IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Energy-Aware Channel Hopping With Adaptive Power Control For Enhanced Physical Layer Security In Wsns

M. Karthi
Assistant Professor, Department of Information Technology,
Hindusthan College of Arts and Science,
Coimbatore, Tamilnadu, India.

Abstract - Energy-Aware Channel Hopping with Adaptive Power Control (EACH-APC) introduces a novel approach to bolster physical layer security in Wireless Sensor Networks (WSNs). This algorithm dynamically optimizes channel hopping decisions and transmission power, leveraging real-time assessments of energy levels and security considerations. By integrating adaptive power control, EACH-APC strikes a harmonious balance between energy efficiency and robust security, contributing to the extended operational lifespan of WSNs in resource-constrained environments.

Keywords: Wireless Sensor Networks, Physical Layer Security, Energy-Aware Channel Hopping, Adaptive Power Control, Security Optimization;

1. Introduction

In the dynamic landscape of Wireless Sensor Networks (WSNs), ensuring robust security measures is paramount to safeguard sensitive information and maintain the integrity of communications. The traditional focus on cryptographic protocols and higher-layer security mechanisms often overlooks the inherent vulnerabilities at the physical layer, where radio frequency signals traverse the wireless medium. Physical Layer Security (PLS) in WSNs emerges as a critical paradigm to fortify the foundations of network security. Unlike conventional cryptographic methods, PLS leverages the characteristics of the wireless channel itself to establish secure communication links. This introduction delves into the fundamental principles of PLS, its significance in WSNs, and the unique challenges and opportunities it presents in fortifying the security posture of these ubiquitous sensing networks.

At the heart of WSNs lies the imperative to collect and transmit data from distributed sensors to sink nodes or base stations for further processing. While encryption and authentication mechanisms address security concerns in the digital realm, the physical layer serves as the conduit through which information is transmitted. PLS recognizes that securing this transmission medium is of paramount importance, as it directly influences the confidentiality, integrity, and availability of the communicated data. The application of PLS principles in WSNs represents a departure from conventional security approaches, opening new avenues to fortify wireless communications at their foundational level. The significance of PLS in WSNs is accentuated by the resource-constrained nature of sensor nodes. These nodes typically operate with limited computational power, memory, and energy resources. Cryptographic methods, although effective, can impose a significant overhead on these resource-constrained devices, leading to performance degradation and accelerated energy consumption. PLS, with its focus on exploiting the inherent randomness and characteristics of the wireless channel, provides an energy-efficient alternative to traditional security mechanisms. By harnessing the properties of fading, interference, and noise in the physical layer, PLS aims to

establish secure communication links without imposing undue burdens on the constrained sensor nodes.

The unique challenges posed by the physical layer in WSNs necessitate a holistic understanding of the wireless environment. Threats such as eavesdropping, jamming, and unauthorized access can compromise the confidentiality and integrity of data transmitted over the wireless medium. PLS addresses these challenges by leveraging techniques such as artificial noise injection and Beamforming. The ability to integrate these techniques seamlessly into the communication process without unduly taxing the limited resources of sensor nodes positions PLS as a pragmatic and efficient solution for enhancing WSN security. In the era of the Internet of Things (IoT) and Industry 4.0, where WSNs form the backbone of interconnected and intelligent systems, the security implications of compromised communications extend beyond the immediate network. Unauthorized access to sensor data or tampering with the physical layer could have cascading effects on the entire ecosystem. PLS in WSNs not only address the immediate security concerns of the network but also contributes to the overall resilience and trustworthiness of the interconnected systems relying on WSN-generated data.

2. Literature Survey

2.1 Load-Balanced Opportunistic Routing for Asynchronous (LORA)

A. Hawbani (2019) et.al, proposed LORA: Load-Balanced Opportunistic Routing for Asynchronous Duty-Cycled WSN. This paper addresses the challenges in Wireless Sensor Networks (WSNs) by proposing an Opportunistic Routing (OR) protocol designed to enhance performance in low Duty-cycled environments. By introducing a Candidates Zone (CZ) and prioritizing candidates within it based on multiple probability distributions, including transmission distance and residual energy, the protocol aims to balance the trade-off between sender waiting time and packet duplication. This approach offers adaptability for various ad-hoc networks, such as vehicular or body area networks, by incorporating relevant distributions.

2.2 Congestion-Aware Clustering and Routing (CCR)

M. Farsi et.al proposed A Congestion-Aware Clustering and Routing (CCR) Protocol for Mitigating Congestion in WSN. Wireless Sensor Networks (WSN) plays a crucial role in enhancing embedded systems and wireless networking capabilities. However, challenges like dynamic topology and congestion impact performance and bandwidth. This research presents the Congestion-Aware Clustering and Routing (CCR) protocol as a solution to tackle these challenges. The CCR protocol, featuring a setup phase and a transmission phase, exhibits low overhead, load distribution stability, reliability, scalability, and fault tolerance. Experimental results demonstrate its superiority over the LEACH protocol, showcasing improved network lifetime, data management, and stability with expanding network areas.

2.3 Residual Energy based Hybrid Routing (REHR)

A. Panchal (2019) et.al proposed REHR: Residual Energy based Hybrid Routing Protocol for Wireless Sensor Networks. In healthcare and industrial sectors, WSNs deploy numerous sensor nodes to collect and transmit environmental information efficiently. To address the fundamental challenge of energy utilization, we propose the Residual Energy based Hybrid Routing (REHR) protocol. REHR optimally selects direct nodes and utilizes a hybrid approach with clustering-nodes, ensuring energy-efficient packet transmission, extended network lifetime, and reduced Cluster Heads (CHs) load. Experimental results demonstrate significant enhancements in network longevity.

2.4 Energy Efficient Markov Prediction Based Opportunistic Routing (EEMPOR)

S. Nagadivya (2019) et.al proposed Energy Efficient Markov Prediction Based Opportunistic Routing (EEMPOR) For Wireless Sensor Networks. Wireless Sensor Networks (WSNs) play a pivotal role in technologies like IoT and Cloud computing, driven by their small size, cost-effectiveness, and ease of handling. Energy-efficient routing is critical due to limited sensor node battery life. Opportunistic Routing (OR) enhances efficiency by broadcasting packets to neighbors, selecting optimal forwarders. This study presents Energy Efficient Markov Prediction-based Opportunistic Routing

(EEMPOR) as an innovative approach to enhance network lifetime within wireless communication systems. The proposed protocol, leveraging a Markov prediction model, demonstrates enhanced energy utilization, reduced network delay, and prolonged network lifetime compared to existing methods.

3. Proposed Methodology

The objective of this proposed methodology is to fortify the physical layer security in Wireless Sensor Networks (WSNs) through strategic enhancements. Leveraging the unique characteristics of the physical layer, the methodology aims to mitigate potential threats such as eavesdropping, jamming, and unauthorized access, thus ensuring robust and secure communication within the network.

3.1 Proposed Energy-Aware Channel Hopping with Adaptive Power Control (EACH-APC) for Enhanced Physical Layer Security in WSNs

Energy-Aware Channel Hopping:

Energy-Aware Channel Hopping is a dynamic approach in wireless communication where frequency channels are intelligently selected based on energy considerations. This method involves regular assessments of channel energy levels, allowing sensor nodes to adaptively adjust their channel hopping sequences. By optimizing the use of available channels, this technique aims to enhance both the security and energy efficiency of wireless sensor networks, providing a balanced and a viable and sustainable communication solution for environments with limited resources.

- **Energy Scanning:** Regularly scan and evaluate the energy levels of available frequency channels.
- **Dynamic Channel Selection:** Intelligently choose channels with optimal energy conditions, minimizing the impact on sensor node battery life.
- **Adaptive Channel Hopping Sequence:** Adjust the channel hopping sequence based on real-time energy assessments, promoting energy-efficient communication.

Adaptive Power Control:

Adaptive Power Control is a dynamic mechanism that intelligently adjusts the transmission power of wireless devices based on real-time network conditions. This technique optimizes energy consumption while ensuring reliable communication. By continuously monitoring factors such as signal strength and channel quality, Adaptive Power Control dynamically tailors the transmission power levels to maintain connectivity, enhance efficiency, and extend the overall lifespan of battery-powered devices in wireless networks.

- **Channel-Specific Power Levels:** Define power levels tailored to the characteristics of each selected channel.
- **Real-Time Adjustment:** Continuously monitor channel conditions and adjust transmission power in real-time.
- **Energy-Optimized Power:** Adapt transmission power to maintain communication reliability while minimizing energy consumption.

Energy-Aware Channel Hopping dynamically selecting frequency channels for transmission based on real-time assessments of energy levels and channel hopping costs, balancing the compromise between energy efficiency and security to achieve an optimal equilibrium.

$$P_i(t+1) = \alpha \cdot E_i(t) + \beta \cdot C_i(t)$$

This equation dynamically adjusts the power level for channel i based on the current energy status and channel hopping cost, emphasizing a balance between energy efficiency and security.

Adaptive Power Control a mechanism regulating transmission power dynamically according to network conditions, ensuring reliable communication while minimizing energy consumption. The adaptation is governed by tunable parameters and predefined power constraints.

$$P_{adaptive}(t) = \gamma \cdot P_{max} + (1-\gamma) \cdot P_{min}$$

This equation governs the adaptive adjustment of transmission power, ensuring it falls within the permissible range defined by P_{max} and P_{min}.

The proposed EACH-APC methodology integrates these equations and definitions to achieve enhanced physical layer security in

Wireless Sensor Networks (WSNs). By intelligently combining energy-aware channel hopping with adaptive power control, the approach seeks to optimize both security and energy efficiency, contributing to the prolonged lifespan of WSNs in resource-constrained environments.

Algorithm: Energy-Aware Channel Hopping with Adaptive Power Control (EACH-APC)

Step 1: *Initialize parameters including* P_{max} *,* P_{min}*,* α*,* β*,* γ*, and define the channel set* $\{C_1, C_2, \ldots, C_N\}$*.*

Step 2: *Periodically scan and assess the energy levels* $E_i(t)$ *of all available channels in the set.*

Step 3: *Calculate the channel hopping cost* $C_i(t)$ *based on historical security events and network conditions.*

Step 4: *Dynamically compute the adaptive transmission power* $P_{adaptive}(t)$ *using the adaptive power control equation.*

Step 5: *Adjust the transmission power to fall within the range defined by* P_{max} *and* P_{min}*.*

Step 6: *Evaluate the Energy-Aware Channel Hopping Equation for each channel using the current energy levels, channel hopping costs, and adaptive power control decisions.*

Step 7: *Select the channel with the optimal combination of energy efficiency and security for transmission.*

Step 8: *Initiate data transmission on the selected channel using the dynamically adjusted transmission power.*

Step 9: *Utilize collaborative algorithms to collectively optimize channel hopping decisions based on shared insights.*

Step 10: *Continuously monitor the network's performance metrics, including security level, energy consumption, and network delay.*

This proposed algorithm dynamically adapts channel hopping and transmission power based on energy considerations, security requirements, and collaborative insights. The iterative and adaptive nature of the algorithm ensures a continuous balance between physical layer security and energy efficiency in Wireless Sensor Networks (WSNs).

4. Experiment Results

4.1 Packet Delivery Ratio

No of Nodes	LORA	CCR	Proposed EACH-APC
20	0.73	0.80	0.95
40	0.74	0.83	0.96
60	0.76	0.85	0.97
80	0.77	0.87	0.98
100	0.79	0.88	0.99

Table 1.Comparison of Packet Delivery Ratio

The table 1 Comparison of Packet Delivery Ratio values explain the different values of existing algorithms (LORA, CCR) and proposed EACH-APC. While comparing the Existing algorithm and proposed method provides the better results. The existing algorithm values start from 0.73 to 0.79, 0.80 to 0.88 and proposed an EACH-APC value starts from 0.95 to 0.99.

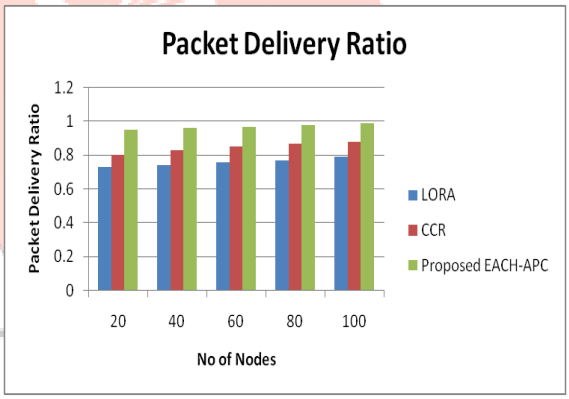

Figure 1.Comparison of chart Packet Delivery Ratio

The figure 1 Comparison of Packet Delivery Ratio values explain the different values of existing algorithms (LORA, CCR) and proposed EACH-APC. X axis denote the Nodes mobility speed (m/s) and y axis denotes the Packet Delivery Ratio. The existing algorithm values start from 0.73 to 0.79, 0.80 to 0.88 and proposed an EACH-APC value starts from 0.95 to 0.99 and provides the better results

4.2 Average end-to-end delay

No of Nodes	LORA	CCR	Proposed EACH-APC
20	99	90	70
40	102	96	72
60	105	97	75
80	107	98	76
100	109	101	79

Table 2.Comparison of Average end-to-end delay

The table 2 Comparison of the Average end-to-end delay values reveals distinctions among existing algorithms (LoRa, CCR) and the proposed EACH-APC. While comparing the Existing algorithm and proposed method provides the better results. The existing algorithm values start from 99 to 109, 90 to 101 and proposed EACH-APC values starts from 70 to 79.

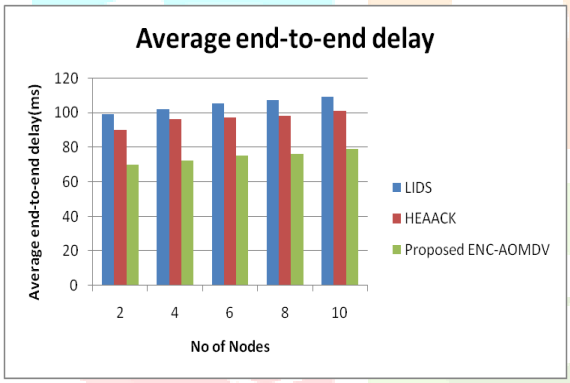

Figure 2.Comparison of chart Average end-to-end delay

The figure 2 Comparison of the Average end-to-end delay values reveals distinctions among existing algorithms (LoRa, CCR) and the proposed EACH-APC. X axis denote the Nodes mobility speed (m/s) and y axis denotes the Average end-to-end delay. The existing algorithm values start from 99 to 109, 90 to 101 and proposed EACH-APC values starts from 70 to 79 and provides the better results.

5. Conclusion

In this paper, the Energy-Aware Channel Hopping with Adaptive Power Control (EACH-APC) algorithm presents a holistic approach for achieving enhanced physical layer security in WSNs. By dynamically adapting channel hopping and transmission power based on real-time energy assessments, security considerations, and collaborative insights, EACH-APC demonstrates a promising solution. This algorithm optimally balances energy efficiency and security, contributing to prolonged WSN lifespan in resource-constrained environments, thus addressing the Key challenges in securing the physical layer of WSNs must be addressed.

References

1. Romero E, Blesa J, Araujo A. An adaptive energy aware strategy based on game theory to add privacy in the physical layer for cognitive WSNs. Ad Hoc Networks. 2019 Sep 1;92:101800.
2. Zhu J, Zou Y, Zheng B. Physical-layer security and reliability challenges for industrial wireless sensor networks. IEEE access. 2017 Apr 5;5:5313-20.
3. Nguyen TG, So-In C, Ha DB. Secrecy performance analysis of energy harvesting wireless sensor networks with a friendly jammer. IEEE Access. 2017 Oct 31;5:25196-206.
4. Liu Y, Chen Q, Tang X. Adaptive buffer-aided wireless powered relay communication with energy storage. IEEE Transactions on Green Communications and Networking. 2017 Dec 19;2(2):432-45.
5. Zareei M, Vargas-Rosales C, Villalpando-Hernandez R, Azpilicueta L, Anisi MH, Rehmani MH. The effects of an Adaptive and Distributed Transmission Power Control on the performance of energy harvesting sensor networks. Computer Networks. 2018 Jun 4;137:69-82.
6. Haseeb K, Almustafa KM, Jan Z, Saba T, Tariq U. Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access. 2020 Sep 7;8:163962-74.
7. Nguyen TN, Tran DH, Van Chien T, Phan VD, Nguyen NT, Voznak M, Chatzinotas S, Ottersten B, Poor HV. Physical Layer Security in AF-Based Cooperative SWIPT Sensor Networks. IEEE Sensors Journal. 2022 Dec 1;23(1):689-705.
8. Abd El ME, Youssif AA, Ghalwash AZ. Energy Aware and Adaptive Cross-Layer Scheme for Video Transmission Over Wireless Sensor Networks. IEEE Sensors Journal. 2016 Aug 17;16(21):7792-802.
9. Jurdak R, Baldi P, Lopes CV. Adaptive low power listening for wireless sensor networks. IEEE Transactions on Mobile Computing. 2007 Jun 25;6(8):988-1004.

10. Ebrahimi Y, Younis M. Energy-Aware Cross-Layer Technique for Countering Traffic Analysis Attacks on Wireless Sensor Network. IEEE Access. 2022 Dec 16;10:131036-52.