Cryptographic load sharing method in critical infrastructure sensor networks

Emil Faure[1,2,*,†], Inna Rozlomii[1,†] and Serhii Naumenko[3,†]

[1]Cherkasy State Technological University, Shevchenko Blvd., 460, Cherkasy, 18006, Ukraine

[2]State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, M. Zaliznyaka Str., 3/6, Kyiv, 03142, Ukraine

[3]Bohdan Khmelnytsky National University of Cherkasy, Shevchenko Blvd., 81, Cherkasy, 18031, Ukraine

Abstract

This paper presents an adaptive method for distributing cryptographic tasks across nodes in sensor networks operating under constrained conditions of critical infrastructure systems. The proposed approach addresses the challenge of resource-aware encryption by introducing a utility-based decision-making algorithm that evaluates each node's residual energy level, current computational load, communication latency, and topological role (e.g., relay, aggregator). A composite utility index is calculated for every candidate node using normalized metrics and empirically determined weight coefficients. The node with the highest utility value is selected to execute the cryptographic operation. The method ensures balanced load distribution and prevents congestion of critical nodes by assigning lower priority to those serving routing or aggregation functions. Additionally, a hybrid encryption strategy is supported: energy-constrained nodes utilize lightweight cryptographic algorithms such as Ascon, GIFT-COFB, and TinyJAMBU, while high-performance nodes are capable of executing more robust or layered encryption schemes. A built-in fallback mechanism allows the procedure to restart in case the selected executor node becomes unavailable, thereby enhancing the system's resilience and adaptability. To evaluate the effectiveness of the proposed method, experimental modeling was conducted using ESP32-S3 microcontroller platforms. The results demonstrate reduced average energy consumption, improved task delegation efficiency, and scalability of the algorithm in local cluster environments. A flowchart of the task delegation procedure and a comparative chart of strategy performance based on load balancing criteria are presented. The method is applicable to secure data transmission in sensor-based monitoring systems within critical infrastructure domains.

Keywords

sensor networks, critical infrastructure, lightweight cryptography, load balancing, STM32, energy efficiency

1. Introduction

Data protection in critical infrastructure is one of the priority areas of modern cybersecurity [1]. Critical infrastructure objects include energy, transport, water supply, financial, medical and telecommunications systems that ensure the sustainability of the functioning of the state and society. They are increasingly actively integrating sensor networks to monitor, analyze and control key technological processes.

Sensor nodes that are components of such networks are characterized by low power consumption, limited RAM, low clock frequency and dependence on autonomous power sources [2]. Because of this, they are vulnerable to attacks, especially when processing and transmitting critical data. Standard centralized approaches to encryption often overload such devices, which leads to rapid battery discharge, network delays and potential system failures [3].

The disadvantages of centralized schemes, in particular the creation of a single point of failure, excessive load on individual nodes and uneven distribution of computing resources, increase the need for adaptive and distributed approaches to protection [4, 5]. In this regard, it is advisable to use models in which the cryptographic load is distributed between nodes taking into account their current energy

CH&CMiGIN'25: Fourth International Conference on Cyber Hygiene & Conflict Management in Global Information Networks, June 20–22, 2025, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

e.faure@chdtu.edu.ua (E. Faure); inna-roz.ukr.net (I. Rozlomii); sergey.naumenko94@vu.cdu.edu.ua (S. Naumenko)
0000-0002-2046-481X (E. Faure); 0000-0001-5065-9004 (I. Rozlomii); 0000-0002-6337-1605 (S. Naumenko)

state, computing potential and role in the overall network structure. The use of centralized encryption in sensor networks of critical infrastructure is accompanied by a number of problems caused by the limited resources of the nodes themselves and the influence of external factors. Each node operates under conditions of limited battery capacity, limited processor and memory performance, and is also subjected to load due to the complexity of encryption algorithms, the amount of transmitted data and the frequency of exchange [6]. Such a configuration leads to overload, delays and potential failures in the network, Figure 1.

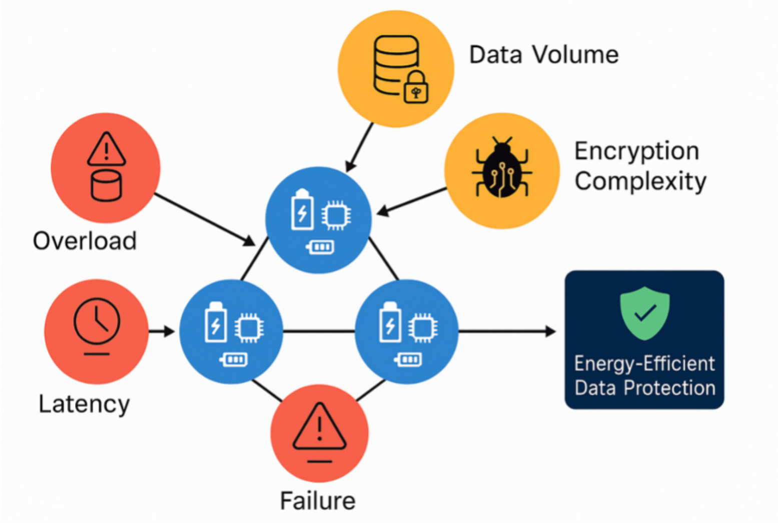


Figure 1: Problems of centralized protection in sensor networks.

As shown on Figure 1, the combined effect of resource constraints and external load factors leads to critical consequences that threaten the stability of the entire network. Achieving energy-efficient data protection is possible only if the current capabilities of the nodes are taken into account and a dynamic approach to distributing cryptographic operations is applied.

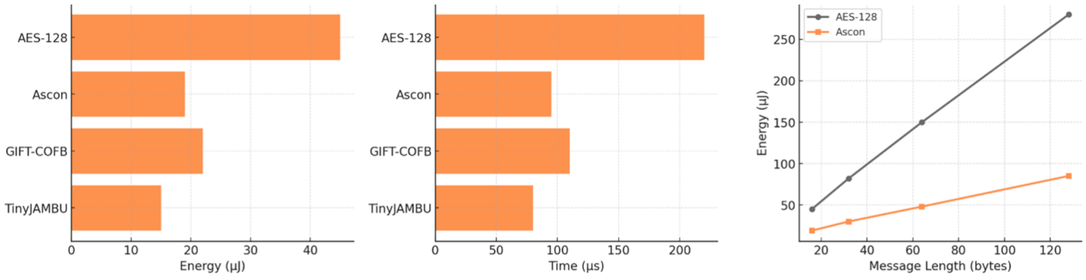
The aim of the research is to develop a method for effectively distributing the cryptographic load between the nodes of a sensor network, taking into account their energy state, computing resources and topological role. The proposed approach ensures optimization of the use of node resources and increases the stability of critical infrastructure networks during encryption operations.

2. Theoretical background and related works

Information security in sensor networks used in critical infrastructure remains an active research topic in the scientific community [7, 8]. The main focus is on the development of energy-efficient solutions capable of providing a high level of protection under conditions of limited hardware resources. The issues of constructing cryptographic protocols for devices with limitations in terms of computing power, memory and power are discussed in works [9, 10, 11], which emphasize the need to abandon classical algorithms in favor of lightweight cryptographic primitives.

In particular, works [12, 13, 14] investigate the impact of the chosen encryption algorithm on energy consumption and data processing time in nodes such as STM32, ESP32 and the like. The authors of [15] note that the use of AES-128 even in a simplified implementation leads to significant energy losses in autonomous sensor devices.

Figure 2 illustrates the comparative characteristics of power consumption and execution time of modern cryptographic algorithms when implemented on the STM32 microcontroller, which is widely used in embedded critical infrastructure systems. The graph also shows the change in power consumption depending on the message length for the AES-128 and Ascon algorithms.



a)

b)

c)

Figure 2: Comparison of crypto algorithms by power consumption and performance on STM32: a) power consumption per 128-bit block; b) encryption execution time; c) dependence of power consumption on message length.

The graph shows that the Ascon, GIFT-COFB, and TinyJAMBU algorithms provide a significant reduction in power consumption and processing time compared to AES-128. These results confirm the feasibility of using lightweight ciphers in sensor devices with limited power resources.

In response to these challenges, standardized lightweight algorithms are actively developed, in particular, Ascon (selected by NIST as the main standard [16]), GIFT-COFB, and TinyJAMBU, which demonstrate a better balance between security and power consumption [17].

In parallel, research is ongoing on the analysis of energy models of computations in sensor nodes. In [18], a model is presented that takes into account three main components of power consumption: encryption, data transmission, and query processing. The results of the research confirm that the transmission phase is the most energy-consuming, but encryption becomes critical if it is centralized.

Approaches to dynamically distributing computations in the network are also gaining popularity. Works [19, 20] propose concepts for distributing cryptographic load depending on the current energy state of nodes. This allows not only to avoid overloading individual components, but also to extend the overall network lifetime. In the context of security of distributed computing environments, approaches to optimizing applications in container orchestration systems deserve attention. In work [21], it is demonstrated how strategic choice of the scheduler can increase the security of application execution by taking into account the context of the environment, resources and isolation characteristics. In [22], a software platform for comparing load balancing strategies in orchestration systems is presented, which allows evaluating trade-offs between efficiency, task distribution uniformity and impact on resource consumption. Despite the fact that these studies focus on containerized systems, the principles of dynamically taking into account the current characteristics of nodes inherent in them can be effectively adapted for sensor networks with limited resources.

However, despite the existence of individual solutions, a single model has not yet been formed that would comprehensively take into account the interaction between the network structure, the state of the nodes' energy resources, and the choice of protection algorithms. Solving this problem requires further research in the direction of modeling the relationship between data security and energy costs, taking into account the real load and limitations of devices in the critical infrastructure environment.

3. Problem statement and model design

The problem of data protection in sensor networks of critical infrastructure is the need to ensure confidentiality and integrity of information under conditions of limited node resources [23]. Traditional centralized approaches involve performing cryptographic operations in the coordination center or on the nodes closest to it [24]. In such schemes, the computational load quickly accumulates, which leads to overloading of individual components, increased delays and increased energy consumption.

In order to eliminate these shortcomings, a model of dynamic distribution of cryptographic load between sensor nodes is proposed, which takes into account the following factors:

- current level of residual energy of the node;
- computing capacity and speed;
- role of the node in the network topology (border, intermediate, coordination);
- volume of input/output data that requires protection.

The proposed model is implemented in the form of a system of rules for assigning cryptographic load. When a request for data protection is received, the network selects the optimal executing node based on the above criteria. In case of excessive load or critical battery level, another node may be designated as the initiator.

The architecture of the network, in which distributed processing and encryption are implemented, is shown in Figure 3. The diagram takes into account the interaction of sensor nodes with different levels of available resources and illustrates the process of delegating cryptographic operations between nodes within the same cluster.

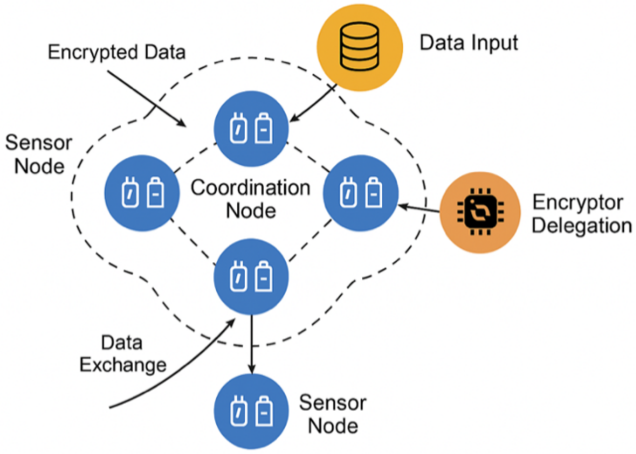


Figure 3: Sensor network architecture with dynamic cryptographic load distribution.

Unlike the static architecture depicted in Figure 3, the functional diagram in Figure 4 details the sequence of actions between the initiator, potential executors, and the selected node that performs encryption. It allows you to track the entire request processing cycle - from task formation to returning an encrypted message, taking into account dynamic resource evaluation and decision-making. Fig. 4 shows a generalized diagram of the interaction of nodes within one secure exchange. It demonstrates the process of initialization, resource evaluation, executor selection, data transmission for encryption, and return of the result.

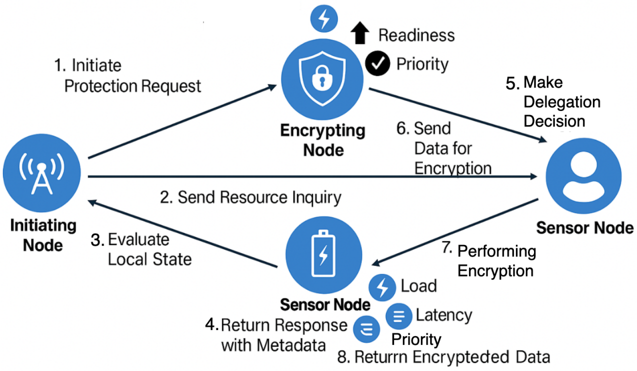


Figure 4: Scheme of interaction of sensor nodes during distribution of cryptographic tasks.

Within the critical infrastructure sensor network, a model has been implemented in which each node can act as both a data source (initiator) and a potential executor of a cryptographic operation. The interaction between nodes for data protection includes the following stages:

1. Initiation of a data protection request. The initiator sensor node generates a message that needs to be encrypted. It starts the procedure for evaluating available nodes within the local cluster.
2. Transmission of a resource assessment request. The initiator sends requests to neighboring nodes to collect information about their current energy level, computational load, and delays.
3. Nodes evaluate their own state. Each node calculates local metrics: remaining battery charge, number of active tasks, processor power, encryption processing time.
4. Transmission of responses with metadata. Nodes send metadata (not the data itself) to the initiator: resource assessment, priority, readiness to perform a cryptographic operation.
5. Making a delegation decision. The initiator, having received the responses, selects an executor node based on a multi-criteria function (for example, a weighted estimate of energy, delay, and load).
6. Transferring data for encryption. The message that requires encryption is transferred to the selected executor node.
7. Performing encryption. The selected node applies the appropriate cryptographic algorithm (for example, Ascon) to the transmitted data.
8. Returning encrypted data. The encrypted message is returned to the initiator node or sent directly to the recipient in the network (depending on the topology).

To implement the model presented in Figure 4, it is necessary to formalize the criteria used when selecting a node to delegate a cryptographic operation. This allows the solution to be adapted to the load conditions, the current state of energy consumption and the role of the nodes in the network. The corresponding rules are given in Table 1.

Table 1
Criteria for Selecting a Node to Perform a Cryptographic Operation

Criterion	Eligibility conditions	Influence on choice
Remaining battery charge	$> 40\%$	High priority
Encryption execution time	< 100 µs	Medium priority
Available load on the node	< 3 active tasks	High priority
Role in the network	Not a critical router	Medium priority
Distance to initiator	≤ 2 transitions	Medium/low

The development of such criteria allows for flexible adaptation of the model to the current state of the network, ensuring both minimization of energy consumption and increased resistance to overloads.

4. Proposed method

Based on the previous analysis, a method for selecting a cryptographic operation executor in critical infrastructure sensor networks is proposed. The method is implemented as a decision-making procedure that uses a set of criteria and weighting factors determined taking into account the energy state, load, and role of the nodes.

The process of delegating a cryptographic task is initiated when the initiator node generates a request for data protection. Then the following sequence of actions is performed:

1. The initiator sends a broadcast request to neighboring nodes with a request to provide meta-information about their state.
2. Each recipient node evaluates local parameters (remaining charge, delays, load, role in the network) and generates a response.

3. The initiator calculates the integral utility index U_i for each node i.

$$U_i = w_1 \cdot E_i + w_2 \cdot (1 - L_i) + w_3 \cdot (1 - T_i) + w_4 \cdot R_i \tag{1}$$

where: E_i is the normalized remaining battery charge; L_i is the normalized current load; T_i is the normalized delay estimate R_i is a binary parameter indicating the desired role (1 — acceptable role, 0 — critical router); w_1, w_2, w_3, w_4 are weights determined empirically or adaptively.
Increasing the value of w_1 leads to the advantage of energy-saturated nodes, while w_3 reduces the response waiting time.
After calculating the integral indicator U_i for each node, the initiator selects the executor. To demonstrate the practical application of formula (1), an example of calculating U_i for four candidate nodes is given in Table 2. The input data was obtained from experimental modeling of the operating conditions of a sensor network with STM32 microcontrollers, using typical values of energy parameters and delays given in [25, 26].
As can be seen from Table 2, the highest value of the integral indicator is for Node A, which indicates its priority as the executor of the cryptographic operation in this scenario. In this case, not only the energy resource is taken into account, but also the current load, delays and the role of the node in the network. This approach ensures adaptability to the real conditions of the sensor network.

Table 2
Calculating the Utility Index Ui for Candidate Nodes

Node *i*	Energy E_i	Load L_i	Delay T_i	Role R_i	U_i
Node A	0.80	0.30	0.25	1	0.84
Node B	0.60	0.10	0.40	1	0.79
Node C	0.70	0.50	0.20	0	0.71
Node D	0.50	0.20	0.15	1	0.75

4. The node with the maximum value of U_i is assigned as the executor of the cryptographic task.
5. In the event of equality of several indicators, the selection is made according to an additional criterion – minimum delay or closest location.

In the event of failure of the selected node, it is possible to re-initialize the procedure with the exclusion of the inaccessible node. This property increases the fault tolerance and adaptability of the system.

An important feature of the proposed approach is the consideration of the role of the node in the topology. In particular, nodes that perform the functions of relays or data aggregators, as a rule, have a higher level of load. Their assignment as cryptographic task executors can lead to overload and routing failures. Therefore, such nodes receive a reduced priority in the evaluation process $(R_i = 0)$.

In addition, the method supports a hybrid cryptographic strategy that involves choosing the type of algorithm depending on the current state of the node. Nodes with limited energy potential or high load automatically use lightweight cryptographic algorithms such as Ascon, GIFT-COFB, or TinyJAMBU [27, 28, 29]. These lightweight algorithms were recommended by NIST in 2023 as a basis for applications with limited resources [30, 16]. More productive nodes can use full-featured algorithms or multiple encryption.

This approach allows you to reduce the average energy consumption in the network, extend the autonomous operation of sensor nodes, and reduce the risk of overloading critical nodes.

The proposed method is scalable, since the calculation of the integral indicator U_i is performed only at the local cluster level. This allows avoiding global synchronization and maintaining efficiency as the number of nodes in the network increases. Its computational complexity is linear: $O(n)$, where n is the number of candidate nodes for the task.

The sequence of implementation of the procedure for selecting an executor of a cryptographic task is shown in Figure 5. The flowchart covers the main stages: request initiation, collection of meta-information about the state of the nodes, calculation of the integral utility index, selection of the optimal executor, delegation of the task, and return of the encryption result. This approach provides adaptability to the current state of the network and optimization of resource consumption.

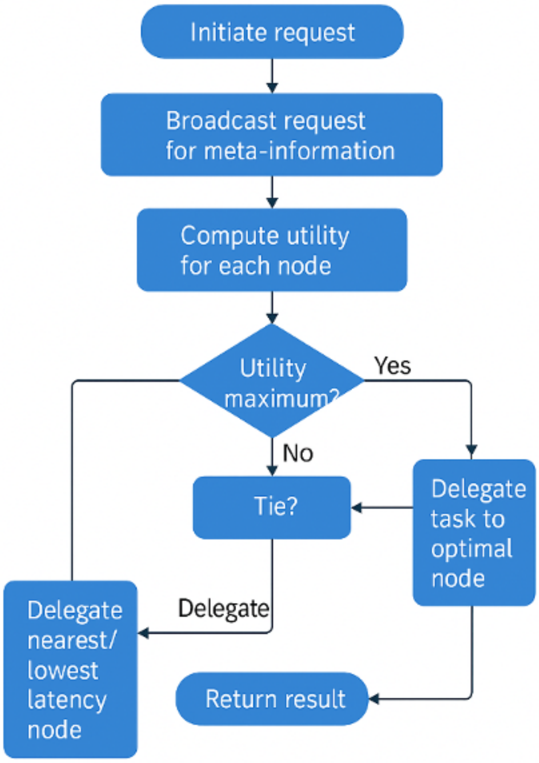

Initiate request
Broadcast request for meta-information
Compute utility for each node
Utility maximum?
Yes
No
Tie?
Delegate task to optimal node
Delegate
Delegate nearest/ lowest latency node
Return result

Figure 5: Flowchart of the algorithm for selecting a cryptographic task executor in a sensor network.

As shown in Figure 5, the algorithm starts with the initialization of a request for data protection. The initiator node sends a broadcast request to its neighbors to collect meta-information about their current state. Each sensor node calculates local metrics – the level of residual energy, latency, load, and its role in the topology – and sends this information to the initiator.

Based on the collected information, the initiator calculates an integral utility metric for each candidate node. If no unique leader is found and several nodes have the same U_i value, an additional stage – Tie – is performed, in which an additional selection criterion is applied. This can be the minimum latency, the distance to the initiator, or the energy efficiency of the selected algorithm.

After the final determination of the executor, the initiator passes the data to it for encryption. After the cryptographic operation is completed, the encrypted message is returned to the initiator node or sent directly to the next recipient. This scheme allows you to reduce the load on individual nodes, avoid overloads, and ensure long-term stability of the network operation in conditions of limited resources.

5. Experimental evaluation

To verify the effectiveness of the proposed model, an experimental simulation of a sensor network was conducted using STM32F103C8T6 boards (the so-called “Blue Pill”), built on the ARM Cortex-M3 core [31]. These boards are widely used in embedded systems due to their good balance between performance and power consumption. The microcontrollers of this series operate at a frequency of up to 72 MHz, have 20 KB of RAM and 64 KB of flash memory, support low-power modes, and operate at a supply voltage of 2.0–3.6 V, which corresponds to the operating conditions of autonomous sensor nodes [32]. In the test network, eight nodes were simulated, which were dynamically combined into clusters of up to five devices. Network interaction included the transmission of encrypted messages with a length of 128 to 1024 bits, using the AES-128 (in a simplified implementation) and Ascon algorithms – in accordance with NIST requirements for resource-dependent devices [33]. To assess the power consumption of each node, an INA219 digital current sensor was used, and to measure processing and encryption delays – software profiling on the microcontrollers themselves.

During the experiment, the load levels on the nodes were varied by emulating additional tasks, and the residual power charge was gradually reduced to analyze the adaptability of the model to changing conditions. This allowed us to obtain a realistic assessment of the effectiveness of the proposed approach in conditions close to operation in critical infrastructure.

To assess the effectiveness of the developed method, a series of tests were conducted, during which three approaches to delegating cryptographic tasks in a sensor network were compared:

- centralized encryption on one fixed node;
- random assignment of an executor among available nodes;
- proposed method with dynamic executor selection based on multi-criteria utility function.

Each experiment consisted of 100 cycles of message encryption of different lengths (128, 256 and 512 bits) in a network with active nodes that had different levels of charge and load. The main evaluation metrics were: average energy consumption of one encryption cycle, execution delay and percentage of uniformity of load distribution between nodes.

The results of the experiment are shown in Figure 6. The graphs compare the dynamics of energy consumption, processing time and the degree of load of nodes depending on the selected delegation strategy. As can be seen, the proposed model demonstrates the lowest average energy consumption among all options and at the same time provides moderate delay, significantly reducing the peak load on individual nodes.

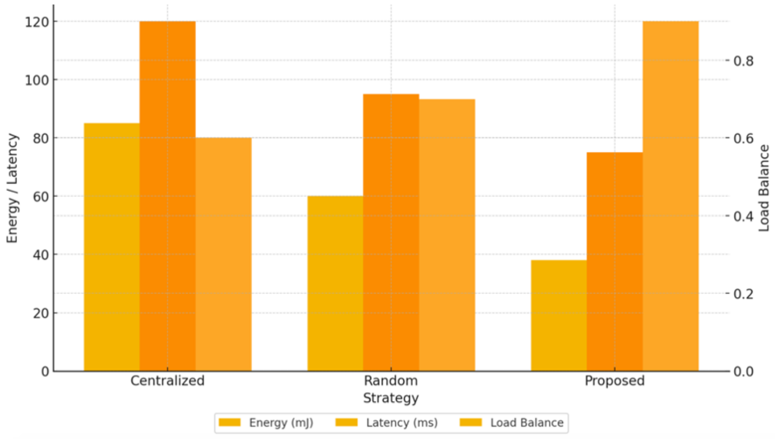


Figure 6: Comparison of Load Distribution Approaches.

The advantage of a dynamic multi-criteria selection strategy is that it adapts to the current state of the network, which allows maintaining stable performance even in cases of degradation of individual nodes. In addition, uniform load distribution contributes to the extension of the overall system life, which is a critical factor for application in autonomous operation conditions in critical infrastructure facilities.

6. Discussion

The proposed method of distributing cryptographic load in sensor networks of critical infrastructure allows to achieve adaptive balancing between the level of information protection and resource constraints of nodes. Its key difference is the consideration of a set of relevant metrics when choosing a cryptographic operation executor: the energy state of the node, computational load, latency and role in the network topology.

Experimental results have demonstrated a decrease in the average load on central and relay nodes, which helps to reduce the risk of overloads and increases the stability of network routes. Delegating calculations to less loaded and energy-efficient nodes that do not perform critical routing functions ensures the extension of the autonomous operation of the network.

An important advantage of the method is the support of a hybrid cryptographic strategy. This allows nodes to independently choose a cryptographic algorithm depending on their current state, for example, to use lightweight algorithms (Ascon, GIFT-COFB) in the case of limited resources. This approach reduces energy consumption without compromising security characteristics.

The method also provides fault tolerance of the system: in case of loss of connection with the selected node, the procedure can be initiated again with the exclusion of the unavailable participant. This is especially important for use in critical infrastructure, where the failure of a single node should not lead to failures in the functioning of the entire system.

The scalability of the solution has been confirmed by simulation tests: the calculation of the integral indicator is performed locally, without the need for global synchronization, which makes the method suitable for large decentralized networks.

7. Conclusions

The article proposes a method for distributing cryptographic load in sensor networks of critical infrastructure, which takes into account the current energy state of nodes, the level of their computational load, latency and role in the network topology. The method is implemented as an adaptive procedure for delegating cryptographic operations to nodes that are able to effectively perform these tasks, taking into account their own resources.

The simulation results have demonstrated the effectiveness of the approach: reduced energy consumption, load balancing, increased fault tolerance and reduced risk of overloading of key nodes were achieved. In addition, the use of a hybrid cryptographic strategy with a dynamic choice between full-featured and lightweight algorithms (in particular, Ascon, GIFT-COFB, TinyJAMBU) allowed adapting protection to the current state of computing resources.

The proposed method demonstrates scalability, since it works within the local cluster and does not require global synchronization. Its application can be extended to other classes of distributed systems with limited resources, including unmanned systems and medical sensor networks.

Acknowledgements

This research was funded by the Ministry of Education and Science of Ukraine under grant 0123U100270.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] E. Faure, I. Rozlomii, A. Yarmilko, S. Naumenko, Protection of iot networks: cryptographic solutions for cybersecurity management, in: Proceedings of the Third International Conference on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN 2024), volume 3925 of *CEUR Workshop Proceedings*, 2024, pp. 24–34.

[2] O. Kanoun, S. Bradai, S. Khriji, G. Bouattour, D. El Houssaini, M. Ben Ammar, C. Viehweger, Energy-aware system design for autonomous wireless sensor nodes: A comprehensive review, Sensors 21 (2021) 548.

[3] Z. Huanan, X. Suping, W. Jiannan, Security and application of wireless sensor network, Procedia Computer Science 183 (2021) 486–492.

[4] K. Madhuri, A new level intrusion detection system for node level drop attacks in wireless sensor network, Journal of Algebraic Statistics 13 (2022) 159–168.

[5] J. S. Al-Azzeh, M. A. Hadidi, R. S. Odarchenko, S. Gnatyuk, Z. Shevchuk, Z. Hu, Analysis of self-similar traffic models in computer networks, International Review on Modelling and Simulations 10 (2017) 328–336. doi:10.15866/iremos.v10i5.12009.

[6] S. Urooj, S. Lata, S. Ahmad, S. Mehfuz, S. Kalathil, Cryptographic data security for reliable wireless sensor network, Alexandria Engineering Journal 72 (2023) 37–50.

[7] S. Daousis, N. Peladarinos, V. Cheimaras, P. Papageorgas, D. D. Piromalis, R. A. Munteanu, Overview of protocols and standards for wireless sensor networks in critical infrastructures, Future Internet 16 (2024) 33.

[8] M. Zaliskyi, R. Odarchenko, S. Gnatyuk, Y. Petrova, A. Chaplits, Method of traffic monitoring for DDoS attacks detection in e-health systems and networks, in: CEUR Workshop Proceedings, volume 2255, 2018, pp. 193–204.

[9] I. Rozlomii, A. Yarmilko, S. Naumenko, Innovative resource-saving security strategies for iot devices, Journal of Edge Computing (2025). URL: https://doi.org/10.55056/jec.748.

[10] S. Pandey, B. Bhushan, Recent lightweight cryptography (lwc) based security advances for resource-constrained iot networks, Wireless Networks 30 (2024) 2987–3026.

[11] P. Singh, B. Acharya, R. K. Chaurasiya, Lightweight cryptographic algorithms for resource-constrained iot devices and sensor networks, in: Security and Privacy Issues in IoT Devices and Sensor Networks, Academic Press, 2021, pp. 153–185.

[12] H. H. Pham, D. C. Bui, N. V. H. NGUYEN, V. H. Le, Q. T. Dinh, V. P. Hoang, Side-channel attack on implementation of aes t-box encryption on stm32 microcontroller board, in: 2024 1st International Conference On Cryptography And Information Security (VCRIS), IEEE, 2024, pp. 1–6.

[13] S. Seniman, B. Siregar, R. M. Pelle, F. Fahmi, Securing sensor data transmission with ethernet elliptic curve cryptography secure socket layer on stm32f103 device, Indonesian Journal of Electrical Engineering and Computer Science 22 (2021) 507–515.

[14] J. Soto-Cruz, E. Ruiz-Ibarra, J. Vázquez-Castillo, A. Espinoza-Ruiz, A. Castillo-Atoche, J. Mass-Sanchez, A survey of efficient lightweight cryptography for power-constrained microcontrollers, Technologies 13 (2024) 3.

[15] M. Al-Mashhadani, M. Shujaa, Iot security using aes encryption technology based esp32 platform, International Arab Journal of Information Technology 19 (2022) 214–223.

[16] I. Elsadek, E. Y. Tawfik, Efficient programable architecture for lwc nist fips standard ascon, in: 2024 12th International Symposium on Digital Forensics and Security (ISDFS), IEEE, 2024, pp. 1–5.

[17] T. Sun, D. Shen, S. Long, Q. Deng, S. Wang, Neural distinguishers on tinyjambu-128 and gift-64, in: International Conference on Neural Information Processing, Springer Nature Singapore, Singapore, 2022, pp. 419–431.

[18] S. Sivakumar, J. Logeshwaran, R. Kannadasan, M. Faheem, D. Ravikumar, A novel energy optimization framework to enhance the performance of sensor nodes in industry 4.0, Energy Science & Engineering 12 (2024) 835–859.

[19] D. S. Misbha, Lightweight key distribution for secured and energy efficient communication in wireless sensor network: An optimization assisted model, High-Confidence Computing 3 (2023) 100126.

[20] Y. Cheng, Y. Liu, Z. Zhang, Y. Li, An asymmetric encryption-based key distribution method for wireless sensor networks, Sensors 23 (2023) 6460.

[21] Y. V. Voievodin, I. O. Rozlomii, Advanced software framework for comparing balancing strategies in container orchestration systems, in: Proceedings of the doors-2024: 4th Edge Computing Workshop, volume 3666 of *CEUR Workshop Proceedings*, 2024, pp. 60–69.

[22] Y. Voievodin, I. Rozlomii, Application security optimization in container orchestration systems through strategic scheduler decisions, in: CPITS-2024: Cybersecurity Providing in Information and Telecommunication Systems, volume 3654 of *CEUR Workshop Proceedings*, 2024, pp. 471–478.

[23] Y. K. Saheed, O. H. Abdulganiyu, T. Ait Tchakoucht, A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and scada systems for smart city infrastructures, Journal of King Saud University - Computer and Information Sciences 35 (2023) 101532.

[24] G. M. Makrakis, C. Kolias, G. Kambourakis, C. Rieger, J. Benjamin, Industrial and critical infrastructure security: Technical analysis of real-life security incidents, IEEE Access 9 (2021) 165295–165325.

[25] Z. Pan, L. Wang, D. Liu, Design of home energy saving monitoring system based on stm32, in: 2024 6th International Conference on Computer Communication and the Internet (ICCCI), IEEE, 2024, pp. 193–199.

[26] B. Ravelo, M. Guerin, W. Rahajandraibe, V. Gies, L. Rajaoarisoa, S. Lallechere, Low-pass ngd numerical function and stm32 mcu emulation test, IEEE Transactions on Industrial Electronics 69 (2021) 8346–8355.

[27] M. Ul Islam, M. Nazish, I. Sultan, M. Tariq Banday, Ascon lightweight security standard for the internet of things devices—a study, in: International Conference On Innovative Computing And Communication, Springer Nature Singapore, 2024, pp. 503–517.

[28] A. Caforio, D. Collins, S. Banik, F. Regazzoni, A small gift-cofb: lightweight bit-serial architectures, in: International Conference on Cryptology in Africa, Springer Nature Switzerland, Cham, 2022, pp. 53–77.

[29] O. Dunkelman, S. Ghosh, E. Lambooij, Full round zero-sum distinguishers on tinyjambu-128 and tinyjambu-192 keyed-permutation in the known-key setting, in: International Conference on Cryptology in India, Springer International Publishing, Cham, 2022, pp. 349–372.

[30] Y. Averyanova, et al., UAS cyber security hazards analysis and approach to qualitative assessment, in: S. Shukla, A. Unal, J. V. Kureethara, D. Mishra, D. Han (Eds.), Data Science and Security, volume 290 of *Lecture Notes in Networks and Systems*, Springer, Singapore, 2021, pp. 258–265. doi:10.1007/978-981-16-4486-3_28.

[31] M. Barton, R. Budjac, P. Tanuska, I. Sladek, M. Nemeth, Advancing small and medium-sized enterprise manufacturing: Framework for iot-based data collection in industry 4.0 concept, Electronics 13 (2024) 2485.

[32] A. Khalifeh, F. Mazunga, A. Nechibvute, B. M. Nyambo, Microcontroller unit-based wireless sensor network nodes: A review, Sensors 22 (2022) 8937.

[33] A. Băneasă, R. Donca, S. Besoiu, D. Buleandră, Lightweight implementation of the aes encryption algorithm for iot applications constrained by memory and processing power, in: 2024 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR), IEEE, 2024, pp. 1–6.