Chapter 20
New Trends of Edge Computing Techniques for Trusting Analysis of Networks

Samaher Al-Janabi
https://orcid.org/0000-0003-2811-1493
Babylon University, Iraq

ABSTRACT

Specification, design, and development principles of the future internet are enmeshed in the communication system. This term encompasses the emergence of future large multi-dimensional high-speed heterogeneous and interconnected networked ICT infrastructures to facilitate new groundbreaking trends like the internet of things (IoT) together with the communication system. In this research, an analysis of NdR structures has been carried out, and a comparison to chordal rings of 4th degree made. It was found that there do not exist optimal NdR structures with the number of nodes in one ring greater than 5. It was discovered that there is a close correlation between NdR structures and 4th-degree chordal rings that make it possible to choose NdR structure with the minimum diameter and average path length based on the analysis of correlated chordal ring graphs. It simplifies and shortens the process of choosing the best length of the inner ring chord.

INTRODUCTION

One of the critical problems in designing communication systems is in choosing the topology of the internal communication network as it has a major impact on the efficiency, speed, reliability and cost of the entire system (Al-Janabi & Salman, 2021). Nowadays, the analysis of normal network structures is one of the most important issues in communications and computer science.

These networks can be modeled by symmetric digraphs, i.e., a directed graph G with vertex set V(G) and edge set E(G), such that, if [vi, vj] is in E(G), then [vj, vi] is also in E(G). So any edge of a digraph connecting vertices vi and vj can be replaced by two directed edges [vi, vj] and [vj, vi] (Monther & Tawalbeh, 2020).

DOI: 10.4018/978-1-6684-6697-1.ch020

The best service and reliability parameters can be obtained by forming complete networks (described by a complete graph), but due to cost and practical implementation issues only small networks can be built in this way. In (Gemalto, 2020) a survey of known topologies has been presented. Among the analyzed topologies that would be used in designing the distributed structures, the authors of this article have chosen rings as they are simple, extensible and widely used today. They are characterized by connectivity equal to 2, implying survivability in case of damage of one edge or node. They are inexpensive (number of edges is equal to the number of nodes), regular and symmetric, but possess poor transmission parameters.

Halfway between the complete graph and the ring is the chordal ring structure (Tawalbeh et al., 2020). It is a ring with additional chords, and can be defined by the pair (p,Q), where p is the number of nodes in the ring and Q is the set of chords. Each chord connects every pair of nodes at a distance qi within the ring. The application of this type of structure is useful due to its simplicity, regularity, resistance to damages, simplicity of routing, and good extension possibilities (Gemalto, 2020).

We have divided the objectives into groups, being these groups aligned with the structure. In the following, we briefly explain each of the different groups and detail the specific objectives inside them. The first group of objectives is the one that maps with WP1, that is, the objectives related to the study of the IoT and cloud computing scenarios, from where we will proceed with the analysis and specification of the safety measure security requirements, followed by specification and design of the security framework.

- ***Identification, analysis, and specification of the security requirements for IoT and cloud computing scenarios.*** We will initially study the general features that distinguish IoT scenarios, paying particular attention to those allies specified in the area of Security. Subsequently, we will study the impact that requirements of IoT scenarios might have upon the specification of current safety measures services as well as the need for new ones to be developed. We will provide an analysis of the challenges posed by the IoT environment in the context of cloud computing and the hosting of big data, based on both real-world and envisioned scenarios, and investigate the need for new safety measures services that IoT environments might call for. The result of this research is intended to provide the basis for the technical work in SIoTCP, including the design of the basic and advanced services, and the definition and validation of the SIoTCP Platform.
- ***Specify Safety Measures Secure Framework***. This goal envisions the creation and specification of a flexible and configurable framework wherein the safety measures services developed in SIoTCP can be integrated. The framework is intended to be the paramount pillar to serve as the foundation for the creation of the safety measures services platform and should be able to support different layer models such a TCP/IP and cross-layer. It should be flexible enough to allow for the integration and configuration of diverse safety measures and extend them as required. Desired properties are therefore modularity and composability, facilitating thus the integration of novel safety measures services in the future. The second group of objectives is aligned with WP2. The objectives we include here are those related not only to the development of basic safety measures services but also to the development of services that could be labeled as "low level", in the sense that our services strongly related to networking and communications issues, namely: secure network-level communication, intrusion detection, and balance between QoS and different levels of security protection. Hence, the list of objectives for this group is the following:
- ***Specify Basic Safety Measures Services***. No basic or complex service can be designed unless the underlying cryptographic primitives run successfully in the constrained device. Hence, we will