CHAPTER 8

SUMMARY OF FINDINGS AND FUTURE SCOPES FOR FURTHER RESEARCH

Chapter 8

Summary of Findings and Future Scopes for further research

8.1. Introduction

In this section, we present the conclusion of the thesis. Future research direction of this thesis is given in the subsequent section.

During the course of this research, we have done a thorough study of various methods of clock synchronization used in the distributed networks. One of the most challenging aspects of clock synchronization is making it fault tolerant even in the presence of malicious clocks. The malicious clocks can disturb the synchrony of the clocks in the network if they are one third or more of the total clocks in number. Based on our study and analysis of the clock synchronization problem, we have developed two novel clock synchronization methods. These algorithms are named WASA and AWASA. These algorithms are developed using mathematical tools to optimize. It is also ensured that the algorithms are fault tolerant, which synchronizes clocks even in presence of faulty clocks including the malicious clocks. The first algorithm gives improved precision as compared to some of the previously proposed methods. The WASA guarantees clock synchronization in presence of malicious clocks if the upper bound of malicious nodes is just under one-third of the network size. An improvement of 33% in precision is achieved in the worst-case scenario as compared to [Pfluegl and D. M. Blough , 1995]. Even though the worst-case scenario occurrence is very less but our study provides meaningful analytical insight. This analysis may have application in the high integrity systems especially in safety critical systems.

The second algorithm AWASA offers clock synchronization with better accuracy and precision. The algorithm is suitable for fully connected network. AWASA achieve at least 33% tighter accuracy and precision in the worst-case scenario. Even the worst-case scenario occurrence is very less but our study provides meaningful analytically insight. AWASA guarantees clock synchronization in presence of mischievous clocks if the upper bound of mischievous nodes is just under one-third of the network size. Using this algorithm, we are able to achieve highly accurate and precise synchronization when there is presence of GPS/GLONASS/IRNSS etc clock value. The algorithm also works in absence of such trusted

clock values as well. However, since a reference clock value is not present, the algorithm will give highly precise synchronization value only. In our current work, we provide the analysis for static network. In future work we will try to achieve synchronization for a dynamic connected network.

We have carried out details simulation of both the algorithms and as the algorithms are mathematically optimized, we obtained excellent results as expected from our theoretical analysis. The simulations are performed for various conditions with varying system and designed parameters. The simulation results for all conditions are also explained in details in this thesis.

Why to go for fault tolerant Clock Synchronization System: We expect malicious faults will be an increasing concern given the two major technological trends: (i) Increasing reliance on distributed topologies and (ii) decrease in dependability of modern IC and their susceptibility to malicious failures. An example is the concept of "fly-by-wire" systems, which is based on distributed architecture [Kevin Driscoll, et al, 2003]. Many of such systems are employed in safety-critical systems where tolerance to failures especially malicious failures is imperative. According to Moore's law the density of the integrated circuits roughly doubles every two years. This law has proved true for the last few decades. With further miniaturization of ICs, increasing clock frequencies and decreasing power supply voltages, [C. Constantinescu, 2002] concludes that the dependability of modern ICs is decreasing and they may be prone to malicious failures. Hence, a robust fault tolerant clock synchronization system is necessary to counter the effect of malicious faults.

Limitation of the algorithm presented: When designing the algorithms, we have suppressed some complexities in order to focus on the basic functionalities of the algorithms. We have considered various type of clock failure in the network while ignoring some of the possible failure in the network like link failure. The algorithms are formulated with a fully connected static distributed network in the mind. Though, intuitively, our guess is, that the algorithm will work even for the other type of network topologies but further verification is warranted.

8.2. Future Research Direction

During the course of this thesis, we have identified areas where future research can be pursued. The followings are some of the directions on which further study can be done:

8.2.1. Relaxation of Network Requirement.

We have designed our algorithm to take care of a fully and partially connected static network in our thesis. We can further explore the feasibility of the algorithm in a more relaxed network environment. An analytical study followed by the verification of the performance of WASA and AWASA in a partial connected network can be carried out. The possibility of various provisions like nodes joining and leaving the network, sub-section of the network getting disconnected etc can also be looked into.

8.2.2. Wireless Network.

In the thesis we have concentrated on connected and partially network while developing the algorithms. A similar study for wireless can be also done. Further a new algorithm providing high accuracy and tighter precision can be designed for such network. This algorithm can also be made fault tolerant which can work on partial and dynamically changing network. Such an algorithm once developed will be of much utility.

8.2.3. Collusion of Nodes

One of the most interesting topics, which we have studied during the course of this thesis, is the malicious nodes. Malicious nodes also called byzantine nodes have unpredictable behaviour. Further study can be done about their properties especially how they behave as a group. Whether these nodes can collude to destabilize the network? If they can collude, how they collude and their behaviour thereafter will be of significant importance. If they do not seem to collude, can we make them collude to our advantage, can be another research direction. A careful study of the malicious behaviour may help us manipulate them more meaningfully for various applications.