ICSNC 2023

The Eighteenth International Conference on Systems and Networks Communications

ISBN: 978-1-68558-099-5

November 13th – 17th, 2023

Valencia, Spain

ICSNC 2023 Editors

Eugen Borcoci, National University of Science and Technology POLITEHNICA Bucuresti (UNSTPB), Romania

Marko Jantti University of Eastern Finland, School of Computing, Finland

ICSNC 2023

Forward

The Eighteenth International Conference on Systems and Networks Communications (ICSNC 2023), held on November 13 - 17, 2023 in Valencia, Spain, continued a series of events covering a broad spectrum of systems and networks related topics.

As a multi-track event, ICSNC 2023 served as a forum for researchers from the academia and the industry, professionals, standard developers, policy makers and practitioners to exchange ideas. The conference covered fundamentals on wireless, high-speed, mobile and Ad hoc networks, security, policy based systems and education systems. Topics targeted design, implementation, testing, use cases, tools, and lessons learnt for such networks and systems

The conference had the following tracks:

- TRENDS: Advanced features
- WINET: Wireless networks
- HSNET: High speed networks
- SENET: Sensor networks
- MHNET: Mobile and Ad hoc networks
- AP2PS: Advances in P2P Systems
- MESH: Advances in Mesh Networks
- VENET: Vehicular networks
- RFID: Radio-frequency identification systems
- SESYS: Security systems
- MCSYS: Multimedia communications systems
- POSYS: Policy-based systems
- PESYS: Pervasive education system

We welcomed technical papers presenting research and practical results, position papers addressing the pros and cons of specific proposals, such as those being discussed in the standard forums or in industry consortiums, survey papers addressing the key problems and solutions on any of the above topics, short papers on work in progress, and panel proposals.

We take here the opportunity to warmly thank all the members of the ICSNC 2023 technical program committee as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors that dedicated much of their time and efforts to contribute to the ICSNC 2023. We truly believe that thanks to all these efforts, the final conference program consists of top quality contributions.

This event could also not have been a reality without the support of many individuals, organizations and sponsors. We also gratefully thank the members of the ICSNC 2023 organizing committee for their help in handling the logistics and for their work that is making this professional meeting a success. We gratefully appreciate to the technical program committee co-chairs that contributed to identify the appropriate groups to submit contributions.

We hope the ICSNC 2023 was a successful international forum for the exchange of ideas and results between academia and industry and to promote further progress in networking and systems communications research. We also hope that Valencia provided a pleasant environment during the conference and everyone saved some time for exploring this beautiful city

ICSNC 2023 General Chair

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

ICSNC 2023 Steering Committee

Marc Kurz, University of Applied Sciences Upper Austria, Faculty for Informatics, Communications and Media, Austria
Jin-Shyan Lee, National Taipei University of Technology (Taipei Tech.), Taiwan
Rony Kumer Saha, BRAC University, Bangladesh
Eugen Borcoci, University Politehnica of Bucharest, Romania

ICSNC 2023 Publicity Chair

Lorena Parra Boronat, Universitat Politecnica de Valencia, Spain
Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain
Jose Miguel Jimenez, Universitat Politecnica de Valencia, Spain

ICSNC 2023

Committee

ICSNC 2023 General Chair

Jaime Lloret Mauri, Polytechnic University of Valencia, Spain

ICSNC 2023 Steering Committee

Marc Kurz, University of Applied Sciences Upper Austria, Faculty for Informatics, Communications and Media, Austria
Jin-Shyan Lee, National Taipei University of Technology (Taipei Tech.), Taiwan
Rony Kumer Saha, BRAC University, Bangladesh
Eugen Borcoci, University Politehnica of Bucharest, Romania

ICSNC 2023 Publicity Chair

Lorena Parra Boronat, Universitat Politecnica de Valencia, Spain
Sandra Viciano Tudela, Universitat Politecnica de Valencia, Spain
Jose Miguel Jimenez, Universitat Politecnica de Valencia, Spain

ICSNC 2023 Technical Program Committee

Maysam Abbod, Brunel University London, UK
Ahmed M. Abdelmoniem, KAUST, Saudi Arabia
Abdelkaher Ait Abdelouahad, Chouaib Doukkali University, Morocco
Baadache Abderrahmane, University of Benyoucef Benkhadda, Algeria
Ishtiaq Ahmad, University of South Australia, Australia
S. Arnaud R. M. Ahouandjinou, University of Abomey-Calavi (UAC) / Coastal Opal University (ULCO), France
Lucio Agostinho Rocha, Federal University of Technology Paraná (UTFPR), Brazil
Francisco Airton Silva, Universidade Federal do Piauí, Brazil
Zahid Akhtar, State University of New York Polytechnic Institute, USA
Pedro Ákos Costa, NOVA University of Lisbon & NOVALINCS, Portugal
Abdullah Al-Alaj, Virginia Wesleyan University, USA
Adel Aldalbahi, KFU College of Engineering, Saudi Arabia
Osama Aloqaily, University of Ottawa, Canada
Abdallah A. Alshehri, Saudi Aramco, Dhahran, Saudi Arabia
Reem Alshahrani, Taif University, Saudi Arabia
Mohammed Al-Sarem, Taibah University, Saudi Arabia
Sarah Al-Shareeda, University of Bahrain, Bahrain
Mourad Amad, Bouira University, Algeria
Marios Avgeris, Carleton University, Ottawa, Canada
Muhammad Sohaib Ayub, Lahore University of Management Sciences (LUMS), Pakistan

V. Balasubramanian, Arizona State University, USA
Abu Barkat Ullah, University of Canberra, Australia
Ilija Basicevic, University of Novi Sad, Serbia
Mohamed Benmohammed, University Constantine2, Algeria
Robert Bestak, Czech Technical University in Prague, Czech Republic
Muhammad Danial Bin Zakaria, Universiti Sultan Zainal Abidin, Malaysia
Razvan Bocu, Transilvania University of Brasov, Romania
Eugen Borcoci, University "Politehnica"of Bucharest (UPB), Romania
Alexandros-Apostolos A. Boulogeorgos, Aristotle University of Thessaloniki, Greece
Christos Bouras, University of Patras, Greece
Marilisa Botte, Federico II University of Naples, Italy
Anis Boubakri, ESPRIT, Tunsia
An Braeken, Vrije Universiteit Brussel, Belgium
Francesco Buccafurri, University of Reggio Calabria, Italy
Dumitru Dan Burdescu, University of Craiova, Romania
Eduardo Castilho Rosa, Federal University of Uberlandia, Brazil
Hao Che, University of Texas at Arlington, USA
Adil Chekati, University of Tunis El Manar, Tunisia
Fuxiang Chen, University of Leicester, UK
Dickson K.W. Chiu, University of Hong Kong, Hong Kong
Domenico Ciuonzo, University of Naples "Federico II", Italy
Jorge A. Cobb, The University of Texas at Dallas, USA
Estefanía Coronado Calero, i2CAT Foundation, Spain
Fabio D'Andreagiovanni, CNRS - French National Centre for Scientific Research, France
Eronides da Silva Neto, CESAR Innovation Institute, Recife, Brazil
Monireh Dabaghchian, George Mason University, USA
Orhan Dagdeviren, Ege University | International Computer Institute, Turkey
Felipe S. Dantas Silva, Federal Institute of Education, Science, and Technology of RN (IFRN), Brazil
Saikat Das, Utah Valley University, Orem, USA
Vincenzo De Angelis, University of Reggio Calabria, Italy
Mehmet Demirci, Karadeniz Technical University, Turkey
Margot Deruyck, Ghent University - IMEC - WAVES, Belgium
Soumyabrata Dev, University College Dublin, Ireland
Omar Dib, Wenzhou-Kean University, China
Luis Diez, University of Cantabria, Spain
Rogério Dionísio, Polytechnic Institute of Castelo Branco, Portugal
Mustapha Djeddou, National Polytechnic School, Algiers, Algeria
Amir Djenna, University of Constantine, Algeria
Steve Eager, University of the West of Scotland, UK
Amna Eleyan, Manchester Metropolitan University, UK
Mohammed Eltayeb, California State University, Sacramento, USA
Müge Erel-Özçevik, Celal Bayar University, Turkey
Marcos Fagundes Caetano, University of Brasília, Brazil
Brandon Foubert, Inria Lille-Nord Europe, France
Ramin Fouladi, Bogazici University, Istanbul, Turkey
Marco Furini, University of Modena and Reggio Emilia, Italy
Sonia Mettali Gammar, University of Manouba Tunis, Tunisia
Zhiwei Gao, Northumbria University, UK

Maggie E. Gendy, Arab Academy for Science, Technology and Maritime Transport - Communications and Networking, United Arab Emirates
Alireza Ghasempour, University of Applied Science and Technology, Iran
Katja Gilly de la Sierra-Llamazares, Universidad Miguel Hernández, Spain
Ariel Goes de Castro, Universidade Federal do Pampa, Brazil
Diogo Gomes, University of Aveiro, Portugal
Dalton Cézane Gomes Valadares, Federal Institute of Pernambuco (IFPE), Brazil
Barbara Guidi, University of Pisa, Italy
Terry Guo, Tennessee Technological University, USA
Peter Haber, Salzburg University of Applied Sciences, Austria
Rushdi Hamamreh, Al-Quds University, Jerusalim
Khaled Hamouid, Université de Batna 2, Algeria
Luoyao Hao, Columbia University, USA
Abdelkrim Haqiq, Hassan 1st University, Morocco
Shahriar Hasan, Mälardalen University, Sweden
Omar Hashash, Virginia Tech, USA
Simon Hayhoe, University of Bath, UK
William "Chris" Headley, Ted & Karyn Hume Center for National Security / Virginia Polytechnic Institute & State University, USA
Shahram S. Heydari, Ontario Tech University, Canada
Md Shafaeat Hossain, Southern Connecticut State University, USA
Seyed Mohsen Hosseini, Polytechnic University of Bari, Italy
Yuzhou Hu, ZTE Corporation, China
Darko Huljenic, Ericsson Nikola Tesla, Croatia
Maria Francesca Idone, University of Reggio Calabria, Italy
Farkhund Iqbal, College of Technological Innovation, Abu Dhabi, UAE
Faouzi Jaidi, University of Carthage | Higher School of Communications of Tunis & National School of Engineers of Carthage, Tunisia
Dorota Jelonek, Czestochowa University of Technology, Poland
Jobish John, University College Cork, Ireland
Magnus Jonsson, Halmstad University, Sweden
Bijoy A. Jose, Cochin University of Science and Technology, India
Yasushi Kambayashi, NIT - Nippon Institute of Technology, Japan
Faouzi Kamoun, ESPRIT School of Engineering, Tunis, Tunisia
Murizah Kassim, Universiti Teknologi MARA, Malaysia
Sokratis K. Katsikas, Norwegian University of Science and Technology, Norway
İlker Korkmaz, Izmir University of Economics, Turkey
Sondes Ksibi, University of Carthage | Higher School of Communications of Tunis, Tunisia
Lov Kumar, BITS-PILANI, Hyderabad, India
Sonal Kumari, Samsung R&D Institute, India
Marc Kurz, University of Applied Sciences Upper Austria, Austria
Cecilia Labrini, University of Reggio Calabria, Italy
Francesco G. Lavacca, Fondazione Ugo Bordoni, Italy
Sara Lazzaro, University of Reggio Calabria, Italy
Gyu Myoung Lee, Liverpool John Moores University, UK
Jin-Shyan Lee, National Taipei University of Technology (TAIPEI TECH), Taiwan
Wolfgang Leister, Norsk Regnesentral, Norway
João Leitão, NOVA School of Science and Technology | NOVA University of Lisbon & NOVA LINCS,

Portugal
Kin K. Leung, Imperial College, UK
Yiu-Wing Leung, Hong Kong Baptist University, Kowloon Tong, Hong Kong
Hongda Li, Clemson University, USA
Sebastian Lindner, Hamburg University of Technology, Germany
Chunmei Liu, National Institute of Standards and Technology, USA
Peng Liu, National Institute of Standards and Technology / Georgetown University, USA
Rafael Lopes, State University of Ceará (UECE), Brazil
Hui Lu, State University of New York (SUNY) at Binghamton, USA
Zhongqiang Luo, Sichuan University of Science and Engineering, China
Saida Maaroufi, École Polytechnique de Montréal, Canada
Kiran Makhijani, Futurewei, USA
Joe J. Mambretti, Northwestern University, USA
Zoubir Mammeri, IRIT - Paul Sabatier University, Toulouse, France
Sathiamoorthy Manoharan, University of Auckland, New Zealand
Johann M. Marquez-Barja, University of Antwerp - imec, Belgium
Akanksha Marwah, University of Delhi, India
Rashed Mazumder, Institute of Information Technology (IIT) | Jahangirnagar University, Bangladesh
Michael McGrath, Intel Labs, USA
Rashid Mehmood, King Abdul Aziz University, Jeddah, Saudi Arabia
Abdelkrim Meziane, Research Center on Scientific and Technical Information CERIST, Algeria
Lotfi Mhamdi, University of Leeds, UK
Claudio Miceli de Farias, Federal University of Rio de Janeiro, Brazil
Bashir Mohammed, Lawrence Berkeley National Laboratory, USA
Waldir Moreira, Fraunhofer Portugal AICOS, Portugal
Alireza Morsali, Humanitas Solutions, Canada
Abdelouahab Moussaoui, Ferhat Abbas University - Sétif 1, Algeria
Ranesh Kumar Naha, University of Tasmania, Australia
Ankur Nahar, Indian Institute of Technology, Jodhpur, India
Apurva Narayan, The University of British Columbia / University of Waterloo, Canada
Leila Nasraoui, University of Manouba, Tunisia
Amiya Nayak, University of Ottawa, Canada
Ranyelson Neres Carvalho, University of Brasília (UnB), Brazil
Prasad Netalkar, Qualcomm, USA
Christopher Nguyen, Intel Corp., USA
Huu-Nghia Nguyen, Montimage, Paris, France
Muath Obaidat, City University of New York, USA
Olusola Odeyomi, Wichita State University, USA
Luciana Oliveira, CEOS.PP ISCAP Polytechnic of Porto, Portugal
Alma Oračević, University of Bristol, UK
Achour Ouslimani, Quartz Laboratory - ENSEA, France
Grammati Pantziou, University of West Attica, Athens, Greece
Luciana Pereira Oliveira, Instituto Federal de Educação, Ciência e Tecnologia da Paraíba, Brazil
Ricardo José Pfitscher, Federal University of Rio Grande do Sul (UFRGS), Brazil
Kandaraj Piamrat, LS2N/University of Nantes, France
Paulo Pinto, Universidade Nova de Lisboa, Portugal
Vicent Pla, Universitat Politècnica de València, Spain
Mattia Quadrini, Romars s.r.l , Rome, Italy

Saulo Queiroz, Federal University of Technology - UTFPR, Ponta Grossa, Brazil
Raqeebir Rab, Ahsanullah University of Science and Technology, Bangladesh
Carlos Rabadão, Polytechnic of Leiria, Portugal
M. Mustafa Rafique, Rochester Institute of Technology,USA
Vittorio Rampa, Consiglio Nazionale delle Ricerche - Istituto di Elettronica, di Ingegneria dell'Informazione e delle Telecomunicazioni - Politecnico di Milano, Italy
Piotr Remlein, Poznan University of Technology, Poland
Olivier Renaudin, Universitát Autonoma de Barcleona (UAB), Spain
Leon Reznik, Rochester Institute of Technology, USA
Michele Roccotelli, Polythecnic University of Bari, Italy
Jose Manuel Rubio Hernan, Télécom SudParis, France
Saif Sabeeh, Poznan University of Technology, Poland
Rony Kumer Saha, BRAC University, Bangladesh
Dhaou Said, Sherbrooke University / Ottawa University, Canada
Damian San Roman Alerigi, Saudi Aramco, Saudi Arabia
Luis Enrique Sánchez Crespo, Universidad de Castilla-La Mancha, Spain
Ignacio Sanchez-Navarro, University of the West of Scotland, UK
Bassem Sellami, University of Tunis El Manar, Tunisia
Sawsan Selmi, Higher School of Communication of Tunis, Tunisia
Fouzi Semchedine, University of Setif 1, Algeria
Alireza Shahrabi, Glasgow Caledonian University, Scotland, UK
Chen Shen, Georgetown University / National Institute ofStandards and Technology, USA
Muhammad Shuaib Siddiqui, i2CAT Foundation, Spain
Rute C. Sofia, fortiss GmbH, Munich, Germany
Hazem Soliman, Arctic Wolf Networks, USA
Erik Sonnleitner, University of Applied Sciences Upper Austria, Austria
Wendley Souza da Silva, Federal University of Ceará (UFC), Brazil
Marco Aurelio Spohn, Federal University of Fronteira Sul (Universidade Federal da Fronteira Sul) - Chapeco/SC, Brazil
Alvaro Suárez Sarmiento, Universidad de Las Palmas de G. C., Spain
Young-Joo Suh, Pohang University of Science and Technology (POSTECH), Korea
Liyang Sun, New York University, USA
Do-Duy Tan, Ho Chi Minh City University of Technology and Education (HCMUTE), Vietnam
Getaneh Berie Tarekegn, National Taipei University of Technology, Taiwan
Suresh Thanakodi, Universiti Pertahanan Nasional Malaysia, Malaysia
Vasileios Theodorou, Intracom Telecom, Greece
Behrad Toghi, University of Central Florida, USA
Michael W. Totaro, University of Louisiana at Lafayette, USA
Alex F. R. Trajano, Instituto Atlântico, Fortaleza, Brazil
Angelo Trotta, University of Bologna, Italy
Costas Vassilakis, University of the Peloponnese, Greece
Washington Velásquez, Escuela Superior Politécnica del litoral, Ecuador
Haibo Wang, University of Kentucky, USA
Chengshuo Xu, University of California, Riverside, USA
Kun Yang, Zhejiang Ocean University, China
Abdulsalam Yassine, Lakehead University, Canada
Xizhe Yin, University of California, Riverside, USA
Daqing Yun, Harrisburg University, USA

Habib Zaidi, Geneva University Hospital, Switzerland / University of Groningen, Netherlands / University of Southern Denmark, Denmark
Pavol Zavarsky, Framatome, Canada
Chuanji Zhang, Microsoft, USA
Yunpeng (Jack) Zhang, University of Houston, USA
Kai Zhao, University of California, Riverside, USA
Yao Zhao, ShanghaiTech University, China
Yimeng Zhao, Facebook, USA
Gaoqiang Zhuo, Castlight Health, USA

Copyright Information

Table of Contents

Peer to Peer Grid Topology with Full Mesh Networking Technology and its Applications

Wenqiang Song
Jit Research Institute
Jilin University Zhengyuan Information Technologies
Beijing, China
email:wenqiang_song@jit.com.cn

Chuan He
Jit Research Institute
Jilin University Zhengyuan Information Technologies
Beijing, China
email:chuan_he@jit.com.cn

Zhaoyang Xie
School of Cyberspace Science and Technology Institute
Beijing Institute of Technology
Beijing, China
email:zhaoyangxie@bit.edu.cn

Yuanyuan Chai
Jit Research Institute
Jilin University Zhengyuan Information Technologies
Beijing, China
email:yuanyuan_chai@jit.com.cn

***Abstract*—The continuous development of computer network technology has accelerated the pace of informatization, and at the same time, network security issues are becoming increasingly prominent. Networking technology with different network topologies is one of the important means to solve network security problems. Zero trust network solves the Virtual Private Network (VPN) problem through peer to peer authorization and continuous verification, but most of the solutions use a central proxy device, resulting in the central node becoming the bottleneck of the network. This paper put forward the Hard Network Address Translation (NAT) traversal formula based on the birthday paradox, which solves the long-standing problem of Hard NAT traversal. Based on this, a full mesh networking technology based on the variable parameter full dimensional spatial peer-to-peer grid topology was proposed, which realizes peer-to-peer resource interconnection for both the methodological level and the engineering level.**

Keywords-Zero trust; Birthday paradox; Hard NAT; port scanning; NAT traversal; full mesh networking technology.

I. INTRODUCTION

Network security is an important branch of the IT industry, with the goal of protecting network systems, data, and services from unauthorized access and attack [1][2]. With the spread of the internet and the acceleration of digitalization, the importance of network security is becoming increasingly prominent. In the early days, network security mainly focused on preventing the intrusion of malicious software, such as viruses and worms [3]. However, as the means of network attacks have become increasingly complex, the scope of network security has expanded to include preventing data breach, protecting user privacy, and preventing identity theft, among other aspects.

A Virtual Private Network (VPN) is a network security technology that creates encrypted network connections, allowing users to securely access remote or public networks. The advent of VPNs can be traced back to the 1990s [4] when businesses began seeking a solution to connect remote offices and employees securely and economically.

Zero Trust is a network security model whose core concept is "never trust, always verify". The emergence of this model is a reflection on the traditional "firewall" security model. In the traditional model [5], companies usually set up firewalls at the boundaries of their networks, and once users pass the firewall, they can access all resources within the network.

VPN and Zero Trust networking [6] are the two existing networking modes, each with its own characteristics. The security of VPN is based on geographical boundaries, but the granularity is relatively coarse, making it difficult to cope with dynamic changes in the security situation. Zero Trust networks solve the problem of VPN through end-to-end authorization and continuous verification, but most solutions adopt centralized proxy devices, making the central node a bottleneck and single point of failure in the network. Another possible implementation is peer-to-peer full mesh communication, but it is necessary to solve the NAT traversal problem.

This paper aimed to solve the core problem in Zero Trust networking. And as a prerequisite for the implementing full mesh networking, a Hard NAT traversal formula based on the birthday paradox was put forward, which solves the long-standing Hard NAT traversal problem [7]. In addition, the full mesh networking technology based on variable parameter full dimensional spatial peer-to-peer grid topology proposed in this article can also solve the problems and drawbacks of zero trust networking, achieve peer-to-peer resource interconnection, and meet the network communication requirements of full mesh networking, covering all types of networking solutions such as site to site networking.

In the second section, we present the virtual network model and explain our contributions in this article. In the third section, we introduced The Hard NAT Traverse Problem and Penetration Formula. In the fourth section, we introduced our solution, Full Mesh, which is a Networking Technology Based on Variable Parameter Full Dimensional Space.

II. Networking Requirements

Network Address Translation (NAT) is an address translation technology that can modify the IP address in the header of an IP datagram to another IP address, and achieve address reuse by using the translated port number. NAT is widely used as a transitional technology to alleviate the exhaustion of IPv4 public network addresses, due to its simple implementation. However, NAT also poses a potential security risk, as it can make it difficult to trace the origin of network traffic and can be used to hide malicious activities. Therefore, it is important to implement appropriate security measures, such as firewalls and intrusion detection systems, to ensure the security of networks that use NAT.

A. The difference between zero trust networking and VPN networking

Zero Trust and VPN are both technologies used to establish secure connections between two computers. However, they have some significant differences:

Zero Trust is a cloud-based architecture that allows data exchange between different organizations without a common trust basis, which uses encryption to protect the privacy and integrity of data, and uses authentication and authorization techniques [8]. In contrast, VPN is a technology used to establish a secure network connection between two organizations and also uses encryption to protect data, but it also uses Virtual Private Network (VPN) protocols to hide users' internet activity.

In addition, Zero Trust architecture is typically used to share data between different organizations, such as in healthcare, financial services, or government agencies. VPN is typically used to connect remote users to enterprise networks or to connect two enterprise networks together.

B. Issues with existing networking methods

The security of VPN is based on the division of geographical boundaries (intranet and internet), which has a relatively coarse granularity. Once inside the VPN boundary, access to the entire system is allowed. The security authentication of VPN is static and cannot respond well to the dynamic changes in security situations [9].

Zero Trust solves the problems of VPN by implementing end-to-end authorization and continuous verification. However, most Zero Trust solutions typically use a centralized proxy device to proxy traffic to access services. Although this solves the inherent problems of VPN's boundary division and continuous verification, the centralized topology of the proxy device causes it to become a bottleneck and a single point of failure in the network. Another possible implementation of Zero Trust [10] is for all communication nodes to implement point-to-point full mesh communication with each other, which can overcome the problems of VPN and avoid the typical issues of centralized topology in Zero Trust solutions. However, due to the existence of a large number of NAT devices in the current network, the problem of NAT traversal needs to be solved first to achieve truly feasible full mesh communication.

III. The Hard NAT Traversal Problem And Formula

When two devices in different private networks want to communicate to each other, we will face the NAT traversal problem. Two kinds of NAT traversal problems are discussed in this section, and we attempt to propose a solution to the problem.

A. The Hard-NAT problem

The traversal problem occurs when two private networks want to communicate over the Internet and the NAT device is unable to properly route the packets to the correct destination because they are both using private IP addresses. The most common scenario [11] for this problem is when both devices are on different private networks and they cannot communicate directly because their private IP addresses cannot be properly forwarded to each other over the Internet.

There are two types of traversal problems: Soft NAT traversal and Hard NAT traversal. Soft NAT traversal is usually caused by a NAT device that is not properly configured or does not have UPnP turned on. Universal Plug and Play (UPnP) is a universal network protocol that allows devices to automatically configure port mapping rules so that ports can be opened and closed automatically when needed. If a NAT device does not have UPnP enabled or does not configure the port mapping rules correctly, this can lead to Soft NAT traversal problems.

The Hard NAT refers to a stricter form of NAT, also known as Symmetric NAT. In Hard NAT, the NAT device assigns each connection a unique port number that can only be used for that connection and cannot be used by any other connection. This assignment results in external devices not being able to directly access devices in the private network, which can lead to Hard NAT traversal problems. By using asymmetric port mapping, Hard NAT makes it impossible for external devices to directly access devices on the private network. When a device on a private network wants to communicate with an external device, it usually needs to use some special techniques and protocols, such as Session Traversal Utilities for NAT (STUN), Traversal Using Relay NAT (TURN), Interactive Connectivity Establishment (ICE), etc., to solve the Hard NAT traversal problem.

In Easy NAT, the NAT device assigns each internal device a public IP address and port number that is unique to that device, and external devices can access that device through that address and port number. Compared to Hard NAT, Easy NAT uses a relatively loose port mapping method, which makes it easier for external devices to access devices on the private network. When a device initiates a connection to the outside, the NAT device uses the public IP address and port number of this device to map this connection. When an external device initiates a connection to this device, the NAT device decides which device to forward this connection to based on the destination IP address and port number of the connection. Easy NAT is a relatively loose NAT translation method that uses a relatively loose port mapping method, which makes it relatively easy for external devices to access devices on the private network. However, Easy NAT also has some security issues, and the appropriate security configuration should be considered.

We call Hard NAT and its variants "Endpoint-Dependent Mapping" (EDM). But Hard NAT is a big problem for us, as long as there is such a device in the path, the previous scheme will not work. In addition, certain networks block NAT traversal, which has a much greater impact than this Hard NAT. For example, we found that UCBerkeleyguestWiFi blocks all outgoing UDP traffic except DNS traffic. No matter what NAT hacks are used, there is no way to get around this block. Therefore, a reliable fallback mechanism is needed.

This section discusses the NAT traversal problem in the network, including Soft NAT traversal and Hard NAT traversal, and two types of NAT translation methods, Easy NAT and Hard NAT. For the Hard NAT traversal problem, the use of techniques and protocols such as STUN, TURN, and ICE are proposed to solve the problem. However, some networks that block NAT traversal would require a reliable fallback mechanism.

B. The Hard-NAT traversal formula based on the birthday paradox

The main problem is that the Easy NAT side does not know which address (IP port combination) to send data to on the Hard NAT side, but must also send data to the Hard NAT side to open the firewall on that side.

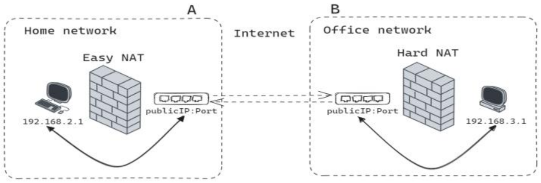


Figure 1. Easy NAT and Hard NAT traversal

As shown in Figure 1, we have known some ip-port combinations for the hard side, because we have run STUN. Assuming for a moment that the IP address is correct, then it is the port that needs to be addressed. There are 65535 possible port numbers. We can scan them one by one and find the correct port number in 10 minutes at worst, if we scan 100 per second. It can solve the problem, but not very cleverly. And it looks so much like port scanning to the IDS software (because that's what we're actually doing) that it's basically going to be blocked.

Using the birthday paradox theory, we can do much better than port scanning! Instead of scanning 65535 possible ports one by one, we can open 256 ports at once on the Hard NAT side by establishing 256 sockets which can send data to the Easy NAT side and let the Easy NAT side randomly probe the target ports.

The birthday paradox is the probability that at least two people out of no less than 23 people have the same birthday is greater than 50%. For example, in an elementary school class of 30 students, the probability of two people having the same birthday is 70%. In a large class of 60 students, the probability is greater than 99%. The birthday paradox is a "trick" in the sense that it creates a logical contradiction. However, this mathematical fact is so counterintuitive that it is called a paradox. The mathematical theory of the birthday paradox has been applied to the design of a cryptographic attack method - the birthday attack.

In the Hard NAT traversal problem, A side is Easy NAT and B side is Hard NAT, the ports of A are fixed (one and known), and B hypothetically opens 256 ports (but it is impossible to know what these 256 port numbers are), which we can scan a total of m (m=t*R) times.t is the scan time and R is the scan frequency.

If we consider the total number of ports that can be used in the end to be from 1025 to 65535, then the problem can be simplified as following: there are a total of (65535-1024) balls in a pool, of which there are B black balls, and the probability that we will catch the black ball if we catch it A times is the results we want. Here B is the number of ports opened on the B side, for example 256, A is the number of times the A side probed. Based on the birthday paradox, the Hard NAT traversal formula (1) is as following:

$$P = 1 - \prod_{i=0}^{A-1} \frac{K - B - i}{K - i} \qquad (1)$$

where, P is the final calculated probability that it can be successfully traversed, the constant K is the total number of available ports (from 1025 to 65535), A is the number of probes on the A side (i.e., scan-time*scan-frequency), and B is the number of open ports on the B side (e.g., 256).

Figure 2 shows the variation of connection success probability with the number of random probes for 128, 256, and 512 ports opened in Hard NAT. Figure 2 compares the number of probes required to achieve 99% success probability when different numbers of ports are opened in Hard NAT. Notice that the higher the number of opened ports, the less probes are needed to reach 99% success probability. Based on engineering experience and resource consumption in real-world usage, we generally use 256 as the number of opened ports on the hard side for NAT traversal.

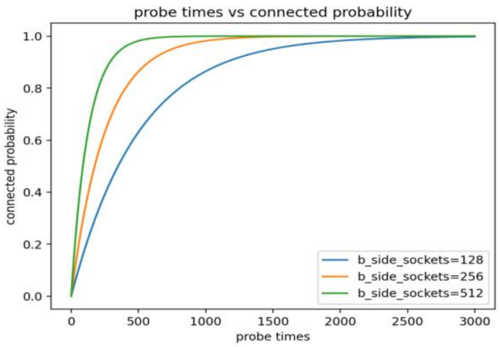


Figure 2. the probability of a successful connection as a function of the number of random probes (with 128, 256, and 512 ports opened in Hard NAT, respectively).

IV. FULL MESH NETWORKING SCHEME AND APPLICATIONS

This Section mainly discusses the full mesh networking scheme based on variable parameter full dimensional space that can be realized by using the birthday paradox based NAT traversal technology on the basis of NAT traversal capability, gateway requirements and encryption requirements. These networking schemes basically cover all existing VPN network application scenarios and have high flexibility and scalability.

A. *Preliminaries*

The NAT traversal formula (2) based on birthday paradox can be simplified as following:

$$P = det(t, R, n) \qquad (2)$$

where, P represents the total traversal rate, t represents the total scanning time, R represents the scanning rate (times/s), and n represents the total number of ports scanned. Usually, n is taken as 256. According to the previous conclusion, under the condition of limiting R to 100 times per second, the P value can reach 50% within 2 seconds of t, and P value can be above 99.9% before t reaches 20 seconds.

Based on the calculation of NAT traversal capability, which is P, the full mesh networking scheme based on variable parameter full dimensional space can be summarized as formula (3):

$$T = hom(G, P, \theta) \qquad (3)$$

Where, G is Gateway, in which 0 means a network without gateway and 1 means a network with a gateway. P is the NAT traversal rate, in which 0 means unsuccessful traversal and 1 means successful traversal. θ is end-2-end encryption, in which 0 means end-2-end encryption is not in place and 1 means end-2-end encryption is in place.

The full mesh networking technology based on variable parameter full dimensional space proposed in this article can comprehensively cover the following four networking schemes at both the theoretical level and engineering level, including 1) Point-2-Site scheme when G=1 and P=0, θ=1 2) Site-2-Site scheme when G=1 and P=0, θ= 0 3) Site-Mesh scheme when G=1 and P=1, θ= 1 and 4) Full-Mesh scheme when G=0 and P=1, θ= 1.

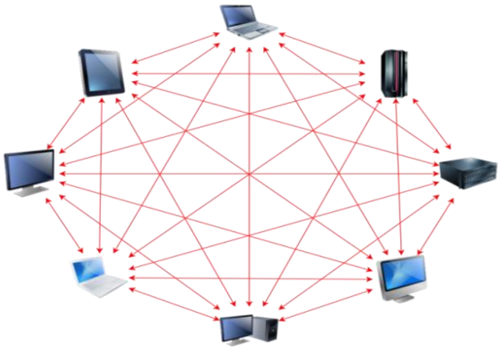


Figure 3. Figure of Full Mesh

Full mesh scheme is the most ideal network form that meets all zero trust requirements, as shown in the figure 3. Each computing node (including physical and virtual) joins a peer-to-peer fully connected network through an SDP agent, and the connection between any two points is encrypted and access permissions are individually separately.

B. *Applications*

The full mesh networking technology based on variable parameter full dimensional space proposed in this article can be used in many different applications.

First and most popular application is to form a private VPN network for enterprises. Compared to normal VPN applications, a full mesh solution could perfectly and permanently solve the following problems: 1). Single point of failure 2) Performance bottleneck and 3) High Data latency.

In a normal VPN network, all traffic will go through the central VPN server. This server becomes a single point of failure as well as a bottleneck of performance. Using a full mesh solution, traffic travels between each pair of nodes directly through the Internet without going through any central point, thus no single point of failure. System performance depends not upon the bandwidth of the central server, but the bandwidth between each node.

Consider the latency of the system, suppose our central VPN server is located in Boston, and we have two roaming nodes one in Los Angeles, which we call it A, and another in San Francisco which we call it B. When A needs to communicate to B, the data traffic will go from Log Angeles to Boston then from Boston to San Francisco. With a full mesh solution, data traffic could simply go from Logs

Angeles to San Francisco. The typical latency would drop from around 80-100ms to 10-20ms, which is huge for certain applications such as gaming.

The second application is Internet of Things （IoT） devices. Usually IoT devices need to be put in a private network and the quantity of the devices is very large. Constructing such a private network is a heavy burden to the IoT Systems, but our full mesh solution will benefit from its peer-2-peer feature. The large quantity of IoT devices can easily form an overlay private network without any difficulty.

V. CONCLUSION AND FUTURE WORK

In order to solve the problem of NAT traversal when devices need to access each other on the internet, we propose a peer to peer grid topology with full mesh networking technology. We first discussed networking requirements and two different types of network configurations: VPN and Zero Trust networking.

When discussing the NAT traversal issue, we introduced the concepts of Soft-NAT and Hard-NAT traversal and compared the two NAT traversal methods, Easy-NAT and Hard-NAT. For the Hard-NAT traversal problem, we suggested using technologies and protocols such as STUN, TURN, ICE, and also proposed a fallback mechanism to cope with situations where some networks may block NAT traversal entirely.

Next, we detailed the network penetration technology based on the birthday paradox, which can solve the problem of being unable to determine the target port when data communication occurs between Easy NAT and Hard NAT.

Finally, we discussed the variable parameter full-dimensional peer-to-peer networking schemes that can be achieved using the network penetration technology based on the birthday paradox. These networking schemes basically cover all existing network application scenarios of VPNs and have high flexibility and scalability. Through this section's introduction, readers can better understand networking requirements, the NAT traversal issue, and the network penetration technology utilizing the birthday paradox, thus better addressing actual network application scenarios.

In the future, we plan to apply this full mesh networking technology to the actual VPN networking and zero-trust solution, and test its actual performance under heavy traffic.

ACKNOWLEDGMENT

Thanks to the teachers and researchers of the Research on satellite communication security system Project Team of the Jilin Science and Technology Office. Thanks to everyone!

REFERENCES

[1] S. Lee, and MN Kim “This is my paper”, ABC Transactions on ECE, Vol. 10, No. 5, pp120-122.

[2] A Gizem and O Ayese (2009) Communications and Networks, Network Books, ABC Publishers.

[3] S. Vinoth, et al. "Application of cloud computing in banking and e-commerce and related security threats." Materials Today: Proceedings 51: 2172-2175.

[4] Mughal, A Arif. "Well-Architected Wireless Network Security." Journal of Humanities and Applied Science Research 5.1 : 32-42.

[5] X Wu, et al. "Threat analysis for space information network based on network security attributes: a review." Complex and Intelligent Systems: 1-40.

[6] F Li. "Network Security Evaluation and Optimal Active Defense based on Attack and Defense Game Model." 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE, 2023.

[7] B Bijender, et al. "Big Data Architecture for Network Security." Cyber Security and Network Security: 233-267.

[8] Ghelani, Diptiben, KH Tan, and KRK Surendra. "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking." Authorea Preprints.

[9] Hasan, K Mohammad, et al. "A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things." IET Communications 16.5: 421-432.

[10] Pramanik, Sabyasachi, et al., eds. Cyber Security and Network Security. John Wiley and Sons, 2022.

[11] Ghelani, Diptiben. "Cyber Security in Smart Grids, Threats, and Possible Solutions." Authorea Preprints.

Using Attribute Certificates to Support Cryptographic Algorithm Flexibility

Steffen Fries, Rainer Falk
Siemens AG
Technology
Munich, Germany
e-mail: {steffen.fries|rainer.falk}@siemens.com

***Abstract*—Asymmetric cryptography is broadly used to protect confidentiality, integrity, and authenticity of data transfer. Typical applications are authentication and key agreement in secure communication protocols, and digital signatures for authentication and integrity protection of documents and messages. Digital certificates confirm the public key of a user. They are used for user authentication performed during the handshake by common cryptographic security protocols like Transport Layer Security, Datagram Transport Layer Security, or by authentication and key agreement protocols like the Internet Key Exchange or Group Domain of Interpretation. The cryptographic algorithm for public-key-based user authentication is fixed by the user's certificate. More flexibility to support multiple cryptographic algorithms for user authentication is needed, e.g., by the introduction of new, quantum-safe cryptographic algorithms. Attribute certificates can be used to support flexibly multiple cryptographic algorithms for user authentication, supporting a stepwise transition towards newer cryptographic algorithms.**

Keywords–communication security; cryptographic agility; post-quantum cryptography; attribute certificates; industrial automation and control system; Internet of Things; automation control systems.

I. INTRODUCTION

Asymmetric cryptography and digital signatures are a cornerstone in many security architectures. Main applications of digital signatures are user (entity) authentication and integrity protection of data at rest and in transit. The user utilizes his private key for authentication. A peer verifies the authentication using the corresponding public key. Digital certificates, e.g., according to the X.509 standard, confirm the user identity associated with the user's public key [1].

Besides entity authentication, digital signatures provide integrity protection of the signed content, which may be a document or, in case of the initial phase of security protocols, protect the negotiation of security parameters for a communication session as used in common security protocols like Transport Layer Security (TLS) [2] and Datagram Transport Layer Security (DTLS) [3], or in "pure" authentication and key agreement protocols like the Internet Key Exchange (IKEv2) [4] or the Group Domain of Interpretation GDOI) [5] protocol.

Due to advances in quantum computing, currently used asymmetric cryptographic algorithms like RSA (Rivest, Shamir, Adleman) or ECDSA (Elliptic Curve Digital Signature Algorithm) are endangered, as there underlying mathematical problems, like factorization and discrete logarithm problems (see also [6]) can be solved efficiently using a cryptographically relevant quantum computer leveraging Shor's algorithm (see also [7]). Symmetric cryptographic algorithms can also be attacked using Grover's algorithm (see also [7]), but for them it is currently seen sufficient to double the key length without a change of the algorithms (see also [8]).

While the standardization and the journey to introduce new, post-quantum asymmetric algorithms that withstand such attacks is still ongoing, the discussion of transition approaches for currently used cryptographic algorithms to new algorithms has already started (see [9]). In this context, different strategies are being discussed, like the combined or hybrid use of classical and post-quantum algorithms. This also relates to the utilized credentials, which may come in different formats like hybrid certificates supporting alternative cryptographic algorithms in the same certificate (see [1]). However, only a single second public key of a single second cryptographic algorithm can be included. As multiple quantum-safe cryptographic algorithms are currently standardized, a more flexible approach to support multiple public keys for authentication of a single user is needed.

Note that the case of post-quantum cryptographic algorithms is taken here as example. Crypto agility as the ability to adopt to alternative cryptographic algorithms, is a general design objective for protocols and architectures to ensure that new algorithms with similar boundary conditions can be deployed easily.

Transition is specifically important for industrial use cases, as the component lifetime here is much longer compared to consumer electronics. Therefore, it is important to elaborate ways to allow an upgrade of systems already in the field not only with new algorithms, but also with new or enhanced credentials for entity authentication.

This paper is structured in the following way. Section II provides an overview about related work. Section III gives an overview on public key certificates and attribute certificates to show the general structure and approach. Section IV investigates a new approach utilizing attribute certificates to support migration. Section V concludes the paper and provides an outlook to potential future work.

II. Related Work

The NIST challenge on replacement algorithms for digital signatures finishes after six years. Three digital signature candidates have been selected for standardization (see [10]):

- CRYSTALS-Dilithium
- FALCON
- SPHINCS+

These algorithms have different parameters and different parameter sizes as the classical algorithms like RSA or ECDSA. The key size can be significantly larger compared to classical cryptographic algorithms. This parameters and key sizes need to be supported by implementations and most importantly also in the context of existing user authentication credentials like X.509 certificates.

The migration or transition to quantum-safe cryptographic algorithms is a complex undertaking. The National Institute for Standards and Technology NIST has published a draft guideline on the migration to post-quantum cryptography [9].

Transition of cryptographic algorithms has been worked on in the context of ITU-T X.509 [1] with the support of alternative cryptographic algorithms as investigated in the following Section III.A.

With the IETF, a further standardization organization investigates into the different options of migration towards post-quantum cryptographic algorithms. Here the emphasis lies on utilizing hybrid approaches in protocols like TLS [2] or DTLS [3]. Besides integrating new algorithms in ciphersuites also approaches like Key Encapsulation (KEM, [11]) are being discussed to avoid generation of digital signatures on constraint devices.

III. Public key and Attribute Certificates

X.509 certificates are used for entity authentication and integrity protection. As shown in Figure 1, the concept of a public key certificate is the binding of an entity’s identity to a public key, which has a corresponding private key. This private key is kept secret by the entity and can be used to authenticate the entity. The certificate itself is issued by a trusted third party, a certification authority, that digitally signs the certificate. This signature is verified by the relying party as part of certificate path validation to a root certificate.

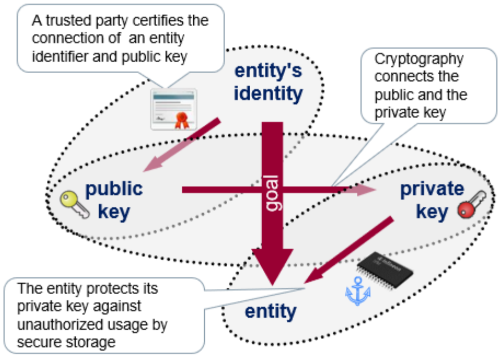

A trusted party certifies the connection of an entity identifier and public key
entity's identity
Cryptography connects the public and the private key
public key
goal
private key
The entity protects its private key against unauthorized usage by secure storage
entity

Figure 1. Concept of Binding Public Keys to Identities

These certificates are called public key certificates, as they bind the public key to an entity’s identity. In addition, there attribute certificates are defined, which can be seen as temporary enhancement of public key certificates. They do not contain public keys but additional attributes that are connected to the holder of the public key certificate as shown in Figure 2. As visible in the figure, an attribute certificate has a validity period, which may vary based on the application use case. As the attribute certificate can be assumed as a temporary enhancement of a statements contained in a public key certificate, it may be short-lived or it may have a similar validity as the public key certificate. Figure 2 also shows that the issuing authority may be different for the attribute certificate as for the public key certificate. This fact may be interesting in cases where a separation of duty is targeted.

The following subsections will provide more details on both certificate types.

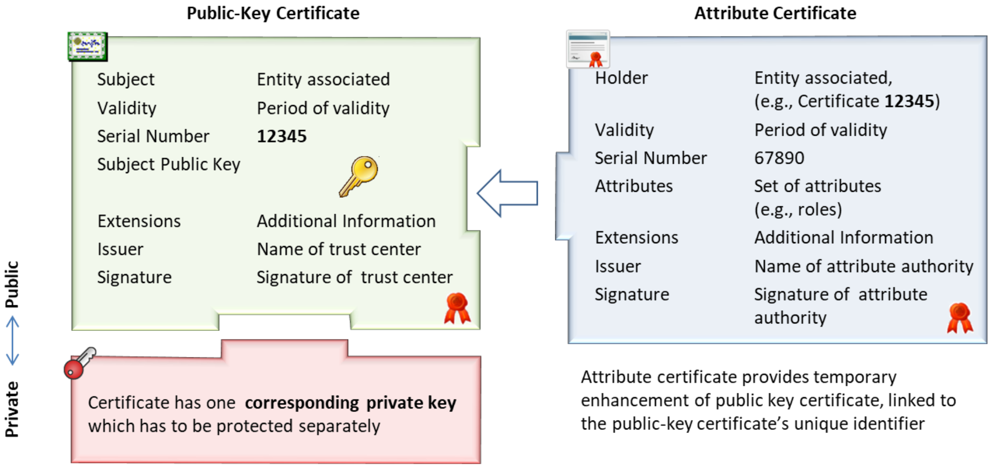
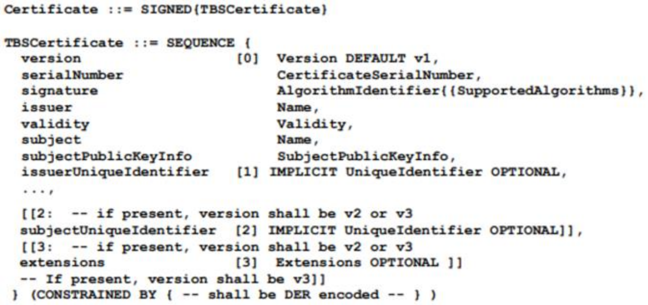

Public-Key Certificate
Subject
Entity associated
Validity
Period of validity
Serial Number
12345
Subject Public Key
Extensions
Additional Information
Issuer
Name of trust center
Signature
Signature of trust center
Certificate has one corresponding private key which has to be protected separately
Public
Private
Attribute Certificate
Holder
Entity associated, (e.g., Certificate 12345)
Validity
Period of validity
Serial Number
67890
Attributes
Set of attributes (e.g., roles)
Extensions
Additional Information
Issuer
Name of attribute authority
Signature
Signature of attribute authority
Attribute certificate provides temporary enhancement of public key certificate, linked to the public-key certificate's unique identifier

Figure 2. Concept of Public Key Certificates and Attribute Certificates

A. Public Key Certificates

ITU-T X.509 [1] is the public key certificate and attribute certificate framework widely applied in Information technology (IT) solutions an increasingly being used in Operational Technology (OT) solutions. It defines the structure and content of public key certificates as well as the verification of the components.



```
Certificate ::= SIGNED{TBSCertificate}

TBSCertificate ::= SEQUENCE {
  version                    [0]  Version DEFAULT v1,
  serialNumber                    CertificateSerialNumber,
  signature                       AlgorithmIdentifier{{SupportedAlgorithms}},
  issuer                          Name,
  validity                        Validity,
  subject                         Name,
  subjectPublicKeyInfo            SubjectPublicKeyInfo,
  issuerUniqueIdentifier     [1] IMPLICIT UniqueIdentifier OPTIONAL,
  ...,
  [[2:  -- if present, version shall be v2 or v3
  subjectUniqueIdentifier   [2] IMPLICIT UniqueIdentifier OPTIONAL]],
  [[3:  -- if present, version shall be v2 or v3
  extensions                [3]  Extensions OPTIONAL ]]
  -- If present, version shall be v3]]
 } (CONSTRAINED BY { -- shall be DER encoded -- } )
```

Figure 3. Public Key Certificate structure (see [1])

As shown in Figure 3, the certificate is a signed structure, containing the `subject` as the name of the entity and the `subjectPublicKeyInfo` structure with information about algorithm and the contained public key. The certificate is signed by an issuing certificate authority. Besides further components the certificate structure can also be extended using the `extensions` component.

To support alternative algorithms, X.509 defines three extensions to convey the:

- `subjectAltPublicKeyInfo` – alternative public key
- `altSignatureAlgorithm` – alternative signature algorithm (used to sign the public key certificate) and
- `altSignatureValue` – alternative signature value.

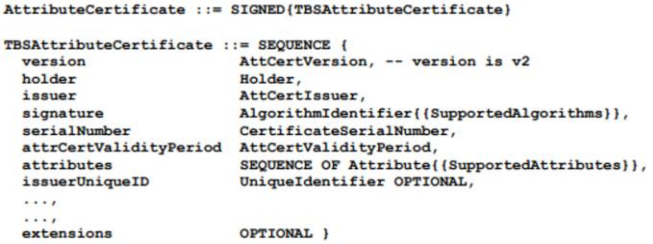
Using theses extensions allows a relying party depending on its capabilities to either utilize classical cryptographic algorithms or alternative (here post quantum) algorithms for the verification of the certificate (and potential digital signatures performed with the public key corresponding to the contained public key. Depending on the security policy of the relying party, both signatures of the certificate may need to be verified.

This approach is limited to a single alternative key for a public key in practical application, i.e., limited to a single alternative cryptographic algorithm. Simply adding multiple alternative keys to the authentication certificate would increase the certificate size significantly.

B. Attribute Certificates

Besides public key certificates, ITU-T X.509 [1] also defines the structure and content of attribute certificates, as well as the binding to public key certificates and the verification of contained components. Note that besides the binding to public key certificates, an attribute certificate may also be bound to a name of an entity or some fingerprint of information.

An attribute certificate may be seen as temporary enhancement of a public key certificate.



```
AttributeCertificate ::= SIGNED{TBSAttributeCertificate}

TBSAttributeCertificate ::= SEQUENCE {
  version                  AttCertVersion, -- version is v2
  holder                   Holder,
  issuer                   AttCertIssuer,
  signature                AlgorithmIdentifier{{SupportedAlgorithms}},
  serialNumber             CertificateSerialNumber,
  attrCertValidityPeriod   AttCertValidityPeriod,
  attributes               SEQUENCE OF Attribute{{SupportedAttributes}},
  issuerUniqueID           UniqueIdentifier OPTIONAL,
  ...,
  ...,
  extensions               OPTIONAL }
```

Figure 4. Attribute Certificate structure (see [1])

As shown in Figure 4, similar to public key certificates an attribute certificate is also a signed structure, containing the `holder` as the name of the entity, information about the issuer, including the signature algorithm and values as well as the possibility to define extensions of the attribute certificate. Like for public key certificates, to support alternative algorithms, X.509 defines two extensions to convey the:

- `altSignatureAlgorithm` –alternative signature algorithm (used to sign the attribute certificate) and
- `altSignatureValue` – alternative signature value.

The standard does not foresee the capability to contain an alternative public key of the holder as additional attribute. The next section discusses the merits of providing this information as well as further, policy related information in the context of an attribute certificate.

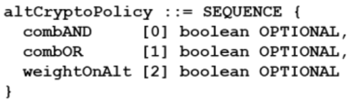
IV. Proposed New Attributes

As discussed in Section III, not all extensions defined for public key certificates are defined for inclusion in attribute certificates. This paper therefore proposes to use the `subjectAltPublicKeyInfo` extension also in attribute certificates to convey an alternative public key and information about the corresponding cryptographic algorithms, e.g., a public key for a post quantum asymmetric algorithm like FALCON, DILITHIUM, or SPHINCS+. This allows to associate and utilize alternative public keys to already existing certificates. As multiple attribute certificates can be issued for a single user certificate, implicitly various different cryptographic algorithms can be supported in a flexible way by issuing multiple corresponding attribute certificates.

Attribute certificates contain attributes, and providing an alternative public key as attribute is proposed as novel approach. It is intended to support smooth transition to public-key certificates using solely alternative, in the case here, post quantum cryptographic algorithms. As they are intended as temporary enhancement of public key certificates, this approach is seen appropriate. It is even possible to issue attribute certificates for an entity's public key certificate at a later point in time.

For migration to post-quantum cryptography, it is necessary to also support a security policy which handles the transition from one cryptographic algorithm to an alternative cryptographic algorithm (in the case here for digital signatures). Such a policy may require verifying only one signature, both signatures (classic and alternative), and may also provide a weight on the verification result, e.g., by the order of operations. Such a security policy may be configured per relying party. In case of automation networks, it may be part of the engineering data for the Intelligent Electronic Devices (IED).

An alternative approach to the device configuration of security policies is the provisioning of the policy as part of the certificate, also in the form factor of an extensions. This paper proposes such an extension as shown in Figure 5 that may be applied in both certificate types, i.e., to public key certificates as well as to attribute certificates.



```
altCryptoPolicy ::= SEQUENCE {
  combAND     [0] boolean OPTIONAL,
  combOR      [1] boolean OPTIONAL,
  weightOnAlt [2] boolean OPTIONAL
}
```

Figure 5. Proposed Migration Policy Extension

The extension allows to specify the following security policies for the associated alternative public key:

- `combAND` requires the verification of the signature performed with the classic asymmetric algorithm as well as the alternative algorithm.
- `combOR` requires the verification signatures created with of either the classical or the alternative cryptographic algorithm,
- `weightOnAlt` indicates if the alternative algorithm has a higher weight in the evaluation. Note that this can be used in conjunction with `combOR` for the selection of classical or alternative signatures and also for the `combAND` case in cases, in which one signature verification may fail.

The extension may be included in the certificate as critical extension to ensure that it will be evaluated by the relying party. The inclusion into public key certificate can be done to associate a fixed security policy to the two contained public keys. There is also a benefit by placing the extension into an attribute certificate even in cases where the second public key is not contained in the attribute certificate but in the public key certificate. This approach allows to change the security without the need to issue a new public key certificate, enabling dynamic policy changes.

V. Conclusion and Outlook

This paper provides an overview on the need for a transition from currently used classical cryptographic algorithms to new, alternative cryptographic algorithms. More specifically, the focus is placed on the use of digital signatures and credentials conveying the public key within X.509 certificates.

In that respect, a novel approach for using alternative asymmetric algorithms in the context of these X.509 certificates has been described. It is proposed to support alternative public keys and associated information in attribute certificates, which enhances the application of already defined certificate extensions for public key certificates also for attribute certificates. By this approach, multiple cryptographic algorithms can be supported flexibly by issuing multiple attribute certificates corresponding to the different public keys of a user. Moreover, a further security policy extension is proposed that allows a dynamic adaptation of the security policy for the transition from classic cryptographic algorithms towards alternative, e.g., post quantum algorithms.

The discussed approach is currently in its infancy and needs to be implemented and tested to get practical experience. This is seen as the next consequent step. Due to the use of an already existing extension to transport the alternative public key, further investigation of the transport of algorithm specific parameters is not seen necessary as already considered in the originally defined extension.

Besides the necessity to perform more investigation of the side conditions of this approach and also a proof-of-concept implementation, it is seen necessary to also discuss this approach within standardization. This is due to the fact that most interacting systems are built with products from different manufacturers. Therefore, standardization is necessary to ensure interoperability of different manufacturers products.

References

[1] ITU-T X.509 ISO/IEC 9594-8:2020, Rec. ITU-T X.509 (2019), Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, https://www.itu.int/rec/T-REC-X.509-201910-I/en, [retrieved: August, 2023]

[2] E. Rescorla, IETF RFC 8446, “Transport Layer Security (TLS) Protocol v1.3”, August 2018, https://tools.ietf.org/html/rfc8446, [retrieved: August, 2023]

[3] E. Rescorla, H. Tschofenig, and N. Modadugu, IETF RFC 9147, “The Datagram Transport Layer Security (DTLS) Protocol Version 1.3”, April 2022 https://datatracker.ietf.org/doc/html/rfc9147, [retrieved: August, 2023]

[4] C. Kaufman, P. Hoffman, Y. Nir, P.Eronen, and T. Kirvinen., IETF RFC 7296, „Internet Key Exchange Protocol Version 2 (IKEv2)“, October 2014, https://datatracker.ietf.org/doc/html/rfc7296, [retrieved: August, 2023]

[5] B. Weis, S. Rowles, and T. Hardjono, IETF RFC 6407, “The Group Domain if Interpretation”, October 2011, https://datatracker.ietf.org/doc/html/rfc6407, [retrieved: August, 2023]

[6] A. J. Menezes, P. C. v. Oorschot, and S. A. Vanstone, “Handbook of Applied Cryptography”, CRC-Press, October 1996, ISBN: 0-8493-8523-7

[7] D. J. Bernstein, J. Buchmann, and E. Dahmen, “Post-quantum cryptography”, Springer, Berlin, 2009. ISBN 978-3-540-88701-0

[8] L. Cehen et al., NISTIR 8105, “Report on Post-Quantum Cryptography”, April 2016, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf, [retrieved: August, 2023]

[9] W. Newhouse, M. Souppaya, W. Barker, and C. Brown, “Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography”, Volume A “Executive Summary”, NIST Special Publication 1800-38A, April 2023, https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms [retrieved: August, 2023]

[10] NIST Announcement, “PQC Standardization Process: Announcing Four Candidates to be Standardized”, July 2022, https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4, [retrieved: August, 2023]

[11] Giacon, F., Heuer, F., and B. Poettering, "KEM Combiners", January 2018, https://doi.org/10.1007/978-3-319-76578-5_7, [retrieved: August, 2023].

Measurement of Competitiveness in the Colombian Mobile Telecommunications Market based on the Linda Index

Cesar Hernandez, Ernesto Cadena, Luis Pedraza
Technological Faculty
Universidad Distrital Francisco José de Caldas
Bogotá, Colombia
email: cahernandezs@udistrital.edu.co, ecadena@udistrital.edu.co, lfpedrazam@udistrital.edu.co

Abstract— **The mobile telecommunications services market has great relevance in the socioeconomic growth of a country and the reduction of the digital divide. However, the high demand for these mobile telecommunications services has produced a high concentration in this market, which can lead to an oligopoly or even a market monopoly. In order to prevent this, the state must generate adequate policies for the measurement and monitoring of market concentration levels. This article aims to measure concentration in the Colombian mobile telecommunications market. To achieve the above, the databases of mobile internet revenues, traffic, and accesses of the telecommunications companies operating in Colombia from 2012 to 2022, both for postpaid (fixed charge) and prepaid (on demand), provided by the Communications Regulatory Commission, were used, and through the Linda index, the corresponding measurement of the concentration indexes was made. In terms of the overall revenue (prepaid plus postpaid) of the telecommunications companies, the main result was that, in the case of the Colombian mobile telecommunications services market, there is a moderate concentration.**

Keywords-competition; linda's index; market concentration; measurement; mobile internet; revenue; telecommunications market.

I. INTRODUCTION

The mobile telecommunication services market is moving in increasingly flexible and adaptable environments to the customers' needs. In addition, there is a bandwidth increase due to the emergence of various services and applications on mobile internet, increasing the volume of data sales and becoming a solid source of income for Internet Service Providers (ISPs). As a result, competition among ISPs to maintain and attract new customers to their businesses is increasing significantly, and they are forced to analyze the quality of service and experience to improve interaction with their customers. However, the providers' interest lies in keeping these customers and increasing the volume of consumption of their services [1][2].

Studies have been carried out to analyze the current state of the mobile telecommunications market in Latin American countries and show the need for elements such as adequate spectrum management and alignment with established policies on telecommunications services. As a result of these studies, the concentration analysis in these markets is identified as a central point of study to improve competitiveness and reduce the digital divide, facilitating regional development and identifying potential investments. It is determined that countries that allocate greater bandwidth and achieve more competitive market structures obtain a greater amount of demonstrable social benefits. Countries such as Mexico have initiated this task, and the analysis of the spectrum, its allocation, and management is included among the essential variables as a relevant topic of study, appropriating the lessons of more mature markets [3][4].

Globally, it is clear that Information and Communications Technologies (ICTs) are a relevant factor leading to socioeconomic development and growth in a competitive environment that enables countries, companies, and individuals to reap the benefits. It has proven to have a great impact in areas such as commerce, health, and education, provides new job opportunities, and can help people and companies to remain competitive by running their processes more efficiently. For example, in Europe, its relevance can be seen with the creation of a digital agenda in the Europe 2020 Strategy that seeks to achieve sustainable and inclusive growth for the European economy, which aims to develop a digital economy based on knowledge and innovation [5]-[7].

A competitive market has various benefits, among which good quality, more and better options for goods and services, and low prices stand out in favor of the consumer; in favor of companies the increase in production, giving a boost to the economy in general. According to the Organization for Economic Cooperation and Development (OECD) Economic Outlook published in June 2020, global activity is projected to fall by 6% this year. Likewise, global unemployment rose from 5.4% in 2019 to 9.2% in 2020, all this under the assumption that there is no additional crisis due to the COVID-19 contagions. On the other hand, the World Economic Forum estimates that foreign direct investment will fall between 30% and 40% globally.

This article aims to measure the concentration in the Colombian mobile telecommunications market. To achieve this, we used the databases of mobile internet revenues, traffic, and accesses of the telecommunications companies operating in Colombia from 2012 to 2022, both for postpaid (fixed charge) and prepaid (on demand), provided by the Communications Regulation Commission (CRC), and through Linda's index we measured the corresponding concentration indexes.

The structure of this paper is as follows: section II provides a description of mobile telecommunications services market in Colombia. Section III presents the Linda index. Section IV describes the methodology used. Section V presents the results of the measuring concentration in the mobile telecommunications services market in Colombia. Section VI presents the results analysis. Finally, section VII presents the conclusions.

II. Mobile Telecommunications Services Market in Colombia

Based on figures presented during the third quarter of 2022 by the Ministry of Information and Communication Technologies (MinTIC), the total number of mobile Internet accesses in Colombia reached 39.1 million, 3.4 million more than those registered in the same quarter of the previous year, as shown in Figure 1 [8].

Until September 2022, the provider with the largest number of mobile Internet accesses was Claro (20.6 million), followed by Movistar (8.9 million), TIGO (6.8 million), and WOM (1.7 million), as shown in Figure 2 [8].

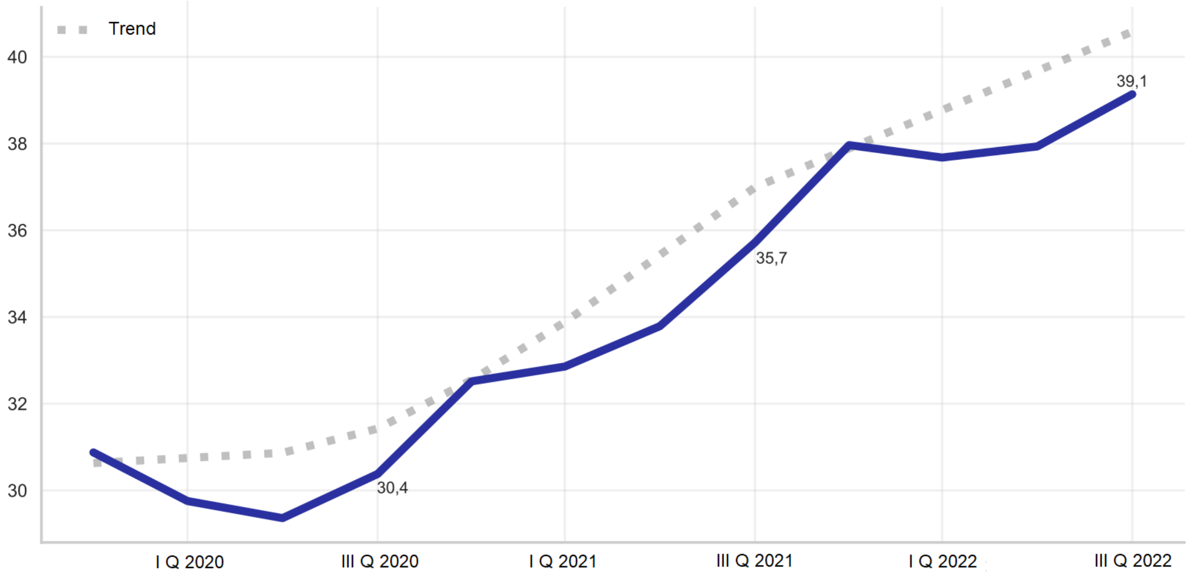


Figure 1. Accesos a internet móvil en millones [8]

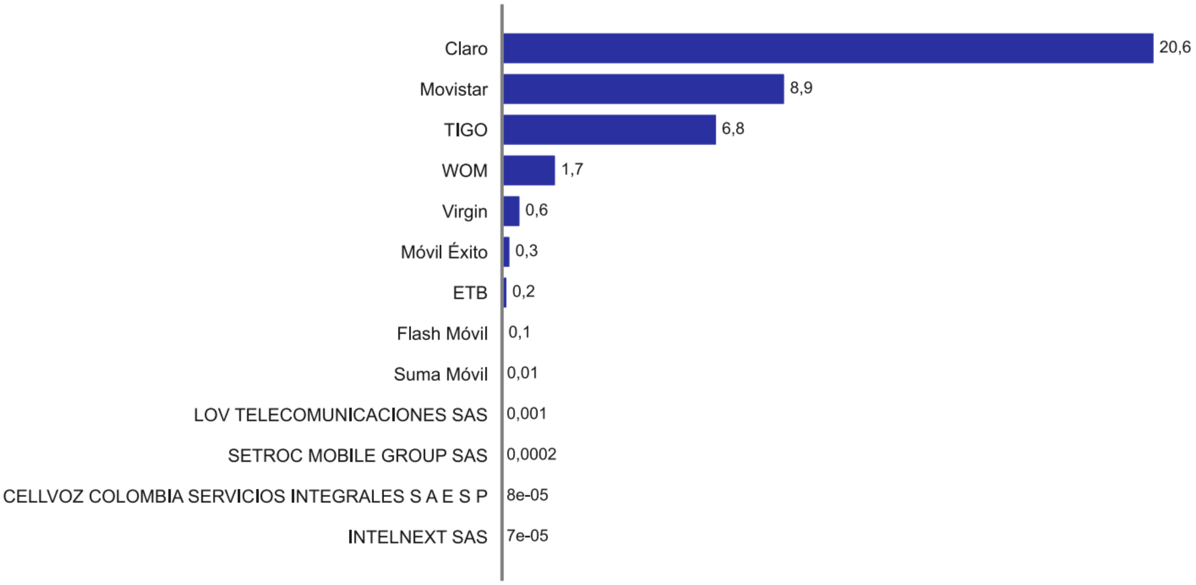


Figure 2. The number of mobile providers accessed by providers [8]

At the end of the third quarter of 2023, the principal mobile internet access technology in subscription mode was 4G, with 32.9 million accesses, while, with a downward trend, 3G technology has 5.4 million and 2G registers 0.9 million accesses, as shown in Figure 3 [8]. In Figure 3, a greater tendency to use the 4G technology network can be observed, largely due to the advantages that better technology brings.

ISBN: 978-1-68558-099-5

During the third quarter of 2022, operating revenues in Colombian pesos for prepaid and postpaid modality, excluding taxes, produced by the provision of mobile telephony service were close to $ 400 billion for postpaid and $ 163 billion for prepaid, as shown in Figure 4 [8]. Figure 4 shows a higher level of income from the postpaid modality than from the prepaid modality; this is because the prepaid modality works on demand and it is generally people with low economic resources who take this modality.

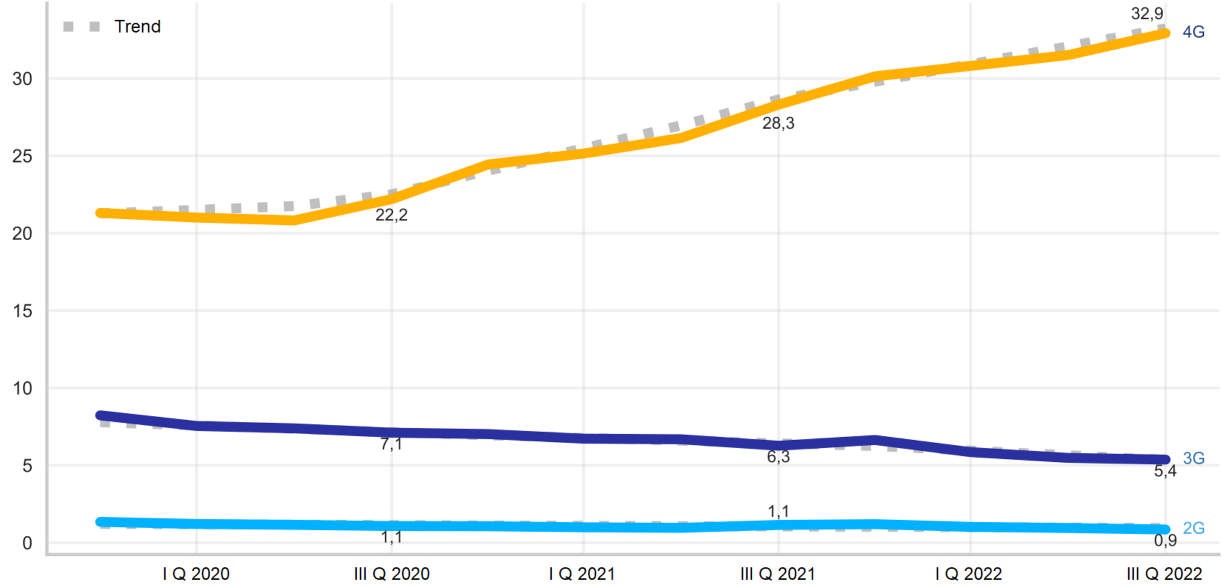


Figure 3. Mobile Internet access by technology [8]

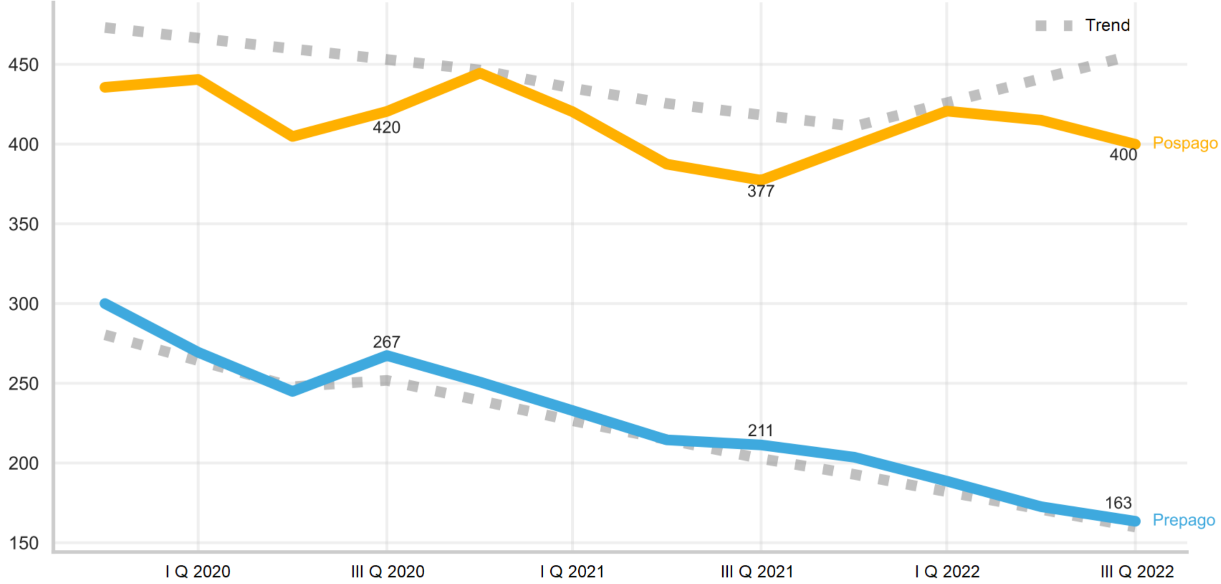


Figure 4. Operating revenues in billions of pesos [8]

III. Concentration Index

The concentration index of a market shows the number of participants and their position in it. In effect, the concentration index will be higher the smaller the number of participants in said market and the more unequal their participations are.

Concentration was measured using three of the most widely used indexes in the global telecommunications market: the Stenbacka dominance index, the Herfindahl-Hirschman index (HHI), and the Linda index. The results obtained with the Linda index are described in this paper.

A. Linda Index

This indicator is usually used to measure the possible existence of oligopoly and inequality between different market shares. Moreover, similar to the concentration ratio, it is calculated for a number n of leading companies in the market so that their joint relative incidence can be calculated about the rest of the participants at that end of the market (supply or demand); mathematically, this indicator can be defined as shown in (1) [9][10].

$$L = \frac{1}{N(N-1)}\sum_{i=1}^{N-1}\frac{\overline{X}_i}{\overline{X}_{N-i}} \quad (1)$$

Where $\bar{X}_i$ is the average market share of the first i firms, and $\bar{X}_{N-i}$ is the average market share of the remaining firms. This indicator presents values between zero and infinity, where values close to zero are obtained for markets with low concentration, and higher values (greater than one) represent highly concentrated markets (see Table I) [9][10].

TABLE I. LINDA'S INDEX INTERPRETATION [9][10]

Concentration	Range
Low	<0,2
Moderade	0.2 a 0.5
High	0.5 a 1
Very High	>1

Low concentration implies high market competitiveness; high concentration implies low competitiveness; and a very high concentration implies the presence of a monopoly or oligopoly.

B. *Stenbacka Dominance Index*

The Stenbacka index is defined as a dominance threshold based on the shares of the two hugest companies in the market. The value of the Stenbacka index estimates a threshold above which the leading firm could have market power; equation (2) calculates this threshold.

$$S^D = \frac{1}{2}[1 - \gamma(S_1^2 - S_2^2)] \quad (2)$$

Where:

S1 and S2 correspond to the market share of the two market largest companies, with 0 ≤ Si ≤ 1.

γ ≥ 0 is a given parameter obtained from the particular characteristics of each market, such as entry barriers and regulations to motivate competition.

C. *Herfindahl-Hirschman Index (IHH)*

The HHI is represented by the sum of the squares of the shares of the companies in the market, as described in equation (3).

$$IHH = \sum_{i=1}^{N} S_i^2 \quad (3)$$

Where:

N is the number of companies in the market.

Si is the market share of the company i in percentage terms.

IV. Methodology

Initially, data corresponding to the analysis variables were obtained, such as traffic, revenue, and accesses, for prepaid and postpaid, corresponding to each telecommunications company that operated in Colombia from 2012 to September 2022 (inclusive). This information was obtained from the post-data database of the Communications Regulation Commission [11]. Subsequently, an organization of the data was performed in Excel to create a database with the information of interest organized chronologically. In the end, nine databases were obtained: (1) fixed charge mobile internet demand traffic (postpaid); (2) fixed charge mobile internet demand revenues (postpaid); (3) fixed charge mobile internet demand accesses (postpaid); (4) on-demand mobile internet demand traffic (prepaid); (5) on-demand mobile internet demand revenues (prepaid); (6) on-demand mobile internet demand accesses (prepaid); (7) global mobile internet demand traffic (postpaid + prepaid); (8) global mobile internet demand revenues (postpaid + prepaid); and (9) global mobile internet demand accesses (postpaid + prepaid).

In a subsequent phase, Linda's index was constructed for each of the nine databases mentioned above. It was decided to calculate this index monthly to obtain more data that would allow a future forecast and projection of the concentration behavior in the Colombian mobile telecommunications market [12]. According to the procedure required to calculate Linda's index, it was necessary that for each period (month), the telecommunications companies were ordered from highest to lowest according to the value of the variable to be analyzed (traffic, revenues, or subscribers).

During the construction of the Linda index, it became evident that when any of the companies had a zero value in the variable of interest, the Linda index was indeterminate, and if it was very close to zero, it increased exponentially. Due to the above, it was decided to eliminate the data equal to zero since the interpretation of these data is fundamental that the company did not operate in that period. Additionally, it was decided to eliminate all data less than 50,000 in the traffic and revenue databases, both in postpaid and prepaid, and overall, since these data produce inconsistent values of the index; the amount of data deleted was 36 in total, which gives approximately a value of less than 0.4% of the total database.

The Linda index determines the level of concentration by groups of companies from 2 to N-1; for example, if there are 3 companies, there is only one Linda, since it compares the group composed of company 1 and 2, against 3. For the months in which more than three companies were operating, more than one Linda index was obtained since this index compares groups of companies. The first Linda obtained is if at least three companies are competing in the market and would correspond to Linda 2 (L2); if there are four companies, L2 and L3 would be obtained, and so on. In other words, the last Linda corresponds to N-2, where N is the number of companies competing in the market. Since there are periods where up to 14 companies operate simultaneously, Linda indexes of up to L12 are obtained, mapping each of them up would mean an extension of this document. Therefore, it was decided to present the L2 Linda index graph for the case of the global revenue (prepaid + postpaid) of each telecommunications company, together with a table showing the rest of the Linda index values for the corresponding scenario.

V. Measuring Concentration In The Mobile Telecommunications Services Market In Colombia

Figure 5 describes the behavior of Linda's index 2 for the case of the overall (prepaid + postpaid) mobile internet revenue of each Colombian telecommunications company from 2012 to 2022. Table II shows the other Linda 2 index values for the corresponding scenario.

According to Figure 5, the first two values of Linda's index are very high compared to the rest, which show an almost uniform trend of low value. The above can be explained by the entry into the market of several telecommunications companies.

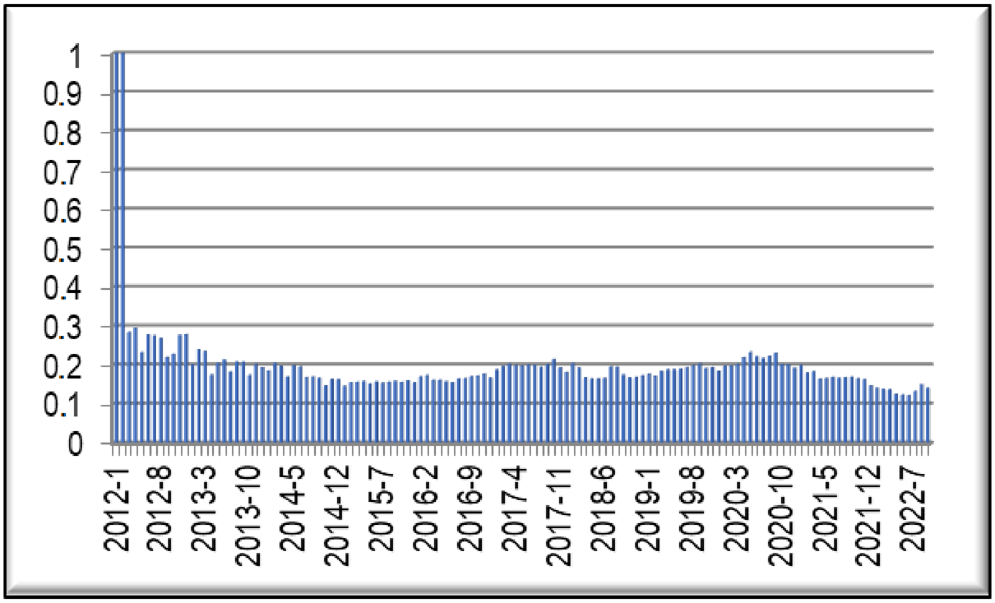


Figure 5. Linda 2 index for the overall mobile internet revenue of Colombian telecommunication companies.

TABLE II. LINDA INDEX FOR THE OVERALL MOBILE INTERNET REVENUE OF COLOMBIAN TELECOMMUNICATION COMPANIES.

Date	Linda Value										
	L2	L3	L4	L5	L6	L7	L8	L9	L10	L11	L12
2012-1	2.24	7.32	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN
2012-2	21.10	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN
2012-3	0.28	8.34	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN
2012-4	0.29	8.42	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN
2012-5	0.23	1.24	3.65	NAN	NAN	NAN	NAN	NAN	NAN	NAN	NAN
…	…	…	…	…	…	…	…	…	…	…	…
2022-1	0.14	0.57	0.86	1.15	1.26	1.80	3.33	136.41	214.11	310.71	NAN
2022-2	0.13	0.56	0.88	1.17	1.30	2.01	3.61	60.93	99.46	220.28	NAN
2022-3	0.13	0.53	0.86	1.15	1.33	2.20	3.37	48.89	83.44	179.01	NAN
2022-4	0.12	0.47	0.91	1.24	1.46	2.42	3.62	27.76	67.01	84.20	182.91
2022-5	0.12	0.46	0.94	1.30	1.65	2.85	4.32	36.35	64.65	137.44	358.08
…	…	…	…	…	…	…	…	…	…	…	…

VI. Results Analysis

The highest value of Linda 2 is given for the global mobile internet demand (postpaid + prepaid) revenue with a value of 21.11 and a standard deviation of 1.85 and for the number of subscribers of the global mobile internet demand (postpaid + prepaid) with a value of 20.72 and a standard deviation of 2.49. On the other hand, the lowest value of Linda is given for global traffic with a value of 0.067 and a standard deviation of 0.0499 and for prepaid traffic with a value of 0.073 and a standard deviation of 0.111.

For postpaid mobile Internet demand (fixed charge), the Linda index values, on average, are between 0.23 and 0.32, so there is a moderate concentration. In the case of prepaid (on-demand) mobile Internet demand, the Linda index values, on average, have differences for the traffic of 0.15, low concentration, revenues of 0.26, moderate concentration, and the number of subscribers of 0.41, moderate concentration. In the overall mobile Internet demand, the Linda index values, on average, have higher differences for traffic 0.14, low concentration, revenue 0.36, moderate concentration, and number of subscribers 0.53, high concentration. However, for the case of global revenue, if the first two periods (2012-1 and 2012-2) are not bearing in mind, the average drops to 0.18, which would give a low concentration.

It is important to emphasize that the Linda 2 index compares the group of the two companies with the highest value of the variable of interest (traffic, revenues, or subscribers) concerning the group of the other companies. In some cases, it is possible to present a higher concentration, evidenced by the group of the 3 or 4 most dominant companies in the market.

VII. Conclusions

The measurement of concentration in the Colombian mobile telecommunications market was carried out using the Linda index using as input variables the income, traffic and mobile internet access of the telecommunications companies operating in Colombia from 2012 to 2022, both for postpaid (fixed charge) and prepaid (on demand).

Linda's values for the global revenue of mobile internet demand evidence a high concentration in the first two months, but then drops low for the rest of the periods, indicating a high competition in this market. In the telecommunications market, the problem of concentration is an issue that usually affects many countries. However, several countries have addressed this problem by increasing the availability of radio spectrum and reallocating portions of it; even beyond this, the spectrum distribution among mobile operators plays a significant role in achieving the goal of a freely competitive market. It has been empirically demonstrated that the accumulation of spectrum by an operator leads to less competition in the mobile voice market, so spectrum management strategies should aim to avoid unnecessary spectrum accumulation, seeking to achieve balance in the market power of telecommunication services.

As future work, it is planned to propose a new concentration measurement index based on the characteristics of the Linda, Stenbacka and Herfindahl-Hirschman indices.

Acknowledgment

The authors would like to thank the Universidad Distrital Francisco Jose de Caldas, Ministerio de Ciencia, Tecnología e Innovación and Comision de Regulacion de las Comunicaciones, for supporting and funding of this project.

References

[1] M. Fiedler, K. De Moor, H. Ravuri, P. Tanneedi, and M. Chandiri, “Users on the move: On relationships between QoE ratings, data volumes and intentions to churn”, in 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), IEEE, 2017, pp. 97-102.

[2] Md. Nekmahmud and S. Rahman, “Measuring the Competitiveness Factors in Telecommunication Markets”, in Competitiveness in Emerging Markets: Market Dynamics in the Age of Disruptive Technologies, D. Khajeheian, M. Friedrichsen, y W. Mödinger, Eds., Cham: Springer International Publishing, 2018, pp. 339-372.

[3] O. S. de Miera Berglind, “Spectrum concentration and market competition. Implications for the use of caps in Mexico”, in 2015 Conference of Telecommunication, Media and Internet Techno-Economics (CTTE), IEEE, 2015, pp. 1-8.

[4] OCDE (2023, jun 12). Informe: Economy Profile of Colombia 2020. [Online]. Available: https://www.doingbusiness.org/content/dam/doingBusiness/country/c/colombia/COL.pdf [retrieved: sep, 2023]

[5] K. Tsilipanos, I. Neokosmidis, and D. Varoutas, “Modeling complex telecom investments: A system of systems approach”, IEEE Transactions on Engineering Management, vol. 62, n.o 4, pp. 631-642, 2015.

[6] A. Mehrotra and S. Menon, “Telecommunication & Networking Changing Customer Profile & Preferences”, in 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), IEEE, 2021, pp. 221-226.

[7] Comisión de Regulación de las Comunicaciones (2023, jun 10). Battery of indicators for the analysis of competition in Communications markets. [Online]. Available: https://postdata.gov.co/story/bateria-de-indicadores-para-el-analisis-de-competencia [retrieved: sep, 2023]

[8] MinTIC (2023, jun 7). Quarterly ICT Bulletin, febrero de 2023. [Online]. Available: https://colombiatic.mintic.gov.co/679/articles-274258_archivo_pdf.pdf [retrieved: sep, 2023]

[9] Comisión de Regulación de las Comunicaciones (2023, jun 11). Postdata: Beyond the data. [Online]. Available: https://postdata.gov.co/ [retrieved: sep, 2023]

[10] J.-P. Lis-Gutiérrez (2023, jun 8). Market concentration and market stability measures: An application for Excel. [Online]. Available: https://doi.org/10.2139/ssrn.2279769 [retrieved: sep, 2023]

[11] Comisión de Regulación de las Comunicaciones (2023, jun 9). CRC Regulatory Agenda 2021 – 2022. [Online]. Available:https://www.crcom.gov.co/sites/default/files/agenda/201229_ar_2021-22_vpub_0.pdf [retrieved: sep, 2023]

[12] Z. Berradi, M. Lazaar, O. Mahboub, and H. Omara, “A Comprehensive Review of Artificial Intelligence Techniques in Financial Market”, in 2020 6th IEEE Congress on Information Science and Technology (CiSt), IEEE, 2021, pp. 367-371.

Feasibility Verification of Access Control System for Telecommuting by Users Reliability Calculation

Atsushi Shinoda
Graduate School of Informatics
Nagoya University
Nagoya, Japan
email: shinoda@net.itc.nagoya-u.ac.jp

Hirokazu Hasegawa
Center for Strategic Cyber Resilience R&D
National Institute of Informatics
Tokyo, Japan
email: hasegawa@nii.ac.jp

Hajime Shimada
Information Technology Center
Nagoya University
Nagoya, Japan
email: shimada@itc.nagoya-u.ac.jp

Yukiko Yamaguchi
Information Technology Center
Nagoya University
Nagoya, Japan
email: yamaguchi@itc.nagoya-u.ac.jp

Hiroki Takakura
Center for Strategic Cyber Resilience R&D
National Institute of Informatics
Tokyo, Japan
email: takakura@nii.ac.jp

***Abstract*—Nowadays, telecommuting, in which users connect to a corporate network from remote locations, such as their homes, is increasing as a measure to prevent COVID-19 spread. However, telecommuting exposes companies to information security risks by allowing users to connect terminals from their home that is out of control. Further security enhancements are required for ensuring secure telecommuting, but they easily cause trade-off issues between security and business efficiency that the administrators have to solve. As a solution to this problem, we have proposed an access control system to minimize the loss of business efficiency while enhancing security. The system calculates the reliability of each connected user and implements network access control. This access control allows connection to many resources for business efficiency if the user's reliability is high, and minimizes the number of resources available for reducing risks if the user's reliability is low. This paper confirmed the feasibility of implementing the system to calculate reliability from realistic indicators and perform network access control using pseudo-corporate network.**

***Index Terms*—Access Control, ACL, SDN, Network Latency, Telecommuting, User Reliability**

I. Introduction

Nowadays, telecommuting, in which users connect to a corporate network from remote locations, such as their homes, is increasing as a measure to prevent COVID-19 spread and due to a development of information technology. It increases the number of work style options and increases business efficiency. However, for corporate networks, remote networks and terminals that are difficult to control by corporate administrators become a risk because their security is not guaranteed compared to terminals at the intranet. There is a need to enhance the security of corporate networks for telecommuting communications, but security enhancement measures often decrease business efficiency.

Therefore, we have proposed a solution to this problem: an access control system that enhances security but does not decrease business efficiency as much as possible [1] [2]. The proposed system calculates the reliability of each Virtual Private Network (VPN) connected user and determines which resources the user can connect to based on the importance of the resources. However, in the previous research, we have only proposed the mechanism of this system and verified the access control based on the pre-defined reliability indicators. We have not verified the feasibility of implementing the system that calculates reliability based on realistic indicators and its access control.

In this paper, we implemented the proposed system and verified how the implementation would affect the corporate network and remote connections. The results of the network latency evaluation in the intranet data transfer process during the remote connection confirmed that the intranet communication was not affected. In addition, the results of the experience degradation evaluation of the remote connection users showed that all connections to the corporate network were less than 1.0 second. However, connections to resources varied from 3.2 seconds at low load to 26.6 seconds with simultaneous remote connections and high load on the intranet.

The rest of this paper is organized as follows: Section II describes related work, Section III outlines the proposed system, Section IV describes the implementation, Section V describes the verification experiments, and Section VI provides a conclusion and future work.

II. Related Work

By registering Access Control List (ACL) in network equipment, such as routers, network access control can be implemented and corporate network can be more secure. Smetters et al. have conducted an extensive and long-term research on how access control with ACL can enhance security [3].

There is also research on using Software Defined Networking (SDN) to dynamically generate ACL to further enhance security [4]. While this research is only for the targeting of IoT devices, SDN is used as an IDS for network access control. We have to make high frequency ACL changes for dynamic access control in the proposed system. Therefore, we also use SDN as one of the easier ways to implement it. However, it can be assumed that ACL is normally configured on the network equipment, and management methods also exist. Liu et al. proposed ACL management method using optimization algorithm, it can make management easier by reducing redundancy, but it is not suitable for rapid ACL changes [5].

Dynamic control with SDN is expected to affect greater load on the network, so the impact on the network should be considered. There have been several research on the impact of SDN control in networks. Iqbal et al. proposed an analytical model for the end-to-end communication latency caused by centralized control using SDN, based on experimental measurements in a virtual environment and testbeds across the US and nine countries [6]. Llopis et al. proposed minimizing critical communication, such as remote surgery, latency reduction method in IoT communications by routing and redirecting to the shortest path using SDN [7]. This two research focus mainly on routing using SDN, whereas proposed system in this paper differs by focusing on network access control. Due to the fact that very few research have used SDN for network access control and measured speed, this paper cannot set a value as a baseline.

The proposed system in this paper uses user reliability to enhance security. For a concept similar to the user reliability, there are two research about scaling the self-report measure of user's security intentions [8] or attitudes [9]. As self-reported data is not accurate and dynamic, proposed system in this paper uses numerical data that can be obtained by automatically as a reliability indicator to calculate user reliability. In addition, there is research about investigation on Chief Information Security Officers' (CISO) awareness of Human-Centered security in corporation. Hielscher et al. indicate that many CISOs may not have enough knowledge about the latest academic Human-Centered security [10]. The system proposed in this paper to automatically determine the user reliability will be more required in the situation where the administrators (such as CISOs) do not have enough knowledge. Research also exist that focus on user's security awareness. While this paper discusses a method to measure user's security awareness, Masssoth et al. proposed learning method that uses AI to improve user's security knowledge and awareness [11].

III. Access Control System Using User Reliability

We explain about details of proposed system and user reliability calculation.

A. Overview of the Proposed System

It is difficult for companies to manage the networks and terminals which connected from outside of the companies. It is a risk to the corporate network because telecommuting communications can become a bridgehead. Therefore, it will be necessary to enhance security (e.g., strictly access control), but this is likely to sacrifice business efficiency. There is a need for a method that balances business efficiency and enhanced security.

Thus, we have proposed an access control system that aims to enhance security while minimizing the loss of business efficiency [1] [2]. This proposed system calculates the reliability of users who connect to the corporate network from outside for telecommuting and determines the user's accessible resources. The user's reliability is calculated based on an index that indicates the user's security awareness, and the importance of each resource is used to determine which resources to allow the user to connect to.

Users with high reliability are granted access to a wide range of resources. In contrast, users with low reliability are granted access to the minimum necessary resources. Furthermore, proposed system has a function that allows users to apply for access permission in case a user with low reliability needs to access a resource to which he/she has been denied access. If approved by the administrators, the user can connect to the resource temporarily for a certain period of time. It also has a dynamic access control function that periodically recalculates reliability to flexibly cope with time-changing network conditions.

B. User Reliability Indicators

The calculation of user reliability is based on indicators of user's awareness of security enhancement. Useable indicators for user reliability calculation are listed below.

- Security Training
  This reliability indicator can have two values, the progress rate of security training courses and test result scores during security training course.
- Incidents History
  This is the number of incidents that the user has caused in the past, such as being the target of a cyber attack that resulted in an information leakage.
- Security Surprise Test
  This is a result of unannounced surprised tests, such as a pseudo malicious e-mail that includes web beacon URL or attachment file includes beacon. If the user opens URL or attachment file, the score becomes bad. In addition, whether the user reported such risky behavior to the administrators comes to be another reliability indicator.
- Result of URL Filtering Detection
  This reliability indicator is the number of a user's attempts to follow malicious or suspicious URLs detected and prevented by the corporate Firewall or Unified Threat Management (UTM).
- Other Reliability Indicators
  Depending on the network environment, there are many other possible indicators, e.g., 'Windows security logs', 'Whether security updates are applied to installed programs', 'Number of spam e-mails received by users', and 'IP address of the telecommuting user's remote network'.

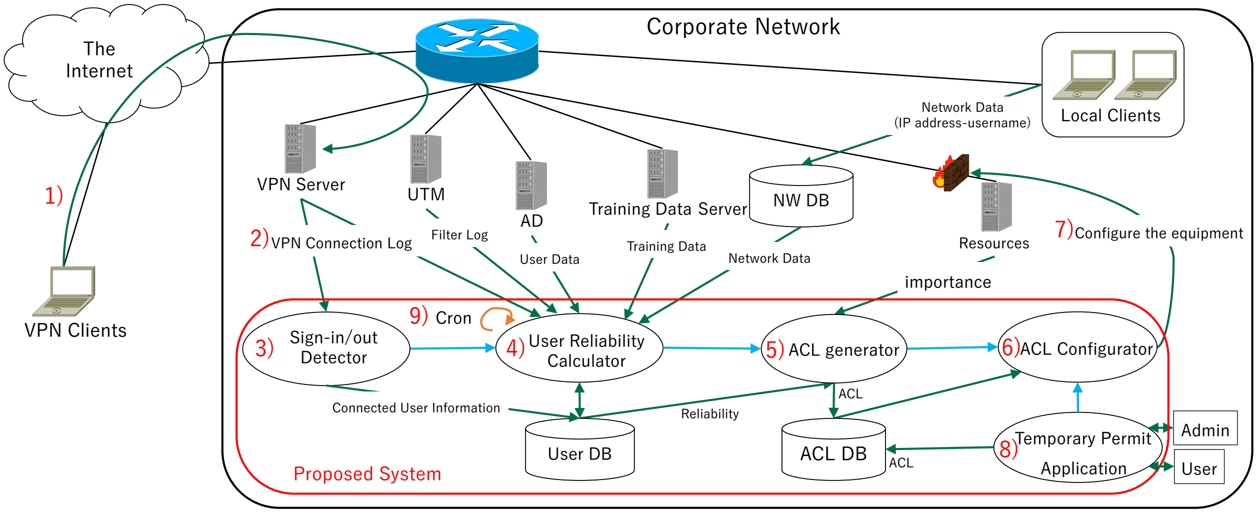


Fig. 1: Architecture of the Proposed System.

C. Calculation of User Reliability

The procedure of the reliability calculation based on each reliability indicator is shown as follows. First, for each reliability indicator, the data is standardized for all users, so that the value becomes relative and can be calculated by addition. Then, the reliability is calculated by adjusting a parameter to set the weight of each standardized reliability indicator. Parameter adjustment can be determined using statistical approaches, such as machine learning, or by dividing reliability indicators into some categories to reduce the number of parameters. Thus, administrator's effort for parameter adjustment may be reduced.

D. Generation of ACL

The proposed system determines the communication permission between the user's terminal and the server storing the important resources. We assume the importance of a resource can be determined by setting the level in advance by administrator or creator (such as setting level of confidentiality), or by using resource importance estimation methods, such as our previous research [12].

For the generation of ACL using network access control, it is necessary to determine the relationship between user reliability, resource importance, and stabilization constant(=threshold). As an example, Formula (1) is access control condition that grants permission to connect.

$$Reliability - Importance > StabilizationConstant \quad (1)$$

The stabilization constant is adjustable as a parameter and can be changed depending on company's security situation. For example, if threat intelligence indicates possible threat detection, such as the company is being targeted, or if a temporary increase of malicious communications to honeypots, or an increase of the number of malicious e-mails, we can increase the stabilization constant to make the company more secure. In contrast, if the situation subsides, the stabilization constant can be decreased to allow access to a wider range of areas to improve business efficiency. Also, by dividing the stabilizing constants by department, the number of parameters to be adjusted will increase, but it will be possible to create ACL that better fit the information being handled.

E. Architecture of the Proposed System

Fig. 1 shows the architecture of the proposed system and the corporate network assumed to apply the system. The description of each function in the processing procedure is as follows.

1) A VPN connection is made to the corporate network from a remote location for telecommuting.
2) The VPN server outputs the connection information such as the assigned IP address and username as a log to the proposed system at the time of connection.
3) Sign-in/out Detector detects the start/exit of the user's VPN connection from the received log and stores the connected user information including VPN connection ID, username, and assign IP address to the User Database (DB).
4) The User Reliability Calculator obtains several kinds of data from Active Directory (AD) and other servers and calculates the user's reliability based on the data. The calculated reliability is sent to the User DB.
5) ACL Generator generates ACL based on user's reliability and resource importance, and stores them in the ACL DB.
6) ACL Configurator receives the ACL stored in the ACL DB and passes them to network equipment.
7) Network equipment implements network access control based on the ACL.
8) The application for temporary permission also generates ACL based on the application and approval, and activates the ACL Configurator.
9) In addition, in order to flexibly cope with time-changing conditions, the ACL Generator is periodically invoked

TABLE I: Details About Network Elements.

Function	Element	Details
Router	Router and VPN Server	NEC IX2310
AD	OS	Windows Server 2019
Proposed System	OS	Rocky Linux 8.8
	SDN Protocol	OpenFlow 1.3
	SDN Controller	Ryu 4.3.4
	Programing	Python 3.6.8
	DB	SQLite 3.26.0
	Log Server	Rsyslog
SDN Switch	OS	Ubuntu 22.10
	SDN Switch	Open vSwitch 3.0.0
Resource Server	Host Machine OS	Windows 10 Professional
	Guest Machine OS	Rocky Linux 8.6
	File Sharing Protocol	SMB
Local Clients	OS	Windows 10 Professional
VPN Clients	OS	Windows 10 Professional
NW Info Server	OS	Rocky Linux 8.6
	File Sharing Protocol	SMB

to review the user's reliability and dynamically perform access control.

IV. Proposed System Implementation

We implemented the access control system described in Section III into a pseudo-corporate network and verified it.

Fig. 2 shows the organization of the pseudo-corporate network in which the proposed system is implemented. Table I shows the detail breakdowns of elements in Fig. 2. In this implementation, unless otherwise noted, all processing is done by programs written in Python.

In this implementation, it is assumed that the network configuration information server (NW Info Server) combines several server functions, such as NW DB and Security Training Server. Therefore, NW Info Server also keeps information related combined functions such as some reliability indicators, client IP address and username correspondence table, and resource importance information. It is also assumed that one server was considered one resource.

The elements shown in Fig. 1 of the proposed system in this implementation are listed below.

A. Sign-in/out Detector

The VPN Server sends the logs using Syslog, and Rsyslog in the Sign-in/out Detector receives them. When received the log, Sign-in/out Detector is activated and extracts connection information (VPN connection number, VPN client's assigned IP addresses and username) from the log, and stores it in the User DB.

B. User Reliability Calculator

Indicators which we implemented for user reliability and their obtaining methods are shown below.

- Progress Rate of Security Training Courses, Test Result Scores During Security Training Course: These are stored in the NW Info Server as an Excel file, and User Reliability Calculator obtains it by Server Message Block Protocol (SMB).
- Incident History: It is associated with each user's information in AD, and User Reliability Calculator obtains it by LDAP.
- Result and Response of Security Surprise Test: These are stored in the NW info server as an Excel file, and User Reliability Calculator obtains it by SMB.
- Result of URL Filtering Detection: URL filtering is implemented by the Router function, and the log of IP address is obtained by Rsyslog. The table of correspondence between IP addresses and username of local clients is placed in the NW Info Server as an Excel file, and User Reliability Calculator obtains it by SMB.

We classified into the following categories. Some indicators classified into multiple categories.

- User Carelessness: Result of Security Surprise Test, Result of URL Filtering Detection, Incident History
- User Awareness of Efforts to Secure: Progress Rate of Security Training Courses, Response of Security Surprise Test
- User Skill Level: Test Result Scores During Security Training Course, Result of Security Surprise Test

The User Reliability Calculator obtains each reliability indicator for all users, standardizes them, and calculates user's reliability. User u's reliability $R(u)$ is as follows (2).

$$R(u) = \frac{1}{|\mathbb{C}|} \sum_{c \in \mathbb{C}} \frac{1}{|c|} \sum_{i \in c} (-1)^{K_i} \times v_i(u) \tag{2}$$

Here,
$\mathbb{C}$: set of categories,
c: category, set of indicators,
i: indicator,
K_i: attribute determined by indicator i,
$v_i(u)$: user u's reliability value of indicator i.

For indicators where higher values indicate less user reliable, '-1' is multiplied in the calculation. Therefore, K_i becomes 0 in case of indicators about 'Progress Rate of Security Training Courses', 'Test Result Scores During Security Training Course', 'Response of Security Surprise Test'. In contrast, K_i becomes 1 in case of indicators about 'Incident History', 'Result of Security Surprise Test', 'Result of URL Filtering Detection'.

Note that if a large number of VPN is connected at the same time, the User Reliability Calculator and ACL Generator will be started again for each connection, which spend large times. Therefore, after the Sign-in/out Detector detects a connection and stores it in the User DB, if more VPN connections are connected, the ACL Generator is not activating in the middle of the process, but only once at the end. The periodic execution is defined by Cron and is executed every minute.

C. ACL Generator

This function generates ACL for each connected VPN user to access resources. The intranet utilizes default deny policy so that we have to set allow ACL to access resources. A permission rule is generated based on the generation condition

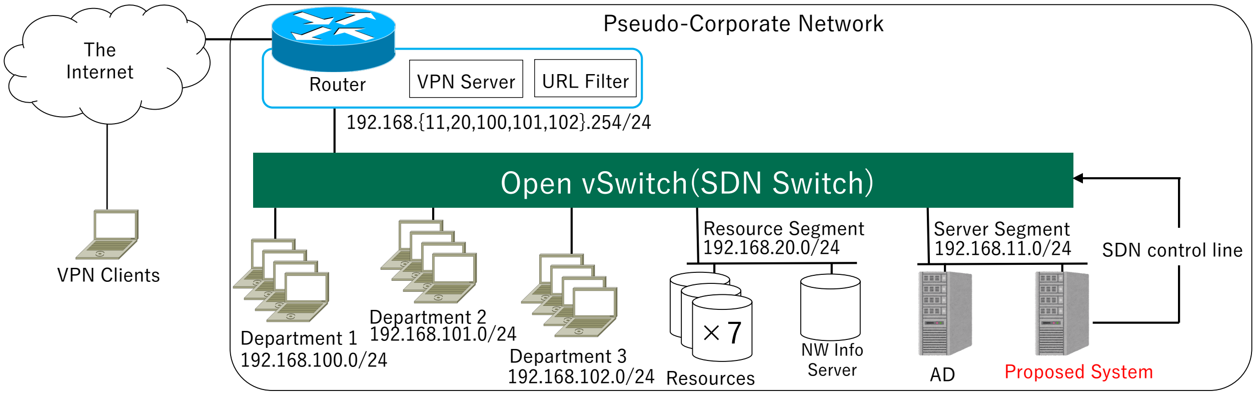


Fig. 2: Experimental Network.

Formula (1). In this implementation, Stabilization Constant value is '0'. The information of resources importance is already specified individually for each resource server, and is placed in the NW Info Server as an Excel file, which is obtained by ACL Generator via SMB.

D. ACL Configurator

The ACL Configurator obtains ACL to be configured from the ACL DB. The ACL Configurator implements Ryu [13] as an SDN (Protocol: OpenFlow) controller and configures the received ACL to the SDN switch by the firewall function of Ryu. In this implementation, access control from the local client to the resource server is performed by SDN, but the ACL are prepared in advance, so they are not affected even if the ACL are updated by a VPN connection.

V. Feasibility Verification Experiment

The proposed system enhances the security of corporate network by providing access control based on the user reliability for telecommuting. However, it is not desirable that the introduction of this system affects connection to and use of the corporate network. Therefore, experiments were conducted on the availability when a large number of remote users are connected to corporate network at the same time or when the corporate network is busy.

A. Overview of the Experiment

We measured the time required for a VPN connection and the time until the resource can be accessed (SMB connection) in the experimental environment. Since the ACL generated change with each additional connection, multiple VPN connections are measured. There are two possible patterns for these multiple connections:

- **Sequential** connections: the number of VPN-connected clients is increased one by one.
- **Simultaneous** connections: all VPN-connected clients are connected at the same time.

In addition, since the load on the SDN and resource server may vary depending on whether the local client is communicating, measurements will be taken for two patterns:

- **None**: no communication from the local client to the resource server.
- **Heavy**: an extremely large amount of communications are transported from the local client to the resource server.

The measurement on the VPN Clients is controlled by PowerShell Remoting and using Measure-Command. The load **Heavy** means sending large PING packets (51.6KB) every 1 second by 5 local clients to resource servers and receiving 600MB file via SMB by 7 clients from resource servers.

For each reliability indicator, the data was generated by random number generation after adjusting the generation range so that the ratio of high:medium:low reliable users is 2:6:2. All measurements were taken three times, and the values in the table are averages of the three.

B. Results of the Feasibility Verification Experiment

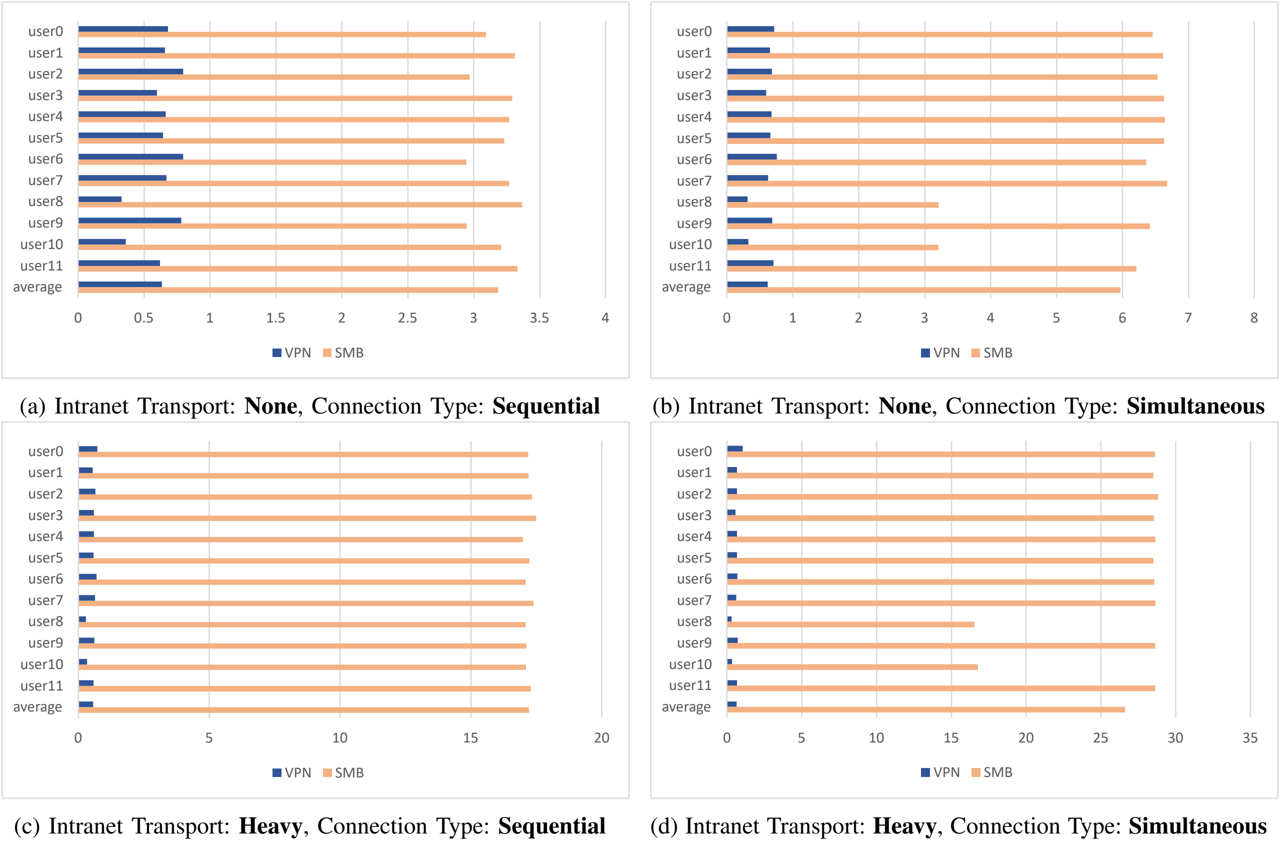
Measured VPN connection times and SMB connection times are shown in Fig. 3.

In the pattern of Transport: **Heavy**, Connection Type: **Simultaneous**, the SMB can not connect to because of too long waiting time, so trying to SMB connection is waiting until PING can be accepted (Note: the measured time at the pattern (**Heavy**, **Simultaneous**) in the Fig. 3d is the sum of the PING waiting time and SMB connection time).

C. Consideration

As shown in Fig. 3, the reason why there was no significant difference in the VPN connection was because the system's reliability calculation process was not started up yet.

The difference in SMB time for the **Sequential** was no more than 1 second, and the SMB connection time did not depend on the number of clients. In the **Simultaneous**, some clients (ID: user8, user10) took the same amount of time as in the **Sequential**, but other clients took twice as long. This was due to the processing of simultaneous VPN connections. Even though PowerShell was used to initiate the batch connection, there was slight difference between user8, user10 and other users. Based on such difference, the proposed system divided the connection into two sets. In fact, during the experiment, two VPN connections succeeded → ACL generator started →



(a) Intranet Transport: **None**, Connection Type: **Sequential**

(b) Intranet Transport: **None**, Connection Type: **Simultaneous**

(c) Intranet Transport: **Heavy**, Connection Type: **Sequential**

(d) Intranet Transport: **Heavy**, Connection Type: **Simultaneous**

Fig. 3: Results of VPN/SMB Connection Waiting Time(second).

other VPN connections succeeded → ACL generator started, and so on.

When the network was under **heavy** load, it took some time for both the **Sequential** and **Simultaneous** to become available. This is because the ACL generator takes more than 10 seconds.

The time command was used to measure the execution time of each function of the proposed system under each situation, and the results are shown in Table II. *get_file process* is a function that User Reliability Calculator obtains a file from the NW Info Server, and it is used about 4 times. *acl_config process* is a function for the ACL Configurator to reflect the ACL database to the SDN switch. *all processes* is a series of processes performed by the User Reliability Calculator, ACL Generator, and ACL Configurator.

From the above, it can be assumed that the waiting time of **Sequential** under **heavy** load is due to *get_file process* being performed about 4 times, and the waiting time of **Simultaneous** is due to it being performed twice as many times by many clients. To solve this problem, it is necessary to shorten the access to some reliability indicators, so the value of the indicators should be calculated in advance and the process of passing it to the system side should be asynchronous, with high frequency.

Just in case, we checked the effect on the local client's communication using **heavy** load for pseudo-corporate network, but there was almost no change in the time taken for communication in both the **Sequential** and **Simultaneous**.

TABLE II: Execution Time for Each Function(second).

Intranet Transport	None		Heavy	
VPN connection clients	0	12	0	12
get_file process	1.361	1.348	3.649	3.641
acl_config process	0.376	0.666	0.380	0.738
all processes	2.248	2.666	11.419	11.715

Impacts of the proposed system is limited because it is only applied immediately after the VPN connection is established. In this experiment, the network is under **heavy** load, which means that some of the bandwidth is overflowing, but it is difficult to imagine a network that is always in this state. However, if SMB communication is performed immediately after the VPN connection is established in a **Simultaneous**, sometimes an error raise and a delay is caused.

VI. Conclusion and Future Work

In this paper, we implemented access control system based on user reliability in the pseudo-corporate network environment. The verification using the network confirmed the feasibility of the proposed method. The proposed system focuses on the user's security awareness and the risk to the corporate network. The purpose of the proposed system is to balance security enhancement and business efficiency as much as possible, which easily cause trade-off issues in network access control.

The system was implemented on a pseudo-corporate network, and in the feasibility verification, waiting time for VPN connections and SMB connections were measured. The impact of the proposed system on VPN connections and the corporate network was limited. The impact of multiple connections was also limited if they were small scale. However, it was confirmed that if the network was under an abnormal load, the waiting time can not be ignored due to the time spent during the reliability calculation and ACL generation.

In future works, the exact validation of user reliability calculation has not been carried out in this paper. In addition, the reliability indicators should be based on as many indicators as possible so that the reliability can be calculated accurately. Furthermore, in order to be simplify and optimize the adjustment of parameters in calculating reliability, the proposed system should introduce a function that uses received feedback and automatically adjusts the parameters. With regard to the proposed system feasibility, the algorithm or system configuration should be reviewed to cope with the situation where significant waiting times were identified in the experiment.

Acknowledgment

This work was partially supported by JSPS KAKENHI Grant Numbers JP19K20268, JP23H03396, JP19K11961.

References

[1] H. Hasegawa and H. Takakura, “A dynamic access control system based on situations of users,” 7th International Conference on Information Systems Security and Privacy, pp. 653-660, 2021.

[2] A. Shinoda, H. Hasegawa, Y. Yamaguchi, H. Shimada, and H. Takakura, “Feasibility verification on impact of frequently access control update based on user reliability,” 9th International Conference on Information Systems Security and Privacy, Abstracts Track, 2023.

[3] D. K. Smetters, N. Good, “How users use access control,” 5th Symposium on Usable Privacy and Security, pp. 1-12, 2009.

[4] A. Hamza, H. H. Gharakheili, and V. Sivaraman, “Combining MUD policies with SDN for IoT intrusion detection,” 2018 Workshop on IoT Security and Privacy, pp. 1-7, 2018.

[5] A. X. Liu, E. Torng, and C. R. Meiners, “Compressing network access control lists,” IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 12, pp. 1969-1977, 2011.

[6] A. Iqbal, U. Javed, S. Saleh, J. Kim, J. S. Alowibdi, and M. U. Ilyas, “Analytical modeling of end-to-end delay in openflow based networks,” IEEE Access, vol. 5, pp. 6859-6871, 2017.

[7] J. M. Llopis, J. Pieczerak, and T. Janaszka, “Minimizing latency of critical traffic through SDN,” 2016 IEEE International Conference on Networking, Architecture and Storage, pp. 1-6, 2016.

[8] S. Egelman, M. Harbach, E. Peer, “Behavior ever follows intention?: a validation of the security behavior intentions scale (SeBIS),” 2016 CHI Conference on Human Factors in Computing Systems, pp. 5257-5261, 2016.

[9] C. Faklaris, L. Dabbish, and J. I. Hong, “A self-report measure of end-user security attitudes (SA-6),” 15th Symposium on Usable Privacy and Security, pp. 61-77, 2019.

[10] J. Hielscher, U. Menges, S. Parkin, A. Kluge and M. Angela Sasse, “Employees Who Don’t Accept the Time Security Takes Are Not Aware Enough: The CISO View of Human-Centred Security,” 32nd USENIX Security Symposium, pp. 2311-2328, 2023.

[11] M. Masssoth, “Next Generation Artificial Intelligence-Based Learning Platform for Personalized Cybersecurity and IT Awareness Training: A Conceptual Study,” The Seventeenth International Conference on Sensor Technologies and Applications, pp 32-37,2023.

[12] Y. Zhou, H. Hasegawa, and H. Takakura, “A resource importance estimation method based on proximity of hierarchical position,” 5th International Conference on Information Science and Systems, pp. 83-89, 2022.

[13] RYU project team, “Ryubook 1.0 documentation,” 2014. https://osrg.github.io/ryu-book/en/html/index.html [retrieved: Oct, 2023]