Scientific Research Publishing

Journal of Sensor Technology, 2025, 15(1), 14-25
https://www.scirp.org/journal/jst
ISSN Online: 2161-1238
ISSN Print: 2161-122X

An Energy-Efficient Cross-Layer Approach for Wireless Sensor Networks Security

Namwinwelbere Dabiré[1], Abdoul-Hadi Konfé[2], Pegdwindé Justin Kouraogo[1]

[1]Mathematics and Computer Science Laboratory (LAMI), Joseph KI-ZERBO University, Ouagadougou, Burkina Faso
[2]Laboratory of Algebra, Discrete Mathematics and Computer Science (LAMDI), Polytechnic School of Ouagadougou (EPO), Ouagadougou, Burkina Faso
Email: donmike980@gmail.com, ahkonfe@gmail.com, kouraogo@gmail.com

How to cite this paper: Dabiré, N., Konfé, A.-H. and Kouraogo, P.J. (2025) An Energy-Efficient Cross-Layer Approach for Wireless Sensor Networks Security. *Journal of Sensor Technology*, **15**, 14-25.
https://doi.org/10.4236/jst.2025.151002

Received: December 12, 2024
Accepted: January 23, 2025
Published: January 26, 2025

Abstract

Wireless sensor networks (WSN) represent an emerging technology that aims to offer major innovations in terms of capabilities. Their use is set to grow steadily in many areas. However, the resource limitations of sensor nodes are a major constraint, especially in terms of security. For this reason, extensive work has been conducted on designing security protocols, making a compromise between the level of security and resource consumption. Most of this work has been based on single-layer approaches that address the security problem at the level of a single layer of the OSI (Open Systems Interconnection) model. In this article, we address the security problem of WSN networks using cross-layer methodology to propose a multi-layer solution. In this solution, the principle is based on the interaction and collaboration of three adjacent layers (physical layer, link layer and network layer). It implements two intrusion detection agents: a local intrusion detection agent and a global intrusion detection agent. The solutions algorithm includes an initialization phase and a detection phase. Several simulations were carried out to demonstrate the feasibility and efficiency of this solution in terms of packet transmission rate and energy consumption in a network of twenty-two sensor nodes. By comparing our solution with those in the literature, we obtained a minimum packet transmission rate and energy consumption.

Keywords

WSN, Cross-Layer Approach, Intrusion Detection System, Security, Energy Efficiency

1. Introduction

The growing need for information and the rapid evolution of microelectronics

and wireless technologies have enabled the creation of small, low-cost (limited resources) electronic devices capable of collecting and processing information in an autonomous and flexible way. These devices can be interconnected and deployed on a large scale, giving rise to a new type of network known as a wireless sensor network (WSN). The development of WSNs was originally motivated by military applications (battle eld surveillance, enemy tracking, etc.). However, their remarkable performance in terms of reliability and low cost has led to a proliferation of their use in civilian applications (environmental monitoring, industry, home automation, health, etc.).

Wireless sensor networks are designed to operate in groups, cooperating to transmit collected data to a central point called a base station or sink. These are most often deployed randomly in hostile, unexplored areas, and must self-organize using wireless communications. The security of this type of network represents a major challenge, since strategic decisions can be made based on the information received by the sensor nodes. Their special characteristics make them highly vulnerable to malicious attacks. Indeed, RCSFs are generally deployed in unknown areas without any physical protection, making them easy to capture and compromise. What's more, the wireless communication environment makes it possible to eavesdrop on traffic exchanged within the network, opening up the horizon for many types of attacks. The limited resources of sensor nodes make the application of conventional security solutions inappropriate. So, in addition to offering a good level of security, security protocols dedicated to RCSFs must respect their resource limitations.

The concept of security in RCSFs is illustrated in **Figure 1** [1], which depicts the typical architecture of a wireless sensor network, including cluster heads and sensor nodes. Ensuring security in such networks involves not only protecting against external and internal attacks but also addressing resource constraints, such as energy depletion. Research by authors such as Aura *et al.* [2], Dimitriou *et al.* [3] and Deng *et al.* [4] has led to the development of security protocols with efficient energy management. These solutions consist of offering single-layer solutions, which address the problem of security and energy saving at the level of a single layer of the OSI model [5]. However, this situation is forcing us to explore new research horizons, including the cross-layer approach. The cross-layer approach is one of the most promising solutions in terms of security. This approach involves designing architecture-based protocols, with several layers of the protocol stack interacting (cross-layer architecture).

The aim of this paper is to propose a cross-layer intrusion detection system based on the interaction of three adjacent layers: network, link and physical. Among other things, we will characterize wireless sensor networks, identify the different types of attacks in this network, capitalize on the limitations of already existing solutions, evaluate the advantages of cross-layer in securing sensor networks and formulate a cross-layer-based solution that enables better security in sensor networks.

In the remainder of this article, we will first explain the theoretical background and state of the art of wireless sensor networks. Then, well discuss the details of the proposed solution. A section will also be devoted to analyzing the performance of the proposed detection system. In addition, a discussion will be made in the next section. Finally, we will conclude.

2. Methodological Approach

Securing sensor networks is a delicate task, given their particular characteristics. Proposing a solution based on a cross-layer approach, therefore, required the use of several methods.

Bibliographical Research

Literature review on sensor networks: This type of network is characterized by wireless communication, dynamic topology, low computing power, limited autonomy, fault tolerance and scaling factor [1].

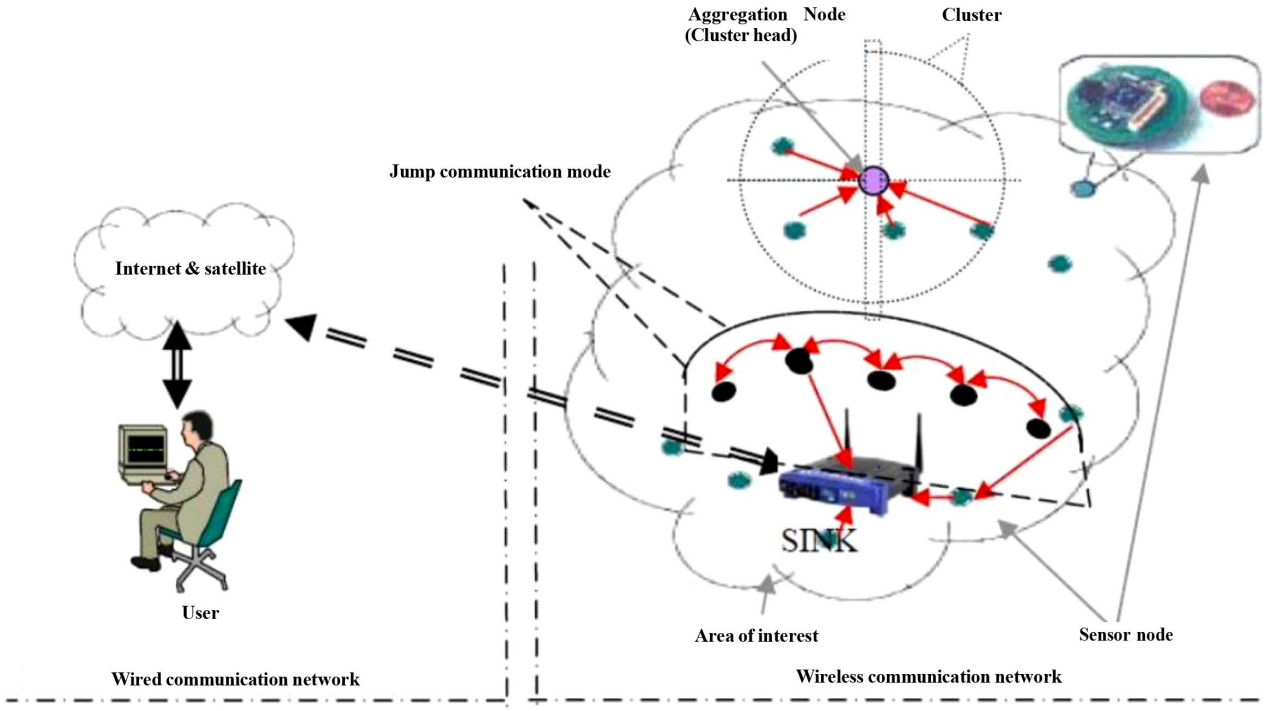

Figure 1. Sensor network [1].

A literature review of existing security mechanisms: Three main categories of attack exist: attacks classified according to their objectives, attacks classified according to the nature of the attacker and attacks classified according to the protocol layer Roosta *et al.* [5].

Table 1 summarizes existing security solutions for wireless sensor networks and their associated limitations [6]. This table provides context for why a cross-layer approach is necessary.

Table 1. Summary of solutions and their limitations [7].

Existing solutions	Limitations
Data encryption	Too costly in energy and storage
Generation key	Exclusion of normal nodes
Localization	Expensive and difficult to implement
Authentication protocol	Time constraint, excessive energy and storage consumption

As shown in Table 1, traditional solutions such as data encryption and authentication protocols are energy-intensive and unsuitable for resource-constrained wireless sensor networks. These limitations highlight the need for more efficient solutions, such as the proposed cross-layer approach, which optimizes resource usage while maintaining robust security. Figure 2 shows the classification of cross-layer architectures.

Literature review on cross-layer architecture: There are two types of cross-layer architecture. Motani and Sasanka *et al.* [8]. Three types of cross-layer approaches are adopted in sensor networks.

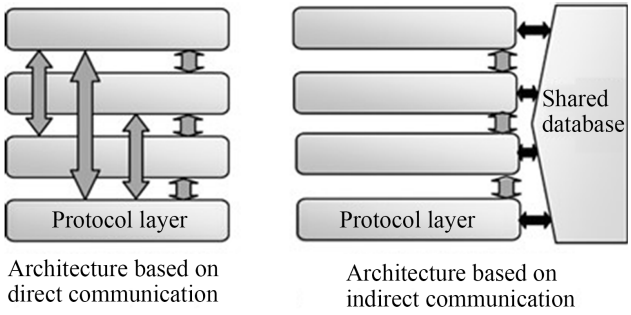

Figure 2. Classification of cross-layer architectures [8].

Literature review on cross-layer solutions: This less-explored field includes cross-layer protocols and cross-layer-based intrusion detection systems.

Table 2 presents three types of cross-layer approaches adopted in wireless sensor networks, detailing their characteristics and advantages.

Table 2. Cross-layer approaches [8].

Bottom-up approach	Communication from lower to higher layers
Top-down approach	Upper layers decide on configuration parameters of lower layers
Mixed (hybrid) approach	Optimum communication between layers

Table 2 categorizes cross-layer approaches into bottom-up, top-down, and mixed (hybrid) methodologies. The hybrid approach stands out as it allows optimal communication between layers, balancing resource efficiency and robust security. This classification justifies the design of the proposed system, which leverages

a hybrid approach for intrusion detection.

3. Proposed Solution

An interlayer-based intrusion detection system is proposed.

3.1. Basic Principle

Its operation is based on the interaction and collaboration of three adjacent layers: the network layer, the link layer and the physical layer. Inter-layer communications are carried out using an intermediary entity. This intermediate entity consists of an interaction interface, a cross-layer data module and an intrusion detection engine.

Interaction interface: This is made up of three interaction sub-interfaces (IR: Network Interface, IL: Link Interface and IP: Physical Interface) whose role is to collect detection information (routing table, PSR values) for the cross-layer data module.

Cross-layer data module: All data collected by the interaction interface is subsequently stored in the cross-layer data module. This module is responsible for creating the cross-layer Detection Information Table (TID) for use by the intrusion detection engine. The module is also responsible for updating the TID table via cross-layer interaction interfaces.

Intrusion detection engine: The cross-layer detection engine analyzes all incoming connection requests (RTS packets), based on a model of normal behavior created from the TID table. The intrusion detection algorithm used is very simple and does not require a great deal of computing power, making it suitable for RCSFs.

In this structural design, each individual sensor node integrates a localized Intrusion Detection Agent based on the Cross-Layer concept, referred to as ADIIC-L (Local Cross-Layer Intrusion Detection Agent). Furthermore, the installation of a Global Inter-Layer Intrusion Detection Agent (G-IDIA) at the base station is also required. The role of the ADIIC-L will be to detect intrusions at the local level of the sensor nodes, while the ADIIC-G agent will handle intrusion detection at the base station level.

3.2. Detection Algorithm

Figure 3 illustrates the architecture of the proposed intrusion detection system. The interaction interface collects data from network layers, while the cross-layer data module organizes this information into detection tables (TIDs). These tables are used by the intrusion detection engine to identify anomalies and ensure efficient intrusion detection. Building upon the architecture of the proposed system illustrated in Figure 3, Figure 4 focuses on the network architecture required to implement this system effectively. The interaction between nodes and the base station ensures seamless data collection and communication. Figure 4 depicts the network architecture used for implementing the proposed system. Sensor nodes

communicate with the base station using both wired and wireless connections. This hybrid design ensures flexibility and robustness in data transmission, which is critical for real-time intrusion detection. The flexibility and robustness of the network architecture shown in Figure 4 provide the foundation for the implementation of the intrusion detection algorithm described in Figure 5. The proposed intrusion detection algorithm operates in two essential phases: the initialization phase and the detection phase, as shown in Figure 5. The initialization phase involves the creation and updating of detection information tables (TIDs) and the activation of detection agents across the network nodes. In the detection phase, sensor nodes monitor incoming packets to identify intrusions. The detection algorithm runs periodically at both the network and physical layers, in parallel with the communication protocol.

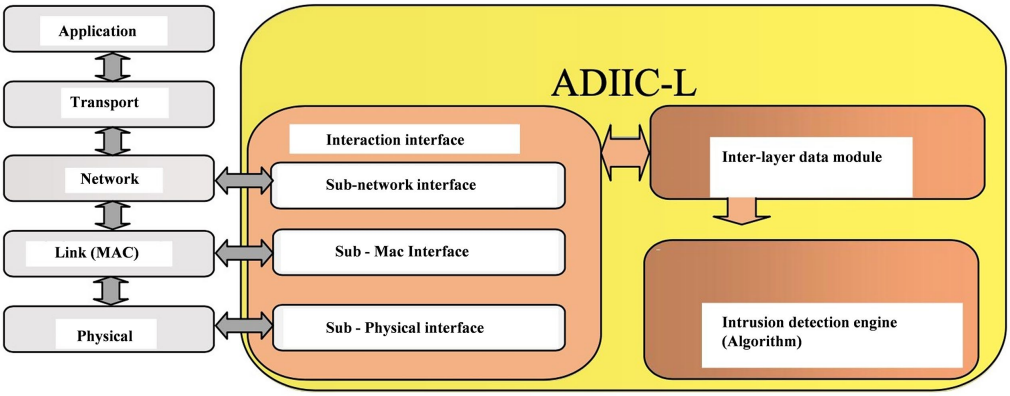

Figure 3. Architecture of the proposed solution.

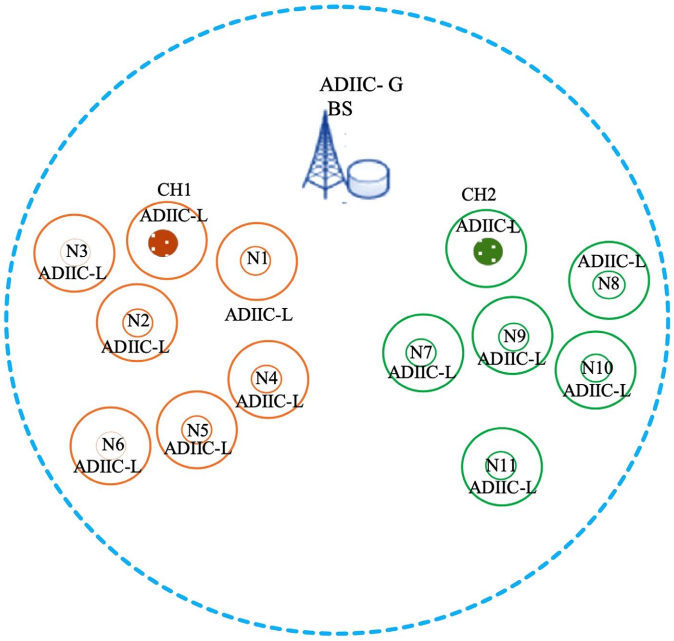

Figure 4. Network architecture showcasing hybrid communication modes and their integration into the proposed system.

The advantages of multilayer solutions are highlighted in Table 3, comparing them to single-layer methodologies.

Table 3. Cross-layer solutions and benefits [9].

Cross-layer solutions	Benefits
Cross-layer protocols	Collaboration between layers low energy and storage consumption
Intrusion detection system	Improved sensor network lifetime

The data in Table 3 emphasizes the collaboration between layers facilitated by cross-layer solutions, resulting in lower energy consumption and improved network lifetime. These findings align with the objectives of the proposed intrusion detection system, which prioritizes energy efficiency alongside robust security.

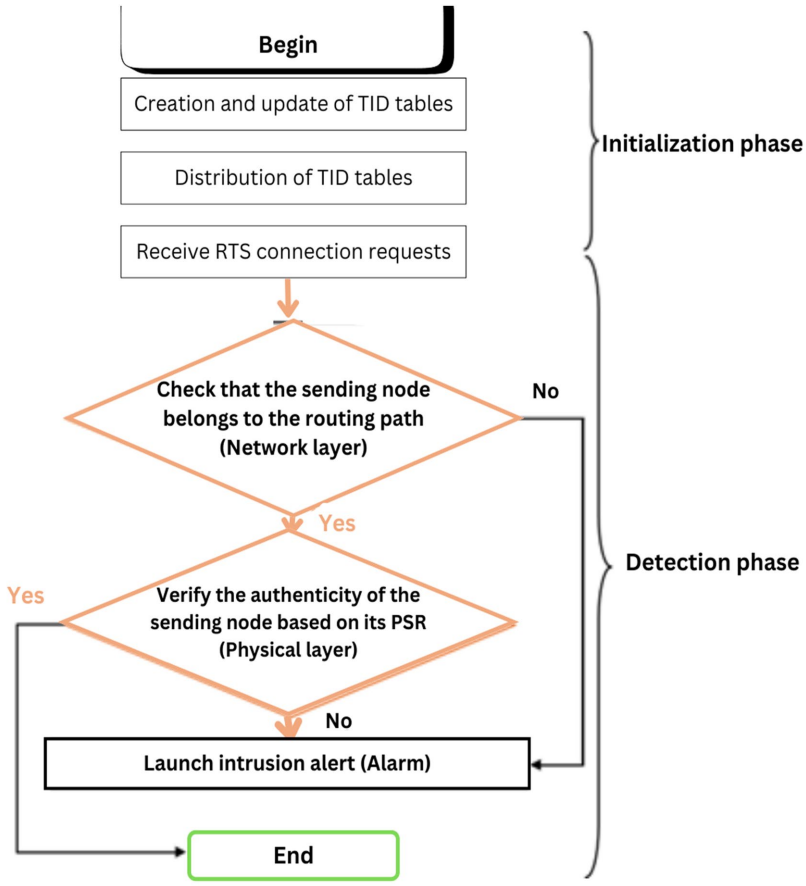

Figure 5. Detection algorithm.

3.3. Probability of Intrusion Detection

The probability of detecting an intruder node is considered a success, and the probability of failing to detect an intruder node is considered a failure. However, this probability of detection depends essentially on two factors: the number of

nodes attacked by malicious nodes, and the probability of not detecting an intrusion. We define the two variables Nat and P_{Det} to represent, respectively, the number of nodes attacked in the network, and the probability of intrusion detection.

We consider the scenario where a sensor node might fail to detect an intrusion if it does not receive any messages from the intruder node (passive attack). Consequently, the probability of not detecting an intrusion is equivalent to the probability of a collision occurring in the transmission link. This probability is defined by the variable P_{Col} (inspired by [1]).

Based on the Binomial distribution, we can define the probability of detecting a single intruder node $P_{\det}(x=1)$ among the number of attacked nodes (Nat) given by the following equation (inspired by [1]):

$$\boldsymbol{P}_{det}(\boldsymbol{x}=1)=\begin{pmatrix}\boldsymbol{Nat}\\ 1\end{pmatrix}(1-\boldsymbol{P}_{col})^{1}*(\boldsymbol{P}_{col})^{Nat-1} \tag{1}$$

Thus, the probability of detecting k intruder nodes is defined as follows (in spired by [1]):

$$\boldsymbol{P}_{det}(\boldsymbol{x}=1)=\begin{pmatrix}\boldsymbol{Nat}\\ \boldsymbol{k}\end{pmatrix}(1-\boldsymbol{P}_{col})^{k}*(\boldsymbol{P}_{col})^{Nat-k} \tag{2}$$

In the proposed DSIIC system, each sensor node can detect intrusions. The detection probability improves as the number of attacker nodes in the network increases. Energy consumption and packet transmission rates are critical metrics for evaluating wireless sensor networks. Low energy consumption ensures longer network lifetime, while high packet transmission rates indicate resilience against attacks.

4. Results

The simulation was conducted on a 22-node network with a static topology, under a black hole attack targeting packet routing. The network employed the AODV routing protocol with a constant bit rate (CBR) traffic model.

Figure 6 shows the simulated sensor network. This network is composed of 22 simulated sensor nodes. Table 4 summarizes the simulated network parameters.

Network layer performance: In order to analyze the behavior of the SDIIC against black hole attacks, we first measured the number of packets received by the BS. Figure 6 shows the simulation results in terms of packets received by the BS in the case of black hole attacks. As can be seen in Figure 7 (in the unsecured case), no message is delivered after 400 seconds of simulation. Table 4 outlines the parameters used during the simulation to evaluate the proposed system under black hole attack scenarios.

Table 4 provides detailed simulation parameters, including node count, topology, traffic rate, and routing protocol. These parameters were carefully chosen to simulate realistic attack conditions and evaluate the performance of the proposed system in terms of packet delivery rates and energy consumption.

Table 4. Simulated network parameters.

Number of network nodes	22
Base station	Node number 21
Base station coordinates	(1840; 424)
Number of intruder nodes	5
Number of clusters	3
Transmission bandwidth	1 Mbps
Data packet size	500 bytes
Activation packet size	130 bytes
RTS, CTS and ACK packet size	20 bytes
Simulation time	720 seconds
Traffic rate	Constant Bit Rate (CBR)
Routing protocol used	AODV
Amount of energy	2 Joules
Electrical energy	50 nJ/bit
Initialization phase execution time	Every 20 seconds

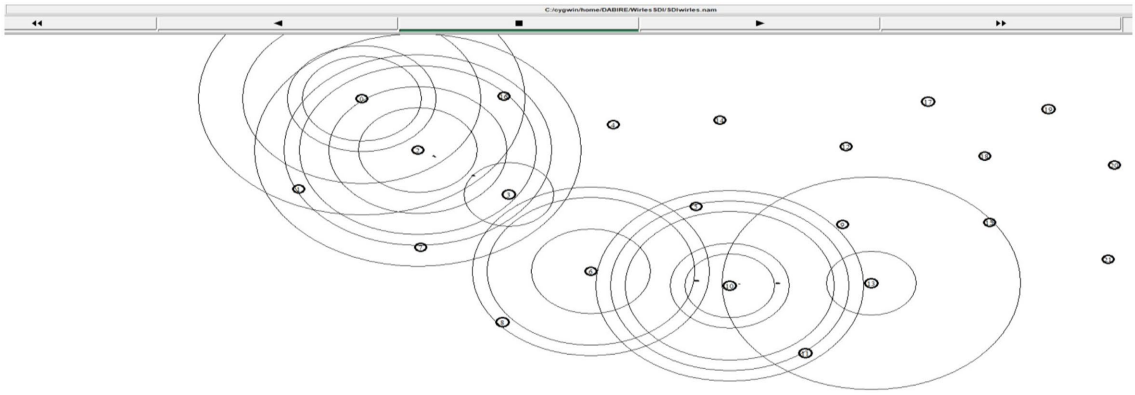

Figure 6. Simulated network.

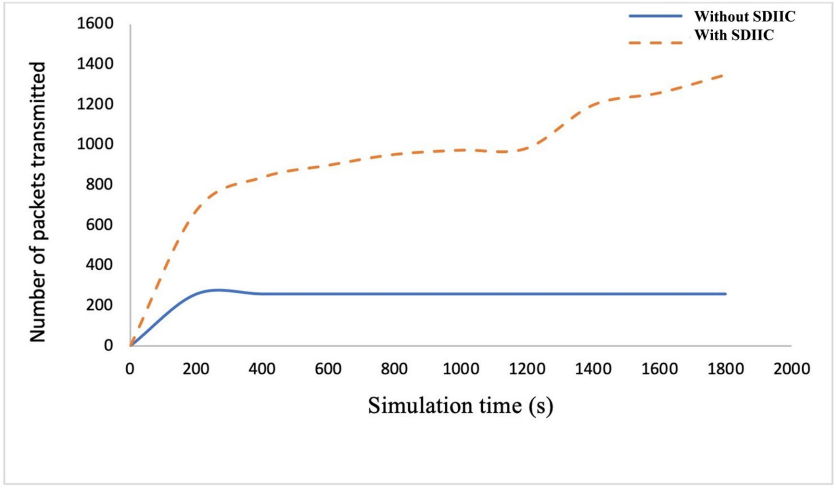

Figure 7. Evaluation of the number of packets under black hole attack.

Link layer performance: The energy dissipation of our security mechanism under broadcast attacks has been evaluated. Compared with the sensor network with SDIIC, our protocol can achieve better energy dissipation, given that the majority of energy-wasting problems are solved (unnecessary or abusive activation, passive listening...).

Physical layer performance: The curves in Figure 7 show the number of packet transmissions. It can be seen that no message will be transmitted to the base station after 650 seconds of the simulation in the case of the network without SDIIC.

5. Discussion

The packet transmission rate under attack conditions in a 22-node sensor network was analyzed to evaluate the performance of the intrusion detection system. This analysis is of vital interest since the primary objective of deploying a sensor network is to acquire information in a strategic area. The results of the present study show that packet transmission in the face of attacks is better with a variation of 200 to 1600 packets, compared with a variation of 200 to 600 for the unsecured network. Similarly, energy, a crucial parameter for the durability of a sensor network, improved in the secured network of twenty-two sensors. Simulation results prove that the energy dissipation of our cross-layer intrusion detection system offers a good level of security, while ensuring a low level of energy consumption. Figure 8 compares the energy consumption of the proposed system with a baseline solution under black hole attack scenarios. The results demonstrate the efficiency of the cross-layer approach in reducing unnecessary communication and optimizing resource usage. Figure 9 illustrates the packet transmission rates achieved by the proposed system under varying levels of attack severity. This metric reflects the system's ability to maintain data flow despite adversarial conditions.

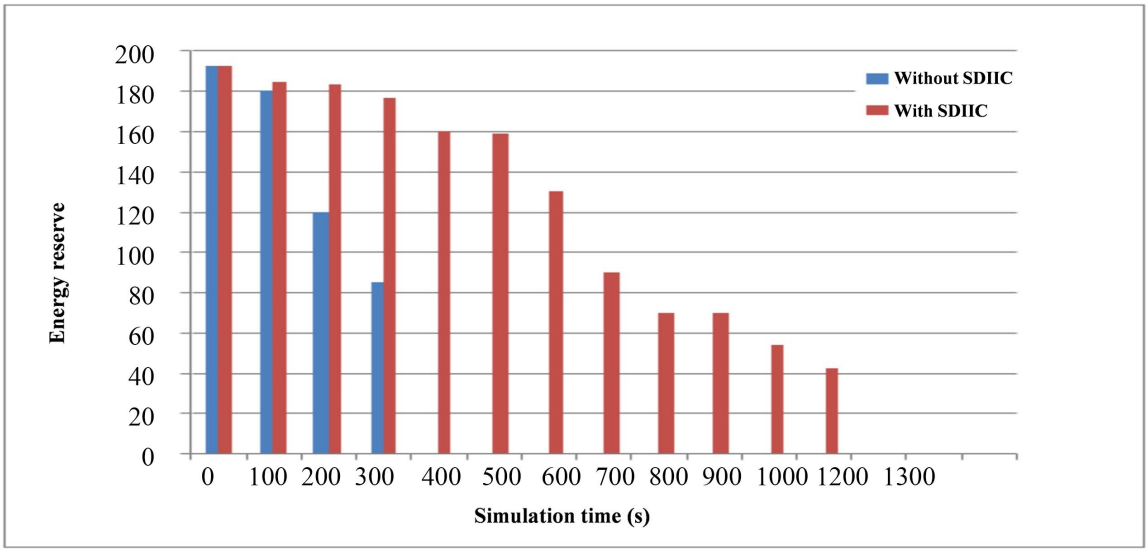

Figure 8. Energy consumption under broadcast attack.

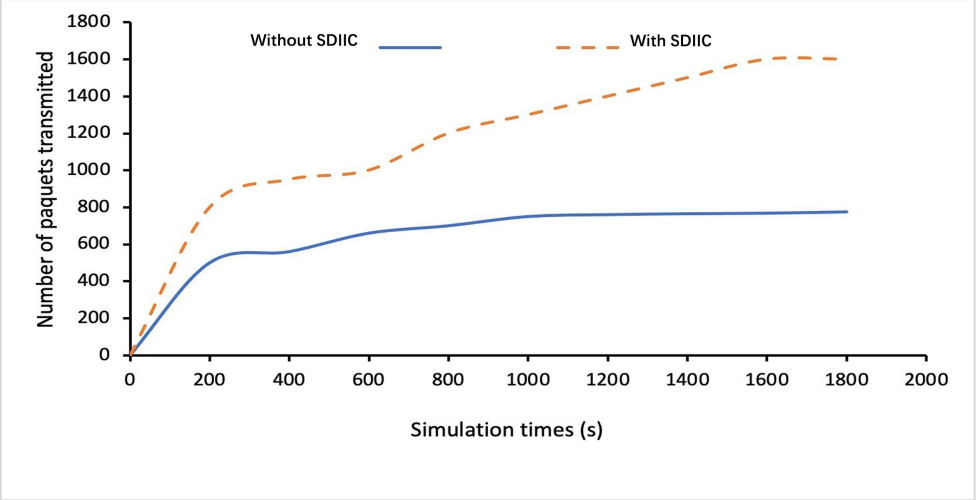

Figure 9. Evaluation of packet transmission rate in selective attack.

Authors such as [8] and [9], who addressed the same subject by simulating a network of 100 sensors, estimated packet transmission rates similar to ours. However, the order of performance of the protocols developed by Bouatia Wassila and Meziane Tani Fadia Selma remains lower than that of our proposed solution. Energy dissipation compared to that in the study by James Robert Harbin *et al.* [10] and Quentin Monnet *et al.* [11] who through their simulation of the MAC CROSS protocol with MATLAB offer similar results in terms of energy dissipation in diffusion attacks. The results demonstrate that the cross-layer approach significantly enhances resilience to black hole attacks, reducing energy consumption and improving packet delivery rates. These findings align with previous studies by Boubiche *et al.* and Rahhal *et al.* [9], who emphasized the importance of inter-layer communication in WSNs.

6. Conclusion

In this article, we have focused on the cross-layer approach in terms of security solutions for wireless sensor networks, a topic of current interest. The aim of this paper is to design a security solution based on the cross-layer approach while respecting the limitations of sensor networks. We have proposed an efficient multilayer solution. Simulation results have been interpreted to distinguish the difference and understand the behavior of the proposed solution. We also analyzed and evaluated the contributions performance in terms of safety and energy savings, using the NS2 simulator. The simulations carried out on this solution demonstrate its effectiveness in countering several types of attack at different layers of the OSI model. This proposal is a step forward in cross-layer approaches, which remain a tool for anticipating attacks on sensor networks.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Akyildiz, I.F., Su, W.L., Sankarasubramaniam, Y. and Cayirci, E. (2002) A Survey on Sensor Networks. *IEEE Communications Magazine*, **40**, 102-114. https://doi.org/10.1109/mcom.2002.1024422

[2] Aura, T., Nikander, P. and Leiwo, J. (2001) Dos-resistant Authentication with Client Puzzles. In: Christianson, B., Malcolm, J.A., Crispo, B. and Roe, M., Eds., *Security Protocols*. *Security Protocols* 2000, Springer, 170-177. https://doi.org/10.1007/3-540-44810-1_22

[3] Dimitriou, T. (2005) Efficient Mechanisms for Secure Inter-Node and Aggregation Processing in Sensor Networks. In: Syrotiuk, V.R. and Chávez, E., Eds., *Ad-Hoc, Mobile, and Wireless Networks*, Springer, 18-31. https://doi.org/10.1007/11561354_4

[4] Deng, H.M., Li, W. and Agrawal, D.P. (2002) Routing Security in Wireless Ad Hoc Networks. *IEEE Communications Magazine*, **40**, 70-75. https://doi.org/10.1109/mcom.2002.1039859

[5] Brownfield, M.I., Mehrjoo, K., Fayez, A.S. and Davis, N.J. (2006) Wireless Sensor Network Energy-Adaptive Mac Protocol. CCNC 2006. 2006 3*rd IEEE Consumer Communications and Networking Conference*, 2006, Las Vegas, 8-10 January 2006, 778-782. https://doi.org/10.1109/ccnc.2006.1593145

[6] Eschenauer, L. and Gligor, V.D. (2002) A Key-Management Scheme for Distributed Sensor Networks. *Proceedings of the* 9*th ACM Conference on Computer and Communications Security*, Washington DC, 18-22 November 20024, 1-47. https://doi.org/10.1145/586110.586117

[7] Misra, S., Bhattarai, K. and Xue, G. (2011) Bambi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. 2011 *IEEE International Conference on Communications* (*ICC*), Kyoto, 5-9 June 2011, 1-5. https://doi.org/10.1109/icc.2011.5962856

[8] Srivastava, V. and Motani, M. (2005) Cross-Layer Design: A Survey and the Road Ahead. *IEEE Communications Magazine*, **43**, 112-119. https://doi.org/10.1109/mcom.2005.1561928

[9] Rahhal, H.A., Ali, I.A. and Shaheen, S.I. (2011) A Novel Trust-Based Cross-Layer Model for Wireless Sensor Networks. 2011 28*th National Radio Science Conference* (*NRSC*), Cairo, 26-28 April 2011, 1-10. https://doi.org/10.1109/nrsc.2011.5873629

[10] Harbin, J.R., *et al.* (2012) The Sybil Attack in Sensor Networks: Analysis Defenses. *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks* (*IPSN*04), Berkeley, 26-27 April 2004, 259-268.

[11] Monnet, Q. and Mokdad, L. (2015) Dos Detection in WSNs: Energy Efficient Designs and Modeling Tools for Choosing Monitoring Nodes. In: Obaidat, M.S., Nicopolitidis, P. and Zarai, F., Eds., *Modeling and Simulation of Computer Networks and Systems*, Elsevier, 795-840. https://doi.org/10.1016/b978-0-12-800887-4.00028-6