, Cambridge, UK: Cambridge University Press, 2005.
25. [HTC, "Inserting SIM and SD - HTC U20 5G - Support | HTC Taiwan," HTC Taiwan, [Online]. Available: https://www.htc.com/tw/support/htc-u20-5g/howto/inserting-sim-and-sd.html. [Accessed: April 8, 2024].
26. Yeastar. (n.d.). VoIP Gateways. [Online]. Available: https://www.yeastar.com/voip-gateways/. [Accessed: April 8, 2024].

 doi:10.20944/preprints202501.1897.v1

27. ITU-T Recommendation H.323: "Packet-based multimedia communications systems," ITU-T H.323, 2009.
28. ITU-T, "Gateway control protocol," ITU-T Recommendation H.248, 2015.