MALWARE PROPAGATION AND GRAY HOLE DEFENSE IN WIRELESS SENSOR NETWORK

A PROJECT REPORT

Submitted by

VINITH SHARAN S

VISSAKAN V

YOGESH N

JEYAKAMAL S

in partial fulfilment for the award of the degree

of

BACHELOR OF TECHNOLOGY

IN

INFORMATION TECHNOLOGY

PSNA COLLEGE OF ENGINEERING AND TECHNOLOGY,
(An Autonomous Institution Affiliated to Anna University, Chennai)

DINDIGUL - 624622

MAY 2024

ABSTRACT

Malware is pervasive in networks and poses a critical threat to network security. However, our understanding of malware behavior in networks remains limited. In this report, we investigate how malware propagates in networks from a global perspective. We formulate the problem and establish a rigorous two-layer epidemic model for malware propagation across different networks.

Wireless Sensor Networks (WSN) are increasingly being deployed in security-critical applications. Due to their inherent resource constraints, they are prone to various security attacks, including Gray Hole attacks, which severely impact data collection. To address this challenge, we propose an active detection-based security and trust routing scheme named Active Trust for WSN. The most significant innovation of Active Trust is its ability to avoid both Black and Gray holes by actively creating a number of detection routes. This allows for quick detection and assessment of nodal trust, thereby enhancing data route security. Comprehensive theoretical analysis and experimental results indicate that the performance of the Active Trust scheme surpasses that of previous studies.

Active Trust significantly improves the data route success probability, resilience against Gray Hole attacks, and optimizes network lifetime Active Trust can significantly improve the data route success probability and ability against Gray Hole attacks and can optimize network lifetime.