Optimal Selection of Lightweight Cipher Algorithm and Topology Construction Protocol in Wireless Sensor Networks

Nemanja RADOSAVLJEVIĆ[1]*, Milena POPOVIĆ[2], Dušan VUJOŠEVIĆ[1], Djordje BABIĆ[1]

[1] School of Computing, Union University, 6 Knez Mihailova Street, Belgrade, 11000, Serbia
nradosavljevic@raf.rs (**Corresponding author*), dvujosevic@raf.rs, djbabic@raf.rs

[2] Faculty of Organizational Sciences, University of Belgrade, 154 Jove Ilića Street, Belgrade, 11000, Serbia
milena.popovic@fon.bg.ac.rs

Abstract: An optimal selection of a WSN topology protocol and a suitable lightweight cipher algorithm is a highly important task, whose success ensures both the maximum utilization and the security of a wireless sensor network. This paper presents a method to determine the optimal combination of a WSN topology protocol and a lightweight cipher algorithm in the context of power consumption throughout an entire network. A selection method based on multi-attribute decision-making methods is proposed. These methods, used for the first time in a study of sensor networks, provide a ranking of the optimal combinations of topologies and encryption algorithms that meet the requirements of wireless sensor networks such as authentication, data integrity, reliability, availability, confidentiality, and energy efficiency.

Keywords: Ciphers, Multi-criteria decision-making, Network topology, Wireless sensor networks.

1. Introduction

Wireless sensor networks (WSN) are used in numerous applications from various fields, such as military industry, medicine, sports, agriculture, ecology, natural capital monitoring, traffic, aviation, construction, etc. An important reason for this research has come from a large number of attacks on wireless sensor networks that are causing problems related to the availability, confidentiality, integrity, and authentication of the data transmitted over the networks, in particular through the exhaustion of the nodes' power supply.

This paper presents an approach to determine the optimal combination of the WSN topology protocol (TP) and lightweight cipher (LWC) algorithm in the context of power consumption throughout an entire network. The original contribution of this work resides in the proposed selection technique, which is based on a multi-criteria decision-making (MCDM) method that has never been used before in this type of context. The proposed selection technique makes the process of analysis and selection of appropriate LWC for the given topology protocol rather straightforward, automatic and standardized compared to alternative manual approaches. Although the proposed work derives from the field monitoring and precision agriculture, it can be used in other areas where LWC and TP are to be selected, especially in the context of health care monitoring or industrial monitoring.

The first phase of the proposed work includes the development of a hypothetical model of an observed area and an arrangement of sensor nodes. The alternatives used further for multi-criteria analysis were described by numerical characteristics, such as the communication radius, the coverage coefficient of the observed area and the coverage outside the examined area coefficient. These characteristics show the possibility of expanding the area without engaging additional sensor nodes, and the number of messages throughout the entire sensor network. The set of alternatives related to topology protocol algorithms has been expanded based on the criteria used for selecting a lightweight cipher algorithm that includes: block size-key size ratio, unrolled rounds number, number of cycles, delay per round, and energy per byte transmitted through the network.

The second phase of the proposed approach consists in the use of the PROMETHEE II method of MCDM for the ranking of alternatives. The result of the proposed selection method is a sorted list of alternative ordered pairs of a protocol used for creating topology and a lightweight cipher algorithm. The ranks obtained for these pairs are derived from the impact of a combination of protocol and cipher algorithm on the security of message transmission and the extension of the life of sensor nodes power supply.

The remainder of this paper is organized as follows. Section 2 describes the existing work related to the presented research. Section 3 presents the problem definition. Section 4 discusses the methodological

https://doi.org/10.24846/v30i4y202104

framework that is providing solution for the problem defined in section 3. Section 5 explains the setup of a simulation environment in three subsections: creating the WSN simulation model, topology protocol simulation and calculation of LWC parameters. In section 6, the PROMETHEE II multi-criteria decision-making method used in this research is presented. The analysis of experimental results is shown in section 7. Section 8 concludes this paper with an analysis of the obtained results and the significance of proposed work.

2. Context of Research

Topology construction protocols depend on the position of nodes in the WSN. A topology also depends on the node communication radius. Based on the topology construction protocol, the nodes select the neighbouring nodes through which they will forward the messages. The primary task of the topology construction protocol is to ensure the interconnection of nodes throughout a network, optimize the bandwidth, and prolong the lifetime of that network. In subsection 2.1, the node efficiency in WSN is briefly presented, related to the three topology protocols under investigation.

The main problem of WSN technology regards the data transmission security. Lightweight cipher algorithms are used to prevent a data integrity attack in WSN. The works addressing the lightweight cipher are mentioned in subsection 2.2 of the literature review. Complex problems in which the decision is made based on several criteria that cannot be directly related to each other are presented in subsection 2.3.

In (Radosavljević & Babić, 2021), a power consumption estimation model for WSN for a given set of topology protocols and lightweight cryptographic algorithms is given. The authors proposed a mathematical model used to select an appropriate combination of topology protocol and cryptographic algorithm.

The problems from these different areas can be solved by applying the multi-criteria decision-making methods.

2.1 The Node Efficiency in WSN

A WSN represents the sensors that collect data on the observed surface area. A set of sensors transmits the collected data to an edge device by multi-hop transmission scheme (Staniec & Debita, 2013). Wireless communication became the accelerator of the growing trends such as smart solutions for grids, cities, homes, and IoT (Hatzivasilis et al., 2018).

Sensor nodes used in WSNs can be intricate if their purpose is to monitor location or to analyse images, or they can be relatively simple, like those monitoring changes in temperature, pressure, humidity, Ph values. Each sensor node has a data sensing function, communication module and power supply unit (Staniec & Debita, 2013). One way to decrease the power consumption for processing and storage is to reduce the number of end-devices (Staniec & Debita, 2013). Engineers have even shown that the genetic algorithm can optimize the efficiency of WSN (Panhwar et al., 2018).

The studies of WSNs are often conceived as simulation experiments on different network topologies and localization algorithms. A study investigating the three topology construction protocols in terms of the coverage and reduction of energy consumption has indicated that the Kneigh tree is the right protocol, as it provides greater coverage than other protocols and consumes less energy (Pachnanda et al., 2013).

2.2 Lightweight Cipher

Data security is an integral part of a WSN's quality. The overview of the encryption algorithms suitable for WSN (Liu et al., 2009) paid particular attention to time-critical systems, energy-efficient, and SRAM-dependent algorithms. The constraints of WSN, such as processing power, battery power supplies, and memory limit, are factors needed for the selection of cipher algorithms, so they were in the focus of yet another comparative analysis (Othman et al., 2012).

A lot of research work has been invested in the development of efficient lightweight block ciphering techniques and in their evaluation. The significance of several LWC algorithms and their specifications are given in (Radosavljević & Babić, 2021). LWC algorithms considered in (Radosavljević & Babić, 2021) are also analysed in this manuscript, including: AES, NOEKEON, LED 128, PRINCE, Piccolo, SIMON 64/96 and KATAN 64. Furthermore, two additional LWC will be analysed and briefly described.

PRESENT, a new block cipher algorithm consisting of 64 bits block in 31 rounds and two key sizes of 80 and 128 bits, has been reported to achieve software and hardware efficiency in comparison to other algorithms that serve similar purposes (Bogdanov et al., 2007). A group of lightweight square ciphers called KLEIN, which are intended for devices such as remote sensors and Radio Frequency Identification (RFID) tags, uses different key lengths, which make these ciphers flexible (Gong et al., 2012).

TWINE 64-bit cipher has been reported to show a satisfactory execution performance on controllers of small hardware capabilities such as sensor nodes (Suzaki et al., 2011). An example of the numerous LWCs with the piece size of 64 bits and 80bits key size is Lblock.

2.3 Multi-Criteria Decision-Making

Researchers have used the methods of MCDM to select set of alternatives, where each alternative has been evaluated by more than one attribute. The selection of the right decision-making criteria about WSN resembles the selection of parameters for the service level agreement about the WSN (Iordache et al., 2017).

Due to simplicity and practicality, the most popular method of MCDM is the simple additive weighting (SAW) method. To choose the best possible course of action, it relies upon the evaluated weights of selected criteria. The ranking in MCDM can include both quantitative and qualitative criteria (Petre et al., 2019). In general, subjective weighting demands methods that are different from those in objective weighting, and researchers have proposed ways to combine them, for example in a case study dealing with the cloud quality of service (Radulescu et al., 2018). Professionals can use sensitivity analysis to compare the weight values of criteria (Zavadskas et al., 2018).

A famous approach, the AHP method, was applied in a study aiming to determine the cost-effectiveness of the concept of smart city in a context of technological criteria (Escolar et al., 2019) and is constantly being improved (Kou el al., 2017). Using the methods TOPSIS and MADME, researchers determined the importance and impact of a sensor node within the WSN based on four criteria (Yin et al., 2019). Many studies compared the MCDM methods in the context of decision criteria, decision-making approaches, and their field of use (Wu & Zhang, 2011).

PROMETHEE method is used for the ranking of alternatives, which requires plenty of parameters from the decision-maker (DM) (Zhaoxu & Min, 2010). Researchers have applied it to networking problems, among many other fields. Thus, it was used for the optimization of the simulated cluster head selection process, whereas the main goals were to create maximal coverage and to save energy (Verma & Sharma, 2020).

3. Problem Definition

The problem dealt with in this paper is the choice of an optimal combination of topology protocol and lightweight cipher algorithms in wireless sensor networks (WSN). The aim is a minimal engagement of resources such as processor power and battery power supply in providing safe data transfer between sensor nodes and base stations, which is one of the most important parts of a complex system such as WSN.

The security issue is an ever-present problem in all WSN application areas. Also, the question of energy efficiency is an ongoing problem for all the devices that have limited charging, especially for the nodes that can be found in areas where it is almost impossible to change the energy source.

It is necessary to use some of the encryption algorithms to protect privacy and preventing data transfer between nodes. However, as it is known that encryption algorithms increase the load of sensor nodes, it is imperative to carefully determine which of the cipher algorithms have less impact on the network performance. As WSN does not have a constant communication structure between nodes, communication performs according to some of the topology construction protocols. The problem to be solved is the choice of optimal combinations of the cipher algorithm and the topology construction protocol.

4. Methodological Framework

For this problem analysis, the methodological framework is divided in two phases, as shown in

Figure 1. The first phase presents the creation of a simulated environment that contains three steps: the setting of a simulation model, the simulation of topology protocols, and the calculation of energy consumption of a lightweight cipher.

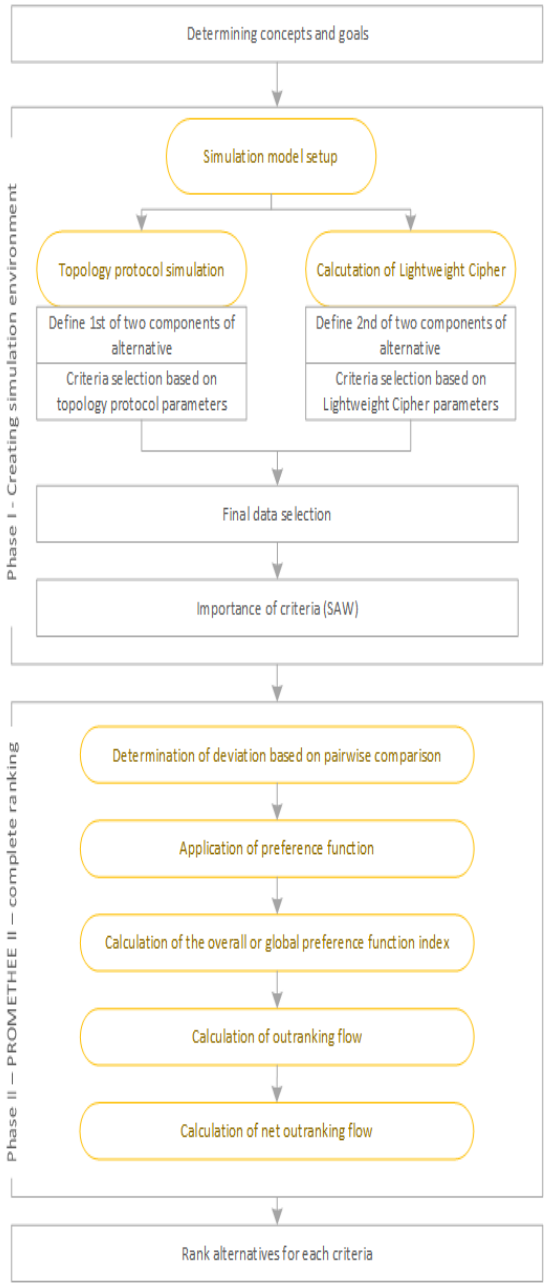

Figure 1. Methodological framework phases

The second phase uses the multi-criteria method PROMETHEE II, which is employed for a complete ranking of all alternatives.

5. Simulation Environment-Phase I

For the analysis and testing of the proposed selection method, a simulation environment was created in the Atarraya simulator (Labrador & Wightman, 2009). The Atarraya simulator supports TPs which are described in Step 2 - Topology protocol simulation. After obtaining the results, which are significant for the use of the multi-criteria decision-making method, they have been divided in three steps as shown in Figure 1. Step 1 encompasses the application of a simulated environment; Step 2 involves the topology protocol; Step 3 represents the simulation and calculation of the lightweight ciphering algorithms.

Step 1 – Creating the WSN simulation model

Table 1 shows the simulation parameters that represent the foundation for further simulation. The examined area, across which sensor nodes are distributed, has been set to 36 ha. The simulation parameters such as Communications radius, Sensing radius, Small and large packet size range are usual parameters upon which the communication within one WSN is established. The communications radius is the radius of each particular node, and it describes the space within which each node communicates with other nodes. The sensing radius is an area taken as completely covered with one node and for which it can be guaranteed that this node correctly reads data. The sensing radius, which has been chosen as one of the parameters for this simulation, may apply to monitor crops in agriculture, forests, water resources, air pollution, etc. Small and large packet sizes are standard packet sizes that are transferred through a sensor network.

Table 1. Simulation parameters

Application area	600 x 600 m
Communications radius	150m
Sensing radius	30m
Small packet size range	15 - 23 bytes
Large packet size range	30 - 60 bytes
Number of nodes	50

Step 2 - Topology protocol simulation

For the simulation scenario from Step 1 the work of topology construction protocol has been simulated in WSN. Topology protocols used in this approach are described in details in (Radosavljević & Babić, 2021). These four protocols have been selected as the most appropriate for the given use

case of field monitoring. The purpose of topology construction protocols such as A3 (Qureshi, 2011), A3 Coverage - A3-Cov (Geng et al., 2019), Energy-efficient connected dominating set (EECDS) (Pachnanda et al., 2013), and CDS rule K (Geng et al., 2019) is the optimization of the number of messages transferred through the entire system and load balancing between sensor nodes.

Figure 2 shows the layout of WSN for each topology. Cluster head (CH) nodes are shown in red, regular nodes (RN) are shown in light blue, whereas the black circle is the communication radius of a sensory node. The sensing radius for cluster head nodes is shown as a red circle.

As WSN distinguishes between two types of sensor nodes - cluster head nodes and regular nodes, as well as between the number of transmitted and received messages per each node, this is one of the basic parameters observed for each topology given in Table 2.

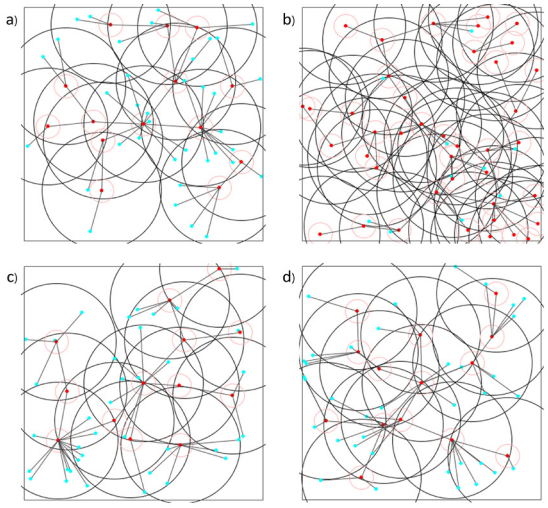

Figure 2. Graphical representation of topology simulation: a) A3 protocol, b) A3 coverage protocol, c) CDS rule K protocol, d) EECDS protocol

Apart from this parameter, the coefficient of the covered area has also been analysed. This coefficient is calculated based on the communication radius of the nodes. Furthermore, the coefficient of the covered area located outside the examined radius has been analysed. It shows the possibility of network expansion without engaging additional resources.

Step 3 - Calculation of LWC parameters

The lightweight ciphers chosen for this phase of the analysis are: AES (Moradi et al., 2011), NOEKEON (Daemen et al., 2000), LED 128 (Guo et al., 2011), PRESENT (Bogdanov et al., 2007), PRINCE (Verma & Sharma, 2020), Piccolo (Cazorla et al., 2013), TWINE (Suzaki et al., 2011), SIMON 64/96 (Beaulieu et al., 2013), and KATAN 64 (Canniere et al., 2009). These ciphers are low-demanding and suitable for application in sensor networks whose nodes have limited resources as a limiting factor for the choice of cipher algorithms.

The criteria that will be used in MCDM are shown in Table 3. These criteria (block size / key size ratio, unrolled rounds, number of cycles, delay per round in nanoseconds and energy per byte which represents the energy needed for ciphering of one byte of data) are considered in detail in (Banik et al., 2016).

The energy per byte column is of great importance because it is related to the number and size of messages shown in Step 2. The block size represents the number of bits that can be ciphered, whereas the key size represents the size of the key, and it directly influences safety. The unrolled rounds are the number of cipher rounds completed in one clock cycle of the processor. The number of

Table 2. Topology protocol simulation results

Topology protocol	Node type	The amount of data transferred (byte)		Coverage	Coverage outside the observed area
		Send	Received		
A3	CH	2176	10589	0.9354	0.2276
	RN	2326	10970		
A3 coverage	CH	4216	19341	1.0000	0.5088
	RN	636	4885		
EECDS	CH	3568	12695	0.9613	0.3010
	RN	5408	17146		
CDS rule K	CH	2647	9661	0.9276	0.2086
	RN	4565	17403		

cycles is the number of CPU cycles necessary for ciphering. Finally, the delay per round is the time elapsed from the moment when the block enters ciphering until the ciphered byte comes out.

Based on data presented in Table 2 and Table 3, a final list of criteria for MCDM analysis has been compiled. The weights obtained using the SAW method define the preferences of all these criteria of this analysis. The SAW method is based on the weighted average. The evaluation score is calculated for each alternative by multiplying the scaled value given to the alternative of those criteria with the weights directly assigned by the DM followed by the summation of the products for all criteria. The main advantage of SAW (Afshari et al., 2010) is that it is a proportional linear transformation of the raw data therefore the relative order of magnitude of the standardized scores remains equal. The final list is given in Table 4.

6. PROMETHEE II - Phase 2

The PROMETHEE II method is a MCDM method used for the complete ranking of alternatives (Brans, 1982). This method is based on a pairwise comparison of alternatives within each criterion and requires two additional facts (Behzadian et al., 2010).

Six types of criteria, shown in Figure 3, are used to improve the selection of a preference function (Brans & Vincke, 1985).

Table 3. Lightweight cipher specification

Cipher	AES	NOEKEON	LED 128	PRESENT	PRINCE	Piccolo	TWINE	SIMON 64/96	KATAN 64
Block size /Key size	128/ 128	128/ 128	64/ 128	64/ 80	64/ 128	64/ 80	64/ 80	64/ 96	64/ 80
Unrolled Rounds	1	1	1	2	1	1	2	2	16
Number of Cycles	11	18	50	17	13	26	19	22	17
Delay per round (ns)	3.32	3.41	5.25	2.09	4.06	3.28	3.10	2.18	2.04
Energy per byte(pJ)	21.92	21.20	82.08	19.44	18.64	22.24	26.80	26.56	17.52

Table 4. List of the criteria, preferences, and weights

Criteria			
Index	**Name**	**Preferences(min/max)**	**Weight**
C1	Block size/Key size Ratio	Min	0.09
C2	Unrolled rounds	Max	0.07
C3	Number of Cycles	Min	0.08
C4	Delay per round (ns)	Min	0.09
C5	Energy per byte (pJ)	Min	0.10
C6	Coverage (%)	Max	0.10
C7	Coverage outside the observed area (%)	Max	0.08
C8	Cluster head node message size - sent (byte)	Min	0.10
C9	Cluster head node message size - received (byte)	Min	0.10
C10	Regular node message size -sent (byte)	Min	0.09
C11	Regular node message size - received (byte)	Min	0.08

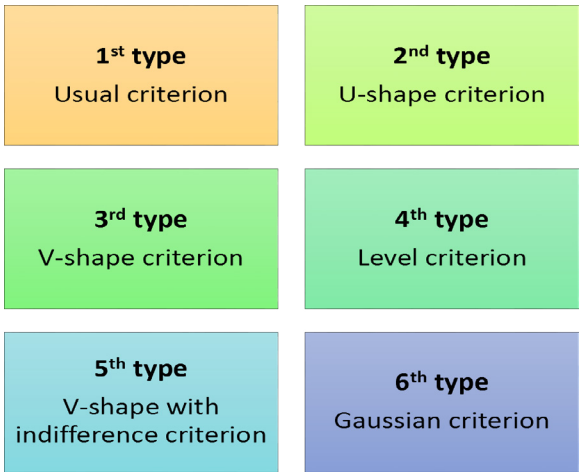

Figure 3. PROMETHEE II - preference function

The values for each type of criterion are the following: strict preference threshold *(p)*, indifference thresh *(q)*, intermediate value between *p* and *q(s)* (Brans & Mareschal, 2003).

The five steps of PROMETHEE II method implementation are (Brans, 1982):

Determining the deviation $d_j(a,b)$ that is the difference between the evaluation of alternative *a* and alternative *b* on each criterion (1):

$$d_j(a,b) = g_j(a) - g_j(b), j = 1,\ldots,n \quad (1)$$

Preference function application of a with regard to *b* on each criterion, as a function of deviation (2):

$$P_j(a,b) = F_j\left[d_j(a,b)\right], j = 1,\ldots,n \quad (2)$$

Calculation of the overall index preferences $\pi(a,b)$ which represents the weighted sum of w_j which is the weight of *j^{th} criterion* (3):

$$\pi(a,b) = \sum_{j=1}^{n} P_j(a,b)\, w_j, \forall\, a,b \in A \quad (3)$$

Calculation of positive $\phi^+(a)$ and negative $\phi^-(a)$ outranking flow of alternative (4):

$$\phi^+(a) = \frac{1}{n-1}\sum_{x\in A}\pi(a,x)$$
$$\phi^-(a) = \frac{1}{n-1}\sum_{x\in A}\pi(x,a) \quad (4)$$

Complete ranking $\phi(a)$ for each alternative (5):

$$\phi(a) = \phi^+(a) - \phi^-(a) \quad (5)$$

7. Analysis of the Results

The data used in this empirical study have been obtained as a result of traffic and energy consumption simulation for secure communication of sensor nodes within the observed WSN. The values of all the criteria for each Lightweight Cipher algorithm and topology protocol are given in Table 4. To rank the alternatives, Decision Lab software is used. The type of criteria (V-shaped for all the alternatives) is defined for each criterion based on the opinion of experts.

The final results (net outranking flow) are given in Figure 4 and Table 5.

The most suitable pair, Topology protocol, and LWC are detected on an alternative, and it represents the use of KATAN64 cipher for ciphering and A3 protocol for forming WSN topology.

Given the fact that each alternative comprises two components, the results demonstrate that the first two best-rated alternatives use KATAN 64 cipher, which leads to the conclusion that this cipher is desirable for application in WSN. KATAN64 ciphering algorithm is not among the safest options observed, but it provides relatively low

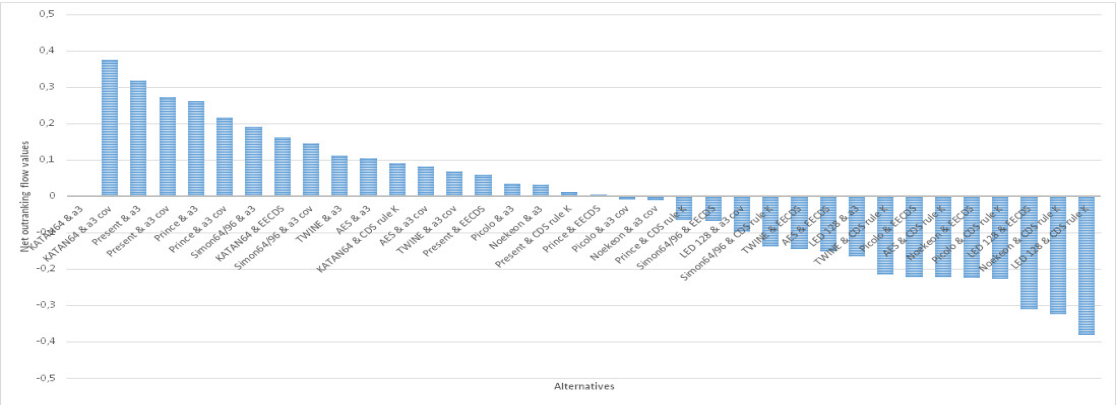

Figure 4. Net outranking flow for all LWC and TP

Table 5. Criteria values and final rank for each alternative

Alternatives	Criteria1	Criteria2	Criteria3	Criteria 4	Criteria 5	Criteria 6	Criteria 7	Criteria 8	Criteria 9	Criteria 10	Criteria 11	Net outranking flow values	Rank
AES &A3	1	1	11	3.32	21.92	0.9354	0.2276	2176	10714	2326	10733	0.1055	11
AES & A3-Cov	1	1	11	3.32	21.92	1	0.5088	4216	21188	636	5027	0.0822	13
AES & EECDS	1	1	11	3.32	21.92	0.9613	0.3011	3568	18976	5408	25615	-0.1516	27
AES & CDS rule K	1	1	11	3.32	21.92	0.9276	0.2086	2647	14386	4565	25992	-0.2222	31
NOEKEON & A3	1	1	18	3.41	21.20	0.9354	0.2276	2176	10714	2326	10733	0.0332	17
NOEKEON & A3-Cov	1	1	18	3.41	21.2	1	0.5088	4216	21188	636	5027	-0.0111	21
NOEKEON & EECDS	1	1	18	3.41	21.20	0.9613	0.3011	3568	18976	5408	25615	-0.2239	32
NOEKEON & CDS rule K	1	1	18	3.41	21.20	0.9276	0.2086	2647	14386	4565	25992	-0.3236	35
LED 128 & A3	0.5	1	50	5.25	82.08	0.9354	0.2276	2176	10714	2326	10733	-0.1656	28
LED 128 & A3-Cov	0.5	1	50	5.25	82.08	1	0.5088	4216	21188	636	5027	-0.0974	24
LED 128 & EECDS	0.5	1	50	5.25	82.08	0.9613	0.3011	3568	18976	5408	25615	-0.3102	34
LED 128 & CDS rule K	0.5	1	50	5.25	82.08	0.9276	0.2086	2647	14386	4565	25992	-0.3808	36
PRESENT & A3	0.8	2	17	2.09	19.44	0.9354	0.2276	2176	10714	2326	10733	0.3178	3
PRESENT & A3-Cov	0.8	2	17	2.09	19.44	1	0.5088	4216	21188	636	5027	0.2735	4
PRESENT & EECDS	0.8	2	17	2.09	19.44	0.9613	0.3011	3568	18976	5408	25615	0.0606	15
PRESENT & CDS rule K	0.8	2	17	2.09	19.44	0.9276	0.2086	2647	14386	4565	25992	0.0111	18
PRINCE & A3	0.5	1	13	4.06	18.64	0.9354	0.2276	2176	10714	2326	10733	0.2618	5
PRINCE & A3-Cov	0.5	1	13	4.06	18.64	1	0.5088	4216	21188	636	5027	0.2175	6
PRINCE & EECDS	0.5	1	13	4.06	18.64	0.9613	0.3011	3568	18976	5408	25615	0.0047	19
PRINCE & CDS rule K	0.5	1	13	4.06	18.64	0.9276	0.2086	2647	14386	4565	25992	-0.0659	22
Piccolo & A3	0.8	1	26	3.28	22.24	0.9354	0.2276	2176	10714	2326	10733	0.0356	16
Piccolo & A3-Cov	0.8	1	26	3.28	22.24	1	0.5088	4216	21188	636	5027	-0.0087	20
Piccolo & EECDS	0.8	1	26	3.28	22.24	0.9613	0.3011	3568	18976	5408	25615	-0.2216	30
Piccolo & CDS rule K	0.8	1	26	3.28	22.24	0.9276	0.2086	2647	14386	4565	25992	-0.2268	33
TWINE & A3	0.8	2	19	3.10	26.80	0.9354	0.2276	2176	10714	2326	10733	0.1125	10
TWINE & A3-Cov	0.8	2	19	3.10	26.80	1	0.5088	4216	21188	636	5027	0.0682	14
TWINE & EECDS	0.8	2	19	3.10	26.80	0.9613	0.3011	3568	18976	5408	25615	-0.1446	26
TWINE & CDS rule K	0.8	2	19	3.10	26.80	0.9276	0.2086	2647	14386	4565	25992	-0.2152	29
SIMON 64/96 & A3	0.667	2	22	2.18	26.56	0.9354	0.2276	2176	10714	2326	10733	0.1907	7
SIMON 64/96 & A3-Cov	0.667	2	22	2.18	26.56	1	0.5088	4216	21188	636	5027	0.1464	9
SIMON 64/96 & EECDS	0.667	2	22	2.18	26.56	0.9613	0.3011	3568	18976	5408	25615	-0.0665	23
SIMON 64/96 & CDS rule K	0.667	2	22	2.18	26.56	0.9276	0.2086	2647	14386	4565	25992	-0.1370	25
KATAN 64 & A3	0.8	16	17	2.04	17.52	0.9354	0.2276	2176	10714	2326	10733	0.4201	1
KATAN 64 & A3-Cov	0.8	16	17	2.04	17.52	1	0.5088	4216	21188	636	5027	0.3758	2
KATAN 64 & EECDS	0.8	16	17	2.04	17.52	0.9613	0.3011	3568	18976	5408	25615	0.1630	8
KATAN 64 & CDS rule K	0.8	16	17	2.04	17.52	0.9276	0.2086	2647	14386	4565	25992	0.0924	12

energy consumption suitable for data ciphering. Here, it should be pointed out that all the LWC under consideration satisfy the required level of security for the given application. In the proposed selection method, the weights used for ranking put more importance on energy consumption compared to security. The weights have been determined based on expert opinion for a given use case, by means of a questionnaire. In the given use case, the experts favour energy consumption criteria compared to other LWC quality criteria such as block size / key size ratio.

Analysing the first-ranked alternatives it is evident that the A3 protocol is the constituent of each alternative with a positive trend. This fact makes it particularly interesting for a further analysis. According to the simulation results, a characteristic of A3 topology protocol is the smallest traffic load. A3 protocol provides a slightly better result compared to A3 coverage, even though A3 coverage has the coefficient value of coverage outside the examined area, on average, higher than other protocols values by 2.14 times. This value is significant for further expansion of WSN without the additional load on the existing sensory nodes.

8. Conclusion

This paper has presented an MCDM approach to the analysis of lightweight cipher and topology protocol. The approach has been based on choosing the relevant criteria for this analysis obtained by simulating the behaviour of sensory nodes in a square area. Applying the methodological framework suggested in this paper, it has been concluded that not all the considered criteria are of equal importance. Their values of significance have been obtained through the simple additive weighting method. PROMETHEE II was further used to discover the final desirability ranking of each alternative.

This study may be significant for the sensory network analyses since the given methodological framework unequivocally shows which LWC and TP combination is the most suitable based on the simulation of the desired parameters. Given the fact that the multi-criteria decision-making method has not been applied so far in choosing a topology protocol or LWC, it is believed that this research will open an entirely new field of application for MCDM methods.

In this paper, the outdoor open-space planar area has been observed. Further research may focus on the areas of irregular shapes, those with a significant height difference regarding the small surfaces, as well as on expanding the list of LWC for ciphering messages. Another line of a future research may be the application of hybrid TP that would use some of the combination protocols that wouldn't be the same in the entire sensor network for the areas of irregular shapes. Another direction of research might be focused on the urban areas where a higher density of sensor nodes is to be expected. Moreover, a future direction of research would be to examine the relative efficiency of lightweight ciphers on different topology construction protocols using the Data Envelopment Analysis (DEA) method or to perform a comparative analysis using the MACBETH method.

REFERENCES

Afshari, A., Mojahed, M. & Yusuff, R., M. (2010). Simple Additive Weighting approach to Personnel Selection problem, *International Journal of Innovation, Management and Technology, 1*(5), 511-515.

Banik, S., Bogdanov, A. & Regazzoni, F. (2016) Exploring Energy Efficiency of Lightweight Block Ciphers. In Dunkelman O. & Keliher L. (eds), *Selected Areas in Cryptography – 22nd International Conference on Selected Areas in Cryptography - SAC 2015, Sackville, Canada, Lecture Notes in Computer Science, Springer, 9566* (pp. 178-194). DOI: 10.1007/978-3-319-31301-6_10

Beaulieu, R., Douglas, S., Smith, J., Treatman-Clark, S., Weeks, B. & Wingers, L. (2013). The SIMON and SPECK Families of Lightweight Block Ciphers, *IACR Cryptology ePrint Archive*, Report 2013/404.

Behzadian, M., Kazemzadeh, R. B., Albadvi, A. & Aghdasi, M. (2010). PROMETHEE: A comprehensive literature review on methodologies and applications, *European Journal of Operational Research, 200*(1), 198-215. DOI: 10.1016/j.ejor.2009.01.021

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A, Robshaw, M. J. B, Seurin, Y. & Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. In *International Workshop*

on Cryptographic Hardware and Embedded Systems: Cryptographic Hardware and Embedded Systems – CHES 2007, Lecture Notes in Computer Science book series – LNCS, 4727 (pp. 450-466). DOI: 10.1007/978-3-540-74735-2_31

Brans, J. P. & Mareschal, V. B. (2003). How to select and how to rank projects: The PROMETHEE method, *European Journal of Operational Research, 24*(2), 228-238. DOI: 10.1016/0377-2217(86)90044-5

Brans, J. P. & Vincke, P. (1985). A preference ranking organization method (The method for multiple criteria decision making), *Management Sciences, 31*(6), 647-656. DOI: 10.1287/mnsc.31.6.647

Brans, P. (1982). *Preference ranking organization method for enrichment valuations (in French language)*, Colloque d'aide à la décision, Université Laval, Quebec, 183-213.

Cazorla, M., Marquet, K. & Minier, M. (2013). Survey and benchmark of lightweight block ciphers for wireless sensor networks. In *10th International Conference on Security and Cryptography (SECRYPT),* (pp. 1-6).

Daemen, J., Peeters, M., Van Assche, G. & Rijmen, V. (2000). *The NOEKEON Block Cipher*. [Online]. Available at: <<http://gro.noekeon.org/>>, last accessed: Oct. 2021.

De Cannière, C., Dunkelman, O. & Knežević, M. (2009). KATAN & KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers. In *Proceedings of the 11th International Workshop, Cryptographic Hardware and Embedded Systems Systems – CHES 2009, Lausanne, Switzerland, Lecture Notes in Computer Science book series – LNCS, 5747* (pp. 272-288).

Escolar, S., Villanueva, F. J., Santofimia, M. J., Villa, D., del Toro, X. & López, J. C. (2019). A Multiple-Attribute Decision Making-based approach for smart city rankings design, *Technological Forecasting and Social Change, 142(C)* 42-55. DOI: 10.1016/j. techfore.2018.07.024

Geng, P., Liu, Y., Yang, J. & Chen, R. (2019). Analysis and improvement of backbone-based topology control for wireless sensor networks, *Journal of Computational Methods in Sciences and Engineering, 19*(1), 179-195. DOI: 10.3233/JCM-180885

Gong, Z., Nikova, S. & Law, Y. W. (2012). KLEIN: A New Family of Lightweight Block Ciphers. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues, RFIDSec 2011: RFID. Security and Privacy*, *Lecture Notes in Computer Science book series – LNCS, 7055* (pp 1-18). DOI: 10.1007/978-3-642-25286-0_1

Guo, J., Peyrin, T., Poschmann, A. & Robshaw, M. J. B. (2011). The LED Block Cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems CHES 2011: Cryptographic Hardware and Embedded Systems – CHES 2011, Lecture Notes in Computer Science book series – LNCS, 6917* (pp. 326-341). DOI: 10. 1007 /978-3-642-23951-9_22

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. & Manifavas, C. (2018). A review of lightweight block ciphers, *Journal of Cryptographic Engineering, 8*(2), 141-184. DOI:10.1007/s13389-017-0160-y

Iordache, G., Paschke, A., Mocanu, M. & Negru, C. (2017). Service Level Agreement Characteristics of Monitoring Wireless Sensor Networks for Water Resource Management (SLAs4Water), *Studies in Informatics and Control, 26*(4), 379-386. DOI: 10.24846/v26i4y201701

Kou, G., Chao, X., Peng, Y., Xu, L. & Chen, Y. (2017). Intelligent Collaborative Support System for AHP-Group Decision Making, *Studies in Informatics and Control, 26*(2), 131-142. DOI: 10.24846/ v26i2y201701

Labrador, M. A. & Wightman, P. (2009). *Topology Control in Wireless Sensor Networks - With a Companion Simulation Tool for Teaching and Research*. Springer Science + Business Media B.V. DOI: 10.1007/978-1-4020-9585-6

Liu, W., Luo, R. & Yang, H. (2009). Cryptography Overhead Evaluation and Analysis for Wireless Sensor Networks. In *2009 WRI International Conference on Communications and Mobile Computing* (pp. 496-501). DOI: 10.1109/CMC. 2009.31

Moradi, A., Poschmann, A., Ling, S., Paar, C. & Wang, H. (2011). Pushing the limits: a very compact and a threshold implementation of AES, *Advances in Cryptology EU-ROCRYPT 2011, Lecture Notes in Computer Science book series – LNCS, 6632* (pp. 69-88). DOI: 10.1007/978-3-642-20465-4_6

Othman, S., B., Trad, A. & Youssef, H. (2012). Performance evaluation of encryption algorithm for wireless sensor networks. In *2012 International Conference on Information Technology and e-Services* (pp. 1-8). DOI: 10.1109/ ICITeS.2012.6216690

Pachnanda, G., Singh, K. & Gangwar, L. (2013). Comparative Analysis of A3, EECDS and KNEIGH Tree Protocols in Wireless Sensor Networks, *International Journal of Electronics and Computer Science Engineering, 2*(3), 987-991.

Panhwar, M. A., Deng, Z., Khuhro, S. A. & Hakro, D. (2018). Distance Based Energy Optimization through Improved Fitness Function of Genetic Algorithm in Wireless Sensor Network, *Studies in Informatics and Control*, *27*(4), 461-468. DOI: 10.24846/ v27i4y201810

Petre, I., Boncea, R., Radulescu, C. Z., Zamfiroiu, A. & Sandu, I. (2019). A Time-Series Database Analysis

Based on a Multi-attribute Maturity Model, *Studies in Informatics and Control, 28*(2), 177-188. DOI: 10.24846/v28i2y201906

Qureshi, H. K. (2011). *Graph-theoretic channel modeling and topology control protocols for wireless sensor networks*, PhD thesis, City University London, London, United Kingdom.

Radosavljević, N. & Babić, Đ. (2021). Power Consumption Analysis Model in Wireless Sensor Network for Different Topology Protocols and Lightweight Cryptographic Algorithms, *Journal of Internet Technology, 22(1)*, 71-80. DOI: 10.3966/160792642021012201007

Radulescu, C. Z. & Radulescu, M. (2018). Group decision support approach for cloud quality of service criteria weighting, *Studies in Informatics and Control, 27*(3), 275-284. DOI: 10.24846/v27i3y201803

Staniec, K. & Debita, G. (2013). An optimal sink nodes number estimation for improving the energetic efficiency in wireless sensor networks, *Elektronika ir Elektrotechnika*, *19*(8), 115-118. DOI: 10.5755/j01.eee.19.8.5407

Suzaki, T., Minematsu, K., Morioka, S. & Kobayashi, E. (2011). Twine: A lightweight, versatile block cipher. In *ECRYPT Workshop on Lightweight Cryptography (LC11)*, (pp. 146-169).

Verma, J. S. & Sharma, S. (2020). Promethee Based Distributed Multihead Energy and Coverage Preserving Clustering Algorithm for Mobile Sensor Nodes, *National Academy Science Letters, 43*(5), 157-161. DOI: 10.1007/s40009-019-00817-x

Wu, W. & Zhang, L. (2011). LBlock: A Lightweight Block Cipher. In *International Conference on Applied Cryptography and Network Security – ACNS 2011, Lecture Notes in Computer Science – LNCS, 6715* (pp. 327-344). DOI: 10.1007/978-3-642-21554-4_19

Yin, R., Yin, X., Cui, M. & Xu, Y. (2019). Node importance evaluation method based on multi-attribute decision-making model in wireless sensor networks, *EURASIP Journal on Wireless Communications and Networking, 234*. DOI: https://doi.org/10. 1186/s13638-019-1563-5

Zavadskas, E. K., Stević, Ž., Tanackov, I. & Prentkovskis, O. (2018). A novel multicriteria approach–rough step-wise weight assessment ratio analysis method (R-SWARA) and its application in logistics, *Studies in Informatics and Control, 27*(1), 97-106. DOI: 10.24846/v27i1y201810

Zhaoxu, S. & Min, H. (2010). Multi-criteria Decision Making Based on PROMETHEE Method. In *2010 International Conference on Computing, Control and Industrial Engineering* (pp. 416-418). DOI: 10.1109/CCIE.2010.110