# Optimized Secure Clustering Scheme for Wireless Sensor Networks

Vincent Karovič, Olena Semenova, Maksym Prytula, Volodymyr Martyniuk, and Vladyslav Kuzniak

***Abstract*—Wireless Sensor Networks (WSNs) are increasingly employed in various applications, that require efficient, energy-saving and secure transmitting mechanisms. Clustering is a key technique in WSN to enhance scalability, reduce energy consumption, and manage communication. However, traditional clustering algorithms often lack adaptability to alterable wireless environments. This study presents an optimized secure clustering scheme for Wireless Sensor Networks that employs a fuzzy inference system to perform adaptive and secure cluster head selection. The proposed scheme is designed for WSN with a static topology, where sensor nodes remain fixed after deployment. This assumption matches Internet of Medical Things (IoMT) applications, such as patient monitoring systems and smart hospital infrastructure, where sensors operate in fixed locations. The proposed fuzzy inference system evaluates parameters of sensor nodes to select optimal cluster heads while mitigating malicious node participation. Next, a genetic algorithm was applied to optimize the parameters of the fuzzy inference system, including the membership function shapes and rule base indices, in order to enhance the accuracy of the proposed clustering scheme. MATLAB simulations demonstrate that the proposed scheme effectively identifies compromised sensor nodes and prevents them from assuming the cluster head role. The security validation confirms that the scheme achieves a high detection rate against internal attacks while extending overall network lifetime and maintaining the low latency. This study provides a feasible solution for secure and intelligent clustering in resource- constrained WSN.**

***Index Terms*—Artificial Intelligence, clustering, fuzzy logic, optimization, security, Wireless Sensor Networks**

## I. INTRODUCTION

As wireless technologies continue to advance, their range of applications expands correspondingly. Among the various innovative wireless networks, Wireless Sensor Networks (WSNs) have emerged as highly state-of-the-art systems, being implemented in nearly all types of environments, whether rural, suburban, or urban [1]. A WSN can be regarded as an assembly of autonomous spatially distributed sensors that are interconnected and capable of detecting, recording and transmitting variations in environmental physical parameters such as sound levels, temperature, pressure, and motion, while centralizing the collected data. The sensors are compact, intelligent, and small in size, and their data are transmitted wirelessly. WSNs find applications in multiple domains, including healthcare, smart home technologies, industrial automation, and environmental monitoring. Their robustness under extreme conditions renders them a vital element in numerous advanced technological systems, such as automatic irrigation systems, target surveillance, access to clinical records, landslide tracking, and predictive analytics for forest fire and disaster management. In this network topology, two factors – energy and security– are regarded as critical [2]. This is attributed to the features of sensor nodes, which, in contrast to traditional local network devices, are constrained by their battery life and resource limitations, including processing power and bandwidth, as well as frequent deployment in insecure situations [3].

WSNs have been widely applied; however, as the complexity of these networks increases, their security becomes increasingly critical. The primary security vulnerabilities arise from the placement of sensors in isolated locations and their spatial distribution. Unfortunately, conventional security measures are often impractical for sensor networks due to the significant overhead they introduce. Numerous researchers have conducted studies on effective security mechanisms that adhere to the resource and memory limitations inherent in WSNs [4]. Like any communication system, sensor networks require fundamental security services to safeguard data and resources against potential threats. To attain a high level of security, sensor networks necessitate lightweight encryption. Each sensor must strike a balance among cost, performance, and security level; however, achieving this equilibrium is challenging. In certain cases, developers compromise security by opting for cost-effective solutions that lack sufficient mechanisms, such as those for key distribution. A WSN demands more adaptable strategies for key distribution throughout the network. There are two primary approaches: traditional methods utilizing symmetric or asymmetric cryptography, and advanced techniques employing elliptic curve cryptography, which are particularly noted for their

Manuscript received 6 January 2026.

Vincent Karovič is with the Department of Information Management and Business Systems, Comenius University in Bratislava, Bratislava, Slovak Republic (e-mail: vincent.karovic6@fm.uniba.sk).

Olena Semenova and Volodymyr Martyniuk are with the Department of Infocommunication Systems and Technologies, Vinnytsia National Technical University, Vinnytsia, Ukraine (e-mails: semenova.o.o@vntu.edu.ua, vm4ukr@gmail.com).

Maksym Prytula and Vladyslav Kuzniak are with the Department of Information Radioelectronic Technologies and Systems, Vinnytsia National Technical University, Vinnytsia, Ukraine (e-mails: prytula@vntu.edu.ua, kuzniakvl@gmail.com).

DOI: 10.36244/ICJ.2026.2.10

efficient resource utilization compared to other public key methods. Furthermore, WSNs must transmit data securely to a central node through multi-hop communication, ensuring both data confidentiality and integrity. WSNs face various threats and attacks, including data loss, communication disruptions, service degradation leading to delays and denial of service [5, 6]. Consequently, the researchers must focus on primary security attributes of WSN: confidentiality, integrity, authentication.

Therefore, security issues must be carefully considered in multiple processes within WSN, including clustering, routing, and data transmitting. However, although numerous clustering algorithms for WSN have been proposed in the literature, most of them primarily focus on energy efficiency and network lifetime optimization while overlooking security considerations. Moreover, existing clustering algorithms often rely on deterministic methods that lack adaptability to dynamic network conditions and evolving attack patterns. Furthermore, limited attention has been paid to the joint optimization of clustering parameters and intelligent decision-making mechanisms, particularly through the use of novel artificial intelligence techniques. As a result, there remains a research gap in the development of secure and efficient intelligent clustering schemes that simultaneously address energy management, resource balance and resilience against malicious activities. Therefore, there is a need for an intelligent and secure clustering mechanism that simultaneously considers energy consumption and communication behavior of sensor nodes. The problem addressed in this paper is the development of an optimized secure clustering scheme capable of accurately evaluating node eligibility for cluster head selection while incorporating protection against abnormal or malicious behavior. To solve this problem, this paper presents a secure clustering scheme based on Artificial Intelligence techniques for WSNs.

The main contributions of this paper can be summarized as follows: 1) an secure clustering scheme for wireless sensor networks is proposed, integrating energy efficiency and security considerations within an intelligent framework; 2) an intelligent fuzzy inference system is developed to evaluate node eligibility for cluster head selection based on its parameters, enabling security-aware decision making; 3) an optimization algorithm is applied to optimize parameters of the fuzzy inference system, improving clustering accuracy.

Overall, the proposed study improves upon traditional clustering approaches by integrating several AI techniques into the scheme and utilizing security-aware parameters, thereby enhancing both accuracy of cluster head selection and resilience against malicious behavior.

The rest of this paper is organized as follows: we discuss the background in Section II and summarize the related work in Section III. The proposed scheme is described in Section IV and simulated in Section V. Its performance is evaluated in Section VI. Finally, we give the conclusions in Section VII.

## II. BACKGROUND

### *A. Clustering issues in WSN*

Clustering methods involve dividing nodes into separate regions known as clusters, each managed by the cluster leader node. By establishing clusters, these networks can achieve required scalability, with the cluster leader node referred to as the cluster head (CH), which coordinates the various regions. The cluster head gathers data from its member nodes, aggregates this information, and transmits it to the base station (BS). Data transmission from CHs to the BS can be performed with single-hop or multi-hop techniques. A CH may be either designated by the sensors within the clusters or predetermined by network designers. Various clustering algorithms have been developed to promote effective communication in WSNs. Notable clustering algorithms include LEACH [7], PEGASIS [8], TEEN [9], and APTEEN [10]. In the context of WSN, clustering has shown notable energy efficiency by enhancing network lifetime, bandwidth, and reducing energy consumption.

Clustering algorithms can be classified into two primary categories: distributed and centralized methods. Distributed systems use local information to form clusters, while centralized methods utilize the global knowledge of the network. The pioneering method for cluster head selection is the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol, which is based on a probabilistic approach [11]. It is noteworthy that each node in the system generates a random number, and if this number is below a specified threshold, the corresponding node will identify itself as the cluster head and send an advertisement message to all other sensor nodes in the network. Each non-cluster head node that receives this announcement considers the communication impact before deciding which cluster head to connect with.

Energy-efficient direction-finding approaches are of significance in the context of reducing energy expenditure, enhancing network efficiency, and prolonging the operational lifespan of networks. This is due to the fact that sensor nodes and base stations engage in the transmission of packets via wireless radio signals [12]. In the clustering process, a direct communication between each node and the CH is to be established. Subsequently, the CH disseminates the aggregated, compressed, and transmitted data to the BS or an alternative CH in the vicinity [13]. It has been demonstrated that a greater quantity of energy is expended when transmitting the same data to the BS directly than when sending it in stages over smaller distances. Consequently, researchers have directed their attention towards the field of clustering.

### *B. Artificial Intelligence*

Traditional clustering algorithms often struggle with dynamic environments and uncertain data. Artificial Intelligence (AI) provides heuristic approaches that may overcome the limitations of traditional deterministic or probabilistic methods [14]. AI techniques, namely Fuzzy Logic, Neural Networks, and Genetic Algorithms, may offer adaptive and intelligent solutions for clustering problem in WSNs. They

have been successfully employed to improve routing, load balancing, energy efficiency and security [15].

Fuzzy logic mimics human reasoning when dealing with uncertain or imprecise data using linguistic variables and fuzzy sets [16]. In WSN clustering, parameters like residual energy, node centrality, and distance to the base station often have vague boundaries, that is why it may benefit from fuzzy representation. Thus, in fuzzy-based clustering, a fuzzy inference system (FIS) can be applied to evaluate node suitability as a CH. The FIS processes all input variables using fuzzy rules to calculate a clustering score or CH suitability index for each node. Furthermore, security-aware fuzzy rules can ensure that only trusted nodes with sufficient resources are elected.

Neural networks (NNs) are computational models inspired by biological neurons and capable of learning patterns and relationships from real data. Traditional clustering methods often rely on predefined rules and algorithms. However, these methods may not adapt well enough to changeable network conditions or complex security threats. NNs, with their ability to learn from data, offer a promising solution for effective CH selection. In WSNs, NNs can learn optimal strategies for CH selection and clustering considering parameters of the nodes and the network. NNs are trained using these data to predict the best nodes for CH roles and optimal cluster sizes. Security-aware training includes identifying and penalizing nodes that exhibit malicious behavior. Neural networks can enhance WSN security by analyzing statistical data to assign trust scores to nodes. Thus, anomalous behavior can reduce a node's trust and CH candidacy.

Genetic Algorithms (GAs) are evolutionary optimization techniques inspired by natural selection processes. In clustering problems, chromosomes of genetic algorithm represent possible cluster configurations or CH assignments. The GA iteratively evolves better clustering schemes reaching an optimal or near-optimal configuration. When applying a GA, sensor nodes with suspicious behavior or low trust scores are penalized in the fitness function, reducing their chance of becoming CHs.

## III. RELATED WORKS

Various countermeasures have been suggested by researchers to ensure efficient and energy-saving clustering in WSN. Secure and reliable clustering schemes for WSN are considered and discussed in [17]. Study [18] introduces an effective fuzzy-based method for continuous node refinement, leveraging the multilayer routing architecture of WSNs. This work aims to enhance the reliable data transmission in cross-layer WSN. Unsuitable sensor nodes are identified based on their fuzziness. However, this study considers only residual energy of a node, neglecting traffic parameters of the network. An Energy Adaptive Distributed Energy-Efficient Clustering approach was proposed in [19] to be employed to ensure the resilience of WSNs throughout their operational lifespan while also improving the efficacy of their device nodes. Here, the main objective was lifetime of the sensor nodes in WSNs, and the further recommendation was for longevity while security issues have not been considered.

Paper [20] employs an ensemble methodology to create an improved hierarchical procedure for low-energy clustering, with the main objective of refining and optimizing the LEACH approach. The comparison results show that the improved method lengthens the network's lifetime by balancing the energy in each cluster. While the traditional LEACH method has been improved, no novel technology has been proposed.

Study [21] proposes a distributed protocol that establishes a cluster architecture and selects a rendezvous node with sufficient power for prolonged operation, situated in proximity to the mobile sink. A novel weight-based tree-construction method is introduced. The clustering approach of this algorithm creates a framework comprising clusters of varying sizes. Nevertheless, the proposed approach in suitable only for application in the Industrial WSN.

Work [22] presents an energy aware fuzzy-neuro clustering algorithm utilizing three key metrics for selecting cluster heads: residual energy, distance and node degrees. The algorithm comprises two main stages, namely clustering and multi-hop routing. Although the MATLAB simulation demonstrate the superiority of the proposed algorithm over the existing ones, it considers no communication security issues that restricts its utilization in complex environment of IoT. Paper [23] develops a clustering algorithm for networks that consumes less power. In this algorithm, few settings are be set before the cluster can be restarted. The clustering cycles operate under the assumption that all nodes possess an equal amount of energy. This algorithm identifies the node designated as the cluster head by evaluating the remaining energy, distance to the base station, and proximity to other members of the cluster. But its serious drawback is a greater amount of control messages. Study [24] suggests a fuzzy logic-based energy efficient clustering hierarchy where clustering is performed within a non-uniform WSN environment, with each node calculating a probability value based on three fuzzy input parameters, namely a node's centrality, residual energy and distance from the base station. The suggested protocol has two main stages – the formation of clusters and the collection of data. The drawback is that the nodes mainly join the closest to them cluster head, i.e., the key metric is the distance.

Paper [25] discusses a hybrid approach designed for the energy-efficient clustering of objects varying in size. Here, the clustering is to be performed across numerous layers. The layers are developed in a base station, which also applies neighboring node information. For data transmission both inter-cluster and intra-cluster directing is used. A significant improvement is a reduction in control messages. Simulation results prove that the proposed method has increased network stability and lifetime of the network. However, such hybrid clustering is quite complicated in implementation, that restricts its area of application.

Fuzzy algorithms for the election of cluster heads in cluster-based hierarchical routing protocols were developed in [13]. Instead of relying on a comprehensive aggregation of factors like remaining energy, proximity to the base station, resident detachment, concentration, and significance, each of these

fuzzy sensing-based frameworks utilizes a selective combination of these attributes in the process of choosing cluster heads. However, due to large number of attributes these algorithms require enhanced memory resources, which makes its implementation challenging. Work [26] proposes to utilize the fuzzy c-means clustering algorithm to establish k optimal clusters. The responsibility for determining the optimal number of clusters is assigned to the base station, which possesses greater computational capabilities and a global view of the network. A key strength of the proposed algorithm is that the initial clusters are predefined, and the subsequent procedure focuses on selecting cluster heads only from these verified and secure groups. This design provides an advantage over many conventional approaches, where cluster formation and CH selection are performed simultaneously. In the CH selection process for each cluster, residual energy and communication cost are used as fuzzy input variables. The drawback of this algorithm is a high computational overhead.

Paper [27] introduces a protocol that builds upon the LEACH protocol by incorporating both energy levels and the distances of nodes within WSN for the selection of CHs. Several methods were suggested to obtain the throughput of contention-free and contention-based protocols. A comparison between different protocols of the same class was performed. A new method to increase the efficiency of LEACH protocol was proposed. Nonetheless, this protocol is applicable solely in scenarios where a BS is present within the sensor field.

The conducted literature review demonstrates that a substantial number of studies have been devoted to solving the clustering problem in WSNs, whereas particular attention is given to modern approaches, especially such as artificial intelligence technologies as recent advances in intelligent methods provide new opportunities to enhance clustering efficiency beyond traditional techniques. However, when addressing the clustering problem, it is essential to simultaneously consider not only energy communication, but also communication traffic features and security issues in WSNs, as they have a significant impact on the reliability of the overall system [28].

While the methodologies presented in [13], [22], and [24] also utilize fuzzy inference systems to compute the chance of sensor nodes for CH election, the optimized secure clustering scheme proposed in this study distinguishes itself by addressing energy efficiency and network security. Unlike the aforementioned approaches, which depend on energy consumption and node's spatial positioning, our scheme integrates traffic-centric parameters, namely, the transmitting and delay ratios. The inclusion of these behavioral indicators promotes the indirect detection of anomalous activity, thereby reducing the risk of assigning the CH role to compromised or malicious nodes.

## IV. PROPOSED METHODOLOGY

### A. Secure clustering scheme

We propose an optimized secure clustering scheme for WSNs, as illustrated in Fig. 1. The overall process consists of three stages: data processing, intelligent cluster head selection, and cluster formation.

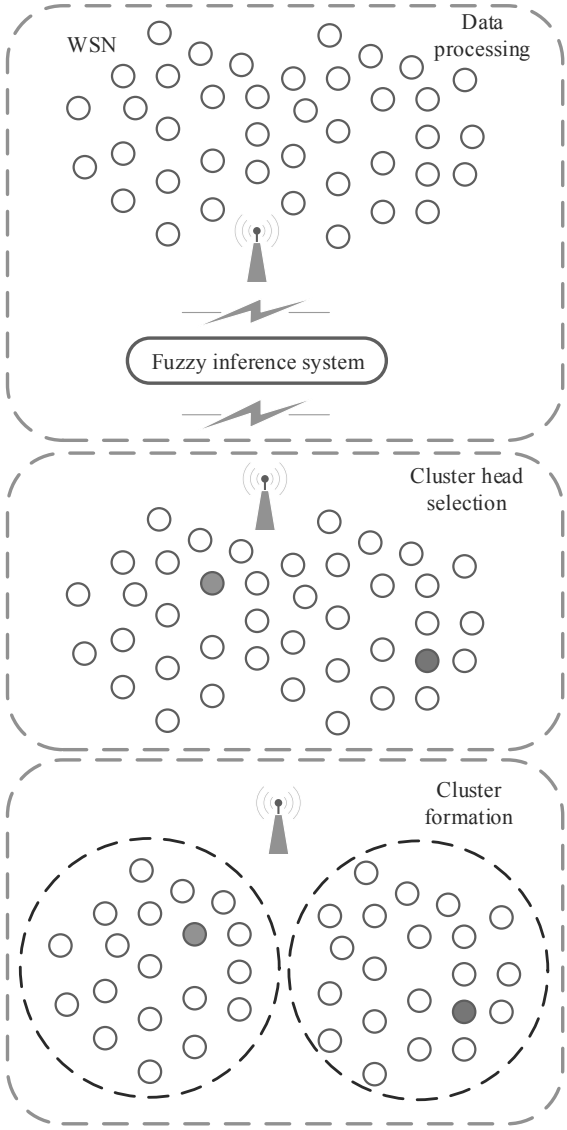


Fig. 1. Optimized secure clustering scheme

Initially, sensor nodes are deployed within the monitoring area and perform data acquisition. Each sensor node must be able to communicate directly with a BS. In IoMT wireless body area networks, this assumption is quite realistic because the distance between body sensors and the local gateway, such as a smartphone or smart hub, is usually only a few meters. During the data processing phase, key parameters describing each node's state are collected and forwarded to the BS for further evaluation. The BS runs the FIS, which serves as the decision-making component of the proposed scheme. By processing the input parameters, it evaluates the suitability (chance index) of each node to act as a cluster head. This index represents the degree to which a node is suitable for assuming the role of cluster head, taking into account not only energy efficiency but also traffic behavior and potential security anomalies. Based on

the computed chance indexes, nodes with the highest values are selected as cluster heads in the cluster head selection phase, as shown in the middle part of the figure. Once the cluster heads are determined, the network proceeds to the cluster formation stage. Ordinary sensor nodes associate with the nearest trusted cluster head in terms of distance, forming logical clusters represented by dashed boundaries in the figure. Within each cluster, member nodes transmit their data to the corresponding cluster head. The cluster heads perform data aggregation to reduce redundancy and securely forward the aggregated information to the base station, thereby enhancing both efficiency and network security.

### *B. Optimized fuzzy inference system*

The core of the proposed optimized secure clustering scheme is a fuzzy inference system.

Fig. 2 illustrates the structure of the FIS used for secure cluster head selection. The left-hand side of the diagram presents the standard processing flow of a Mamdani-type FIS [29]. The process begins with the block labeled "Data for selecting Cluster Head," which represents the crisp input parameters. These inputs are first processed in the fuzzification unit, where they are converted into degrees of memberships by using linguistic terms and membership functions and then forwarded to the inference engine. The inference engine operates based on the rule base, which contains the set of fuzzy if–then rules provided by the experts. Inference engine performs a fuzzy reasoning to map inputs to outputs considering these rules. The aggregated fuzzy output is passed to the defuzzification unit, where it is transformed into a crisp numerical value labeled as the "Chance index." Fig. 2 also illustrates the optimization mechanism. The genetic algorithm, shown on the right side of the diagram, is connected to the rule base, indicating that it is responsible for optimizing the parameters of the FIS, that involves fine-tuning membership functions and adjusting parameters of fuzzy rules to enhance system's performance. As medical sensor nodes have limited battery power, memory, and processing capabilities, the FIS is executed by the BS, which has greater processing power and energy resources. In a real IoMT environment, the BS can be a smartphone, a wearable smart hub, a bedside monitor, or a local hospital gateway.

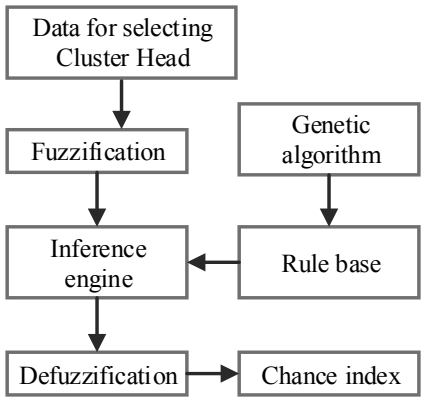


Fig. 2. Optimized fuzzy inference system for secure clustering

### *C. Parameters of the optimized FIS*

The output value of the FIS is the chance index of a sensor node (Ch). It refers to the computed probability of the node to be selected for a cluster head, based on input criteria, that determine its priority.

The proposed FIS has three inputs: residual energy (RE), transmitting ratio (TR), and delay ratio (DR).

The selection of input parameters is motivated by their strong relevance to both network performance and security issues. Although the proposed scheme does not explicitly include a dedicated trust score as a direct input to the FIS, it inherently captures security-related behavior through its input parameters. These parameters act as indirect yet effective indicators of node trustworthiness and reliability, enable the scheme to infer suspicious activity through deviations in communication and energy patterns. Together, these parameters provide complementary indicators, enabling the FIS to detect suspicious behavior of a node. By embedding these behavior-based cues into the fuzzy inference process, the scheme evaluates node credibility, avoiding the overhead associated with maintaining reputation management mechanisms, while still enhancing clustering security.

The residual energy of a sensor node is the amount of remaining battery power available in it. Anomalous depletion of residual energy in a sensor node may indicate the presence of denial-of-service (DoS) or flooding attacks, as such behavior often results from malicious activities that force the node to perform excessive communication or computation.

The transmitting ratio of a sensor node is the proportion of data packets successfully transmitted by the node compared to the total number of packets it was supposed to send. An abnormally high transmitting ratio in a sensor node indicate a network attack, as it suggests the node is being exploited to send excessive data, potentially due to malicious control or flooding-based attacks. Conversely, an abnormally low TR may be related to gray hole attack, black hole attack or replay attack.

The delay ratio of a sensor node is the ratio of the actual end-to-end delay experienced by data packets to the expected or predefined optimal delay. An elevated delay ratio in a sensor indicates a network attack such as selective forwarding or a replay attack, as it reflects increased latency potentially caused by congestion, malicious interference, or deliberate disruption of communication paths.

We have chosen for the inputs such linguistic terms as: "low", "medium", and "high" for RE; "small", "moderate", and "large" for TR and DR. This can be regarded as intuitive categories associated with general assessment terms and facilitates decision-making.

The input values are determined by membership functions, which are of a trapezoid type, which is computationally simple and provides smooth transitions between fuzzy sets, making it well suited for such resource-constrained systems as WSN. Moreover, in this study, normalized input values are used to map all variables into a common range that ensures consistency in fuzzy inference and prevents dominance of any single input.

The residual energy input value is defined as:

$$\mu_{low}(RE)=\begin{cases}1 \;\; if \;\; RE\le 10,\\ \dfrac{30-RE}{30-10} \;\; if \;\; 10<RE\le 30,\\ 0 \;\; if \;\; RE>30.\end{cases} \quad (1)$$

$$\mu_{med}(RE)=\begin{cases}0 \;\; if \;\; RE\le 10,\\ \dfrac{RE-10}{10-30} \;\; if \;\; 10<RE\le 30,\\ 1 \;\; if \;\; 30<RE\le 50,\\ \dfrac{70-RE}{70-50} \;\; if \;\; 50<RE<70,\\ 0 \;\; if \;\; RE\ge 70.\end{cases} \quad (2)$$

$$\mu_{high}(RE)=\begin{cases}0 \;\; if \;\; RE\le 50,\\ \dfrac{RE-50}{70-50} \;\; if \;\; 50<RE\le 70,\\ 1 \;\; if \;\; RE>70.\end{cases} \quad (3)$$

The residual energy represents the remaining battery energy of a sensor node and is expressed as a percentage of the initial node energy, ranging from 0% to 100%. The threshold values used in (1)–(3) were selected to divide the energy range into three operational regions corresponding to low, medium, and high energy levels. Nodes with RE below 30% are considered energy-constrained and therefore less suitable for the cluster head role due to the increased risk of premature energy depletion. The medium-energy region 30–70% represents nodes with sufficient energy to participate in network operations, while nodes with RE above 70% are considered highly suitable candidates for cluster head selection. These thresholds were chosen based on commonly adopted energy management principles in WSN clustering, where cluster heads are preferably selected from nodes with relatively high residual energy to balance energy consumption and extend network lifetime.

The transmitting ratio input value is defined as:

$$\mu_{sm}(TR)=\begin{cases}1 \;\; if \;\; TR\le 20,\\ \dfrac{40-TR}{40-20} \;\; if \;\; 20<TR\le 40,\\ 0 \;\; if \;\; TR>40.\end{cases} \quad (4)$$

$$\mu_{mod}(TR)=\begin{cases}0 \;\; if \;\; TR\le 20,\\ \dfrac{TR-20}{40-20} \;\; if \;\; 20<TR\le 40,\\ 1 \;\; if \;\; 40<TR\le 60,\\ \dfrac{80-TR}{80-60} \;\; if \;\; 60<TR<80,\\ 0 \;\; if \;\; TR\ge 80.\end{cases} \quad (5)$$

$$\mu_{lar}(TR)=\begin{cases}0 \;\; if \;\; TR\le 60,\\ \dfrac{TR-60}{80-60} \;\; if \;\; 60<TR\le 80,\\ 1 \;\; if \;\; TR>80.\end{cases} \quad (6)$$

The delay ratio input value is defined as:

$$\mu_{sm}(DR)=\begin{cases}1 \;\; if \;\; DR\le 30,\\ \dfrac{50-DR}{50-30} \;\; if \;\; 30<DR\le 50,\\ 0 \;\; if \;\; DR>50.\end{cases} \quad (7)$$

$$\mu_{mod}(DR)=\begin{cases}0 \;\; if \;\; DR\le 30,\\ \dfrac{DR-30}{50-30} \;\; if \;\; 30<DR\le 50,\\ 1 \;\; if \;\; 50<DR\le 70,\\ \dfrac{90-DR}{90-70} \;\; if \;\; 70<DR<90,\\ 0 \;\; if \;\; DR\ge 90.\end{cases} \quad (8)$$

$$\mu_{lar}(DR)=\begin{cases}0 \;\; if \;\; DR\le 70,\\ \dfrac{DR-70}{90-70} \;\; if \;\; 70<DR\le 90,\\ 1 \;\; if \;\; DR>90.\end{cases} \quad (9)$$

For the output, such linguistic terms as “very weak”, “weak”, “average”, “strong”, “very strong” were chosen.

The output value of chance index is determined by membership functions, which are of triangular type, as:

$$\mu_{vw}(Ch)=\begin{cases}1 \;\; if \;\; Ch\le 0,\\ \dfrac{25-Ch}{25} \;\; if \;\; 0<Ch\le 25,\\ 0 \;\; if \;\; Ch>25.\end{cases} \quad (10)$$

$$\mu_{w}(Ch)=\begin{cases}0 \;\; if \;\; Ch\le 0,\\ \dfrac{Ch}{25} \;\; if \;\; 0<Ch\le 25,\\ \dfrac{50-Ch}{50-25} \;\; if \;\; 25<Ch\le 50,\\ 0 \;\; if \;\; 50<Ch.\end{cases} \quad (11)$$

$$\mu_{av}(Ch)=\begin{cases}0 \;\; if \;\; Ch\le 25,\\ \dfrac{Ch-25}{50-25} \;\; if \;\; 25<Ch\le 50,\\ \dfrac{75-Ch}{75-50} \;\; if \;\; 50<Ch\le 75,\\ 0 \;\; if \;\; 75<Ch.\end{cases} \quad (12)$$

$$\mu_{st}(Ch)=\begin{cases}0 \;\; if \;\; Ch\le 50,\\ \dfrac{Ch-50}{75-50} \;\; if \;\; 50<Ch\le 75,\\ \dfrac{100-Ch}{100-75} \;\; if \;\; 75<Ch\le 100,\\ 0 \;\; if \;\; 100<Ch.\end{cases} \quad (13)$$

$$\mu_{vst}(Ch)=\begin{cases}0 \;\; if \;\; Ch\le 75,\\ \dfrac{Ch-75}{100-75} \;\; if \;\; 75<Ch\le 100,\\ 1 \;\; if \;\; Ch>100.\end{cases} \quad (14)$$

The proposed secure clustering FIS operates according to 27 fuzzy rules, which define the relationship between input data and the corresponding control action (Table 1). The fuzzy rule

base was constructed using an analytical evaluation of sensor node characteristics under various network conditions. The linguistic rules were formulated to reflect intuitive relationships between node's parameters, and its suitability for acting as a cluster head. The rule weights were initially set uniformly to ensure balanced influence of all rules and will be subsequently refined during the optimization process.

TABLE I
FUZZY RULES

| Rule | RE | TR | DR | Ch |
|---|---|---|---|---|
| 1 | Low | Small | Small | Weak |
| 2 | Low | Small | Moderate | Very weak |
| 3 | Low | Small | Large | Very weak |
| 4 | Low | Moderate | Small | Very weak |
| 5 | Low | Moderate | Moderate | Very weak |
| 6 | Low | Moderate | Large | Very weak |
| 7 | Low | Large | Small | Weak |
| 8 | Low | Large | Moderate | Weak |
| 9 | Low | Large | Large | Weak |
| 10 | Medium | Small | Small | Average |
| 11 | Medium | Small | Moderate | Weak |
| 12 | Medium | Small | Large | Weak |
| 13 | Medium | Moderate | Small | Average |
| 14 | Medium | Moderate | Moderate | Average |
| 15 | Medium | Moderate | Large | Average |
| 16 | Medium | Large | Small | Strong |
| 17 | Medium | Large | Moderate | Strong |
| 18 | Medium | Large | Large | Average |
| 19 | High | Small | Small | Strong |
| 20 | High | Small | Moderate | Strong |
| 21 | High | Small | Large | Strong |
| 22 | High | Moderate | Small | Very strong |
| 23 | High | Moderate | Moderate | Very strong |
| 24 | High | Moderate | Large | Very strong |
| 25 | High | Large | Small | Very strong |
| 26 | High | Large | Moderate | Very strong |
| 27 | High | Large | Large | Strong |

## V. COMPUTER SIMULATION

### A. Simulation of FIS

To validate the operability of the developed secure clustering FIS, we have utilized the Fuzzy Inference System Toolbox in MATLAB program, which has powerful Graphical User Interface. We assigned the inputs and output, and specified the rule base.

To check the functionality of the FIS, a series of simulations was carried out to generate the required output values, during which multiple experiments with various values of input parameters were performed.

Fig. 3 illustrates the outcome of one simulation of the FIS obtained in MATLAB for a specific set of input parameters. Each row corresponds to a fuzzy rule from the rule base provided in Table 1. The first three columns show the membership functions associated with the input variables (residual energy, transmitting ratio, and delay ratio) according to (1)–(9), while the last column shows the membership function of the output variable (the chance index) according to (9)–(14). The vertical lines indicate the current crisp input values, and the dashed horizontal lines represent the corresponding membership degrees. The shaded regions in the output membership functions represent the activation of the fuzzy rules. The final defuzzified value is displayed at the right top of the figure. A detailed description of the rule viewer and fuzzy inference process can be found in the MATLAB Fuzzy Logic Toolbox documentation [30].

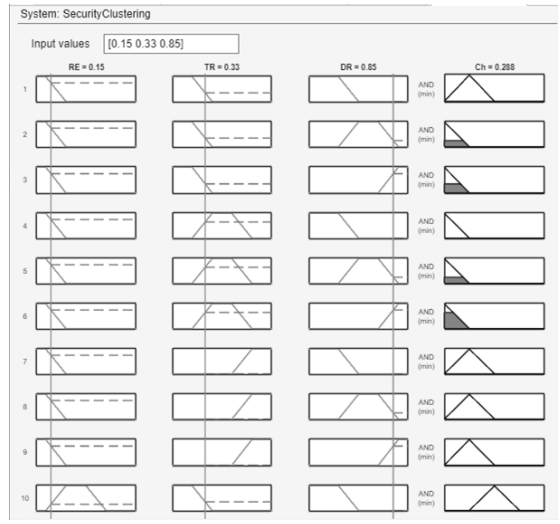

Fig. 3. FIS simulation

In this simulation, the residual energy equals 0.15, the transmitting ratio equals 0.33, the delay ratio equals 0.85. The calculated by the FIS chance index equals 0.288, which corresponds to a low suitability level for cluster head selection.

After having regarded the results of the simulations, the authors concluded that the simulated FIS operates properly.

### B. FIS Optimization

In this investigation, we optimized the parameters of the developed fuzzy inference system using a genetic algorithm in MATLAB. The optimization process aims to enhance the FIS performance by tuning membership functions and rule weights. MATLAB software provides a suitable environment for integrating fuzzy logic systems with optimization techniques. This approach is expected to yield improved control accuracy and system stability.

GAs were chosen as optimization technique due to their capability to handle nonlinear search spaces. The MATLAB GA tool iteratively generates populations of parameter sets (called chromosomes), applies selection, crossover, and mutation operations, and evolves toward an optimal solution. The process continues until convergence criterion is met, after which the best-performing parameter set is selected for the final implementation of the fuzzy inference system.

The chromosome for the developed FIS combines the parameters of all membership functions with the numerical weights of the fuzzy rule base. The chromosome can be expressed as a vector $\mathbf{p} = [\mathbf{q} \mid \mathbf{r}]$, where the first segment $\mathbf{q}$ contains the parameters of all input and output membership functions, whereas the second segment $\mathbf{r}$ encodes the structure of 27 fuzzy rules.

The developed FIS contains three input variables each with

three trapezoid membership functions encoded as

$$q_{in,m}=[q_{4(m-1)+1}, q_{4(m-1)+2}, q_{4(m-1)+3}, q_{4(m-1)+4}] \quad (15)$$

and one output variable with five membership functions encoded as

$$q_{out,t}=[q_{36+3(t-1)+1}, q_{36+3(t-1)+2}, q_{36+3(t-1)+3}]. \quad (16)$$

Altogether, the membership-function segment contains 51 parameters (genes):

$$q=[q_{in,1},\ldots,q_{in,9},q_{out,1},\ldots,q_{out,5}]. \quad (17)$$

The remaining part of the chromosome encodes the fuzzy rule base using 108 numerical genes. Each of the 27 rules is represented by four genes: three genes corresponding to the three input variables and one gene describing the output variable. Thus, rule k is encoded as

$$r_k=(r_{4(k-1)+1}, r_{4(k-1)+2}, r_{4(k-1)+3}, r_{4(k-1)+4}). \quad (18)$$

The full chromosome is the concatenation of the MF-parameter block and the rule-base block:

$$\mathbf{p}=[q_{in,1},\ldots,q_{in,9},q_{out,1},\ldots,q_{out,5},r_1,...,r_{27}]. \quad (19)$$

For the optimization process, a training dataset $\{(x_i, y_i)\}_{i=1}^{M}$ was assigned. For each sample $x_i$ the fuzzy system produces an output $\hat{y}_i = f_{\mathrm{FIS}}(x_i; p)$ obtained through fuzzification, rule aggregation and defuzzification with chromosome $p$.

The quality of a chromosome is quantified through the objective function that measures the discrepancy between the FIS output with parameters $p$, denoted as $f_{\mathrm{FIS}}(x_i; p)$ and the desired output $y_i$. In this study the root mean squared error (RMSE) is used as the fitness measure. So, the objective of the optimization is to minimize the RMSE:

$$J(p)=\sqrt{\frac{1}{M}\sum_{i=1}^{M}\left(y_i - f_{\mathrm{FIS}}(x_i; p)\right)^2}. \quad (20)$$

Thus, the optimization problem is:

$$p^* = \underset{p_{\min}\le p\le p_{\max}}{\operatorname{argmin}} \; J(p). \quad (21)$$

The final optimized FIS is obtained by substituting the optimal chromosome:

$$\mathrm{FIS}^* = f_{\mathrm{FIS}}(p^*). \quad (22)$$

This optimized system represents the best configuration of membership functions and rule base parameters found by the genetic algorithm with respect to the training dataset. This optimized system minimizes the prediction error on the training dataset and provides an improved model for estimating the priority of sensor nodes.

For the GA optimization process, the population size was 159 individuals. A crossover rate of 0.8 was applied to promote effective information exchange between parent solutions, while a mutation rate of 0.05 was used to preserve genetic diversity and avoid premature convergence. The training dataset used for optimization was generated through simulation by varying the input parameters within their normalized ranges and computing the corresponding desired output values based on predefined performance criteria. The original RMSE value was $216\times10^{-6}$ and after the optimization the RMSE value was $176.6\times10^{-6}$

Fig. 4 presents the training convergence curve of the genetic algorithm applied to optimize the parameters of the FIS within the proposed secure clustering scheme in MATLAB. The horizontal axis represents the generation number, the vertical axis shows the value of the optimization cost (minimum fitness value). The fitness function corresponds to the objective minimized during training, reflecting the error between the desired and obtained FIS outputs. At the initial generations, the optimization cost is relatively high, indicating that the randomly initialized population does not yet provide an optimal parameter configuration. The overall decreasing trend of the curve confirms the stability and effectiveness of the genetic optimization process in refining the membership functions and rule parameters of the FIS. As shown in the figure, the genetic algorithm terminated at generation 52. This confirms that the algorithm has reached a near-optimal solution.

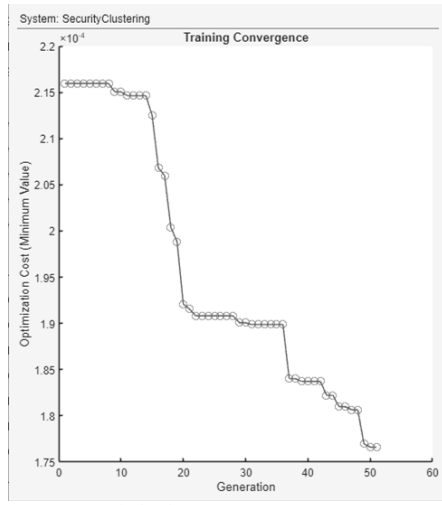


Fig. 4. FIS optimization

### C. FIS validation

The developed secure clustering FIS was validated in MATLAB environment by applying the System Validation Tool. The validation was performed on a dataset generated considering the data from the WSN-DS dataset. Fig. 5 presents the validation results of the developed FIS, that is its prediction accuracy. The upper plot illustrates the variation of three input variables across the validation dataset. Here, the inputs demonstrate diverse amplitudes, confirming that the validation was performed on the dataset containing sufficiently varied operating conditions. The horizontal axis, denoted as the Data Point Index, represents the sequential number of a validation sample. The Output corresponds to the chance index value. The bottom plot compares the reference output values from the dataset with the outputs predicted by the FIS. Considering the close alignment between two curves on the bottom plot, we may conclude that there is a strict correspondence between the expected and actual output responses, thus indicating reliable FIS performance under test conditions. Overall, the plot illustrates the ability of the FIS to estimate the cluster-head eligibility index for a node that is subsequently used during the clustering process.

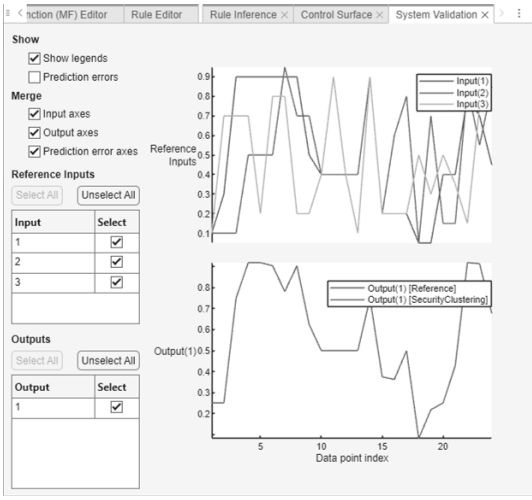


Fig. 5. FIS validation

## VI. EVALUATION

The proposed optimized secure clustering scheme can be employed in the Internet of Medical Things, to organize medical sensor nodes into secure clusters, ensuring reliable monitoring of patient health data. By incorporating security metrics in the decision-making process, the scheme safeguards sensitive medical information from unauthorized access and potential cyber threats, that is essential for IoMT [31].

Although some IoMT applications may involve mobile devices, the proposed framework assumes a relatively static wireless body area network. Two options are possible. The first is patient monitoring in intensive care units, where patients remain in fixed locations and both the sensors and the local gateway are stationary. The second is wearable health monitoring, where a patient may move, but the relative positions of the body sensors and the local cluster head (such as a smartphone or wearable hub) remain nearly unchanged. As a result, communication distances between nodes are stable, allowing the proposed fuzzy clustering scheme to improve energy efficiency and security without the need for frequent route updates.

To evaluate the operability of the proposed clustering scheme, a simulation was conducted in the MATLAB environment. The simulated model assumes a IoMT wireless sensor network, which may be applied for continuous patient monitoring. The network is composed of 100 medical sensor nodes transmitting sensitive physiological data and randomly deployed over a monitoring area of 100×100m. The CHs aggregate the data and forward it to an external BS. Initial energy of each sensor node equals 0.5 J. Packet size of transmitted data is 4000 bits.

The adversary assumptions consider compromised internal nodes capable of launching attacks such as blackhole, flooding, replay attack. For the computer simulation the attack scenario was as follows. Node #10 was modeled as executing a blackhole attack: it participates in routing, receives many packets from neighbors, but intentionally drops them and transmits almost nothing further. This results in a very low transmitting ratio of the node. Node #25 was modeled as executing a flooding attack by generating a huge number of transmission requests, that leads to increase in its transmitting ratio and accelerated energy depletion of neighboring sensor nodes. Node #40 was modeled as executing a replay attack, where previously captured packets were retransmitted to create artificial traffic patterns, this increases delay ratios.

The operability of the proposed fuzzy clustering scheme was compared with that of the conventional LEACH protocol under the discussed attack scenario. Fig.6 and Fig. 7 present the MATLAB simulation results of cluster head selection in LEACH protocol and in the proposed fuzzy-based secure clustering scheme respectively. Here, circles represent sensor nodes randomly deployed in the sensing field, crosses represent nodes under attack, stars represent nodes assigns as cluster heads.

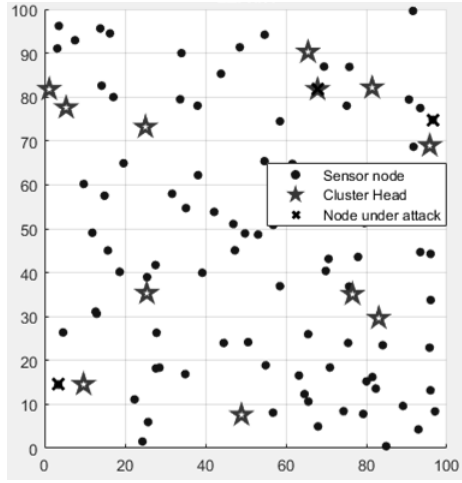


Fig. 6. Simulation of the LEACH protocol in MATLAB

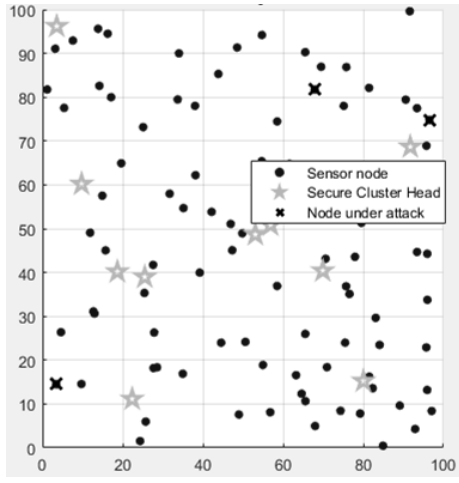


Fig. 7. Simulation of the fuzzy-based clustering in MATLAB

As classical LEACH relies on mathematical probability, it can randomly select a malicious node or a node with low energy as the head. In the graph in Fig.6, illustrating the simulation results, LEACH selected a malicious node as CH, marked as a crossed star. As shown in Fig.7, the proposed fuzzy-based scheme selected only secure nodes as cluster heads by

considering behavioral parameters and indirectly incorporating security indicators, thereby isolating malicious nodes and achieving a more secure clustering structure.

To ensures a comprehensive evaluation of efficiency and security aspects of the proposed clustering scheme, the performance of the two considered approaches was assessed by four metrics: network lifetime, energy consumption, latency, and robustness against attacks. The simulation results demonstrated that the proposed fuzzy scheme prolongs the network lifetime compared to standard LEACH. By penalizing nodes with low RE, the fuzzy scheme promotes more even energy load balancing in the network, that results in a slower decline in the network energy (Fig. 8). Here, the total network residual energy metric represents the aggregate remaining energy of all operational sensor nodes within the network measured at each successive simulation round. In a real scenario, each IoMT sensor node measures its own residual energy. These data are sent to the base station or to the cloud gateway, which aggregates these values from all nodes to compute the total network energy and monitor overall system status.

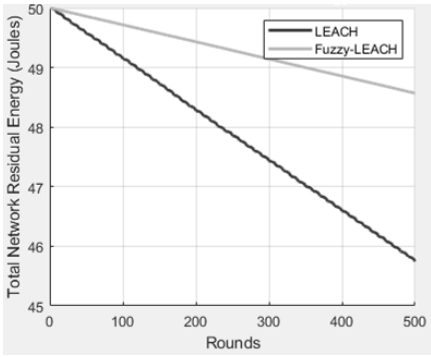


Fig. 8. Total network residual energy in MATLAB simulation

Latency was evaluated by tracking the average delay ratio of the selected CH. As the LEACH neglects the node behavior, it may select these compromised nodes as CHs, that results in latency spikes (fig.9). At the same time, the fuzzy-based scheme excludes nodes with high latency from the CH election.

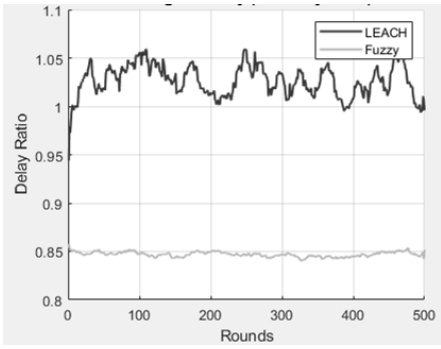


Fig. 9. Average latency in MATLAB simulation

The robustness testing showed that the proposed scheme achieved a near 100% avoidance accuracy; malicious nodes were systematically assigned a "Very Low" Chance Index and were successfully prevented from assuming the CH role in 500 rounds of simulation.

To quantitatively validate the resilience of the proposed fuzzy scheme against the attack scenario, a security analysis was performed based on standard classification metrics. The proposed scheme's capacity to isolate compromised nodes during the CH election phase was evaluated by computing the true positive rate (TPR) and the false positive rate (FPR).

The simulation results demonstrate that the proposed optimized fuzzy scheme achieves a high TPR of 100%, successfully identifying and isolating all simulated malicious nodes across the operational rounds. Furthermore, the scheme shows a low FPR of around 14% (fig. 10). Thus, the high classification accuracy confirms that integrating traffic-behavioral indicators with RE metrics via FL and GA provides a robust and secure clustering mechanism.

```
True Positives (TP)  : 3 (Attacks successfully blocked)
True Negatives (TN)  : 83 (Normal nodes allowed)
False Positives (FP) : 14 (Normal nodes erroneously blocke
False Negatives (FN) : 0 (Attacks missed by the system)
----------------------------------------------------------
Detection Rate (TPR) : 100.00%
False Positive Rate (FPR) :  14.43%
Overall Accuracy     :  86.00%
```

Fig. 10. Security validation metrics (confusion matrix)

In contrast to traditional trust models that require high computational overhead, the proposed scheme integrates trust management component into the FIS. In this scheme, trust is not maintained as a separate feature; it is computed and considered as the node's eligibility metric, the Chance Index. In case when multiple compromised nodes collude, the developed FIS may be deceived. The point is that defending against collusion requires a trust aggregation mechanism, which is beyond the scope of this inquiry. Moreover, the proposed system is developed for implementation in a stationary network topology, which is applicable for IoMT deployments. In highly dynamic environments, the proposed secure clustering scheme may have too high FPR, as it may consider benign moving nodes to be malicious ones.

## VII. CONCLUSION

Ensuring security in WSNs is an essential task because these networks often operate in sensitive remote environments, such as military or healthcare applications, where data integrity and confidentiality are vital. Moreover, unauthorized access can lead to data breaches or system manipulation. Without adequate security measures, WSNs would be quite vulnerable to different types of attacks as implementing security protocols, algorithms and schemes for clustering helps protect the network from malicious threats. Artificial Intelligence has opened new horizons in efficient and intelligent clustering for WSN. These methods enable optimized decision-making, thus improving efficiency and security of such networks.

In this study, a secure clustering scheme for WSNs was proposed, using a fuzzy logic-based approach for the cluster head selection process. A fuzzy inference system was developed for evaluating the suitability of nodes for being elected as cluster heads based on several input parameters, thus enabling more adaptive decision-making mechanism in WSN environment. The developed fuzzy inference system was implemented and simulated in the MATLAB program for

evaluating its effectiveness. To improve the performance of the fuzzy inference system, a genetic algorithm-based optimization procedure was applied to fine-tune its membership functions and rule base. The developed FIS was validated, that confirmed its operability. The proposed in this study optimized secure clustering scheme can be applied in clustering process within IoMT, where data security is often a critical issue.

Future investigations will be focused on integration of additional security parameters with other optimization techniques to further extend the applicability of the proposed approach. Moreover, the proposed secure clustering scheme may be extended through integration with lightweight blockchain mechanisms, validation on a real-world testbed and adaption to mobile WSN to enhance practical applicability.

## REFERENCES

[1] B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," *Journal of Network and Computer Applications*, vol. 60, pp. 192–219, Jan. 2016, DOI: 10.1016/j.jnca.2015.09.008.

[2] F. Afroz and R. Braun, "Energy-efficient MAC protocols for wireless sensor networks: a survey," *International Journal of Sensor Networks*, vol. 32, no. 3, p. 150, 2020, DOI: /10.1504/ijsnet.2020.105563.

[3] Mansour Lmkaiti, Ibtissam Larhlimi, Maryem Lachgar, Houda Moudni and Hicham Mouncif "Framework for Intrusion Detection in IoT Networks: Dataset Design and Machine Learning Analysis", *Infocommunications Journal*, Vol. XVII, No 2, June 2025, pp. 61–71., DOI: 10.36244/ICJ.2025.2.8

[4] O. Olufemi Olakanmi and A. Dada, "Wireless Sensor Networks (WSNs): Security and Privacy Issues and Solutions," *Wireless Mesh Networks - Security, Architectures and Protocols*. IntechOpen, May 13, 2020. DOI: 10.5772/intechopen.84989.

[5] F. Azzedin and H. Albinali, "Security in Internet of Things: RPL Attacks Taxonomy," in *Proc. of the 5th International Conference on Future Networks and Distributed Systems*, pp. 820–825, Dec. 15, 2021. DOI: 10.1145/3508072.3512286.

[6] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, "A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things," *IEEE Access*, vol. 8, pp. 219 709–219 743, 2020, DOI: 10.1109/access.2020.3037359.

[7] J. Kshirsagar and V. Sonaje, "Wireless Sensor Networks and the LEACH Protocol: Analysis of network using certain parameters for clustering and localization.," *International Journal of Computer Applications*, vol. 186, no. 41, pp. 1–6, Sep. 2024, DOI: 10.5120/ijca2024924003.

[8] V. K. Kumar and A. Khunteta, "Energy Efficient PEGASIS Routing Protocol for Wireless Sensor Networks," *2018 2nd International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*. IEEE, pp. 91–95, Sep. 2018. DOI: 10.1109/icmete.2018.00031.

[9] H. B. Magar, P. Sharma, V. Philip, and A. S. Ubale, "Optimizing wireless sensor network performance: TEEN vs. LEACH analysis," *AIP Conference Proceedings*, vol. 3222. AIP Publishing, p. 050003, 2024. DOI: 10.1063/5.0228211.

[10] M. Wang, S. Wang, and B. Zhang, "APTEEN routing protocol optimization in wireless sensor networks based on combination of genetic algorithms and fruit fly optimization algorithm," *Ad Hoc Networks*, vol. 102, p. 102 138, May 2020, DOI: 10.1016/j.adhoc.2020.102138.

[11] P. Subbulakshmi and M. Prakash, "Mitigating eavesdropping by using fuzzy based MDPOP-Q learning approach and multilevel Stackelberg game theoretic approach in wireless CRN," *Cognitive Systems Research*, vol. 52, pp. 853–861, Dec. 2018, DOI: 10.1016/j.cogsys.2018.09.021.

[12] J. Suhonen, M. Kohvakka, V. Kaseva, T. D. Hämäläinen, and M. Hännikäinen, "Low-Power Wireless Sensor Network Platforms," *Handbook of Signal Processing Systems*. Springer New York, pp. 381–419, 2013. DOI: 10.1007/978-1-4614-6859-2_13.

[13] A. Hamzah, M. Shurman, O. Al-Jarrah, and E. Taqieddin, "Energy-Efficient Fuzzy-Logic-Based Clustering Technique for Hierarchical Routing Protocols in Wireless Sensor Networks," *Sensors*, vol. 19, no. 3, p. 561, Jan. 2019, DOI: 10.3390/s19030561.

[14] O. Semenova, N. Kryvinska, A. Semenov, A. Rudyk, and A. Dzhus, "Intelligent Admission Control in Wireless Networks of IoT," *International Journal of Control, Automation and Systems*, vol. 23, no. 4, pp. 1262–1270, Apr. 2025, DOI: 10.1007/s12555-024-0603-z.

[15] Olivér Hornyák, "Intelligent Intrusion Detection Systems – A comprehensive overview of applicable AI Methods with a Focus on IoT Security", *Infocommunications Journal*, Special Issue on AI Transformation, 2025, pp. 61–76, DOI: 10.36244/ICJ.2025.5.8

[16] Mohd Aaqib Lone, Owais Mujtaba Khanday, and Szilveszter Kovács, "Implementation Guidelines for Ethologically Inspired Fuzzy Behaviour-Based Systems", *Infocommunications Journal*, Vol. XVI, No 3, September 2024, pp. 43–56., DOI: 10.36244/ICJ.2024.3.4

[17] P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, L. Buttyán: "Secure and Reliable Clustering in Wireless Sensor Networks: A Critical Survey", *Elsevier Computer Networks*, vol. 56, no. 11, pp. 2726–2741, July 2012, DOI: 10.1016/j.comnet.2012.03.021.

[18] R. Elavarasan and K. Chitra, "An efficient fuzziness based contiguous node refining scheme with cross-layer routing path in WSN," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 2099–2111, Jan. 2020, DOI: 10.1007/s12083-019-00825-0.

[19] R. K. Poluru, M. P. K. Reddy, S. M. Basha, R. Patan, and S. Kallam, "Enhanced Adaptive Distributed Energy-Efficient Clustering (EADEEC) for Wireless Sensor Networks," Recent Advances in *Computer Science and Communications*, vol. 13, no. 2, pp. 168–172, June 2020, DOI: 10.2174/2213275912666190404162447.

[20] P. Xie, M. Lv, and J. Zhao, "An improved energy-low clustering hierarchy protocol based on ensemble algorithm," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 7, Nov. 2019, https://doi.org/10.1002/cpe.5575.

[21] C. Zhu, S. Wu, G. Han, L. Shu, and H. Wu, "A Tree-Cluster-Based Data-Gathering Algorithm for Industrial WSNs With a Mobile Sink," *IEEE Access*, vol. 3, pp. 381–396, 2015, DOI: 10.1109/access.2015.2424452.

[22] A. Daniel, K. M. Balamurugan, R. Vijay, and K. Arjun, "Energy Aware Clustering with Multihop Routing Algorithm for Wireless Sensor Networks," *Intelligent Automation and Soft Computing*, vol. 29, no. 1, pp. 233–246, 2021, DOI: 10.32604/iasc.2021.016405.

[23] H. Li and J. Liu, "Double Cluster Based Energy Efficient Routing Protocol for Wireless Sensor Network," *International Journal of Wireless Information Networks*, vol. 23, no. 1, pp. 40– 48, Mar. 2016, DOI: 10.1007/s10776-016-0300-9.

[24] B. Balakrishnan and S. Balachandran, "FLECH: Fuzzy Logic Based Energy Efficient Clustering Hierarchy for Nonuniform Wireless Sensor Networks," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–13, 2017, DOI: 10.1155/2017/1214720.

[25] S. M. Bozorgi and A. M. Bidgoli, "HEEC: a hybrid unequal energy efficient clustering for wireless sensor networks," *Wireless Networks*, vol. 25, no. 8, pp. 4751–4772, May 2018 DOI: 10.1007/s11276-018-1744-x.

[26] A. Jain and A. K. Goel, "Energy Efficient Fuzzy Routing Protocol for Wireless Sensor Networks," *Wireless Personal Communications*, vol. 110, no. 3, pp. 1459–1474, Oct. 2019, DOI: 10.1007/s11277-019-06795-z.

[27] K. Shaukat *et al.*, "MAC Protocols 802.11: A Comparative Study of Throughput Analysis and Improved LEACH," *2020 17th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology*. IEEE, pp. 421–426, June 2020. DOI: 10.1109/ecti-con49241.2020.9158097.

[28] A. Abdulwahid and M. Salih, "Wireless Sensor Networks Applications, Challenges, and Security Requirements," in *Proc. of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies*, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey. EAI, 2022. DOI: 10.4108/eai.7-9-2021.2314823.

[29] R. Saatchi, "Fuzzy Logic Concepts, Developments and Implementation," *Information*, vol. 15, no. 10, p. 656, Oct. 2024, DOI: 10.3390/info15100656.

[30] MATLAB Fuzzy Logic Toolbox Documentation. [Online]. Available: https://www.mathworks.com/help/fuzzy/building-systems-with-fuzzy-logic-toolbox-software.html

[31] K. Svandova and Z. Smutny, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," *Journal of Multidisciplinary Healthcare*, vol. Volume 17, pp. 2281–2301, May 2024, DOI: 10.2147/jmdh.s459987.

**Vincent Karovič** is a graduate of the Faculty of Management, Comenius University in Bratislava. He has been working at the Faculty of Management, Comenius University, since 2017, where he teaches courses related to cybersecurity and IT management. His research focuses primarily on information systems and cybersecurity. Since his doctoral studies, he has specialized in the management of e-government as an extension of IT management research in the public sector. He is a member of the Department of Information Management and Business Systems and currently serves as the Vice-Dean for IT at the Faculty of Management, Comenius University.

**Olena Semenova** received the MSc degree in Radio Engineering in 2003 and the Ph.D. degree in Computer Systems and Elements in 2007 from Vinnytsia National Technical University, Vinnytsia, Ukraine. She is currently an Associate Professor in the Department of Infocommunication Systems and Technologies at Vinnytsia National Technical University. Her research interests include telecommunication networks and artificial intelligence. She has authored more than 180 scientific and academic publications.

**Maksym Prytula** received the MSc degree in Radio Engineering in 2007 and the Ph.D. degree in Radio measuring instruments in 2021 from Vinnytsia National Technical University, Vinnytsia, Ukraine. He is currently an Associate Professor in the Department of Information Radioelectronic Technologies and Systems at Vinnytsia National Technical University. His areas of research interest include magnetic sensors and magnetic field measurements. He has authored more than 80 scientific and academic publications.

**Volodymyr Martyniuk** received the BSc degree in Telecomunications in 2009 and the MSc degree in Telecomminication and Radiotechnics in 2010 from Vinnytsia National Technical University. He is currently a postgraduate student and works as a JavaScript Technical Lead at Playtika Holding Corp. His research interests include telecommunication networks, artificial intelligence, and programming.

**Vladyslav Kuzniak** received the MSc degree in Medicine in 2022 from Vinnytsia National Medical University and the MSc degree in Computer Science in 2024 from Vinnytsia National Technical University. He is currently a postgraduate student and works as a Head of AI Department at LITSLINK LLC. His research interests include telecommunication networks, artificial intelligence, molecular biology, and medicine.