CHAPTER 1

INTRODUCTION

This chapter discusses the background of this research. This chapter is divided into eight sections, research background, statement of the problem, objective and hypotheses, assumption, scope and delimitation, and significance of the study.

1.1 Research Background

Sensor network in Internet of Things (IoT) is an essential part of Cyber-Physical Systems that integrates the physical and digital worlds [1] and time synchronization becomes a highly crucial element within it [2]; [3]. The use of low-cost, efficient, and low-power sensor network technology in Wireless Sensor Network applications and protocols works in a coordinated and synchronized manner [4]. Everything from managing and debugging networks involves time properties, as in security services, localization, routing, and tracking. Correlating log files accurately among devices in the Wireless Sensor Networks (WSN) area becomes very difficult or even impossible without proper time synchronization, which can lead to behavioral conflicts, device damage, and unnecessary service losses [5]. Therefore, the security of the time synchronization process is a major concern where the properties of the system time settings can be relied upon, namely being secure and guaranteed, especially in algorithmic methods and synchronization protocols approaches.

The time synchronization process can be achieved by adding the current time difference with the local time of a clock to achieve a common time on all nodes in the WSN [4]. This occurs because the imperfections of the hardware clock fabrication result in the local time on a node drifting apart over time, necessitating a synchronization protocol to attain the same pace [6]. Many time synchronization protocols have been developed in recent years to ensure that data collected by sensors in the network have accurate, synchronized timestamps, and consistent data analysis. Protocols such as Network Time Protocol (NTP) and Precision Time Protocol (PTP) in synchronization over wired networks [7]. Reference Broadcast Synchronization (RBS), Time-Sync Protocol for Sensor Network (TPSN), and Flooding Time Synchronization Protocol (FTSP), specifically designed for resource-constrained WSNs using root node as a reference clock [8]; [9]. Furthermore, other protocols leveraging distributed reference clock such as ATS (Average Time Synchronization) and MTS (Maximum Time Synchronization) focus on reaching a common message agreement using averaging or maximum calculation methods in consensus [10]; [11]. Although many protocols have been developed, security concerns are also becoming increasingly critical, given the general nature of open WSN environments and their vulnerability to threats.

The development of time synchronization protocols in Wireless Sensor Networks (WSN) has been a significant focus of research in the last decade as mentioned above, both centralized and distributed-based, but security threat mitigation needs to be improved [12]. Many distributed based synchronization protocols using consensus algorithms have been widely discussed in recent years due to their robustness against

several security threats, such as topological attacks and data manipulation [12]. Protocols such as SATS [13], FTCCS [14], and SMTS [15] are designed to handle message manipulation attacks and demonstrate fast convergence. SATS uses parameter adjustment based on two-hop neighbor information to counter random data injections, while FTCCS employs ILC-MSR (Iterative Learning Control with Multi-Stage Resilience) to address deception attacks. SMTS incorporates message verification and authentication to combat message manipulation attacks. In contrast, NiSTS [16] and RTSP [3] also focus on handling Sybil and message manipulation attacks but with varying speeds and countermeasure techniques, such as maxclique-based identification and message filtering. Protocols like CSNI [17], which use centralized approaches, focus is on node classification to identify and handle Sybil attacks. The secure consensus mechanism of these protocols helps prevent dishonest or malicious nodes from significantly influencing the system time. It is worth noting that the performance of time synchronization and resilience to attacks in consensus algorithms are greatly influenced by the type and changes in topology; therefore, topology attacks are a major concern in this research to measure resilience under changing topology conditions during attacks.

In the context of Wireless Sensor Networks (WSNs) and consensus-based time synchronization methods, Fixed Weight Assignment (FWA), Centralized Weight Assignment (CWA), and Mobile Weight Assignment (MWA) [18] refers to different consensus weighting algorithms. FWA refers to a consensus weighting algorithm where a fixed weight is assigned to each neighboring node in the network. These fixed weights remain constant throughout the synchronization process. CWA involves a centralized node, such as a base station or a central controller, assigning weights to neighboring nodes in the network. These weights are typically based on factors such as node proximity, reliability, or communication quality. Furthermore, MWA is a consensus weighting algorithm where weights assigned to neighboring nodes are dynamically adjusted based on the mobility or changing conditions of nodes in the network. This allows for adaptive weighting to account for changes in network topology or node characteristics over time. However, all three weightings above, whether static like FWA or dynamic like CMA and CWA, are assumed to be indifferent to the topology conditions such as connectivity of a graph. Consequently, there is no assumptions that if such of topological attacks occurs will change those weighting methods. As it is known, the resilience of consensus-based time synchronization is highly dependent on the topology conditions or the adjacency matrix of the sensor network [4]. The adjacency matrix is closely related to the Laplacian graph, and the value of the second smallest eigenvalue on the Laplacian graph gives an idea of how strongly the graph is connected [19].

In mathematics and network theory, the Laplacian matrix or Laplacian operator is a matrix representing the connectivity of a graph or network [20]. In the context of consensus-based time synchronization in WSNs, the Laplacian matrix is often used to model the connectivity and relationships between nodes in the network. Laplacian-based consensus methods leverage properties of the Laplacian matrix to achieve synchronization among nodes by iteratively updating their local clocks based on information exchanged with neighboring nodes. The Laplacian matrix plays a fundamental role in understanding the dynamics of consensus algorithms and their resilience to topology attacks. Therefore, in this study, we propose a graph-based consensus synchronization weighting method on Laplacian eigenvalues to test

synchronization resilience in topology attacks by looking at two main parameters: convergence speed and synchronization accuracy [12].

Findings of this study showed that incorporating Laplacian Gain enhances fault tolerance, reduces convergence iterations by approximately 40.42%, and improves network accuracy by about 9.34%. This demonstrates the crucial role of Laplacian-based consensus methods in maintaining network stability and accuracy under topology changes, recommending their adoption for enhancing WSN resilience against attacks.

1.2 Statement of the Problem

The problem of this research is to measure the extent to which changes in attack trials affect the performance of consensus-based time synchronization systems on various network topologies, including Ring, Star, and Mesh. The convergence speed and accuracy of synchronization in consensus-based time synchronization systems are critically influenced by the network topology. The robustness of the consensus process can be challenged by various topology attacks on the network, such as Edge Attacks like Denial-of-Service attacks and Vertices Attacks like Node Destruction Attacks. It is essential to understand the extent of the impact these attacks have on different network topologies, including Ring, Star, and Mesh topologies, to devise strategies that enhance the resilience and reliability of time synchronization mechanisms under adverse conditions.

1.3 Objective and Hypotheses

The objective of this research is to analyze the impact of topology attacks on the robustness of time synchronization in Wireless Sensor Networks (WSN) using Laplacian-eigen value weighting. This analysis will focus on two main parameters: the convergence speed of synchronization, measured in terms of iteration magnitude, and the accuracy of synchronization, assessed through local and global synchronization error magnitude. Additionally, the research will evaluate the scalability of different topology types in handling such attacks, aiming to determine their robustness and adaptability under adverse conditions.

The premises of hypotheses in this research are as follows:

Premise 1: M. Xue proved that the robustness of consensus-based time synchronization is greatly influenced by the adjacency matrix of the topology [4].

Premise 2: Furthermore, Kriegleder et al. showed that adjacency matrix is closely related to the Laplacian Graph and the second smallest eigenvalue of the Laplacian Graph indicates how strongly the graph is connected [19].

Premise 3: Also from Kriegleder et al. showed that the convergence time decreases in general with the algebraic connectivity of a network, which is valued as the second smallest eigenvalue for feedback weighting [19].

Premise 4: Under topology changes based on M. Xue and Fajrin et al., then it will impact to the robustness of time synchronization [4]; [21].

Thus, the hypothesis in this research was: by incorporating Laplacian Eigen Value

feedback weighting, the clock synchronization condition will be more robust against topology changes in topology attacks.

1.4 Scope and Delimitation

The limitations of this study include specific testing scenarios on the topology, which must adhere to Minimum Spanning Tree (MST) conditions to ensure consensus convergence. Additionally, the communication direction in wireless sensor networks involves two-way communication and no-delay involved, leading to an Undirected Graph pattern when represented graphically in perfect simulation condition. The evaluation of convergence speed relies on the iteration count parameter due to the dependence of time-based calculations on the computational capabilities of the simulation devices. These limitations shape the methodology and analysis approach of the research, highlighting the need for careful consideration and interpretation of the results within these defined constraints.

1.5 Significance of the Study

By employing Laplacian-eigen value weighting, the research delves into the intricate relationship between network topology, adjacency matrices, and Laplacian Graphs. This investigation is vital as it sheds light on the fundamental mechanisms governing consensus-based time synchronization. The evaluation of convergence speed and synchronization accuracy serves as key performance indicators, offering insights into the network's robustness and adaptability in adverse conditions. The hypothesis formulated in this study underscores the potential for Laplacian eigen value feedback weighting to bolster the robustness of clock synchronization, presenting a promising avenue for enhancing network security and reliability in the face of topology attacks.