Chapter 18
Predicting Analytics for Dynamic Mobility Patterns in Mobile Wireless Networks Using Cutting-Edge Method

D. Ponmary Pushpa Latha

https://orcid.org/0000-0003-4000-0294
Division of Digital Sciences, Karunya Institute of Technology and Sciences (Deemed), Coimbatore, India

S. Princy Suganthi Bai
Department of Computer Applications, Hindustan Institute of Technology and Science (Deemed), Chennai, India

K. Lakshmi Piya
Division of Commerce and International Trade, Karunya University (Deemed), Coimbatore, India

D. Joseph Pushparaj
Department of Computer Science and Engineering, PSN College of Engineering and Technology,Tirunelveli, India

Catherine Esther Jones
Division of Digital Sciences, Karunya Institute of Technology and Sciences (Deemed), Coimbatore, India

DOI: 10.4018/979-8-3693-3940-4.ch018

ABSTRACT

The research aims to improve the security of multi-hop wireless ad hoc networks by creating a robust packet loss detection system. The main goal is to distinguish between packet losses caused by link errors and those resulting from insider attacks involving malicious packet dropping. The system analyzes packet loss patterns to combat insider attacks, where nodes exploit network knowledge to selectively drop critical packets. The system enhances accuracy by utilizing lost packet correlations and introduces a HLA-based public auditing architecture to verify the accuracy of reported packet loss information without compromising node privacy. The anticipated outcome will enhance detection accuracy, privacy-preserving auditing, and the implementation of targeted mitigation strategies, thereby enhancing the security and reliability of multi-hop wireless ad hoc networks.

1. INTRODUCTION

The chapter aims to improve the safety of multi-hop wireless ad hoc networks by developing a robust packet loss detection system. The system uses an advanced algorithm to analyze packet loss patterns, leverages lost packet correlations for accuracy, and introduces a public auditing architecture based on Homomorphic Linear Authenticator (HLA) for verification of packet loss details without compromising node privacy. This will contribute to a more secure and reliable network environment. This research aims to enhance the security of ad hoc networks, especially in situations where insider attacks can compromise communication integrity. It aims to provide novel solutions for accurately identifying packet loss, recognizing the limitations of conventional detection algorithms (Sun et al., 2021).

This research requires a deep understanding of wireless ad hoc network architectures, algorithm development proficiency, and security concepts, especially insider attacks. Expertise in homomorphic encryption and linear authentication is crucial for implementing the proposed auditing architecture. Access to real-world datasets is essential for testing and validating the developed algorithms. The goal of the project is to provide a reliable system for detecting packet loss in multi-hop wireless ad hoc networks that can differentiate between link faults and insider assaults. By spotting harmful activity, putting mitigation plans into place, and protecting data integrity with the help of the HLA-based public auditing architecture, the system will improve security. This study will benefit future applications in dynamic communication contexts as well as network security measures (Almesaeed & Jedidi, 2021).