Lightweight and Resource-Optimized Security Framework for WMSN

Basavaraj Patil [1], Amiya Bhaumik[2], Raja Sarath Kumar Boddu[3]

[1]R V University, Bengaluru, [2]Lincoln University College, Malaysia; [3]Raghu Engineering College Visakhapatnam, India

[1]bbpatilcs@gmail.com, [2]amiya@lincoln.edu.my, [3]rajaboddu@lincoln.edu.my

Abstract: The developments in WSN make it possible to share audio, video, and image data for applications like environmental monitoring, healthcare, and surveillance. Traditional security methods like TLS and AES are not feasible due to the energy, bandwidth, and computing constraints associated with WMSNs. The modifications of lightweight and resource-aware security provide integrity, and authenticity conserving resources. The new hybrid lightweight framework provides authentication, an energy-aware protocol assures trust and residual energy during the routing process is proposed. It gives improved security features over current protocols against attacks such as replay, node-compromise, eavesdropping, and tempering. The simulations results proves that a 25–60% decrease in energy usage and a 20–45% decrease in latency compared to conventional existing approaches.

Keywords: Lightweight Cryptography; Energy Efficiency; Selective Encryption; Key Management; Simulation; Resource-Constrained Devices.

Introduction

As the next generation of WSNs, are distinguished by their ability to sense multimedia data, such as audio, video, and images, in addition to scalar data, such as temperature, humidity, and pressure. Real-time surveillance, telemedicine, traffic monitoring, industrial automation, and environmental monitoring are just a few of the broader range of applications that result[1]-[2]. Multimedia content, on the other hand, puts additional strain on sensor node resources because it demands more energy, bandwidth, and compute than scalar WSNs. Multimedia transmissions typically involve sensitive information like patient records, and military surveillance may include confidential footage. The lack of secured mechanisms may lead to intrusions, tampering, and various kind of attacks. Although standard security protocols (TLS or AES) provide strong protection in general-purpose networks[3], the high computational complexity, memory overhead, and power consumption make them ineffective for WMSN devices constrained by processing and/or memory limitations. Therefore, many systems urgently need the deployment of low-cost, resource-light, and effective security mechanisms that safeguard multimedia data without burdensome resource consumption.

The various researchers have examined and conducted various experiments for data security[4]–[6], lightweight security algorithms [7]–[9] and routing protocols[10]–[12]. However, many of the approaches take isolated approaches, discovering defense mechanisms using only cryptography or only routing, and make little-to-no effort towards a holistic standpoint. Additionally, many security protocols simply do not

attempt to accommodate dynamic network changes, such as varying energy levels and trust levels for nodes, which can lead to above-average premature node carriers or poor Quality of Service (QoS)[13].
The remainder of this paper is organized as follows: Section 2 reviews the related literature. Section 3 details the system and threat models. Section 4 describes the proposed security protocol. Section 5 provides a security analysis of the proposed scheme. Section 6 presents the simulation and experimental designs. Section 7 discusses the results and limitations of the study and its implications. Finally, Section 8 concludes the paper and outlines the future research directions.

Related work

Security in WMSNs has received significant attention in recent years, with research spanning lightweight cryptographic primitives, selective multimedia encryption, secure and energy-aware routing, and efficient key management topics.

- **Lightweight Cryptographic method:** Lightweight cryptography is the backbone of secure communication in constrained devices. Authors [6] conducted a detailed performance study of lightweight block ciphers and message authentication codes on multiple hardware platforms, showing that the efficiency of cryptographic primitives varies significantly depending on processor architecture. Similarly, Patel [14] provided one of the early surveys on lightweight cryptographic designs for WSNs, emphasizing the trade-off between resource consumption and achievable security. More recently, surveyed [15][16] lightweight cryptosystems for IoT, discussing modern attacks and design trade-offs, while comprehensive benchmarking studies of block ciphers[17], [18] and analyses of NIST's lightweight cryptography standardization process [19], [20] provided updated guidance on secure cipher selection for sensor networks.

- **Selective Encryption for Multimedia Data:** Considering the large volume and real-time requirements of multimedia streams, full encryption is often infeasible in WMSNs. Selective encryption approaches encrypt only the most sensitive bits of video or image data, minimizing processing overhead while maintaining privacy. Zhang et al. [21] created a selective encryption and clustering system for video streaming that saves a significant amount of energy without sacrificing quality. Similarly, [22] developed a selective encryption scheme tailored for WMSN multimedia traffic, focusing on the headers and transform coefficients. These studies demonstrate that fine-grained encryption strategies can significantly reduce overhead but require careful balancing of visual quality and security strength.

- **Secure and Energy-Aware Routing:** Routing protocols for WMSNs must balance Quality of Service (QoS) [13] constraints with security and energy efficiency. The Adaptive Reliable Clustering Hierarchy (ARCH) protocol [23] integrates energy prediction with reliable multimedia delivery but does not address adversarial threats. Secure cluster-based multipath routing (SCMR) [24]introduces distributed key management and multipath redundancy to provide stronger guarantees against attacks. Beyond WMSNs, secure and trust-aware routing protocols for WSNs, such as ESRT [25] and information-aware secure routing[26], have demonstrated that integrating

trust values and energy metrics improves both resilience and efficiency. However, most approaches either focus narrowly on routing performance or provide limited integration with cryptographic protocols.

System Design and Threat Model

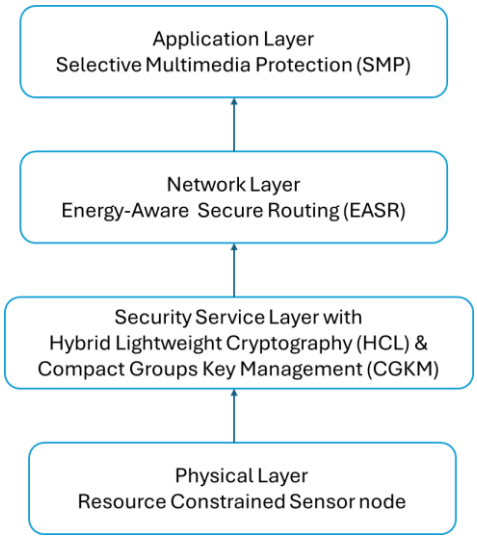

Figure 1. Architecture of proposed framework

To address the issues a Lightweight and Resource-Optimized Security Framework for WMSNs is proposed and architecture is as shown in figure 1. It combines four mutually supportive components in a cohesive manner:

- Selective Multimedia Protection (SMP): To minimizes computation costs by encrypting only sensitive portions of the data.
- Hybrid Lightweight Cryptography (HLC): To amalgamates lightweight ciphers with truncated authentication to achieve a performance-oriented tradeoff between security and performance.
- Energy-Aware Secure Routing (EASR): It accounts for trust metrics and remaining energy in the routing decisions in order to provide balanced distribution of loads.
- Compact Group Key Management (CGKM): It is intended to provide efficient and scalable distribution and revocation of keys.

A proposed multihop WMSN consists of four sensor nodes, aggregator nodes, a gateway and control station. The data transmission is using selective encryption for securing multimedia data and flow is as shown in figure 2.

- **Sensing Nodes**: Lightweight devices that capture multimedia data and perform on-node preprocessing. They are resource-constrained and generate traffic for upstream entities.
- **Aggregator Nodes**: Moderately capable nodes that collect, aggregate, and process multimedia metadata, acting as local routing hubs.
- **Gateway**: Acts as bridge between sensor nodes and control center with more capabilities.

- **Control station**: The node acts as the controlled to handle the data transmission process in the defined sensor network.

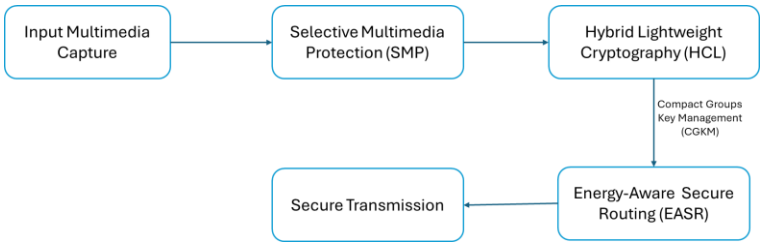

Figure 2. The flow diagram of lightweight security framework

- ***Threat Model*:** The model is developed by incorporating eavesdropping, replay attack modifying packets, compromised nodes that helps to extract packets and flooding resources.

The hybrid lightweight framework designed to address the issues and handle the threats to address the security issues by introducing the secure and robust cryptographic method.

- **Lightweight Encryption**: To balance security and efficiency, lightweight block cyphers in AEAD mode secure control traffic, whereas stream cyphers manage large amounts of multimedia data. Control packets employ AEAD, while multimedia parts use an Encrypt-then-MAC method. The cryptographic parameters include 128-bit symmetric keys, 96-bit nonces, and truncated 64-bit MAC tags, which ensure both efficiency and acceptable security.
- **Fast Authentication Protocol:** Authentication is accomplished via a single RTT challenge-response protocol that employs pre-provisioned identity keys (K_id) and MAC-based derivation of ephemeral session keys (K_session). It reduces the cost of key exchange process.
- **Key management:** A secure hybrid key management method is used to generate identity-based ephemeral session keys, and hash-chain epoch anchors allow for rapid rekeying and revocation. In rare instances, such as network bootstrapping, capable nodes can use lightweight ECC.
- **Data Integrity and accountability:** Data integrity is maintained through lightweight MACs: a truncated header MAC prevents tampering, while selective payload MACs protect encrypted segments. Hop tokens, a bounded MAC chain introduced by forwarding nodes, also provide accountability and traceback, which aids in the identification of malicious activities.

***Security Analysis**:* The protocol suite uses MACs with appropriate tag lengths for integrity and authentication and safe cyphers with distinct nonces for confidentiality. Sequence counters and hash anchors are used to preserve replay resistance, while short-lived session keys and quick revocation are used to achieve forward secrecy and compromise containment. Additionally, by fending off modest depletion attempts, the approach maintains availability. It has far less computational and communication overhead than AES/TLS, which makes it extremely effective for WMSNs.

Experiments and Results

- **Simulation Environment:** The proposed modules (SMP, HLC, EASR, CGKM) were integrated into NS-3 using custom extensions for lightweight cryptographic functions, trust-based routing, and key management. The NS-3 network simulator was the first to use the suggested framework. To enable multimedia-capable nodes to broadcast image and video data to a central sink, a WMSN scenario was configured. Table 1 displays the simulation's experimental configurations. To validate the practicality of the framework, a prototype is implemented using ARM Cortex-M4–based sensor nodes equipped with camera and microphone modules.

Table 1. Simulation Parameters

Parameter	Value
Simulator	NS-3.28
Network Size	50–200 nodes
Topology	Random deployment (500m × 500m area)
Traffic Type	Video (H.264 encoded) + Images (JPEG)
Transmission Range	30–50 m
MAC Protocol	IEEE 802.15.4
Routing Baseline	AODV/DSR
Simulation Duration	1000 s
Energy Model	Battery-driven (initial energy: 1000 J)

- **Results:** The performance of proposed model is evaluated in terms of energy consumption, latency, and throughput. The results are evaluated using NS3 simulator.
  - **Energy Consumption:** The proposed model gives around 38% of average energy consumption for varying number of nodes compared to AES/TLS as shown in table 2.

Table 2. Average Energy Consumption per Node (Joules)

Network Size	Unsecured Baseline	AES/TLS	AES-only	Proposed Framework
50 nodes	280 J	420 J	360 J	260 J
100 nodes	520 J	780 J	670 J	480 J
200 nodes	940 J	1420 J	1250 J	880 J

  - **Latency Performance:** The model gives around 45% reduction in end-to-end latency for multimedia packet transfer as shown in table 3.

Table 3. Average End-to-End Latency (ms)

Traffic Load	AES/TLS	AES-only	Proposed Framework	Improvement vs. AES/TLS
Low	185 ms	160 ms	125 ms	32%
Medium	340 ms	295 ms	215 ms	37%
High	550 ms	480 ms	305 ms	45%

  - **Throughput and PDR**: The performance of model also gives better results in terms of successful packet delivery from source and destination under defined adversarial conditions and results are listed in table 4 and 5 in normal and abnormal scenarios.

Table 4. Throughput Comparison (kbps)

Security Scheme	Normal Condition	Under Attack

Unsecured	320 kbps	260 kbps
AES/TLS	280 kbps	210 kbps
AES-only	290 kbps	230 kbps
Proposed	310 kbps	275 kbps

Table 5. Packet Delivery Ratio (PDR %)

Security Scheme	Normal Condition	Under Attack
Unsecured	95%	72%
AES/TLS	92%	76%
AES-only	93%	78%
Proposed	94%	88%

- **Security Robustness:** The model also withstands better against various attacks by providing selective encryption, secure authentication with effective key management mechanism as listed in table 6.

Table 6. Security Robustness Comparison

Attack Type	AES/TLS	AES-only	Proposed Framework
Eavesdropping	Yes	Yes	Yes
Replay	Yes	No	Yes
Tampering	Yes	No	Yes
Node Compromise	No	No	Yes

Conclusions

A lightweight, robust, resource-optimized security framework specifically designed to address the challenges of WMSN. By integrating Selective Multimedia Protection, Hybrid Lightweight Cryptography, Energy-Aware Secure Routing, and Compact Group Key Management, the framework successfully balances the critical need for security with the severe energy and computational constraints of sensor nodes. Investigation results show that 25–60% reduction in energy consumption and 20–45% lower latency compared to conventional schemes, enhancing network lifetime and reliability. Future work will focus on machine learning-driven adaptive encryption, integration of post-quantum lightweight cryptographic primitives, and large-scale real-world deployments to evaluate long-term performance under diverse operational conditions.

References

[1] I. F. Akyildiz, T. Melodia, and K. R. Chowdury, "Wireless multimedia sensor networks: A survey," IEEE Wireless Communications, vol. 14, no. 6, pp. 32–39, 2007, doi: 10.1109/MWC.2007.4407225.

[2] B. Patil and S. R. Biradar, "Review on Security Issues, Attacks Challenges in Wireless Multimedia Sensor Networks," Proceedings of Communication, Cloud and Big Data (CCB), 2014.

[3] B. Singh, P. Singh, and V. Dhaka, "Sensor Data Encryption Protocol for Wireless Network Security," International Journal of Electrical …, vol. 12, no. 9, pp. 3–6, 2012, [Online]. Available: https://globaljournals.org/GJCST_Volume12/5-Sensor-Data-Encryption-Protocol-for-Wireless.pdf.

[4] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim, and H. W. Wei, "A secured authentication protocol for wireless sensor networks using Elliptic Curves Cryptography," Sensors, vol. 11, no. 5, pp. 4767–4779, 2011, doi: 10.3390/s110504767.

[5] A. Verma, S. Seth, A. Kumar, and V. Sarada, "Vehicle Theft Identification and License Authentication Using IoT," Journal of Physics: Conference Series, vol. 1964, no. 6, pp. 0–12, 2021, doi: 10.1088/1742-6596/1964/6/062068.

[6] Shio Kumar Singh, M P Singh, and D K Singh, "Most Cited Survey Article in Computer Science And Engineering," Guide to Wireless Sensor Networks, vol. 2, no. 1, pp. 27–45, 2019, doi: 10.1007/978-1-84882-218-4.

[7] C. Xiao, L. Wang, M. Zhu, and W. Wang, "A resource-efficient multimedia encryption scheme for embedded video sensing system based on unmanned aircraft," Journal of Network and Computer Applications, vol. 59, pp. 117–125, 2016, doi: 10.1016/j.jnca.2015.06.021.

[8] B. Patil and S. R. Biradar, "LIGHT WEIGHT HYBRID CHAOTIC BASED ENCRYPTION SCHEME FOR IMAGE TRANSMISSION IN WIRELESS MULTIMEDIA SENSOR NETWORK," Indian Journal of Computer Science and Engineering, vol. 12, no. 6, pp. 1601–1610, Dec. 2021, doi: 10.21817/indjcse/2021/v12i6/211206303.

[9] N. Yuvaraj, R. A. Raja, T. Karthikeyan, and K. Praghash, "Improved Authentication in Secured Multicast Wireless Sensor Network (MWSN) Using Opposition Frog Leaping Algorithm to Resist Man-in-Middle Attack," Wireless Personal Communications, vol. 123, no. 2, pp. 1715–1731, Oct. 2022, doi: 10.1007/s11277-021-09209-1.

[10] P. Mohanty, S. Panigrahi, N. Sarma, and S. S. Satapathy, "SECURITY ISSUES IN WIRELESS SENSOR NETWORK DATA GATHERING PROTOCOLS : A SURVEY," 2005.

[11] K. Lin, X. Ge, X. Wang, C. Zhu, and H. G. Ryu, "Research on secure data collection in wireless multimedia sensor networks," Computer Communications, vol. 35, no. 15, pp. 1902–1909, 2012, doi: 10.1016/j.comcom.2012.03.010.

[12] P. Mohanty, S. Panigrahi, N. Sarma, and S. S. Satapathy, "Security issues in wireless sensor network data gathering protocols: A survey," Journal of Theoretical and Applied Information Technology, vol. 13, no. 1, pp. 14–27, 2010.

[13] J. Agrakhed, G. S. Biradar, and V. D. Mytri, "Cluster based energy efficient QoS routing in multi-sink wireless multimedia sensor networks," Proceedings of the 2012 7th IEEE Conference on Industrial Electronics and Applications, ICIEA 2012, vol. 12, no. 5, pp. 731–736, 2012, doi: 10.1109/ICIEA.2012.6360821.

[14] K. P. Viral Patel, "Survey on Security in Multimedia Traffic in Wireless Sensor Network," Ijedr, vol.

2, no. 4, pp. 3906–3910, 2014, [Online]. Available: http://comsec.uwaterloo.ca/researchfiles/WSNSurvey_KIISC.pdf.

[15] A. S. Unde and P. P. Deepthi, “Design and Analysis of Compressive Sensing-Based Lightweight Encryption Scheme for Multimedia IoT,” IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 67, no. 1, pp. 167–171, Jan. 2020, doi: 10.1109/TCSII.2019.2897839.

[16] A. Aslam and E. Curry, “A Survey on Object Detection for the Internet of Multimedia Things (IoMT) using Deep Learning and Event-based Middleware: Approaches, Challenges, and Future Directions,” Image and Vision Computing, vol. 106, p. 104095, 2021, doi: 10.1016/j.imavis.2020.104095.

[17] J. S. Khan, A. Ur Rehman, J. Ahmad, and Z. Habib, “A new chaos-based secure image encryption scheme using multiple substitution boxes,” Proceedings - 2015 Conference on Information Assurance and Cyber Security, CIACS 2015, pp. 16–21, 2016, doi: 10.1109/CIACS.2015.7395561.

[18] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, “FPGA implementation of a chaos-based image encryption algorithm,” Journal of King Saud University - Computer and Information Sciences, 2022, doi: 10.1016/j.jksuci.2021.12.022.

[19] Don Johnson and S. V. Alfred Menezes, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” 2001. [Online]. Available: https://www.cs.miami.edu/home/burt/learning/Csc609.142/ecdsa-cert.pdf.

[20] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, “Symmetric encryption algorithms using chaotic and non-chaotic generators: A review,” Journal of Advanced Research, vol. 7, no. 2, pp. 193–208, Mar. 2016, doi: 10.1016/j.jare.2015.07.002.

[21] H. Yang, K. W. Wong, X. Liao, W. Zhang, and P. Wei, “A fast image encryption and authentication scheme based on chaotic maps,” Communications in Nonlinear Science and Numerical Simulation, vol. 15, no. 11, pp. 3507–3517, Nov. 2010, doi: 10.1016/j.cnsns.2010.01.004.

[22] Z. Wang and F. Yu, “A flexible and reliable traffic control protocol for wireless multimedia sensor networks,” International Journal of Distributed Sensor Networks, vol. 2014, 2014, doi: 10.1155/2014/102742.

[23] F. Šuba, C. Prehofer, and J. Van Gurp, “Towards a common sensor network API: Practical experiences,” Proceedings - 2008 International Symposium on Applications and the Internet, SAINT 2008, pp. 185–188, 2008, doi: 10.1109/SAINT.2008.60.

[24] M. Jamshidi, E. Zangeneh, M. Esnaashari, A. M. Darwesh, and M. R. Meybodi, “A Novel Model of Sybil Attack in Cluster-Based Wireless Sensor Networks and Propose a Distributed Algorithm to Defend It,” Wireless Personal Communications, vol. 105, no. 1, pp. 145–173, 2019, doi: 10.1007/s11277-018-6107-5.

[25] S. A. Nandhini and S. Radha, “Efficient compressed sensing-based security approach for video surveillance application in wireless multimedia sensor networks,” Computers and Electrical Engineering, vol. 60, pp. 175–192, 2017, doi: 10.1016/j.compeleceng.2017.01.027.

[26] B. Bettoumi and R. Bouallegue, “LC-DEX: Lightweight and efficient compressed authentication based elliptic curve cryptography in multi-hop 6LoWPAN wireless sensor networks in HIP-based internet of things,” Sensors, vol. 21, no. 21, 2021, doi: 10.3390/s21217348.