DESIGN NETWORK SECURITY MECHANISM TO IMPROVE THE WIRELESS SENSOR NETWORKS LIFE SPAM USING ENERGY TRADE-OFFS TECHNIQUE

Avneesh Gour[*1] & Dr. Nishant Kumar Pathak[2]

[*1]Research Scholar (Regn. No: SU/Ph.D./CSE/2022/04), Shobhit Institute of Engineering & Technology (A NAAC Accredited Deemed to-be- University), MEERUT, U.P., INDIA

[2](Assistant Professor, CSE) Shobhit Institute of Engineering & Technology (A NAAC Accredited Deemed to-be- University) MEERUT, U.P., INDIA

Abstract:

Applications for wireless sensor networks (WSNs) are developing quickly, and performance assessment and analysis approaches are now faced with new issues in the field of energy efficiency. The examination of security trade-offs and energy efficiency is one of the important challenges. The energy analysis module for the QoP-ML (quality of protection modelling language) is suggested in this study as a way to examine the impact of different security levels on a protocol's energy usage. A further expansion of the QoP-ML language that improves the capabilities to analyse intricate wireless sensor networks is the advanced communication module. The Jindo Bridge in South Korea served as the case study for WSN deployment, and lifespan routines with varying levels of security were simulated. The findings demonstrate that the implementation of varied security levels can lead to significant variations in performance and energy use, and therefore, longevity. Therefore, the desired lifespan and security level should be balanced by the WSN protocol designers. To fulfil the aforementioned requirements, the newly released Qo-PML extension and the AQoPA (automated quality of protection analysis) tool have been created.

Keywords: Design, Network Security, Mechanism, Wireless Sensor, Life Spam, Energy, Trade-Offs, Technique.

DOI: 10.24297/j.cims.2023.5.22

1. Introduction

The development of information and communication methods for wireless sensor networks (WSNs) is accelerating in the modern world. They now require analysis and performance review due to this advancement. Energy efficiency is one of the WSN application-related issues that has received the most research [1, 2]. Additionally, it is necessary to evaluate the search for trade-offs between energy efficiency and security assurance. A significant problem that has to be solved is how to design secure protocols that meet the necessary performance.

The conventional method makes the assumption that the optimum course of action is to implement the most robust security measures, hence making the system as secure as feasible. Unfortunately, this leads to an unjustified increase in system burden due to an overestimation of security measures [3, 4]. The aforementioned issues can be resolved by determining the necessary quality of protection (QoP) and modifying some security mechanisms to address these concerns (QoP modelling).

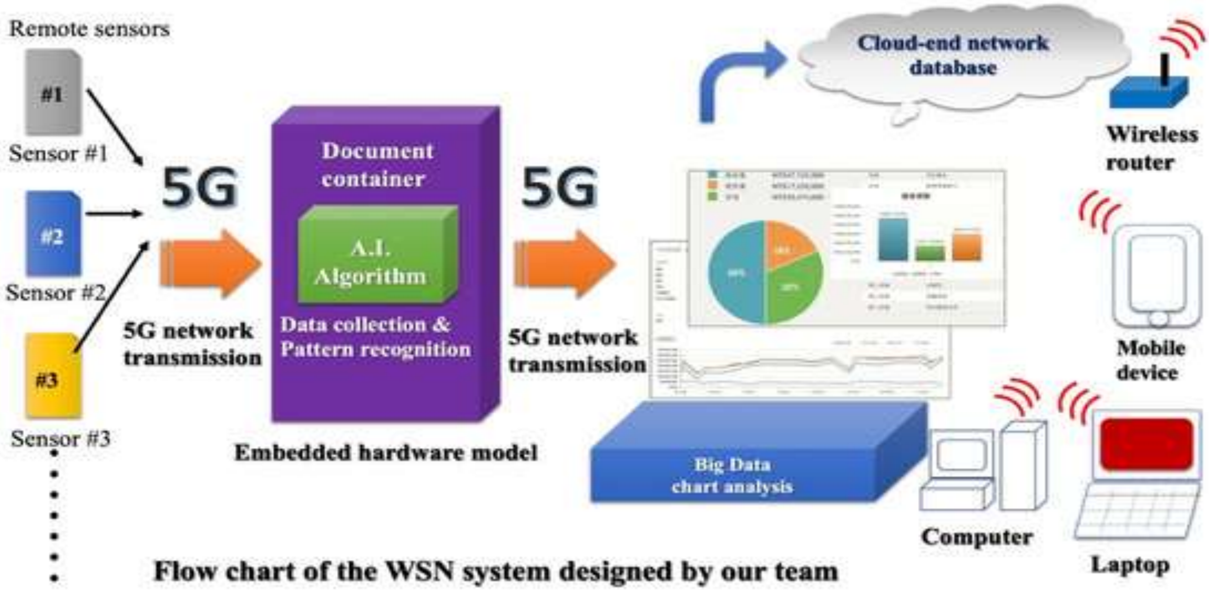

Fig.1: Design Network Security Mechanism to Improve the Wireless Sensor Networks Life Spam Using Energy Trade-Offs Technique Flow Chart.

Due to the limited battery capacity of the sensors, which shortens the network lifetime, several energy-efficient solutions have been put forth in the literature. Many of them focus on routing and message protocols as well as the MAC and PHY layers (standards [5-7] and [8, 9]). Application-specific solutions, such as data reduction (aggregate, compression), as well as novel energy-harvesting technologies, are also available, albeit [10]. Every energy-efficient solution is evaluated and contrasted with its predecessors.

Both experiments and simulations can be used to conduct measurements. The simulation is employed instead since the first option is frequently extremely difficult to implement. Numerous methods of assessment are available, including model-driven architectural analysis, Petri net analysis, state transition modelling based on Markov chains, and data flow or bit analysis. One can make advantage of real-time technologies like [11].

(i) All of the QoP-ML's aforementioned restrictions are eliminated by this new module [20] .
(ii) In order to analyse the impact of certain processes on energy usage and system lifespan, we offer an energy efficiency module [19][18].

(iii) The Automatic Quality of Protection Analysis Tool (AQoPA) has been updated to include the two modules described in this work. In QoP-ML, complex system models are automatically evaluated and optimised by the AQoPA [15][16].

(iv) For a sophisticated wireless sensor network, we give a case study of energy efficiency analysis and security trade-offs. We aim to demonstrate how to establish a balance between security and energy efficiency using this example.

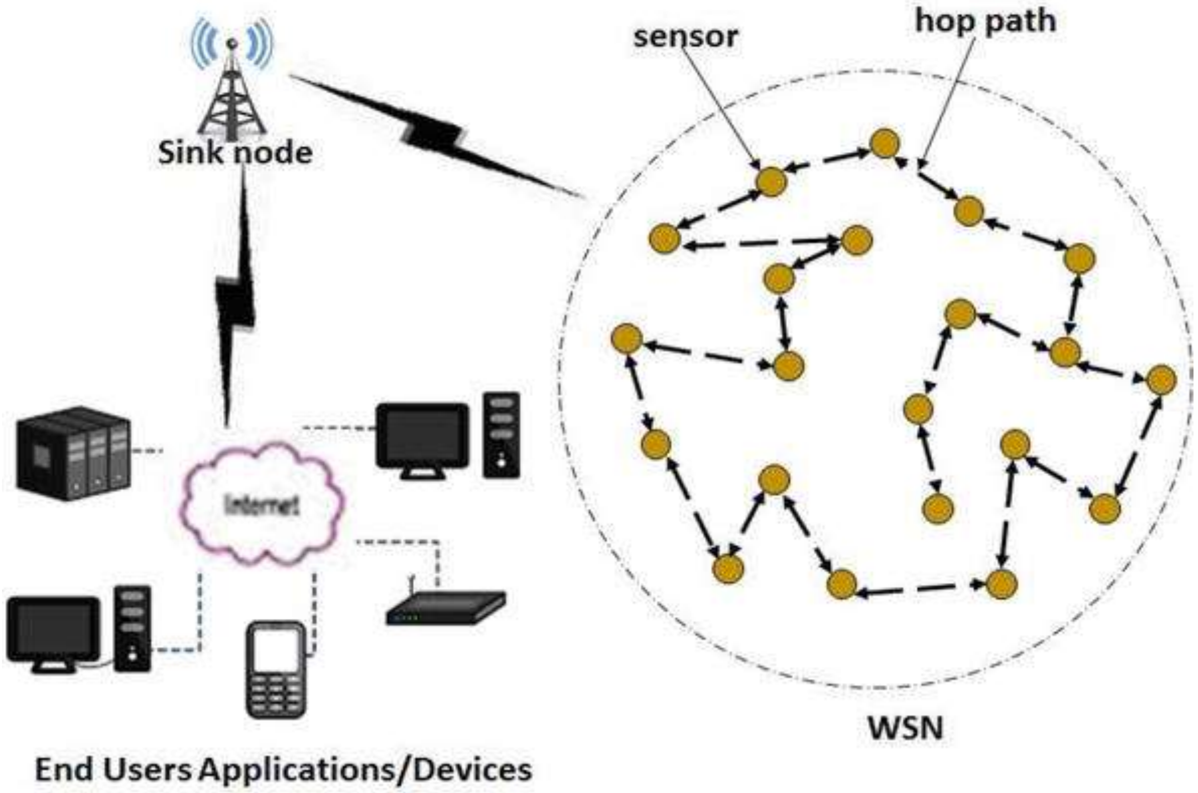

Fig.2: Design Network Security Mechanism to Improve the Wireless Sensor Networks Life Spam Using Energy Trade-Offs Technique process.

The following is a summary of this paper's significant contributions.

(i) As part of the protocol performance analysis, we propose an addition to the QoP-ML that enables us to do a complicated network analysis. Additionally, we present an enhanced communication module that incorporates packet filtering, routing, and network topology into the analysis process. The case study is based on a WSN that is now operating and installed on South Korea's Jindo Bridge [2][9].All of the QoP-ML's aforementioned restrictions are eliminated by this new module.

(ii) In order to analyse the impact of certain processes on energy usage and system lifespan, we offer an energy efficiency module.

(iii) The Automatic Quality of Protection Analysis Tool (AQoPA) has been updated to include the two modules described in this work. In QoP-ML, complex system models are automatically evaluated and optimised by the AQoPA.

(iv) For a sophisticated wireless sensor network, we give a case study of energy efficiency analysis and security trade-offs. We aim to demonstrate how to establish a balance between security and energy efficiency using this example. The case study is based on a WSN that is now operating and installed on South Korea's Jindo Bridge [2][9].

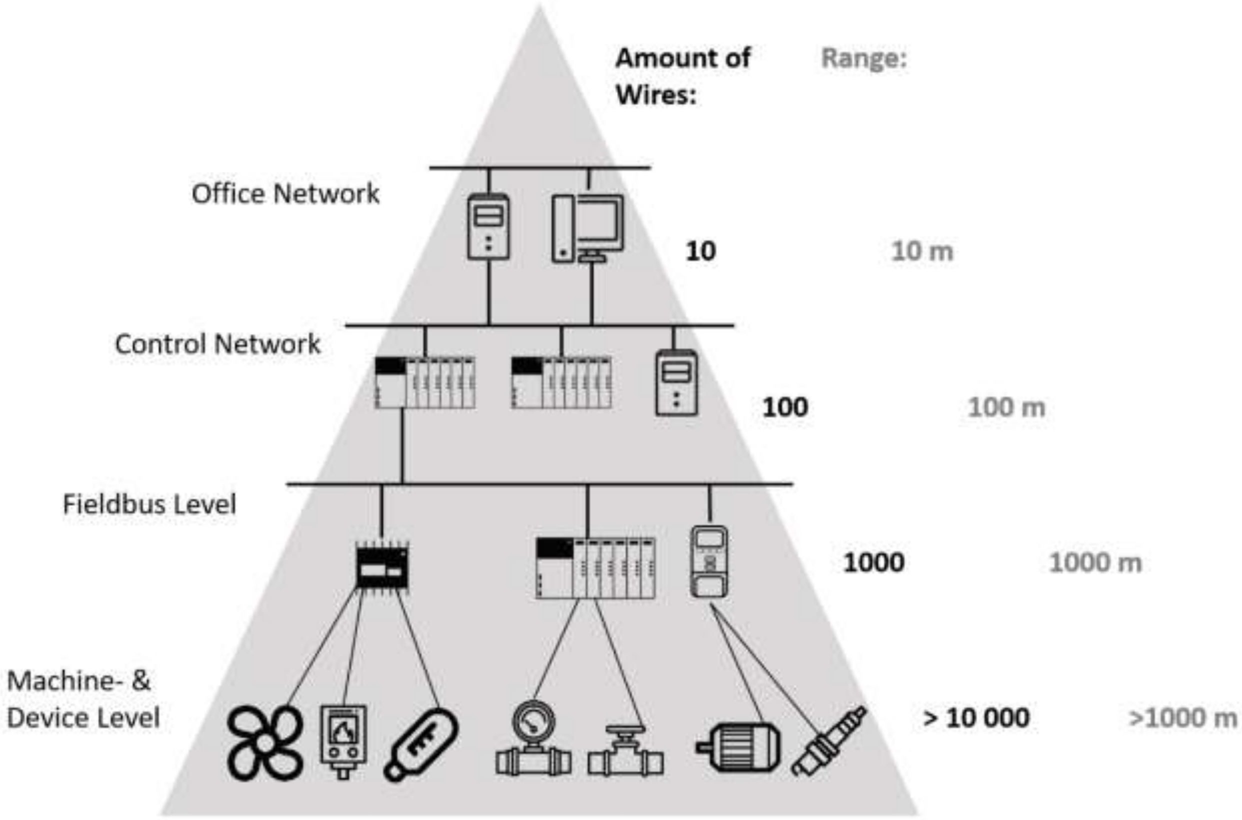

Fig.3: Design Network Security Mechanism to Improve the Wireless Sensor Networks Life Spam Using Energy Trade-Offs Technique Method.

QoP-ML

Ksiezopolski proposes the quality of protection modelling language in the work [35], which offers a modelling language for creating abstractions of cryptographic protocols with a focus on the specifics of the quality of protection. The QoP-ML is meant to express a set of actions referred to as a cryptographic protocol. A multilevel protocol analysis has been added by the QoP-ML, extending the ability to describe the state of a cryptographic protocol.

General View.

Because the QoP-ML structures offer a high degree of abstraction, we are able to concentrate on the quality of protection analyses. Processes, functions, communication channels, variables, and QoP metrics make up the QoP-ML. The main process, which stands in for a single computer (host), is a collection of processes, which are global objects. Channels establish the environment in which a process is conducted, whereas functions represent a single action or a series of activities. A process describes behaviour. The QoP measurements outline how channels and functions affect the level of protection. The syntax, semantics, and algorithms of the QoP-ML are provided in the publication [3][5].

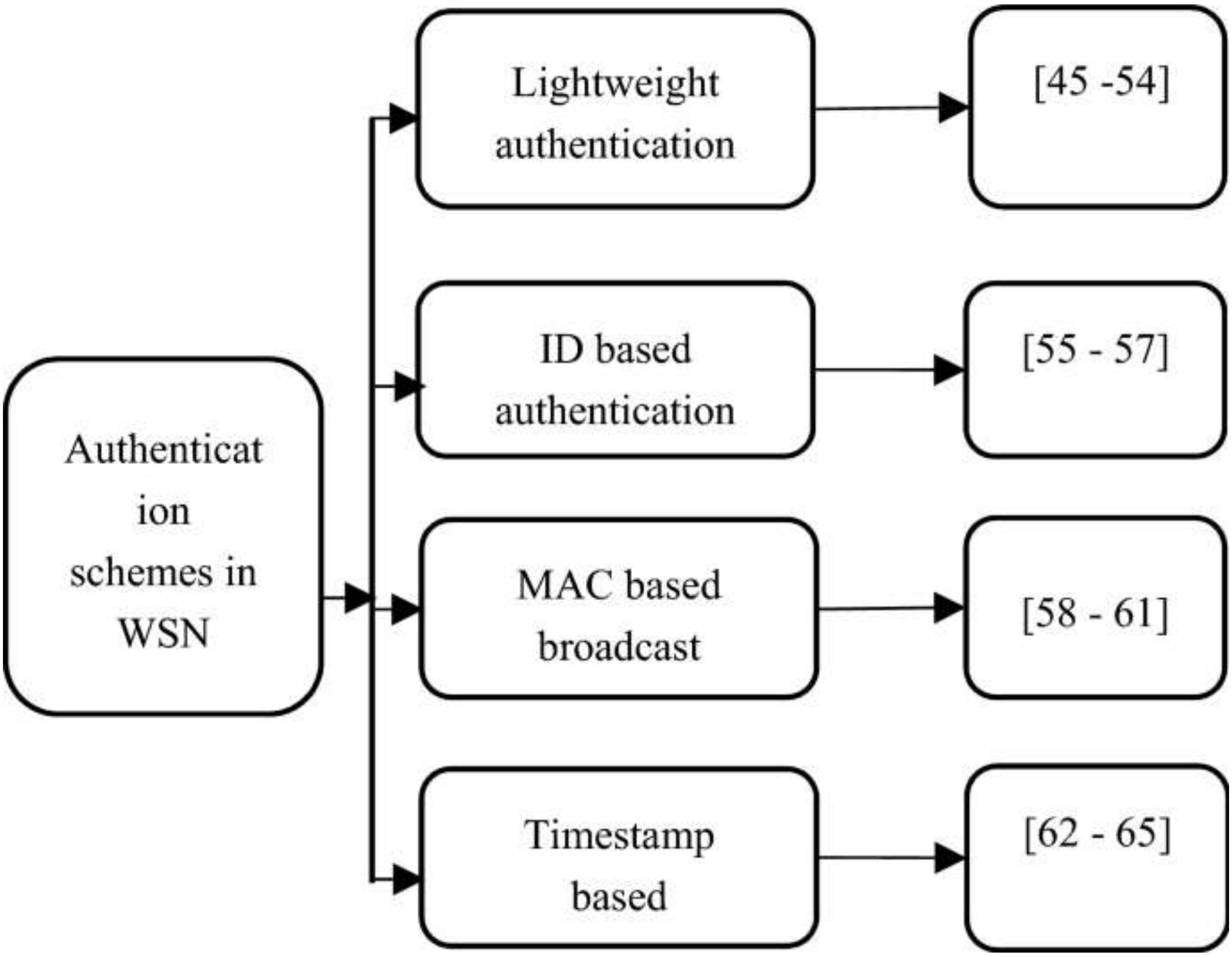

Fig.4: Design Network Security Mechanism to Improve the Wireless Sensor Networks Life Spam Using Energy Trade-Offs Technique Process

Data Types

An unlimited number of variables are utilised to describe communication routes, processes, and functions in the QoP-ML. Variables are used to hold data regarding a system or a particular operation. The QoP-ML lacks any unique data types, sizes, or value ranges because it is an abstract modelling language. Prior to usage, variables do not need to be defined. When they are initially utilised, they are automatically declared. For all processes defined inside a host, the scope of variables declared inside a high hierarchy process (host) is global.

Functions

Functions that alter the states of variables and send objects across communication channels alter the behaviour of the system. The arguments of a function, which specify two different sorts of components, must be set when the function is defined. Additional parameters placed in square brackets affect the level of protection provided by the system, whereas functional parameters written in round brackets are essential for the execution of a function. There are no restrictions on argument names.

Equation Rules

The quality of the analysis of the protection protocol is significantly influenced by equation rules. A collection of equations that establish the equality of function calls make up the equation rules for a certain protocol. For instance, the encrypted data remains unchanged when the same key is used to decode it.

Process Types

The core objects in the QoP-ML are processes, which are collections of elements representing system activity (functions, message transmission). In a genuine system, a single computer handles both the execution and maintenance of processes. Sets of processes are combined into the host process, a higher hierarchy process, in the QoP-ML. For all processes grouped within of this structure, any variable utilised in a high hierarchy process (host) has a global scope. In most cases, variables utilised by one high hierarchy process cannot be used by another. Only when a variable is transmitted across a communication channel is this operation feasible.

Message Passing

Channels are used to transfer messages between hosts and processes in the FIFO (first-in, first-out) sequence, and they are used to describe communication between processes. A channel must be defined before a message is transmitted since its declaration includes information about the channel's buffer size and other features. Communication is asynchronous when channels are defined with a nonzero buffer size.

While synchronous communication is indicated by a buffer size of 0. In synchronous communication, the sender will only send data across a channel that the receiver is actively listening to. When the buffer channel's capacity is at least 1, a message can be transmitted over it even if nobody is actively listening to it. When the listening process in this channel is put into action, the receiver will get this message.

Security Metrics

The suggested QoP-ML may simulate system behaviour, which is officially characterized by a cryptographic protocol. One of this language's primary goals is to abstract the level of security provided by a specific implementation of the examined cryptographic protocol. The effect of system protection is reflected through functions in the QoPML. The quality of the protection parameters are set and the specifics of the function are given when a function is declared. These variables have no bearing on a protocol's flow, but they are essential for a thorough protection analysis.

In such an analysis, security metrics, the following structure of the QoP-ML, and QoP parameters for the functions are integrated. One can abstract functions' temporal performance, their impact on the security requirements for a cryptographic protocol, or other QoP analysis-relevant elements in this framework.

2. Advanced Network Analysis Module

The old network analysis module (from QoP-ML)'s flaws are eliminated by the new network analysis module. In a nutshell, the first issue is the inability to identify the message's recipient when several hosts are using the same channel, and the second one is the inability to identify the message's sender in order to send the answer back. The QoPML model has to be updated with new methods and structures in order to overcome the restrictions listed above. We go through three new methods in this section: topology, routing, and packet filtering.

In addition, we present a methodology that offers a temporal analysis of network communication processes. The time it takes for a message to go from the sender to the recipient might change depending on the network path that is used. The model enables one to ascertain a channel's properties and compute the transmission time. The BNF (Backus-Naur form) [36] standard is used to give the syntax of all structures described in this article in the Supplementary Material, which is accessible at http:// dx.doi.org/10.1155/2015/9434785.

Topology

A graph's vertices and edges—which represent hosts and connections between them—define a topology. Every link that already exists must be specified and given a weight that indicates its quality (the lower the weight, the higher the quality). A link is a unique kind of relationship.

Algorithm for the communication time

```
Require: p, q, wmin
t, n, s
∗ ← 0, 1, ∞
repeat
    z ← simulate (n, p) . Candidate generation
    t ← t + expon(n, 1) . Poisson process
    s ← t · p(z)/q(z) . Candidate’s score
    if s < s∗
    then . Accept/reject candidate
        s
        ∗
        , n
        ∗ ← s, n
    end if
    n ← n + 1
```

```
until $s^* \le t \cdot wmin$
return n
```

Algorithm of filtering requests

```
public final class HitCounterFilter implements Filter {
  private FilterConfig filterConfig = null;

  public void init(FilterConfig filterConfig)
     throws ServletException {
    this.filterConfig = filterConfig;
  }
  public void destroy() {
    this.filterConfig = null;
  }
  public void doFilter(ServletRequest request,
    ServletResponse response, FilterChain chain)
     throws IOException, ServletException {
    if (filterConfig == null)
      return;
    StringWriter sw = new StringWriter();
    PrintWriter writer = new PrintWriter(sw);
    Counter counter = (Counter)filterConfig.
      getServletContext().
      getAttribute("hitCounter");
    writer.println();
    writer.println("===============");
    writer.println("The number of hits is: " +
      counter.incCounter());
    writer.println("===============");
    // Log the resulting string
    writer.flush();
    System.out.println(sw.getBuffer().toString());
    ...
    chain.doFilter(request, wrapper);
    ...
  }
}
```

Energy Analysis and Lifetime Prediction Module

The addition of the energy analysis and lifespan prediction module to the QoPML and its implementation as an extension to the AQoPA are two of the paper's primary contributions. Energy analysis. The energy analysis module's goal is to assess the modelled system's energy usage. The time analysis module, which monitors the timings of operations and communication stages, must be incorporated into the performance analysis process in order to calculate these values. Energy use is determined as the total of the energy used by basic CPU-only processes (such as security and other arithmetic calculations) and radio-based communication operations (such as listening, receiving, and transmitting).

The following formula is used to determine how much energy one CPU or communication activity uses: Eop = T I V, where Eop is the energy used by a CPU or a communication operation, op is the operation's index, T is the operation's duration, I is its electric current, and V is the host's voltage. The time is obtained via the time analysis module, and each host's voltage is set to constant. The last component, the current, can be specified individually for each operation or collectively for a set of operations. With the current header, metrics are used to specify its value. The current is specified in the medium structure for communication stages.

The energy module analysis examines each host's energy usage as follows: EH is the host's energy consumption, EHCPU is the total energy consumption of all CPU activities and operations using a separately specified electric current, and EHCOMM is the energy consumption of all other components.

3. Results

Contains the findings of the energy consumption and longevity predictions for the scenarios that were provided (Table 4). The maximum amount of energy used by one sensor throughout the execution of one scenario is shown in the Energy consumption column. The number of days that have passed since the battery of any sensor was last charged is shown in the Lifetime prediction column. According to Table 5's findings, different quantities of distant sensing events can have a big impact on how long wireless sensor networks last. Due to an increase in the number of sensing events, the lifetime of the first three situations is almost six times longer.

The lifespan of scenario number 4 (24 insecure sensing occurrences) is nearly double that of scenario number 6, which has the highest level of security. A good compromise appears to be the final scenario with the same amount of sensing events for all three security levels. The findings indicate that the balance between acceptable energy usage and security level should be sought by WSN protocol designers. The obtained findings imply that it is sometimes unavoidable to provide security at the price of energy usage. Prior to implementing specified solutions, it is necessary to thoroughly assess the environment under consideration and select the solution that best satisfies the given criteria (in terms of, for example, time or energy usage).

The suggested method can automatically respond to the query, "What is the performance difference between the created scenarios?" This study allows you to weigh the ways of information security against the necessary performance. Additionally, this research enables us to develop scenarios for situations that call for more security or efficiency. A rapid and major shift in environmental conditions, such as a sudden change in the weather that suggests more stringent efficiency needs, can be one of these occurrences. On the other side, the use of higher security may be necessary if unexpected communication is detected. In conclusion, the system has the ability to change its mode of operation in certain circumstances (adaptable security [15]).

4. Conclusions

The enhanced communication module is presented by the authors of this study as an addition to the QoP-ML. The module described here enables us to carry out intricate network analysis as part of protocol performance evaluations. It is used to analyse the time and effort spent on each phase of communication. The addition of the energy analysis and lifetime prediction modules to the QoP-ML is another contribution of this research. As an addition to the AQoPA tool, which is used for automatic usage in performance analysis, the modification of the QoP-ML is also implemented. The authors analyse an existing wireless sensor network installed on the Jindo Bridge in South Korea using the suggested communication paradigm.

Predicting the lifespan of the current network with extra security features is the goal of such a study. In order to gather more accurate acceleration data, the authors provide novel scenarios in which the real sensor network's functioning is changed and the number of sensing events is raised. Ten situations with various security levels are examined in the case study. The findings enable us to make judgements about how security characteristics affect the amount of time and energy wireless sensor networks use.

The case study that is being given demonstrates how the addition of security features can significantly affect network longevity. Therefore, the desired lifespan and security level should be balanced by the WSN protocol designers. To complete this goal, the AQoPA tool and the QoP-ML have been developed.

References

1. P. K. Sahoo, "Efficient security mechanisms for mhealth applications using wireless body sensor networks," Sensors, vol. 12, no. 9, pp. 12606–12633, 2022.
2. L. X. Hung, N. T. Canh, S. Lee, Y.-K. Lee, and H. Lee, "An energy-efficient secure routing and key management scheme for mobile sinks in wireless sensor networks using deployment knowledge," Sensors, vol. 8, no. 12, pp. 7753–7782, 2022.
3. B. Ksiezopolski, Z. Kotulski, and P. Szalachowski, "Adaptive approach to network security," in Computer Networks, vol. 39 of Communications in Computer and Information Science, pp. 233–241, Springer, Wisla, Poland, 2021.

4. P. Szalachowski, B. Ksiezopolski, and Z. Kotulski, “On authentication method impact upon data sampling delay in wireless sensor network,” in Computer Networks, vol. 79 of Communications in Computer and Information Science, pp. 280–289, Springer, Ustron, Poland, 2021.
5. IEEE 802.15.4 Standard, 2015, http://www.ieee802.org/15/pub/ TG4.html.
6. Zigbee Alliance, 2015, http://www.zigbee.org/.
7. IEEE 802.15 wpan task group (tg6) body area networks, 2015, http://www.ieee802.org/15/pub/TG6.html.
8. P. O. Kamgueu, E. Nataf, T. Djotio, and O. Festor, “Energybased metric for the routing protocol in low-power and lossy network,” in Proceedings of the 2nd International Conference on Sensor Networks (SENSORNETS 2013), pp. 145–148, Barcelona, Spain, February 2020.
9. U. Hunkeler, H. L. Truong, and A. Stanford-Clark, “MQTT-S— a publish/subscribe protocol for wireless sensor networks,” in Proceedings of the 3rd IEEE/Create-Net International Conference on Communication System Software and Middleware (COMSWARE ’08), pp. 791–798, January 2020.
10. T. Rault, A. Bouabdallah, and Y. Challal, “Energy efficiency in wireless sensor networks: a top-down survey,” Computer Networks, vol. 67, pp. 104–122, 2014.
11. The ns-3 network simulator, 2008, http://www.nsnam.org/.
12. D. Blouin and E. Senn, “CAT: an extensible systemlevel power consumption analysis toolbox for model-driven design,” in Proceedings of the 8th IEEE International NEWCAS Conference (NEWCAS ’10), pp. 33–36, 2019.
13. J. Li, H. Y. Zhou, D.-C. Zuo, K. M. Hou, H. P. Xie, and P. Zhou, “Energy consumption evaluation for wireless sensor network nodes based on queuing Petri net,” International Journal of Distributed Sensor Networks, vol. 2014, Article ID 262848, 11 pages, 2014.
14. A. K. Agarwal and W. Wang, “On the impact of quality of protection in wireless local area networks with IP mobility,” Mobile Networks and Applications, vol. 12, no. 1, pp. 93–110, 2007.
15. B. Ksiezopolski and Z. Kotulski, “Adaptable security mechanism for dynamic environments,” Computers & Security, vol. 26, no. 3, pp. 246–255, 2017.
16. E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W. H. Sanders, “Adversary-driven state-based system security evaluation,” in Proceedings of the 6th International Workshop on Security Measurements and Metrics (MetriSec ’10), pp. 5:1–5:9, ACM, September 2010.
17. S. Lindskog, Modeling and tuning security from a quality of service perspective [Ph.D. thesis], Chalmers University of Technology, Gothenburg, Sweden, 2015.
18. A. Luo, C. Lin, K. Wang, L. Lei, and C. Liu, “Quality of protection analysis and performance modeling in IP multimedia subsystem,” Computer Communications, vol. 32, no. 11, pp. 1336– 1345, 2009.

19. C. S. Ong, K. Nahrstedt, and W. Yuan, "Quality of protection for mobile multimedia applications," in Proceedings of the International Conference on Multimedia and Expo (ICME '03), vol. 2, pp. II-137–II-140, Baltimore, Md, USA, July 2019.
20. D. C. Petriu, C. M. Woodside, D. B. Petriu et al., "Performance analysis of security aspects in UML models," in Proceedings of the 6th International Workshop on Software and Performance (WOPS '07), pp. 91–102, ACM, New York, NY, USA, February 2017