ABSTRACT

Sensor networks on the Internet of Things (IoT) are vital for Cyber-Physical Systems, integrating physical and digital worlds. Effective time synchronization is critical for managing these networks, involving processes such as security, localization, routing, and tracking. Without proper synchronization, log file correlation among devices becomes challenging, leading to potential conflicts and service losses. Ensuring secure time synchronization is essential, using robust algorithms and protocols. Time synchronization aligns local clock times across nodes, countering hardware clock drift. Distributed consensus algorithms have shown robustness against threats like Denial of Service (DoS) attacks and data manipulation, but their performance is heavily influenced by network topology changes, making topology attacks a significant research focus. The resilience of consensus-based time synchronization relies on the network's topology, represented by the adjacency matrix and Laplacian graph eigenvalues, indicating connectivity strength. Fixed Weight Assignment (FWA), Centralized Weight Assignment (CWA), and Mobile Weight Assignment (MWA) are consensus weighting algorithms used in WSN synchronization, each adapting differently to network conditions. However, these methods often overlook the impact of topological changes during attacks. This study proposed a graph-based consensus synchronization weighting method using Laplacian eigenvalues to test resilience against topology attacks, focusing on convergence speed and synchronization accuracy. The findings 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 speed convergence and accuracy under topology changes, recommending their adoption for enhancing WSN resilience against attacks.

Keywords: IoT Security, Time Synchronization, Clock Attack, MWA, Laplacian-Based