VISVESVARAYA TECHNOLOGICAL UNIVERSITY

“JNANA SANGAMA”, BELAGAVI – 590 018

TECHNICAL SEMINAR SYNOPSIS

ON

“LIGHT WEIGHT AUTHENTICATION OF DEVICES IN WIRELESS SENSOR NETWORK”

Submitted in partial fulfilment of the requirement

for the award of the degree of

BACHELOR OF ENGINEERING

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted By

INDU A : 4GH22CS401

Under the Guidance of

Prof Shylaja N S, BE, M. Tech

Assistant Professor

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

GOVERNMENT ENGINEERING COLLEGE, HASSAN - 573201

2024-25

ABSTRACT

Wireless Sensor Networks (WSNs) have gained significant attention due to their critical role in applications such as healthcare monitoring, smart cities, military surveillance, industrial automation, and environmental monitoring. These networks consist of resource-constrained sensor nodes that operate in open and often unsecured environments, making them highly susceptible to various security threats, including unauthorized access, spoofing, replay attacks, and data tampering. Ensuring secure communication in WSNs is essential to maintaining data integrity, confidentiality, and network availability.

Traditional authentication mechanisms, such as public key infrastructure (PKI) and RSA-based cryptographic techniques, impose significant computational and energy burdens, rendering them impractical for WSNs with limited processing power, memory, and battery life. To address these challenges, lightweight authentication techniques have been developed, offering a balance between security and efficiency. These approaches include hash-based authentication, elliptic curve cryptography (ECC), lightweight symmetric key protocols, and hybrid authentication schemes designed to mitigate security risks while minimizing computational and energy overhead.

This paper explores and evaluates various lightweight authentication mechanisms, analyzing their effectiveness in securing WSNs against potential cyber threats. The study focuses on the trade-offs between security, computational efficiency, energy consumption, and implementation feasibility. By integrating optimized authentication methods, WSNs can achieve enhanced security, ensuring reliable and secure data transmission in real-world applications.

INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of spatially distributed, low-power sensor nodes that communicate wirelessly to monitor and collect data from their environment. These networks play a critical role in applications such as healthcare monitoring, environmental sensing, smart cities, industrial automation, and military surveillance. The widespread adoption of WSNs is driven by their ability to provide real-time data collection and communication with minimal human intervention.

However, the deployment of WSNs in open and often hostile environments makes them highly susceptible to various security threats. Attackers can exploit vulnerabilities in the network to launch attacks such as eavesdropping, node impersonation, replay attacks, and denial-of-service (DoS) attacks. Ensuring the security and integrity of data transmission in WSNs is, therefore, a major challenge.

Traditional authentication mechanisms, such as public-key cryptography, impose significant computational and energy demands, which are not feasible for resource-constrained WSN nodes. As a result, lightweight authentication techniques have emerged as a promising solution. These methods, including hash-based authentication, elliptic curve cryptography (ECC), and lightweight symmetric key protocols, aim to provide robust security while minimizing computational overhead and power consumption.

This paper explores various lightweight authentication techniques for securing WSNs, evaluating their effectiveness in terms of security strength, computational efficiency, and energy consumption. By implementing efficient authentication mechanisms, WSNs can achieve secure communication and resilience against cyber threats, ensuring reliable operation in critical applications.

OBJECTIVES

- To analyze the security challenges in WSNs.
- To evaluate existing lightweight authentication techniques.
- To propose an efficient authentication mechanism tailored for WSNs.
- To ensure minimal computational and energy overhead while maintaining security.
- To implement and test the proposed authentication model.

CONCLUSION

Security is a major concern in the applications of wireless sensor networks, many mechanisms have been designed to enhance the security in wireless sensor networks. Understanding the significance of authentication in wireless sensor networks, in this paper we proposed a mechanism for authentication of nodes in wireless sensor networks mu-tually. The proposed mechanism is lightweight as it involves simple operations. The security analysis of the proposed mechanism has been done by modelling it in Scyther tool and it has been verified that the mechanism is safe and free from potential security attacks. The proposed mechanism shall not only enhance the security of the network but also is resource aware. Hence, it is suitable for resource constraint wireless sensor networks.