SEC-MAC: A Secure Wireless Sensor Network Based on Cooperative Communication

Yassmin Khairat[1]*, Tamer O. Diab[2], Ahmed Fawzy[3], Samah Osama[4], Abd El- Hady Mahmoud[5]
Informatics Research Department, Electronics Research Institute (ERI), Cairo, Egypt[1, 4]
Electrical Engineering Department-Faculty of Engineering (Benha University), Benha, Egypt[1, 2, 5]
Nanotechnology Lab, Electronics Research Institute (ERI), Cairo, Egypt[3]

***Abstract*—Wireless Sensor Networks (WSNs) are essential for a wide range of applications, from environmental monitoring to security systems. However, challenges such as energy efficiency, throughput, and packet delivery delay need to be addressed to enhance network performance. This paper introduces a novel Medium Access Control (MAC) protocol that utilizes cooperative communication strategies to improve these critical metrics. The proposed protocol enables source nodes to leverage intermediate nodes as relays, facilitating efficient data transmission to the access point. By employing a cross-layer approach, the protocol optimizes the selection of relay nodes based on factors like transmission time and residual energy, ensuring optimal end-to-end paths. The protocol's performance is rigorously evaluated using a simulation environment, demonstrating significant improvements over existing methods. Specifically, the protocol enhances throughput by 12%, boosts energy efficiency by 50%, and reduces average packet delivery delay by approximately 48% than IEEE 802.11b. These results indicate that the protocol not only extends the lifespan of sensor nodes by conserving energy but also improves the overall reliability and efficiency of the WSN, making it a robust solution for modern wireless sensor networks. Security in Wireless Sensor Networks (WSNs) is crucial due to vulnerabilities like eavesdropping, data tampering, and denial of service attacks. Our proposed MAC protocol addresses these challenges by incorporating authentication techniques, such as the handshaking protocol. These measures protect data integrity, confidentiality, and availability, ensuring reliable and secure data transmission across the network. This approach enhances the resilience of WSNs, making them more secure and trustworthy for critical applications such as healthcare and security monitoring.**

Keywords*—Wireless Sensor Networks (WSNs); energy efficiency; Media Access Control (MAC); cooperative communication; handshaking algorithm

I. Introduction

Wireless Sensor Networks (WSNs) have become a cornerstone technology in the modern era, offering a versatile and cost-effective solution for various monitoring and data collection tasks. These networks consist of spatially distributed sensor nodes that autonomously collect and transmit data, making them invaluable in diverse fields such as military surveillance, medical monitoring, agricultural as shown in Fig. 1, environmental tracking, and commercial applications [1], [2]. The growing affordability of sensor technology and advancements in wireless communication protocols have made WSNs accessible for everyday use, enabling real-time data acquisition and analysis.

Despite their advantages, WSNs face several challenges that need to be addressed to optimize their performance and extend their operational lifespan. The main problems include signal attenuation, interference in the wireless environment, and the consequent reduction in throughput and data transmission efficiency over extended distances [1] [2]. Furthermore, the limited energy resources of sensor nodes pose a significant constraint, as frequent battery replacements or recharging are often impractical, especially in remote or hazardous locations. Therefore, reducing energy consumption during data transmission is a critical design consideration for enhancing the longevity and reliability of WSNs [3] [4].

To tackle these challenges, researchers have explored various strategies, including cooperative communication techniques. Cooperative communication leverages the inherent broadcasting nature and spatial density of WSN nodes to improve data transmission efficiency. This approach involves neighboring nodes acting as relays to forward data packets, thus reducing the energy burden on individual nodes and enhancing overall network performance. Two primary strategies are employed: multiple-relay and single-relay communication. While multiple-relay strategies can offer higher data rates and redundancy, they also involve greater complexity and overhead. Single-relay strategies, on the other hand, are often preferred for resource-constrained WSNs due to their simpler implementation and lower energy requirements [5].

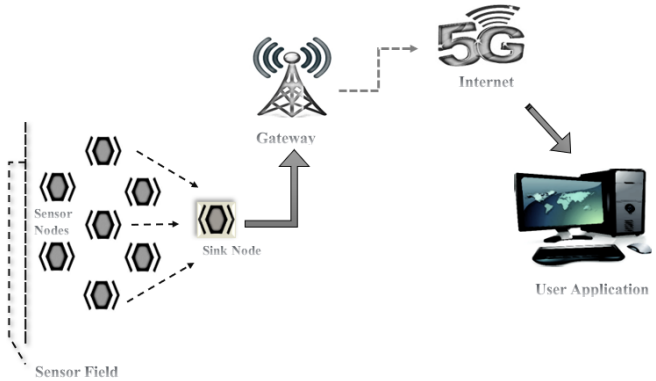

Fig. 1. Schematic diagram of WSN architecture.

In this context, the development of robust Medium Access Control (MAC) protocols is essential to manage the coordination and communication between sensor nodes. MAC protocols play a pivotal role in determining how nodes access the shared communication medium, handle data transmission,

and manage energy consumption. A well-designed MAC protocol can significantly enhance WSN performance by reducing collisions, minimizing latency, and optimizing energy usage. Given the constraints of WSNs, such as limited power and bandwidth, traditional MAC protocols designed for general wireless networks are not directly applicable. Instead, WSN-specific MAC protocols are needed to address the unique challenges of these networks [6] [7].

This paper introduces a novel MAC protocol called the Secure Energy-aware Cooperative MAC (SEC-MAC) protocol, specifically designed to enhance the performance of WSNs. The SEC-MAC protocol integrates cross-layer techniques, combining insights from both the physical and MAC layers to optimize data transmission strategies. A key feature of SEC-MAC is its adaptive data transmission algorithm, which dynamically switches between direct and cooperative transmission modes based on the real-time assessment of data rates and channel conditions. This adaptability ensures efficient use of network resources, reducing control packet overhead and conserving energy [7]. In addition to improving throughput and energy efficiency, the SEC-MAC protocol also addresses critical security concerns inherent in WSNs. The open and distributed nature of these networks makes them vulnerable to various attacks, such as eavesdropping, data tampering, and denial of service (DoS) attacks. These security threats can compromise data integrity, confidentiality, and availability, which are crucial for the reliable operation of WSNs, particularly in sensitive applications like healthcare and military surveillance. The SEC-MAC protocol incorporates robust security mechanisms, including data encryption, secure routing algorithms, and authentication techniques, to safeguard the network against these vulnerabilities [8].

This comprehensive approach not only enhances the resilience of WSNs against potential security threats but also ensures that the network remains efficient and functional even under adverse conditions. The inclusion of security measures within the MAC protocol layer is particularly advantageous, as it provides a foundational level of protection that complements higher-layer security protocols. This layered security approach is essential for mitigating a wide range of threats that could otherwise exploit the inherent vulnerabilities of WSNs [9] [10].

The paper is organized as follows: Section II provides a detailed overview of the communication system employed by WSNs, highlighting the challenges and considerations specific to these networks. Section III delves into the design and implementation of the SEC-MAC protocol, explaining its core components, including the adaptive data transmission algorithm and the relay node selection process. Section IV delves into handshaking in wireless sensors. Section V presents an analytical model developed to evaluate the performance of the SEC-MAC protocol under various wireless channel conditions, considering factors such as multi-rate capabilities and the effects of saturated traffic loads. Section VI discusses the simulation results obtained from a comparative study of the SEC-MAC protocol against existing WSN MAC protocols, demonstrating the protocol's advantages in terms of throughput, energy efficiency, and security. Finally, Section VII concludes the paper with a summary of the findings and suggestions for future research directions, focusing on further enhancing the efficiency and security of WSNs.

II. Literature Review

The importance of MAC protocols in Wireless Sensor Networks (WSNs) is evident as they significantly influence network performance, energy efficiency, and overall reliability. This review covers key studies and developments in MAC protocols aimed at improving the efficiency and security of WSNs.

Dhivya et al. [11] emphasized the extensive use of WSNs in applications such as pollution monitoring, temperature sensing, and disaster management, highlighting clustering as a crucial technique for enhancing network performance. Singh et al. [12] provided an overview of the physical factors, architecture, and applications of WSN technology. Mohamed et al. [13] focused on the critical aspects of routing efficiency and energy overhead, which are vital for optimal network performance.

Yi et al. [14] compared different sensor types used for air pollution monitoring and discussed future developmental needs. Anisi et al. [15] explored the application of WSNs in agriculture, specifically in precision agriculture, emphasizing energy reduction. Kaur et al. [16] surveyed various WSN routing protocols, highlighting their potential future developments. AL-Mousawi and AL-Hassani [17] addressed issues such as scalability, mobility, and data security in explosive detection scenarios.

Ali et al. [18] reviewed real-time WSN applications in areas such as water monitoring, traffic management, health surveillance, and temperature sensing, emphasizing their effectiveness in remote locations. Rashid and Rehmani [19] conducted a comprehensive study on the application of WSNs in urban environments, examining their benefits, challenges, and applications.

Abdollazadeh and Navimipour [20] proposed methods for investigating and analyzing sensor deployments, categorizing issues based on different deployment techniques and conditions. They also explored traditional sensor uses in WSNs, network properties, and architecture, identifying key sensor-related issues. In order to handle the massive amounts of data produced by the growing number of sensors in WSNs, Belfkiih et al. [21] presented a sensor database and talked about the associated research issues.

Shafiq et al. [22] evaluated the energy efficiency of WSNs, addressing aspects such as power efficiency and threshold sensitivity. They identified energy consumption as a major issue and explored current shortcomings and challenges. Amutha et al. [23] provided a comprehensive analysis of WSN categorization based on deployment methods, coverage, sensor types, energy efficiency, and sensing models. Sharma et al. [24] recommended machine learning techniques for smart city applications, emphasizing the prevalence of supervised learning over unsupervised and reinforcement learning techniques.

Temene et al. [25] examined the mobility properties of WSNs. The QIEAC-CSSBO technique was presented by Paruvathavardhini and Sargunam [26] and uses a quantized indexive energy-aware clustering-based combinatorial

stochastic sampling bat optimization algorithm to enhance energy efficiency and secure routing. Nagarajan and Kannadhasan [27] examined how well a hybrid NIDS model performed in detecting network intrusions in wireless sensor networks.

Paruvathavardhini et al. [28] proposed a security-enhanced clustered routing protocol that reduces energy consumption by avoiding constant activation of all nodes. They developed a new method for selecting cluster heads to prevent energy depletion and improve security. Hosseinzadeh et al. [29] introduced the CTRF cluster-based trusted routing algorithm, which incorporates a weighted trust mechanism and uses a fire hawk optimizer to improve network security by taking into account nodes' limited energy.

Dass et al. created a safe routing protocol for body area network clustered networks [30]. Mainaud et al. [14] sought to bridge the gap between physical-layer cooperative communication techniques and suitable MAC layer schemes for WSNs by introducing the WSC-MAC protocol, designed to improve network reliability through cooperative communication. Liu et al. [13] proposed a node cooperation mechanism where nodes with higher channel gain and adequate residual energy assist in relaying data packets, enhancing network lifetime and energy efficiency. Nacef et al. [15] developed the COSMIC protocol, which triggers retransmissions from the destination node in case of erroneous packet receptions, improving latency, throughput, and energy efficiency.

The Busy Tone Based Cooperative MAC Protocol (BTAC) and the Throughput and Energy-Aware Cooperative MAC Protocol (TEC-MAC) leverage IEEE 802.11's multi-rate capabilities to support data transmission in WSNs. However, maintaining relay tables in TEC-MAC is time-consuming. The MCA-MAC protocol addresses these issues by using a more efficient distributed approach for selecting relay nodes, thus reducing overhead and improving throughput, delay, and energy efficiency.

Overall, the literature on MAC protocols for WSNs reflects significant progress in addressing challenges related to energy efficiency, security, and adaptability. Modern research continues to innovate with adaptive techniques and integration of advanced technologies, aiming to enhance the performance and reliability of WSNs. Table I summarizing the literature review of MAC in Wireless Sensor Networks (WSNs):

TABLE I. SUMMARY OF KEY CONTRIBUTIONS AND FINDINGS IN MAC PROTOCOLS FOR WIRELESS SENSOR NETWORKS (WSNS)

Ref	Authors	Focus/Contribution	Key Findings/Techniques
[1]	Dhivya et al.	Clustering in WSNs for monitoring pollution, temperature, and disaster management	Emphasized the use of clustering to enhance network performance
[2]	Singh et al.	Overview of WSN technology	Discussed physical factors, architecture, and applications
[3]	Mohamed et al.	Routing efficiency and energy overhead	Highlighted the importance of these factors for network performance
[4]	Yi et al.	Sensor types for air pollution monitoring	Compared sensor types and outlined future development needs
[5]	Anisi et al.	WSN use in agriculture	Focused on energy reduction in precision agriculture
[6]	Kaur et al.	WSN routing protocols	Surveyed protocols and their future potential
[7]	AL-Mousawi and AL-Hassani	Scalability, mobility, and data security in explosive detection	Addressed issues relevant to explosive detection scenarios
[8]	Ali et al.	Real-time WSN applications	Reviewed applications in water, traffic, health, and temperature monitoring
[9]	Rashid and Rehmani	WSNs in urban environments	Examined benefits, challenges, and applications
[10]	Abdollazadeh and Navimipour	Sensor deployments	Proposed methods for analyzing sensor deployments and categorizing issues
[11]	Belfkih et al.	Sensor database management	Introduced a database for managing large volumes of sensor data
[12]	Shafiq et al.	Energy efficiency in WSNs	Evaluated power efficiency and current shortcomings
[13]	Amutha et al.	WSN categorization	Analyzed based on deployment methods, coverage, sensor types, and energy efficiency
[14]	Sharma et al.	Machine learning in smart city applications	Recommended techniques with a focus on supervised learning
[15]	Temene et al.	Mobility properties in WSNs	Examined the mobility properties of WSNs
[16]	Paruvathavardhini and Sargunam	QIEAC-CSSBO technique	Improved energy efficiency and secure routing
[17]	Nagarajan and Kannadhasan	Network intrusion detection	Analyzed performance of a blended NIDS model
[18]	Paruvathavardhini et al.	Security-enhanced clustered routing	Reduced energy consumption and improved security
[19]	Hosseinzadeh et al.	CTRF cluster-based trusted routing	Enhanced network security with a fire hawk optimizer
[20]	Dass et al.	Secure routing in body area networks	Developed a secure routing protocol
[21]	Our Proposed Model	Delay Reduction, Throuhput Improvement, Energy Efficiency Enhancement	Algorithm of relay selection. Cooperative communication technique

III. PROPOSED SEC-MAC PROTOCOL

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you? Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

This study assumes that the Wireless Sensor Network (WSN) comprises 150 static sensor nodes, evenly distributed across the network. Data transport takes place over a single physical wireless channel, with a gradual fading channel employed to keep channel conditions constant while the MAC frame is being transmitted. Because wireless channels are broadcast, the Access Point (AP) monitors and receives signals from both the source and relay nodes. The IEEE 802.11b standard, which offers data transfer speeds of 11, 5.5, 2, and 1 Mbps, is the foundation for the proposed WSN.

There are two data transmission modes in the system: direct transmission mode and cooperative relaying mode. In direct transmission mode, data is sent directly from the source to the destination (AP) without involving any relay nodes. As illustrated in Fig. 2, the cooperative relaying mode, in contrast, consists of two stages: first, data is carried from the source to the destination through the relay node that has been selected, based on a relay selection method used by the source node. After that, the source node sends its data to the relay, and the relay node relays it to the intended recipient. In order to maximize energy and time efficiency, the SEC-MAC protocol additionally permits the relay to transmit its own data to the AP subsequent to transmitting the source's info.

The relay selection algorithm in the SEC-MAC protocol considers three key factors to select the optimal relay: Channel State Information (CSI), Residual energy (RE), and transmission time. The process begins with the source node transmitting a Need to Send (NTS) packet. Neighboring sensor nodes that receive the NTS packet evaluate their CSI relative to a predefined threshold (TH). Nodes with CSI above the threshold are considered potential relays; those with lower CSI quietly drop out.

Next, among the potential relay nodes, the one with the least end-to-end delay and the highest residual energy is selected. Each potential relay calculates an RBackoff

Value using the following equation:

$$R_{Backoff} = \frac{1}{\alpha\, CSI + \delta\, RE + \beta \frac{1}{T_{srd}}} \quad (1)$$

Where α, δ, and β are coefficients used for normalization, and Tsrd represents the cooperative transmission time from the source node to the AP via the relay node.

The direct data transmission time is calculated as follows:

$$T_{sd} = 8LR_{s-d} \quad (2)$$

Where, L is the packet length and R_{s-d} is the data rate from the source to the destination.

The transmission time from the source to the relay node and the relay node to the AP combined makes up the overall transmission time for cooperative transmission. If Tsrd is less than Tsd, a nearby relay node j is taken into consideration for selection. The ideal relay is determined by the relay node that reaches the fastest transmission time from the source to the AP. The flow diagram in Fig. 3 shows the relay selection procedure.

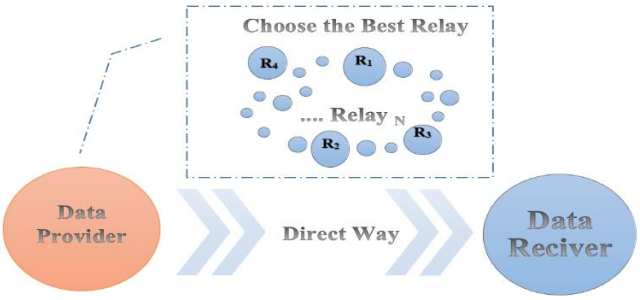

Fig. 2. Co-operative Communication vs. Direct Way Transmitting Data.

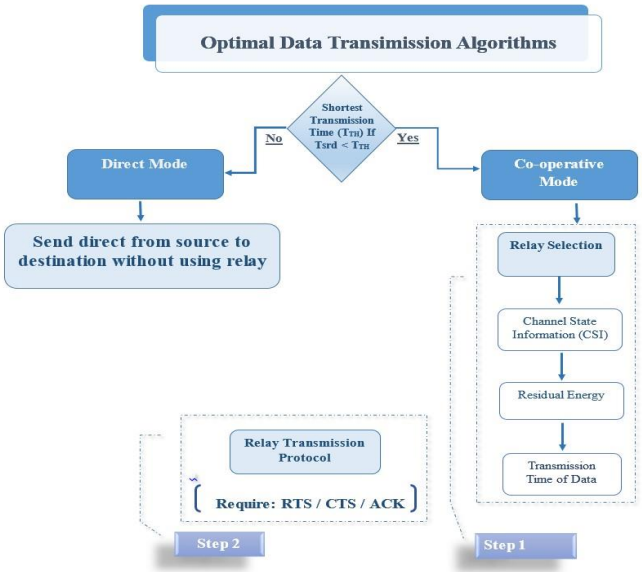

Fig. 3. Flow chart about optimal data transmission algorithms.

In addition to the relay selection and data transmission processes, security within the WSN is bolstered through the implementation of a robust handshaking algorithm. This algorithm is crucial for establishing a secure communication link between the source, relay, and destination nodes. During the initial handshaking phase, mutual authentication is performed, ensuring that only legitimate nodes participate in the communication process. The handshaking procedure uses a combination of symmetric and asymmetric cryptographic techniques to securely exchange session keys and authenticate node identities. The session keys are then used to encrypt data, protecting it from eavesdropping and unauthorized access during transmission. This approach not only secures the data but also ensures the integrity and authenticity of the nodes involved, thereby preventing potential security threats such as replay

attacks and man-in-the-middle attacks. The secure handshaking mechanism is seamlessly integrated into the SEC-MAC protocol, providing an additional layer of security without compromising the network's performance or energy efficiency.

IV. HANDSHAKING IN WIRELESS SENSOR NETWORKS (WSNS)

Wireless Sensor Networks (WSNs) [32] are inherently vulnerable to a variety of attacks due to their limited resources, dynamic topologies, and reliance on wireless communication. Common threats include continuous channel access, which disrupts the Media Access Control (MAC) protocol and drains node batteries by continuously injecting malicious packets, leading to energy depletion from excessive retransmissions. Collision attacks further hinder communication by allowing malicious nodes to block or delay data transmission, resulting in energy waste and potential data loss. Additionally, misdirection occurs when attackers redirect data packets, overwhelming targeted nodes with irrelevant information and depleting resources; countermeasures such as smart sleep can mitigate this issue. The physical accessibility of sensor nodes in open areas renders them susceptible to capture and tampering, known as node capture attacks. Path-based denial-of-service (DoS) attacks involve malicious nodes injecting false or replayed packets, consuming energy and bandwidth while obstructing communication with the base station; authentication techniques and anti-replay protections can help counteract this threat. Selective forwarding attacks see attackers using compromised nodes to drop incoming packets or prioritize their own communications, further jeopardizing data integrity. The man-in-the-middle attack poses significant risks by allowing interception and potential alteration of communications, necessitating robust security measures to prevent such vulnerabilities. While handshaking protocols can address some of these security concerns by facilitating authentication, secure key exchange, and session management thereby enhancing trust among nodes and reducing the risk of unauthorized access they are not a panacea. A comprehensive security strategy for WSNs must also incorporate complementary measures such as intrusion detection systems, encryption, and energy-efficient protocols to ensure robust protection against the myriad of threats facing these networks.

Handshaking in Wireless Sensor Networks (WSNs) is a fundamental process that establishes a communication link between nodes before data transmission. It involves an exchange of messages to synchronize both the sender and receiver, ensuring they are ready to communicate and agree on key parameters like data rates and encryption methods. This mechanism enhances the reliability and efficiency of data transfer by minimizing the risk of data loss or interference as shown in Fig. 4.

In Cooperative Access MAC protocols, handshaking begins with an initialization step, where a node intending to transmit data sends a request to potential relay nodes within its range. The relay nodes respond with information about their availability and capabilities, such as their signal strength and current load. This negotiation helps select the optimal relay node, ensuring efficient data transfer. Once a relay is chosen, a confirmation process follows where both sender and relay node exchange messages to agree on communication parameters, including channel allocation and encryption. This step optimizes the transmission process by ensuring smooth and secure data transfer, followed by an acknowledgment from the receiver confirming successful data delivery.

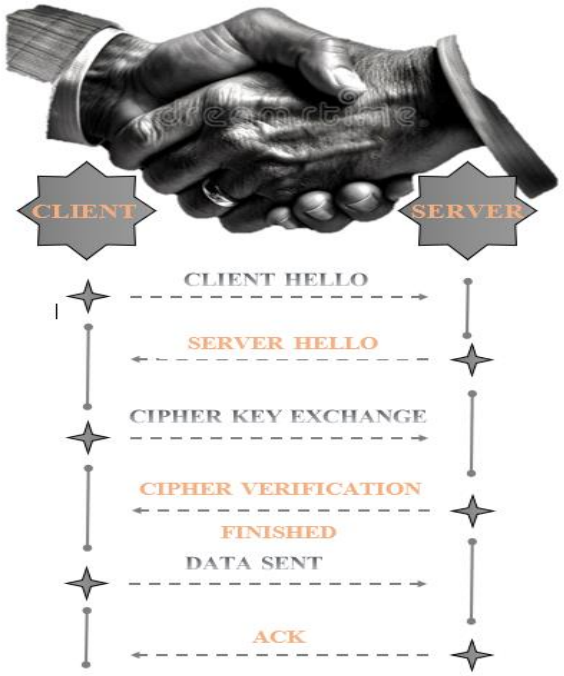

Fig. 4. Handshaking process in WSN.

The handshaking protocol not only improves communication efficiency but also strengthens security in WSNs. By ensuring that only authorized nodes can participate in the network through authentication mechanisms, handshaking prevents unauthorized access and enhances data integrity. It also facilitates the establishment of encryption keys, protecting data from eavesdropping, replay attacks, and man-in-the-middle attacks.

Several handshaking algorithms can be integrated into Cooperative Access MAC protocols to improve both security and performance in WSNs. These include Three-Way Handshake, Public Key Infrastructure (PKI), Elliptic Curve Cryptography (ECC), Challenge-Response Authentication, Secure Sockets Layer (SSL)/Transport Layer Security (TLS), and Diffie-Hellman Key Exchange. Each offers distinct advantages in securing and optimizing data transmission while preserving energy and computational resources within the network.

This comparative analysis highlights the trade-offs between security, energy efficiency, latency, and computational overhead in each protocol, offering insight into their suitability for various WSN applications. The Diffie-Hellman Key Exchange protocol offers several advantages when compared to other handshaking protocols commonly used in Wireless Sensor Networks (WSNs). Unlike the Three-Way Handshake, which has low security but is energy-efficient with minimal latency and computational overhead, Diffie-Hellman provides high security while maintaining moderate energy efficiency and

computational demands. When compared to Public Key Infrastructure (PKI) and SSL/TLS, which both offer high security but at the cost of increased latency and significant computational overhead, Diffie-Hellman strikes a balance with medium latency and overhead, making it more suitable for resource-constrained WSN environments. Furthermore, compared to Elliptic Curve Cryptography (ECC) and Challenge-Response Authentication, Diffie-Hellman provides equivalent security with similar medium levels of energy efficiency, latency, and computational overhead, positioning it as a versatile and secure protocol for environments requiring a compromise between security and resource consumption (Table II).

TABLE II. SUMMARY TABLE ABOUT HANDSHAKING ALGORITHMS

Protocol	Security	Energy Efficiency	Latency	Computational Overhead
Three-Way Handshake	Low	High	Low	Low
Public Key Infrastructure (PKI)	High	Low	High	High
Elliptic Curve Cryptography (ECC)	High	Medium	Medium	Medium
Challenge-Response Authentication	Medium	Medium	Medium	Medium
SSL/TLS	High	Low	High	High
Diffie-Hellman Key Exchange	High	Medium	Medium	Medium

V. ANALYTICAL MODEL

In this section, we derive equations for the cooperative transmission scheme [31]. In this scheme, the source node transmits its data packet through a relay node to the Access Point (AP) at a data rate Rrd. Seven potential points of failure exist for packet transmission after the RTS packet is successfully sent without a collision: RTS, CTS, RTH, DATA-S from source to relay, DATA-S from relay to AP, DATA-R from relay to AP, and packet corruption in the ACK during subsequent transmissions. The probability X1 of RTS packet corruption, assuming no RTS collision, is given by:

$$X1=1-(1-BER_C)^{8LRTS} \quad (3)$$

Where LRTS represents the length of the RTS packet in bytes. Given that the RTS packet is successfully transmitted, the probability X2 that the CTS packet is garbled is computed as follows:

$$X2=1-(1-BER_C)^{8LCTS} \quad (4)$$

Where LCTS is the length of the CTS packet in bytes. Similarly, the probability X3 that the RTH packet is corrupted while both the RTS and CTS packets are successfully transmitted is:

$$X3=1-(1-BER_C)^{8LRTH} \quad (5)$$

Where LRTH is the length of the RTH packet in bytes. Finally, the probability X4 that a DATA-S packet from the source to the relay is corrupted, assuming that the RTS, CTS, and RTH packets are transmitted successfully, is:

$$X4=1-(1-BER_{sr})^{8Ls}(1-BER_C)^{8LPLCP} \quad (6)$$

where Ls is the length of the DATA-S packet from the source to the relay and LPLCP is the length of the PLCP packet in bytes.

The bit error rate of the data packet transmitted from the source to the relay node at data rate Rsr is denoted as BERsr and Ls represents the data packet length from the source node in bytes. Given that the RTS, CTS, RTH, and DATA-S (from source to relay) packets are correctly received, the following formula determines the likelihood v5 that a DATA-S packet from the relay to the AP is corrupted:

$$X5=1-(1-BER_{rd})^{8Ls}(1-BER_C)^{8LPLCP} \quad (7)$$

Where BERrd is the bit error rate of the data packet sent between the relay and the AP at data rate Rrd The probability X6 that a DATA-R packet is corrupted while RTS, CTS, RTH, and DATA-S packets are correctly received is:

$$X6=1-(1-BER_{rd})^{8Lr}(1-BER_C)^{8LPLCP} \quad (8)$$

Where Lr is the relay node's data packet length in bytes. Ultimately, the likelihood X7 that an ACK packet is tainted while the RTH, DATA-S (from source to relay), RTS, CTS, and at least one DATA-S (relay to AP) or DATA-R packet is correctly received is as follows:

$$X7=1-(1-BER_C)^{8LACK} \quad (9)$$

Where LACK is the ACK packet length in bytes.

Let:

- $P_{e1,C}$ be the probability of RTS packet corruption,
- $P_{e2,C}$ be the probability of CTS packet corruption,
- $P_{e3,C}$ be the probability of RTH packet corruption,
- $P_{e4,C}$ be the probability of DATA-S packet corruption from the source to the relay,
- $P_{e5,C}$ be the probability of DATA-S packet corruption from the relay to the AP,
- $P_{e6,C}$ be the probability of DATA-R packet corruption, and
- $P_{e7,C}$ be the probability of ACK packet corruption.

These probabilities are calculated as follows:

$$P_{e,i}^{c} = P_{e1,C} + P_{e2,C} + P_{e3,C} + P_{e4,C} + P_{e5,C} + P_{e6,C} + P_{e7,C} \quad (10)$$

A. Saturated Throughput Analysis

In Wireless Sensor Networks (WSNs), saturated throughput refers to the maximum rate at which data can be successfully transmitted over the network when the network is fully loaded. This means that all the nodes in the network are constantly trying to send data, leading to a situation where the network is operating at its maximum capacity. Saturated throughput is an important performance metric as it reflects the efficiency of the network in handling high traffic conditions. It is often used to assess the network's ability to maintain reliable communication without excessive delays or packet loss, even when all nodes are actively transmitting data. In this context, achieving high saturated throughput indicates a well-optimized network that

can support heavy traffic loads efficiently. Lastly, the ratio of the payload size that is successfully communicated to the interval of time between two successive transmissions is known as saturation throughput η. We can express η as follows according to the adopted definition [7]:

$$\eta = \frac{8L\sum_{i=1}^{N} P_{s,i}(1-P_{e,i})}{E[T1]+E[Ts]+E[Tc]+E[TE]} \quad (11)$$

B. Energy Efficiency Expression

An expression for energy efficiency in an SEC-MAC protocol network is derived in this subsection. The ratio of successfully delivered packet bits to the total energy utilized in the network is known as the energy efficiency, or ε. Nodes expend energy in the following functions: backoff $E_B^{(i)}$, collision $E_C^{(i)}$, transmission overhearing $E_O^{(i)}$, transmission errors $E_E^{(i)}$, and successful transmission $E_S^{(i)}$ [7]

$$\eta = \frac{8L\sum_{i=1}^{N} P_{s,i}(1-P_{e,i})}{E_B^{(i)}+E_C^{(i)}+E_O^{(i)}+E_E^{(i)}+E_S^{(i)}} \quad (12)$$

C. Delay Expression

Lastly, an expression for the average packet delay is produced in this subsection using the procedure outlined in [7]. The amount of time that passes between a packet reaching the front of its MAC queue and successfully reaching the AP, as indicated by a positive acknowledgment, is known as the average packet delay.

Let Di (where i=1, 2,…, N) be a random variable that represents node I's packet latency. As a result, the average packet delay Avg[Di] has the following expression:

$$Avg[D_i]=Avg[D_{b,i}]+Avg[D_{c,i}]+Avg[D_{o,i}]+Avg[D_{s,i}]+[Avg_{e,i}] \quad (13)$$

Where:

- $Avg[D_{b,i}]$ is the typical time it takes to lower the backoff counter,
- $Avg[D_{c,i}]$ is the average delay due to collisions during transmissions,
- $Avg[D_{o,i}]$ is the typical time it takes to hold the backoff counter while other nodes are sending data.
- $Avg[D_{s,i}]$ is the average delay during a successful transmission,
- $Avg[D_{e,i}]$ is the average delay caused by erroneous transmissions.

Consequently, one can compute the whole average packet delay by:

$$D = \frac{1}{N}\sum_{i=1}^{N} Avg[D_i]$$

Let *N* represent the average total number of time slots.

VI. Results and Discussion

The proposed SEC-MAC protocol has been evaluated using MATLAB to analyze the impact of key parameters, such as the number of sensor nodes and packet length, on its performance. Simulation results comparing SEC-MAC, BTAC and IEEE 802.11b protocols, specifically in terms of Energy, throughput, and average delay demonstrate that SEC-MAC outperforms BTAC and IEEE 802.11b.

Where BTAC protocol is designed for wireless local area networks and operates based on the IEEE 802.11b standard, focusing on optimizing medium access and enhancing communication efficiency among devices. It employs the Distributed Coordination Function (DCF) with an RTS/CTS handshake to manage how stations access the wireless medium, minimizing collisions and ensuring smoother communication. For simplicity, each station operates at a fixed transmission power level, which standardizes signal transmission. Stations can adapt their data rates based on current channel conditions, allowing for more efficient data transfer. Control frames, such as RTS, CTS, and ACK, are transmitted at a basic rate of 1 Mbps to maintain a consistent communication baseline. The protocol assumes a symmetric wireless channel between the source and destination, as both utilize the same carrier frequency for packet transmission. Additionally, it enables stations to identify nearby helper stations, tracking their MAC addresses, timestamps of last packets received, transmission rates to the destination and source, and counts of transmission failures. Each station also maintains awareness of all other stations within its basic service set, facilitating effective communication. Overall, the BTAC protocol enhances wireless communication efficiency by optimizing data rates, effectively managing medium access, and utilizing nearby helpers to improve network performance.

The performance of SEC-MAC was assessed under varying data rates. We assume the simulation is based on ideal channel. Fig. 5 and Fig. 6 shows the saturated throughput of the SEC-MAC protocol. The number of sensor nodes in a Wireless Sensor Network (WSN) under optimal channel conditions is indicated by the x-axis. The results reveal that as the network size increases, the throughput also increases exponentially, largely due to the lower data rate caused by the addition of relay nodes. Initially, SEC-MAC performs similarly to BTAC, but as the number of nodes exceeds 40, SEC-MAC demonstrates a notable improvement, with a 12% higher throughput in the saturation region.

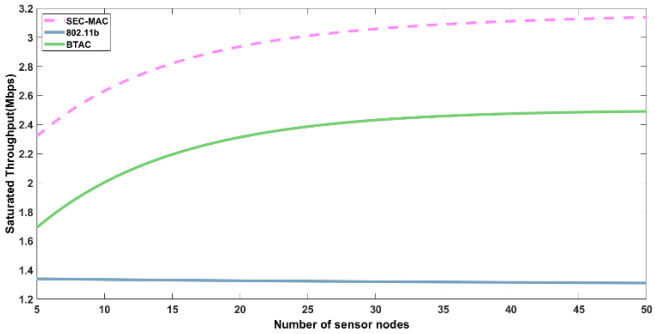

Fig. 5. Saturated throughput in relation to the quantity of nodes under optimal channel conditions.

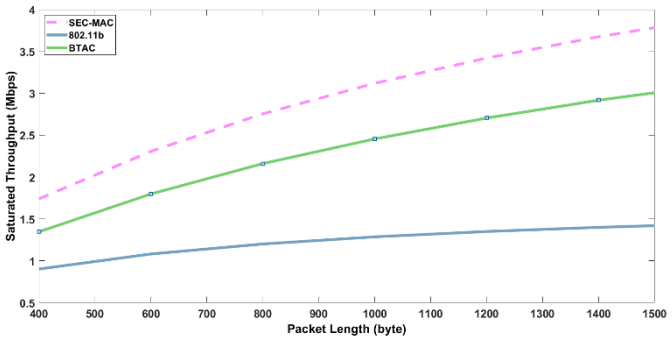

Fig. 6. Peak throughput in relation to packet length under optimal channel circumstances.

Fig. 7 and Fig. 8 provide an energy efficiency comparison, under ideal channel conditions, between the IEEE 802.11b standard and the SEC-MAC protocol at various node densities. The findings indicate that as the number of sensor nodes grows, both protocols experience reduced energy efficiency due to increased node collisions. These collisions result in more frequent packet retransmissions, leading to higher energy usage. In spite of this, SEC-MAC protocol shows a notable benefit over IEEE 802.11b, providing up to 50% more energy savings.This is primarily because SEC-MAC employs an efficient relay selection process, which minimizes retransmission time and reduces overall energy consumption, thereby substantially improving energy efficiency.

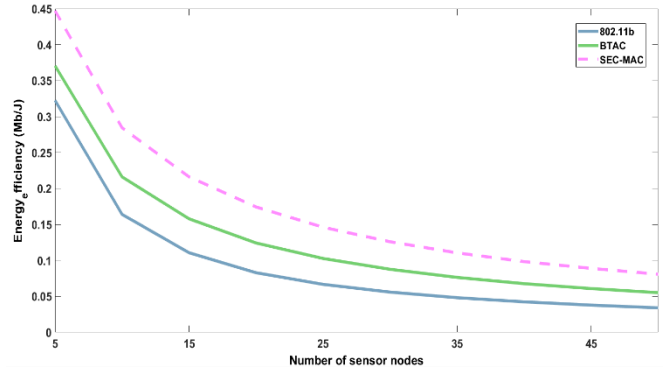

Fig. 7. Energy efficiency as a function of the number of nodes in the optimal channel.

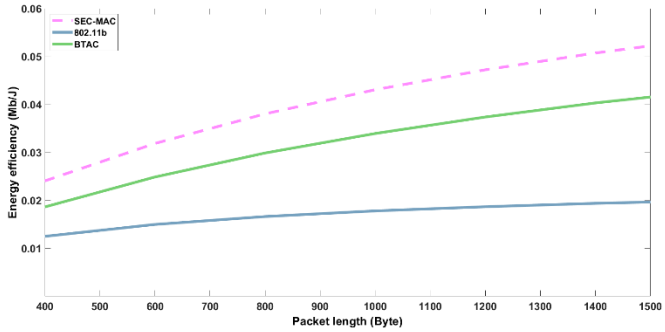

Fig. 8. Energy efficiency in relation to packet length under optimal channel circumstances.

A performance comparison of IEEE 802.11b standard and SEC-MAC protocol in terms of packet delay at various packet lengths is shown in Fig. 9 and Fig. 10. Because larger packets require longer transmission times, both protocols face increasing delays as the packet length rises.Despite this, SEC-MAC consistently outperforms IEEE 802.11b, showing a noticeable reduction in packet delay. This highlights SEC-MAC's greater efficiency in managing data transmission for sensor nodes, particularly when handling larger packet sizes.

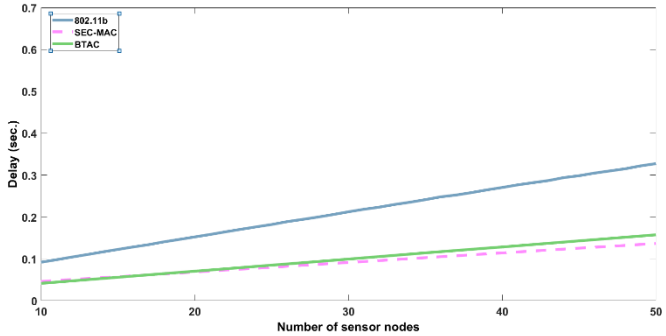

Fig. 9. Packet delay versus number of nodes with ideal channel conditions.

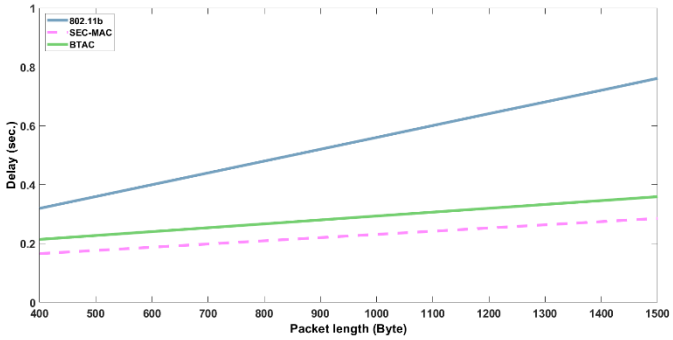

Fig. 10. Packet delay versus packet length with ideal channel conditions.

VII. Conclusion

In this paper, we introduced SEC-MAC, a secure Medium Access Control (MAC) protocol for Wireless Sensor Networks (WSNs) that leverages cooperative communication to enhance network performance. SEC-MAC improves throughput, energy efficiency, and security by allowing low data-rate nodes to select optimal relay nodes for data transmission, reducing delays and packet losses. Additionally, SEC-MAC introduces an innovative transmission scheme where relay nodes can transmit their own data without undergoing the traditional handshake procedure, thus optimizing channel access and saving energy. Cooperative communication is central to SEC-MAC, as it allows nodes to collaborate for more efficient data transmission, improving overall network reliability and performance. This cooperative approach also boosts the network's ability to scale effectively, handling a larger number of nodes without a significant drop in throughput.

Security is a key focus of SEC-MAC, addressing vulnerabilities in WSNs by incorporating cryptographic measures and secure authentication processes to protect data integrity and prevent unauthorized access. The protocol ensures reliable communication even in potentially hostile environments. Simulation results demonstrated that SEC-MAC significantly improves network throughput as the number of

nodes increases compared to BTAC and IEEE 802.11b protocols. By optimizing relay selection and minimizing retransmissions, the protocol enhances energy efficiency, making it ideal for energy-constrained applications like environmental monitoring. Future research should focus on enhancing SEC-MAC's adaptability, performance, and security to expand its applicability. Future research will explore further optimization of SEC-MAC, including its performance in real-world applications like healthcare monitoring, as well as investigating the impact of different traffic models. Overall, SEC-MAC offers an effective solution for secure, energy-efficient, and scalable communication in WSNs, making it a promising protocol for a wide range of applications.

REFERENCES

[1] K. E. Ukhurebor, I. Odesanya, S. S. Tyokighir, R. G. Kerry, A. S. Olayinka, and A. O. Bobadoye, "Wireless Sensor Networks: Applications and Challenges," Wirel. Sens. Networks - Des. Deploy. Appl., Oct. 2020.

[2] D. De, A. Mukherjee, S. K. Das, and N. Dey, "Wireless Sensor Network: Applications, Challenges, and Algorithms," Nature inspired computing for wireless sensor networks, pp. 1–18, 2020.

[3] N. R. Patel and S. Kumar, "Wireless sensor networks' challenges and future prospects," Proc. 2018 Int. Conf. Syst. Model. Adv. Res. Trends, SMART 2018, pp. 60–65, Nov. 2018.

Karimi, A., Amini, S.M. Reduction of energy consumption in wireless sensor networks based on predictable routes for multi-mobile sink. J Supercomput 75, 7290–7313 (2019). https://doi.org/10.1007/s11227-019-02938-y

[4] Manikandan, A., Venkataramanan, C. and Dhanapal, R., "A score based link delay aware routing protocol to improve energy optimization in wireless sensor network," Journal of Engineering Research,Vol. 13, pp.100115,2023.

[5] P. Parwekar, S. Rodda, and N. Kalla, "A study of the optimization techniques for wireless sensor networks (WSNs)," Adv. Intell. Syst. Comput., vol. 672, pp. 909–915, 2018.

[6] A. Hossam, T. Salem, A. A. Hady, and S. Abd El-Kader, "Mca-mac: Modified cooperative access mac protocol in wireless sensor networks," Int. Arab J. Inf. Technol., vol. 18, no. 3, pp. 326–335, 2021.

[7] R. Shanker and A. Singh, "Analysis of Network Attacks at Data Link Layer and its Mitigation," Proc. - 2021 Int. Conf. Comput. Sci. ICCS 2021, pp. 274–279, 2021.

[8] M. Boussif, "On The Security of Advanced Encryption Standard (AES)," 8th Int. Conf. Eng. Appl. Sci. Technol. ICEAST 2022 - Proc., pp. 83–88, 2022.

[9] T. Azzabi, H. Farhat, and N. Sahli, "A survey on wireless sensor networks security issues and military specificities," Proc. Int. Conf. Adv. Syst. Electr. Technol. IC_ASET 2017, pp. 66–72, Jul. 2017.

[10] S. Dhiviya, A. Sariga, and P. Sujatha, "Survey on WSN using clustering," in 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), pp. 121–125, IEEE, Tindivanam, India, February 2017.

[11] M. K. Singh, S. I. Amin, S. A. Imam, V. K. Sachan, and A. Choudhary, "A survey of wireless sensor network and its types," in 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 326–330, IEEE, Greater Noida, India, October 2018.

[12] R. E. Mohamed, A. I. Saleh, M. Abdelrazzak, and A. S. Samra, "Survey on wireless sensor network applications and energyefficient routing protocols," Wireless Personal Communications, vol. 101, no. 2, pp. 1019–1055, 2018

[13] W. Y. Yi, K. M. Lo, T. Mak, K. S. Leung, Y. Leung, and M. L. Meng, "A survey of wireless sensor network based air pollution monitoring systems," Sensors, vol. 15, no. 12, pp. 31392– 31427, 2015

[14] M. H. Anisi, G. Abdul-Salaam, and A. H. Abdullah, "A survey of wireless sensor network approaches and their energy consumption for monitoring farm fields in precision agriculture," Precision Agriculture, vol. 16, pp. 216–238, 2015.

[15] J. Kaur, T. Kaur, and K. Kaushal, "Survey on WSN routing protocols," International Journal of Computer Applications, vol. 109, no. 10, pp. 24–28, 2015.

[16] A. J. AL-Mousawi and H. K. AL-Hassani, "A survey in wireless sensor network for explosives detection," Computers & Electrical Engineering, vol. 72, pp. 682–701, 2018.

[17] A. Ali, Y. Ming, S. Chakraborty, and S. Iram,"A comprehensive survey on real-time applications of WSN," Future Internet, vol. 9, no. 4, Article ID 77, 2017.

[18] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: a survey, " Journal of Network and Computer Applications, vol. 60, pp. 192 –219, 2016.

[19] S. Abdollahzadeh and N. J. Navimipour, "Deployment strategies in the wireless sensor network: a comprehensive review, " Computer Communications, vol. 91-92, pp. 1 –16, 2016.

[20] A. Belfkih, C. Duvallet, and B. Sadeg, "A survey on wireless sensor network databases, " Wireless Networks, vol. 25, no. 8, pp. 4921 –4946, 2019.

[21] M. Sha fiq, H. Ashraf, A. Ullah, and S. Tahira, "Systematic literature review on energy efficient routing schemes in WSN — a survey, " Mobile Networks and Applications, vol. 25, pp. 882 – 895, 2020.

[22] J. Amutha, S. Sharma, and J. Nagar, "WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: review, approaches and open issues, " Wireless Personal Communications, vol. 111, pp. 1089 –1115, 2020.

[23] H. Sharma, A. Haque, and F. Blaabjerg, "Machine learning in wireless sensor networks for smart cities: a survey, " Electronics , vol. 10, no. 9, Article ID 1012, 2021.

[24] N. Temene, C. Sergiou, C. Georgiou, and V. Vassiliou, " A survey on mobility in wireless sensor networks, " Ad Hoc Networks, vol. 125, Article ID 102726, 2022.

[25] J. Paruvathavardhini and B. Sargunam, "Stochastic bat optimization model for secured WSN with energy-aware quantized indexive clustering, " Journal of Sensors, vol. 2023, Article ID 4237198, 16 pages, 2023.

[26] S. V. G, R. Nagarajan, and S. Kannadhasan, "Performance analysis of blended NIDS model for network intrusion detection system in WSN, " in 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1 – 6, IEEE, Erode, India, February 2023.

[27] J. Paruvathavardhini, B. Sargunam, and R. Sudarmani, " A review on energy efficient routing protocols and security techniques for wireless sensor networks, " Applied Mechanics and Materials, vol. 912, pp. 55 – 75, 2023.

[28] M. Hosseinzadeh, J. Yoo, S. Ali et al., "A cluster-based trusted routing method using fire hawk optimizer (FHO) in wireless sensor networks (WSNs), " Scientific Reports, vol. 13, Article ID 13046, 2023.

[29] R. Dass, M. Narayanan, G. Ananthakrishnan et al., "A clusterbased energy-efficient secure optimal path-routing protocol for wireless body-area sensor networks, " Sensors, vol. 23, no. 14, Article ID 6274, 2023.

[30] Mainaud B., Gauthier V., and Afifi H., "Cooperative Communication for Wireless Sensors Network : A Mac Protocol Solution Cooperative Communication for Wireless Sensors Network : A Mac Protocol Solution WSC-MAC : A Cooperative Mac Protocol for Wireless Sensors Network," in Proceedings of 1 st IFIP Wireless Days, Dubai, pp. 1-5, 2008.

[31] Liu K., Wu S., Huang B., Liu F., and Xu Z., "A Power-Optimized Cooperative MAC Protocol for Lifetime Extension in Wireless Sensor Networks," Sensors, vol. 16, no. 10, pp. 1630, 2016.

[32] Nacef A., Senouci S., Ghamri-Doudane Y., and Beylot A., "COSMIC: A Cooperative MAC Protocol for WSN with Minimal Control Messages," in Proceedings of 4 th IFIP International Conference on New Technologies, Mobility and Security, Paris, pp. 1-5, 2011.