Pankaj kumar singh, 2025, 13:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Novel approach of WSN routing to data Communication between Sensor node on Energy Warning

Pankaj kumar singh, Professor Amit Thakur
Department of Electronics and Communication School of Engineering and Technology, Vikram University, Ujjain, Madhya Pradesh

Abstract- Wireless Sensor Networks (WSNs) are widely used in environmental monitoring, healthcare, military, and smart city applications, but their resource-constrained nature makes security and energy efficiency critical challenges. Traditional cryptographic approaches are often unsuitable due to high computation and communication overheads. To address this, we propose a Secured Energy Efficient Key Management (SEEKM) scheme, which ensures confidentiality, authentication, and integrity of sensor data while prolonging network lifetime. In the proposed approach, nodes are preloaded with a small subset of cryptographic keys from a global pool, and secure communication is established only through authenticated neighbors that share common keys. Lightweight session key derivation and message authentication are applied to minimize computational cost, while a first-order radio energy model accounts for transmission and cryptographic energy consumption. Simulation in MATLAB evaluates network performance in terms of packet delivery ratio, alive nodes over time, first node death (FND), half node death (HND), end of network lifetime (EOL), and security drop rate under node compromise attacks. Results demonstrate that SEEKM achieves a favorable trade-off between security and energy efficiency, reducing unauthorized transmissions while extending overall network lifetime compared to conventional key management schemes.

Keywords: wireless sensor network; energy balance; optimal routing; clustering routing protocol.

I. INTRODUCTION

A typical wireless sensor network (WSN) consists of a set of wirelessly interconnected electronic devices, called sensor nodes, along with at least one sink node called base station (BS), which are placed over a given area that is referred as a field of interest (FOI), as illustrated in Figure 1 [1,2,3].

Fig. 1. The architecture of a typical wireless sensor network.

As depicted in Figure 2, a typical sensor node consists of the following main components:

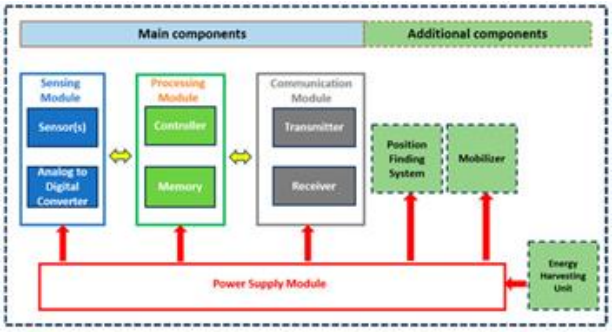

Fig. 2. Architecture of a typical sensor node.

- **Sensing module:** it contains appropriate sensors that are able to monitor ambient conditions.
- **Processing module:** It typically contains a microcontroller or microprocessor and may also comprise additional memory and processing

units. The processing unit plays a critical role in handling the data collected by the sensing unit and controlling the data storage and/or transmission.

- **Communication module:** it is responsible for establishing and maintaining communication between the sensor node and other sensor nodes and/or a BS.
- **Power supply module:** This module refers to the energy source that provides the necessary electrical power to the sensor node. Since sensor nodes in WSNs are often deployed in remote or generally difficult to approach locations, they must rely on self-contained power sources. Typically, this component is a battery. A sensor node may also contain a position finding system and an energy harvesting unit. Furthermore, it may be mobile thanks to the use of an appropriate motion mechanism or system.

II. RESEARCH MOTIVATION

In the target tracking application of wireless sensor networks, a basic problem is target coverage. That is, given a set of targets and a WSN with some sensor nodes deployed over the monitoring field, target coverage problem is defined such that all the targets are continuously monitored or covered by at least one sensor node at any time [8,9]. When there are many nodes in the network running out of energy, the target is easily lost. To ensure that the target's motion is captured, it is necessary to have as many nodes as possible to be alive. This also requires the full use of energy to extend the overall effective working time.

The most direct way to solve the shortage of power supply is to increase the capacity of batteries by forming batteries in parallel or in series. However, in the test, we found that the common lithium-ion batteries often have circuit break or short circuit fault. A battery pack consists of multiple batteries, and the failure of any one of the batteries will cause the failure of the battery pack, so the probability of failure of the battery pack is much higher than that of a single battery. For the system working in the field, it is inconvenient to replace batteries frequently, and the interruption of data acquisition caused by battery failure is intolerable. Balancing energy and prolonging system lifetime are hot issues in wireless sensor networks.

III. WSN ENERGY WARNING

The term Energy Warning generally refers to a situation where the remaining energy of sensor nodes drops below a certain threshold, which may affect the network's lifetime, connectivity, and data transmission.

Explanation:

- In WSNs, sensor nodes are usually battery-powered and deployed in large numbers.
- Since replacing or recharging batteries is difficult (especially in remote areas), energy management is crucial.
- Energy Warning is a condition (or signal) generated when a node's energy level is low, indicating that:
- The node may soon stop functioning.
- Data loss or connectivity issues could occur.
- Network lifetime and stability are at risk.

Key Points of WSN Energy Warning:

- **Threshold-based mechanism** – A warning is triggered when residual energy < threshold.
- **Helps in routing decisions** – Nodes with low energy are avoided in multi-hop routing.
- **Improves network lifetime –** By redistributing workload to healthier nodes.
- **Can be global or local** – Local node warning vs. system-wide energy alert.
- **Supports energy-efficient protocols** – Such as LEACH, TEEN, PEGASIS.

Example:

If a sensor node's battery drops to 20% of its initial energy, the system may issue an energy warning so that routing protocols reroute data through other nodes, preventing early death of that node.

IV. SECURED ENERGY EFFICIENT KEY MANAGEMENT (SEEKM) IN WSN

SEEKM is a security mechanism for Wireless Sensor Networks (WSNs) that focuses on providing

confidentiality, authentication, and integrity of data while also being energy-efficient to prolong the network lifetime.

Since WSN nodes are resource-constrained (limited battery, processing, and memory), traditional cryptographic methods are too heavy. SEEKM is designed to overcome this by using lightweight key management schemes that ensure security with minimal energy consumption.

Key Features of SEEKM

- **Energy Efficiency** – Reduces computational overhead by using lightweight encryption and efficient key distribution methods.
- **Secure Key Establishment** – Ensures that only authorized nodes can generate, share, and update cryptographic keys.
- **Scalability –** Supports dynamic addition of new nodes into the WSN without major reconfiguration.
- **Resilience to Attacks –** Protects against eavesdropping, node capture, replay, and man-in-the-middle attacks.
- **Low Communication Overhead** – Minimizes the number of control messages for key exchange, saving bandwidth and power.

Working Principle

- Each sensor node is preloaded with a small set of cryptographic materials (e.g., partial keys).
- When nodes communicate, shared session keys are derived securely with minimal computation.
- Keys are refreshed periodically or when energy warnings occur to maintain both security and energy balance.
- Hybrid approaches (symmetric + lightweight asymmetric cryptography) are sometimes used to improve security while keeping energy usage low.

V. HYBRID LAYER USER AUTHENTICATION SCHEME (HLUAS)

A Hybrid Layer User Authentication Scheme is a security mechanism designed to provide strong user authentication in resource-constrained environments like Wireless Sensor Networks (WSNs), IoT, or cloud computing, by combining multiple authentication methods across different security layers (application layer, network layer, transport layer, etc.).

It is called hybrid because it integrates two or more authentication techniques (e.g., password-based, biometric, token-based, certificate-based, or cryptographic keys) to achieve both high security and energy efficiency.

Key Features

- **Multi-layer Protection –** Authentication happens at multiple layers (e.g., application & network) to resist attacks.
- **Hybrid Approach –** Combines symmetric/asymmetric cryptography, hash functions, and sometimes biometrics or one-time passwords (OTP).
- **Energy Efficiency** – Lightweight operations are chosen to suit WSN/IoT devices with low battery and memory.
- **Resistance to Attacks** – Protects against impersonation, replay, man-in-the-middle, and node capture attacks.
- **User-Centric** – Ensures only authorized users can access network resources or sensor data.

Working Principle

- **Registration Phase:** A user registers with a trusted authority using credentials (password, ID, biometrics, etc.).

Authentication Phase:

- At the application layer, user identity is verified using credentials/keys.
- At the network/transport layer, secure session keys are exchanged using lightweight cryptographic protocols.
- **Hybrid Mechanism:** Combines password/biometric checks (for user identity) with cryptographic key exchanges (for secure communication).
- **Session Establishment:** After successful verification, a secure session key is generated for encrypted communication.

VI. RESULT AND SIMULATION

The Secured Energy Efficient Key Management (SEEKM) scheme in Wireless Sensor Networks (WSNs) can be simulated in MATLAB by modeling sensor node deployment, communication, and energy consumption along with lightweight cryptographic operations. In this simulation, nodes are first deployed randomly in a sensing field, and each node is preloaded with a subset of cryptographic keys from a global key pool. Neighbor discovery is carried out based on communication range, and only nodes that share at least one common key are considered for secure communication. During each round of data transmission, source nodes derive lightweight session keys and authenticate packets using hash functions or message authentication codes (MACs), while the energy cost of both transmission and cryptographic operations is deducted from the node's battery. If nodes cannot establish a secure link (i.e., no shared key or insufficient energy), packets are dropped, simulating security enforcement. MATLAB tracks network performance metrics such as delivery ratio, number of alive nodes, first node death, and overall network lifetime. By adjusting parameters such as the number of keys per node, energy thresholds, and percentage of compromised nodes, SEEKM performance can be analyzed in terms of both security and energy efficiency.

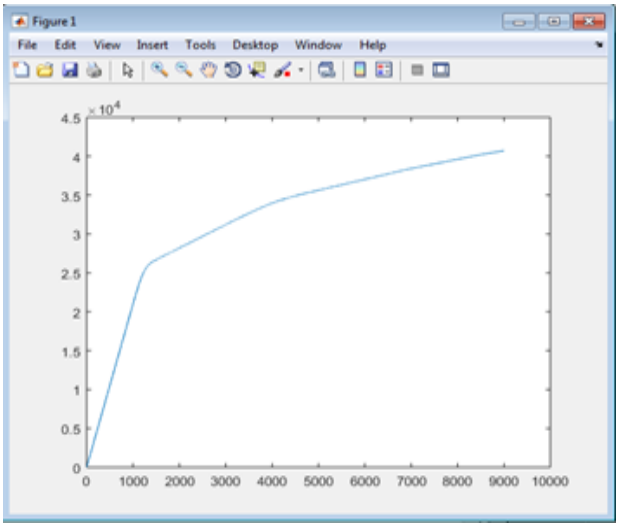

Fig.3. PDR rate.

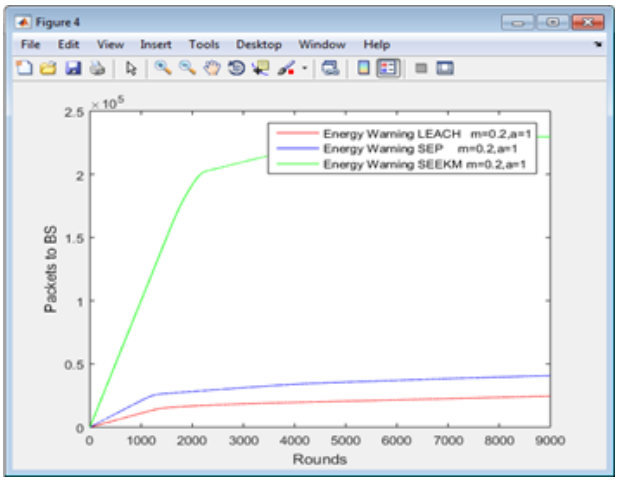

Fig.4. PDR rate and Energy alert generation.

VII. CONCLUSION

The simulation and analysis of the Secured Energy Efficient Key Management (SEEKM) scheme demonstrate that integrating lightweight cryptographic operations with energy-aware routing can significantly enhance both security and network lifetime in Wireless Sensor Networks. The results show that secure communication is maintained through shared key-based authentication while minimizing energy consumption via efficient session key derivation and reduced control overhead. Compared to conventional schemes, SEEKM effectively balances the trade-off between security and energy efficiency, ensuring higher packet delivery ratios, lower unauthorized access rates, and extended operational time before the first and last node failures. Furthermore, the adaptability of SEEKM to node compromise scenarios highlights its resilience and robustness in practical deployments. Overall, SEEKM offers a promising solution for achieving secure, scalable, and energy-sustainable WSNs, making it suitable for mission-critical and long-term applications.

REFERENCE

1. Kumar, M. P., & Hariharan, R. (2022). Improved trustworthy, speed, and energy-efficient GPSR routing algorithm in large-scale WSN. Measurement: Sensors, 24, 100576.

2. Srinivasan, S., Ramesh, T. K., Paccapeli, R., & Fanucci, L. (2022). Industrial functional safety assessment for WSN using QoS metrics. Heliyon, 8(11).
3. Tyagi, V., & Singh, S. (2023). Network resource management mechanisms in SDN enabled WSNs: A comprehensive review. Computer Science Review, 49, 100569.
4. Zin, S. M., Anuar, N. B., Kiah, M. L. M., & Ahmedy, I. (2015). Survey of secure multipath routing protocols for WSNs. Journal of Network and Computer Applications, 55, 123-153.
5. Khan, T., Singh, K., Hasan, M. H., Ahmad, K., Reddy, G. T., Mohan, S., & Ahmadian, A. (2021). ETERS: A comprehensive energy aware trust-based efficient routing scheme for adversarial WSNs. Future Generation Computer Systems, 125, 921-943.
6. Premkumar, M., & Sundararajan, T. V. P. (2020). DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. Microprocessors and Microsystems, 79, 103278.
7. Masood, J. A. I. S., Jeyaselvi, M., Senthamarai, N., Koteswari, S., Sathya, M., & Chakravarthy, N. K. (2023). Privacy preservation in wireless sensor network using energy efficient multipath routing for healthcare data. Measurement: Sensors, 29, 100867.
8. Reshi, I. A., Sholla, S., & Najar, Z. A. (2024). Safeguarding IoT networks: Mitigating black hole attacks with an innovative defense algorithm. Journal of Engineering Research.
9. Kalghatgi, H., Dhawle, M., & Raut, U. (2023). Defense techniques against spoofing attacks in wireless sensor networks. Materials Today: Proceedings.
10. Al-Amiedy, T. A., Anbar, M., Belaton, B., Bahashwan, A. A., Hasbullah, I. H., Aladaileh, M. A., & Mukhaini, G. A. (2023). A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things. Internet of Things, 100741.