2024 IEEE | DOI: 10.1109/QCE60285.2024.00203
uting and Engineering (QCE) | 979-8-3315-4137-8/24/$31.00 ©2024

Jyoti Faujdar[1,3], Muhammad Asad Ullah[2], Mbarka Soualhia[1] and Anne Broadbent[3]
[1]Ericsson Research, Montréal, Quebéc, Canada
[2]Ericsson Research, Stockholm, Sweden
[3]Department of Mathematics and Statistics, University of Ottawa, Ontario, Canada
{jyoti.faujdar, muhammad.asad.ullah, mbarka.soualhia}@ericsson.com
{jfaujdar, abroadbe}@uottawa.ca

***Abstract*—Within the evolving landscape of confidential and trustworthy computing, this paper delves into the prevalent challenges such as secrecy or privacy associated with existing addressing schemes. Taking these issues into consideration, we propose a novel solution, drawing inspiration from distributed quantum computing algorithms, to generate a secret addressing scheme. The objective is to enhance the confidentiality and reliability of computing systems. This proposed solution, inspired from quantum phase estimation (QPE), assigns a unique and confidential address to each node in a network. It also dynamically adapts to changes in the network or system configurations by using the proposed QPE-inspired approach for every new incoming node in the network. We have implemented our solution on a quantum network simulator, namely NetSquid, to assess the effectiveness of our proposed solution under varying conditions, including scenarios with and without noise models. The simulation results of our proposed solution demonstrate both scalability (*e.g.,* it takes $34.5ns$ to address a single computing node with a 3-bit address and $230ns$ with up to 20-bit addresses) and accuracy (*e.g.,* success probability of intended address distribution without noises is 100% and with mild noises it is roughly 80%). Our proposed solution effectively handles the growth of the network while ensuring a consistently high level of accuracy.**

***Index Terms*—secret addressing, distributed quantum computing, confidential and trustworthy computing.**

I. INTRODUCTION

In the rapidly advancing landscape of 5G and beyond technologies, guaranteeing the security, privacy, and reliability of computing systems and data has become paramount. The 5G and beyond computing systems can be relied upon with confidence.

Despite the revolutionary influence of confidential and trustworthy computing, implementing it in 5G and beyond telecommunication networks remains a challenging task. The intricate nature of these networks poses distinct challenges in ensuring the confidentiality and trustworthiness of computing processes. A crucial factor for attaining confidential and trustworthy computing in 5G and beyond telecommunication networks is the development of secure and dependable addressing schemes. These schemes serve as a foundational element, playing a critical role in enhancing the overall security and confidentiality of the network. Therefore, formulating and implementing effective addressing schemes in 5G and beyond telecommunication networks are vital steps in creating a computing environment characterized by confidentiality and trustworthiness.

The existing addressing schemes in a distributed network setup are designed to ensure the uniqueness of assigned addresses. For instance, certain decentralized addressing schemes [5], [6] involve a newly joined node self-assigning an address, utilizing a duplicate address detection procedure to confirm its uniqueness. If the assigned address is not unique, i.e., a repeated one, the node selects another address and repeats the procedure until it finds a new address. In this addressing scheme, all nodes collectively reach an agreement to assign an address to a new node. On the other hand, in neighbor-