A NOVEL AUTHENTICATION AND ACCESS SCHEDULING SCHEME TO IMPROVE THE PERFORMANCE OF WSN

K. Baskar[*], *P. Vijayalakshmi*[†], *K. Muthumanickam*[‡], *A. Arthi*[§]

Abstract: Wireless sensor network (WSN) is a kind of network specifically suitable for place where infrastructure and resources are playing a vital role. Moreover, nodes in a WSN are autonomous in nature. WSNs can be able to solve various real-time problems and issues like smart healthcare, smart office, smart energy, smart home, etc. As energy becomes one of the scarce supplies for this kind of network, attacks against authentication help to validate the legitimacy of sensor nodes become foremost important. Such attacks exhaust the power of nodes that are currently connected to a WSN, thereby reducing their lifetime. In this article, a zonal node authentication technique as well as optimal data access scheduling that renders data deliverance with improved quality of service and network lifetime is proposed. The results obtained from simulation for diverse WSN topologies accentuate the claim of our method over the existing solutions and demonstrate to be efficient in discovering legitimate sensor nodes with the optimal workload. Besides improved network lifetime, efficiency, and throughput, the proposed method also reinforces the security measures of the WSN by integrating node authentication.

Key words: *authentication, access scheduling, performance, security, WSN*

Received: October 14, 2021
Revised and accepted: July 5, 2023

DOI: 10.14311/NNW.2023.33.013

1. Introduction

WSNs are the most widely suitable choice for smart city appliances, like healthcare, surveillance, smart grids, ecological monitoring, etc. With the escalation of the recognition of advancement in wireless standards, the count of sensor nodes included in a WSN raised, and also the requirement for quality of service (QoS) becomes evident. Besides, because of the assorted characteristics of traffic flow, offering and analyzing diverse kinds of QoS necessities is currently one of the most

[*] K. Baskar – Corresponding author; Department of Artificial Intelligence and Data Science, Kongunadu College of Engineering and Technology, Tholurpatti, Tamilnadu, India, E-mail: baskark@kongunadu.ac.in

[†] P. Vijayalakshmi; Department of Computer Science and Engineering, Knowledge Institute of Technology, Salem, Tamilnadu, India, E-mail: viji.vietw@gmail.com

[‡] K. Muthumanickam; Department of Information Technology, Kongunadu College of Engineering and Technology, Tholurpatti, Tamilnadu, India, E-mail: muthumanickam@kongunadu.ac.in

[§] A. Arthi; Department of Artificial Intelligence and Data Science, Rajalakshmi Institute of Technology, Chennai, Tamilnadu, India, E-mail: arthi179@gmail.com

investigated research areas. As a solution to this issue, a method namely a dynamic routing scheme for ensuring the integrity of data and delay-differentiated services was designed in [1]. This method aimed to build a hybrid virtual field that separates all the packets of an application based on QoS requirements and assigns a unique weight to each packet. Afterward, each packet is routed toward the sink node through dissimilar paths. The authors claimed that their method improved the data rate of integrity relied on sensitive applications and also lessen end-to-end communication delay. A decentralized approach of QoS-aware middleware for WSNs that aims to minimize transmission delay between sensor nodes is presented in [2]. A trustworthy hardware-driven prototype was designed with the idea of offering better checkpoint provision in a distributed approach. Through this reliability-driven representation, the mobile host/node transmits the tested data to all its neighbors acting as a stable storage point. Furthermore, the reliability-driven design also acted as a way for recovering data during task execution. The algorithm presented in the aforesaid solutions namely zone header node election primarily divides the underlying network using a node authentication scheme and works on measuring the distance between all available sink nodes of the zone's header. Traditionally, sensor distribution network applications in nature have primarily included compute-intensive tasks such as engineering applications and scientific simulations. Nevertheless, with the development of contemporary web and networking expertise, novel creation of different applications that rely on clustering techniques in a WSN. The clustering-reliant applications are utilized in a large database, data mining, shared interactions, multimedia responders, effective reality, distributed revelation, web responder, telemedicine, and shared computing.

Recent WSN-based real-time applications are mostly collaborative, thus, besides requiring higher overall performance, require end-to-end based QoS features. For an instance, an image appliance built-in with rendering from current nodes of a cluster could require including higher bandwidth rate from each host to a front-end host of that cluster. Hence, the delivered information can be included with chosen frames and can be transmitted to the intended client node over the WSN. Likewise, for a file server relying on a clustering technique, a telemedicine appliance transmitting medical video might involve guaranteeing sufficient bandwidth distribution beginning from one host to another host. Hence, it can be driven to the client node over the WSN. To offer effective end-to-end based communication in a WSN, it is important to offer QoS for real-time applications during both communication and computation operations. Many such applications moreover exhibit packet broadcasting properties; thus, become accustomed based on the desired QoS intensity and availability of resources. Mehta et al. [3] presented a protection method against privacy violation in WSNs under an adversary model and determined a lower overhead value on the communication cost required for attaining a known and accepted location privacy. This method is capable of continuously monitoring the location privacy of vital objects.

Authentication becomes the essential primary pace to guarantee the truthful communication of data besides the security measures of a WSN [4, 5]. It's critical to make sure that only authorized users have access to a WSN's sensor nodes. As a result, privacy and security issues become the prevalent challenges for WSNs, and solutions like device access control [6, 7], password-based agreement solutions [8], authentication for a vehicle to grid environment [9], authentication and data access control mechanism for WSNs [10] and multifactor mechanism for ensuring data access in WSN [11] are presented in the past. Yet, such protocols or algorithms still suffered from improving QoS metrics that need to be addressed. A solution that is designed without holding security measures is becoming the root cause of numerous threats. The lifetime of a WSN is the major impacting issue in offering various network services. The power energy of the sensor nodes only decides the overall lifetime of the entire underlying network. By exploiting the power energy of each sensor node in an efficient way, the entire lifetime of the underlying network can be enhanced to a certain extent. The way of maximizing the lifetime of WSNs has been figured out in numerous ways in the past. However, scheduling the sensor nodes in a WSN by following several strategic schemes would diminish the energy exhaustion and enhance the overall lifetime of the network.

The open nature of the wireless communication medium between diverse sensor nodes of the WSN has been usually shared between them. However, if there are several sensor nodes have data packets for transmission to an intended recipient, then they would all attempt to broadcast together at an identical time. This scenario would generate heavy traffic and interference at some paths.To handle this issue, a scheduling mechanism is applied. Moreover, when the entire sensor nodes attempt broadcasting data using the same route, they need to wait for a longer time to access the medium; hence energy drop happens in every sensor node of the WSN and also influences the overall existence of the underlying network. This issue is resolved by assigning wake-up reminders to all sensor nodes, hence only pre-allocated sensor nodes could engage in data transmission at a particular time and energy loss has also possibly been minimized. There is another candidate solution namely the time division multiple access mechanism, however, it affects system throughput and also raises the delay of the data packets as well.

There exists $n + 1$ total number of paths connecting a source node and its communication partner in a WSN. Whenever there are several routes available at any time, the energy expenditure of an intermediate sensor node should be deemed to enhance the overall lifetime of the network. Although there exist many paths, the important constraints of the sensor nodes should be taken into consideration. A transmission support measurement is determined for path selection to complete these types of activities. In similar way, for any existing logical path, the lifetime improvisation support feature is determined to improve the overall lifetime of the WSN. Due to the unreceptive characteristics of sensor nodes, authentication has become a foremost concern that influences many important metrics like performance, energy expenditure, etc. Our proposed authentication system permits only legitimate sensor nodes to get involved in access scheduling to build sustainable access scheduling. The summary of the key contributions of our proposed approach is as follows:

- We investigated existing solutions through an organized literature analysis to discover convincing studies concerning the authentication of sensor nodes in a WSN.

- Our approach utilizes a centralized gateway to verify the legitimacy between sensor nodes and users. Our method besides considers the role of improving the performance of the underlying network through a dynamic scheduling algorithm. The information collected during this phase is also shared by the aforesaid authentication stage.

- The presented approach integrates the dynamic access scheduling method in the authentication stage and smears over the sensor nodes. The proposed method is also assessed to confirm its stability and efficiency.

2. Literature review

This section briefs about different attacks that target WSNs and security measures that can help WSNs perform better. There exist different types of attacks that can have diverse execution approach to target a WSN as follows.

- *Confidentiality of data* – Data confidentiality is a critical network security requirement that requires all sensitive data in the transmission and storage practice to be kept private. It is not permitted to disclose the information's content to any unauthorized user.

- *Data reliability* – An attacker cannot obtain the true content of information if confidentiality is guaranteed, but the recipient cannot assure that the information it accepts is exact since malevolent intermediate nodes can intercept, manipulate, or disturb the information during transmission. You can verify that the data won't change during the transference process by identifying data integrity.

- *Data accuracy* – The data freshness view emphasizes that each piece of data received is the most recent from the sender, causing it to stop receiving redundant data. The major goal of ensuring data freshness is to avert replay assaults.

- *Accessibility* – Availability necessitates sensor-reliant networks which can constantly give genuine users information access according to predetermined parameters. However, by falsifying and interfering with signals or using other ways to disrupt the system's availability, like denial of service attacks, the attacker can paralyze some or all of the sensor network.

- *Stability* – Dynamic variation in the underlying topology, as well as the disappearance or addition of nodes, makes wireless sensor networks highly dynamic and uncertain. As a result, wireless sensor networks should be able to respond to a range of security assaults, and moreover, even if an attack succeeds, still the performance of WSN can mitigate the impact.

- *Control of access* – To assure the authenticity of wireless sensor networks, access control involves the capacity to identify the individuals who access them. Users who are permitted to access the system, what type of system assets may be accessed, and how these resources can be used are all determined by access control.

Deploying any new technology over a WSN relied upon applications poses various issues like constrained battery resources, power, etc. Moreover, protecting important and vulnerable locale in WSNs is predominantly defenseless against security-compromising issues. One such issue is to either compromise a legitimate sensor node or introduce a fake sensor node through some means in WSNs.

2.1 Review of existing solutions against authenticating sensor nodes in WSNs

Watro et al. [12] proposed a public key that relied upon an authentication scheme suitable for WSN-based real-time applications. Intending to improve the security potency of the aforesaid protocol, a dynamic two-factor authentication relied upon protocol exploit smartcard and password information was presented in [13]. Khan et al. [14] presented a better solution with improved performance compared to Das et al. protocol [13]. Afterward, a shared authentication method relying on an elliptical curve cryptographic system is proposed in [15], however with no reduction in computational cost. Gope et al. [10] introduced a two-factor authentication protocol scheme for WSNs, however, Luo et al. [11] discovered that the two-factor security scheme exhibits some weaknesses and presented a better version. Still, the improved version is insecure. Turkanović et al. [16] proposed a temporal cum credential relied on a protocol for WSNs. But this security protocol failed to resist against few attacks like masquerade attacks and smart digital card attacks. A secret key agreement between the communication parties cum authentication scheme for WSNs is presented in [8]. However, this method failed to provide a solution against eavesdropping and identity pilfering attacks.

Subsequently, Banerjee et al. [17] developed a better version of the security scheme for preventing the aforementioned attacks. Conversely, Banerjee's solution also has failed to prevent impersonation attacks, brute force attacks, perfect forward secrecy, and secrecy of maintenance. Hence, we plan to propose a novel and lightweight scheme to avoid the aforementioned security issues.

2.2 Review of existing solutions against scheduling of sensor nodes in WSNs

Feng et al. [18] proposed a scheduling scheme that considers delay features while performing data aggregation operations to improve the lifetime of nodes. A shortest-route tree-based approach has been utilized to achieve the schedule. However, this scheme failed to consider the power energy of intermediate nodes that exists between the source and destination. Lu et al. [19] proposed a scheduling policy for self-learning that relied on data aggregation to facilitate the scheduling algorithm to be carried out during frame transmission. This approach failed to check the authenticity of the entities involved in transmission. Neamatollahi et al. [20] proposed a dynamic hyper round policy relied on a scheduling algorithm that exercises the power energy of sensor nodes for access scheduling hence maximizing the lifetime of the network can be achieved. Though this approach helps to improve the lifetime of the underlying network, it did not consider services like device or data integrity and authenticity. Wang et al. [21] presented an article on the multipurpose optimization scheduling approach to awakening sleeping sensor nodes in a heterogeneous WSN and also re-consider its coverage area. However, this solution failed to optimize the scheduling process. Chen et al. [22] proposed an energy-proficient broadcast scheduling scheme that incorporates each node's time slots when it is active. This method relied on an auxiliary graph and capable of exploiting the sensor node's active time slots to plan for access scheduling. But graph-based analysis typically takes a longer time to produce the desired outcome.

Hasan et al. [23] presented a path segmentation approach for improving the lifetime of the WSN through optimizing the sensor node's energy conservation. This method tried to improve the lifetime of the WSN only by considering each intermediate node involved during route establishment. An energy-proficient clustering procedure for enhancing the existence of the network was proposed by Liu et al. [24]. This method works by collecting all the sensor nodes and forming clusters based on energy efficiency. In addition, a cluster head node is selected based on important metrics like the residual energy of an individual node, the total number of data transmissions, and transmission coverage. But device authentication is one of the vital issues to be addressed in WSN which the authors failed to offer. Hajji et al. [25] presented a multi-restriction adaptive routing algorithm to improve the overall lifetime of a WSN. It produces a tree model for determining a route which utilized information like the sensor node's power energy and topological structure. However, tree-based analysis model would incur a longer time to determine an optimal route.

Kumar et al. [26] implemented backtracking relied-on scheduling scheme to support a WSN. It works on Langford compartmental creation that utilizes a pre-coded trajectory approach and collects all vital data for improving the lifetime of the WSN. The authors only focused on considering mobile sink nodes as a vital issue to determine the network lifetime. Gangwar et al. [27] presented a method which uses vital parameters of WSNs like deployment of sensor nodes, traffic, location of the destination node, and activity list for improving the existence of WSNs and performing access scheduling. This statistical approach aims to investigate only the performance of sensor nodes in an agroecological network. Idoudi et al. [28] proposed clustering scheme relying on an access scheduling scheme that makes use of local clustering multichannel forecasting and scheduling methods to improve the throughput rate. This approach focused to improve the network throughput by optimizing spatial reuse. We deduced from all of the ideas described in this section that optimizing network performance by scheduling and extending the lifetime of WSNs is still in its infancy. None of the methods focused on combining device authentication and access schedule to extend the life of the WSN. The authentication of sensor nodes prior to route establishment and data access is a critical design challenge for a WSN. As a result, we suggest a solution for WSNs that tackles the two major concerns and then builds a novel scheme to resolve them.

3. Proposed method

We propose a novel scheme to include both authentication and access scheduling on the WSN before permitting data exchange or any computational task to improve the overall lifetime of the underlying WSN. The suggested authentication scheme does not depend on one specific secret key model but utilizes a single secret key, i.e., a symmetric enciphering scheme which relies on the utilization of a network secret key plus a random nonce produced by the sensor node. For better understanding, different notations represented in the following sections are given in Tab. I.

Acronym	Remarks
$SN_{\mathrm{i}}/SN_{\mathrm{j}}$	Transmitting source sensor node and receiving sensor node
N_{j}	Unique nonce
K_{nk}	Network-wide secret key
$h(\cdot)$	Hash function
$K_{SN_{\mathrm{i}}}/K_{SN_{\mathrm{j}}}$	Enciphering secret key of $SN_{\mathrm{i}}/SN_{\mathrm{j}}$
$K^{\mathrm{j}}_{\mathrm{nk}}$	$(K_{\mathrm{nk}}, N_{\mathrm{j}})$, i.e., symmetric key produced by a sensor node
$PR_{SN_{\mathrm{i}}}/PR_{SN_{\mathrm{j}}}$	Private key of key of $SN_{\mathrm{i}}/SN_{\mathrm{j}}$
$PU_{SN_{\mathrm{i}}}/PU_{SN_{\mathrm{j}}}$	Public key of key of $SN_{\mathrm{i}}/SN_{\mathrm{j}}$
ID(SN_{j})	Unique identifier of SN_{j}

Tab. I *Various notations used.*

3.1 Initialization phase

Most of the security solutions discussed in the previous section for securing each sensor node of a WSN consider various parameters like intermediate storage space, processing power, and energy expenditure. The vital challenge lies in keeping the management operations more valuable despite the fact that even though an eavesdropper would compromise a sensor node, it should be much harder to discover all other secret keys of the network. This could be achieved by shielding all confidential information more securely through a suitable cryptographic system. We designed a novel method for producing a unique network secret key and an inimitable secret key for each sensor node which has a logical relationship with the network secret key. And, these tasks can be attained during WSN initialization. The essential steps of the WSN initialization phase are given as follows and it is given in Algorithm 1.

Algorithm 1 WSN initialization phase.

```
repeat
  when a new node joins
      $K_{\mathrm{nk}} \leftarrow h(K_{\mathrm{nk}})$
      $SN_{\mathrm{j}} \leftarrow \mathrm{key}(K_{\mathrm{j}})$
      $SN_{\mathrm{i}}$ broadcast $N_{\mathrm{j}}$
  Each $SN$ resides in the coverage area receives $N_{\mathrm{j}}$.
  $SN_{\mathrm{i}}$ generates key $K_{\mathrm{nk}}$
until sucessful authentication.
```

The network-wide global or secret key, K_{nk} is created by the designer and safely kept with its hash code $h(K_{\mathrm{nk}})$ to prevent password attacks. At the time of installation, each sensor produces a unique nonce N_{j} and also creates its enciphering key,

$K^{\mathrm{j}}_{\mathrm{nk}} = (K_{\mathrm{nk}},\, N_{\mathrm{j}})$. For instance, a sensor node SN_{i} might create its enciphering key, $K_{\mathrm{E}}^{SN\mathrm{i}} = (K_{\mathrm{nk}}, r_{SN_{\mathrm{i}}})$, where r denotes a random nonce. Every SN broadcast its unique nonce N_{j} for a while. Every node resides the current network transmission range receives N_{j} from its nearest node and might produce its unique enciphering key utilizing K_{nk}. Moreover, each SN that resides in the current network preserves a table that contains a pair of keys concerning each other SN in the current network. By utilizing the available information in each SN, two SNs can exchange necessary information between them.

3.2 Authentication and access scheduling phase

The proposed mutual authentication cryptosystem is making use of the request and reply mechanism. Whenever a sender node SN_{i} transmits data to its intended communicating partner, the recipient sensor node SN_{j} through a secure scheme, the request and reply mechanism begins. During message reception, each sensor node should complete the authentication phase that can be achieved by initiating secure communication involving any SN_{i} and SN_{j}. The overall diagrammatic representation that depicts the way the authentication phase can be accomplished is shown in Fig. 1. The authentication phase is designed with the intention to offer services like authentication, confidentiality, and integrity.

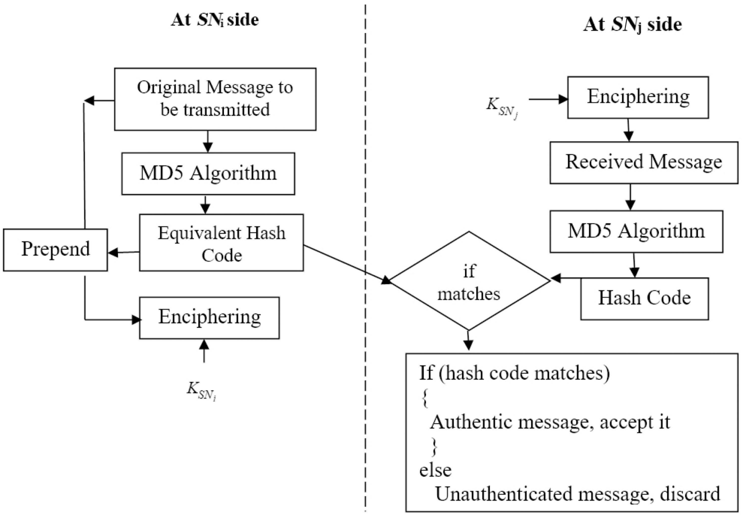

Fig. 1 *Processing flow of the authentication phase.*

The SN_{i} generates the message intended to transmit to its communication party SN_{j}. Message digest version 5 is utilized to determine its equivalent hash code and the outcome is embedded with the original message. The SN_{i} makes use of $K_{SN_{\mathrm{i}}}$ to encipher the message to be transmitted and hash code generated which is already generated. By utilizing the network key along with nsn, the SN_{j} node generates $K_{SN_{\mathrm{i}}}$. Next, by applying the newly generated key, $K_{SN_{\mathrm{j}}}$ the SN_{j} deciphers the received message and obtains the hash code. The SN_{j} reproduces a fresh copy of the hash code by taking the received data as input. If the computed hash code matches with the received hash code, then the received message is considered original and authentic. Algorithm 2 describes the entire process of the authentication phase.

Algorithm 2 Authentication process.

```
$h(K_{\mathrm{nk}}) \leftarrow K_{\mathrm{nk}}$ $\{K_{\mathrm{nk}}$ is the network-wide master key$\}$
Select random nonce $r$
Broadcast $r$ for a while
Compute $K_{SN_{\mathrm{i}}}$
$h(M) \leftarrow \mathrm{MD5}(M)$ $\{M$ can be either message or vital information about an $SN\}$

$M^{|} \leftarrow h(M) \parallel M$ {where $^{|}$ denotes a new variable and $\parallel$ denotes concatenation}
Transmit $Enc(M^{|}, SN_{\mathrm{i}})$
Compute $K_{SN_{\mathrm{j}}}(K_{\mathrm{nk}}, N_{\mathrm{j}})$
$Dec(K_{SN_{\mathrm{i}}}(M^{|})) \leftarrow (h(M), M)$
Generate $h^{|}(M) \leftarrow \mathrm{MD5}(M)$
Verification:
if $h(M) == h^{|}(M)$ then
  Authentication successful
else
  Discard request
end if
```

3.3 Secured data access

The presented technique involves the utilization of the breadth-first search concept for achieving secure data processing through access scheduling. This procedure exploits two important parameters: 'x' denotes the present load in each SN and 'y' represents the processing power or capability of an SN. To determine the present load condition on an SN, we used another parameter, $q(SN) = x/y$. Each SN that resides in the current WSN radio coverage range obtains an access scheduling request from all its neighboring SNs.

For example, suppose SN_{i} is heavily loaded, then it will request other nodes in the WSN by transmitting a request packet for a while which contains its unique identifier and access information (ID(SN_{j}), S_{i}). A nearest neighboring, SN_{j} will validate the received ID (identifier) against the IDs stored in its data storage. If matches, SN_{j} will expect to know the access details inferred from the previously received control packet. Conversely, if there is no match found then the SN will discard the control packet to evade a potential distributed denial of service attack. At the time of dealing with the data access details at SN_{i}, the receiving node, SN_{j} validates the access information by referring to q. Whenever the q value is equal to 0.75 and the existing resource availability index value (i.e., $x - y$) for completing the requested jobs from SN_{i}, then SN_{j} starts initiating the positive sign by sending an acknowledgment packet to SN_{i}.

If SN_{j} recognized that it has obtained the essential resources to complete the requested job, then SN_{j} handles the replied data packet to SN_{i}. If not, SN_{j} never reacts to the sensor node, SN_{i}. When the two constraints satisfy, SN_{j} acknowledges to SN_{i} by sending a response packet in an encrypted form that comprises its identity ID(SN_{j}), related secret key, and present status existing resource. Then, the SN_{i} does additional data accessing and uses its private key K_{pk} to decipher the received packet Dec(ID $\parallel K_{SN_{\text{i}}} \parallel q$). Then, SN_{i} validates the received ID of SN_{j} against the one stored in its catalog and if matches, SN_{i} selects the node key $K_{SN_{\text{i}}}$ and does a comparison against the received key in earlier stage. If $K_{SN_{\text{j}}}$ is equal to $K_{SN_{\text{i}}}$, then SN_{i} agrees to accept the acknowledgment packet from SN_{j}, otherwise discard it to prevent distributed denial of service attack. The SN_{i} node does a comparison of the value of q against all the authentic acknowledgments to determine lightly loaded SN. Finally, SN_{i} dispatches jobs to the authenticated sensor nodes for completion. Algorithm 3 describes the important steps of the safe and secure access scheduling process.

Algorithm 3 Scheduling process.

```
BEGIN
Read $SNL$ {where $SNL$ denotes list of $SN$}
for each $SN$ do
  if $Integration(i=1:size(SNL))$ and $SNL(i).PassedAuthentication$ then
    Route $r = RouteEstablish(SNL(i))$
  end if
  for each Route $r$ do
    Optimal route $or = Integration(i=1:size(r):maximum(r))$
    Scheduling $s = Integration(i=1:size(or))$
  end for
  for each $s$ of $SN$ do
    if $s \in or$ then
      $SN.Wakeup()$;
    else
      $SN.Sleep()$
    end if
  end for
end for
```

4. Results and discussions

We utilized NS2 as our simulation environment which would help to evaluate the performance of the proposed authentication and access scheduling technique. The experimental model was tested on a Dell machine incorporated with an Intel Core i7 CPU and 8 GB RAM. Each testing sample was assessed 10 times and its average value is determined to validate our proposed novel scheme. We considered the size of a data packet and control packet as 50 bytes and 20 bytes respectively. In addition, the data delivery operation in an SN is only executed when the power energy of that SN is about 50 J. The important simulation parameters associated with the simulation environment is listed in Tab. II.

Parameter	Remarks
Network coverage area ‘W × H’	2000 m × 2000 m
Node count	10, 20, 30, 40, 50, 60, 70
Transmission range ‘T’	200 m
Data rate	250 kBps
Data packets and size	7, 14, 21, 28, 35, 42, 49, 500 kB
No. of testings	10
Node’s primary energy	50 J

Tab. II *Simulation parameters.*

The following metrics are used to determine the overall performance of the suggested scheme and also to compare it with existing solutions.

(i) *Network lifetime (NL)* – This metric denotes the average count of data packets transmitted by an SN and should be received before the expiration of energy of the first node appears as a neighbor to SN. The NL metric helps to demonstrate the efficiency of an underlying routing protocol in the maintenance of the WSN’s lifetime.

(ii) *Data loss rate (DLR)* – The DLR parameter denotes the total quantity of data loss taking place at the time of data transmission from the SN to destination node DN.

(iii) *Transmission delay (TY)* – The delay time in transmission represents the amount of time taken to transmit a desired packet to the intended receiver.

Based on the underlying network coverage area and rate of data transmission, the existence of the network maintained by the proposed method and two existing methods 3F [9] and SSA [19] in WSN is examined. The network lifetime of a WSN is determined using data packets (DP) to be transmitted and discarded by an SN and its formula is given in Eq. (1).

$$NL = DP(Size_{\mathrm{s}}) - DP(Size_{\mathrm{d}}). \tag{1}$$

Tab. III lists different results obtained from the simulation that can help to analyze and validate the performance of the underlying WSN. Through simulation, we tried to transmit DP of varied sizes from 100 kB to 500 kB broadcast at the irregular time and the probability of drop rate of DP size of the proposed method is compared with that of the 3F and SSA. From the tabulated data, we inferred that there is an enhancement in the size of DP and NL of the proposed method compared to existing solutions.

The NL efficiency for various DP sizes from 100 kB and 500 kB of different approaches including our proposed method is compared in Fig. 2. Random networks can root each SN’s important characteristics like DP size, radio transmission range, and residual energy of diverse analysis of a WSN to deal with the underlying network’s lifetime. To facilitate the performance evaluation of our method, the same simulation environment with the identical time against our proposed

	WSN lifetime (s)		
Size of *DP* (kB)	Proposed method	3F	SSA
100	92	77	67
200	147	131	124
300	273	235	229
400	331	311	391
500	494	472	468

Tab. III *Comparing the efficiency of the proposed work.*

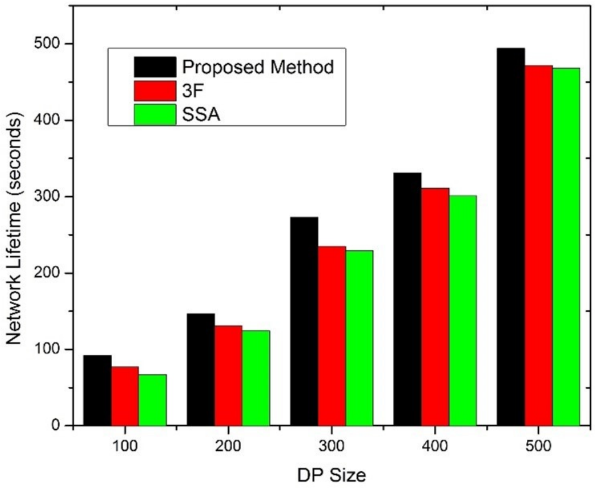

Fig. 2 *Comparing NL of various approaches including proposed method.*

method, 3F, and SSA solutions were investigated. As revealed in Fig. 2, the proposed method gives enhanced network efficiency compared to existing two schemes 3F and SSA irrespective of any *DP* size. This is achieved by selectively choosing intermediate *SN* nodes based on the present energy level at each *SN* between the source and sink. Our proposed method show a nine percent improved lifetime achievement in contrast to 3F and fourteen percent superior to SSA. The simulation results obtained for the proposed method shows an enhanced *NL* as it employs the zone-based data forwarding technique in a WSN that partition the underlying network according to zone distance evaluation. Determining the *DLR* of a WSN is also a vital performance metric which should be kept as low as possible for network sustainability. The *DLR* of the WSN is determined based on the size of *DP* being transmitted and the total count of *DP* obtained by the receiver at a particular time as shown in Eq. (2).

$$DLR = Size(D_{\mathrm{s}}) - Size(D_{\mathrm{r}}), \tag{2}$$

where, $Size(D_{\mathrm{s}})$ and $Size(D_{\mathrm{r}})$ denotes the size of the data packet to be transmitted and size of the data received by the receiver in a WSN. There are total of 100 sensor nodes deployed with fixed data sizes and the same testing is repeated 10 times. When the size of the *DP* is raised, the overall performance of each method used for evaluation improves, as shown in Tab. V. Our proposed method causes minimal *DLR* since it follows the optimal distance discovering technique for finding the transmission cost. In addition, the proposed method shows improved performance compared to the performance of other existing methods.

	WSN lifetime (seconds)		
Size of *DP* (kB)	Proposed method	3F	SSA
100	23	30	33
200	26	32	35
300	31	36	38
400	28	22	24
500	23	35	38

Tab. IV *Evaluation of DLR parameters.*

An evaluation involving *DP* size from 100 kB to 500 kB with different data transmission and data loss is calculated as shown in Fig. 3. It is inferred that when the *DP* size is about 300 kB the *DLR* through the proposed method is 31 kB, 39 kB by the 3F method, and 40 kB by the SSA method. This is anticipated because of the minor variation when handling bandwidth relied service provisioning

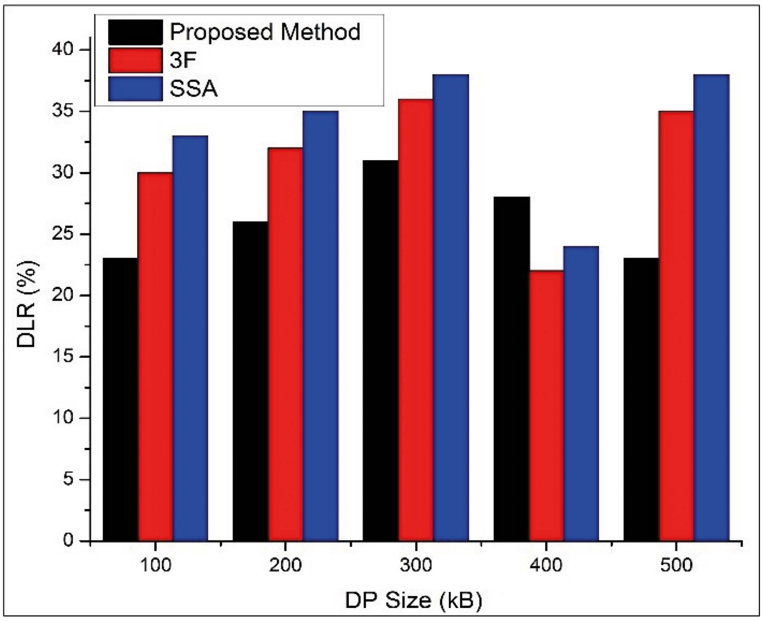

Fig. 3 *Performance assessment using DLR.*

Moreover, we inferred that when the proposed method handles a large amount of data for a lengthy time, the data packets belonging to different size was considered minimal in the case of the 3F method and the SSA method. From Fig. 3, it is true that the proposed method's DLR has considerably increased when the DP size is 400 kB, but showed a 36% of improved data rate and 65% compared to SSA. The combined utilization of zone-based route establishment and bandwidth relied on service provision keeps the proposed method highly accessible to all the SNs and offers effective security, thus providing a minimal rate of data loss. To demonstrate the performance achievement of the proposed method, we explored the important performance metric namely TY, and compare it with 3F and SSA. Each time, an SN propels data to its communicating partner; it uses the sink SN and zone header for intermediate transmission and reaches its partner. The TY metric is intended to measure the time required by each SN to reach its intended recipient node at the time of delivering data as shown in Eq. (3).

$$TY = (E_{\mathrm{t}}) - (A_{\mathrm{t}}) \cdot (N_{\mathrm{DP}}), \tag{3}$$

where E_{t} and A_{t} represent the actual and anticipated time for data deliverance concerning the number of data packets N_{DP} to be transmitted during each testing stage. The final simulation result concerning TY of the proposed approach compared to existing solutions is tabulated in Tab. V. It is achieved by measuring the number of data packets being sent at a particular time.

	Transmission delay (ms)		
Number of packets (kB)	Proposed method	3F	SSA
7	28.23	34.32	38.14
14	34.21	40.09	47.47
21	40.65	45.15	52.93
28	47.15	53.16	58.09
35	36.09	42.63	51.99
42	43.20	50.54	54.50
49	49.33	53.77	59.78

Tab. V *Comparing TY of different methods including the proposed method.*

In Fig. 4, the comparison between the existing data deliverance mechanism and our proposed method concerning to TY is analyzed. It is observed that when the DP size is raised, the zone header election technique that relies on distance measure be likely to segment the underlying WSN according to distance metric and enable the data forwarding process using the embattled zone header node. This indicates saving transmission time during preferred data forwarding. Thus, the proposed method is designated to be able to minimize the TY parameter for dissimilar packets with different sizes. The method exhibits the capability to explore minimal transmission delay at the time of transmitting a large number of DPs between the SN and its DN through capitalizing network coverage area.

Incorporating data access scheduling with a lightweight authentication technique through optimal policy plan results with reduced TY value as incurred by the proposed method. By utilizing bandwidth optimization-relied service prerequisite appliances, isolated zone header information is obtained by measuring the

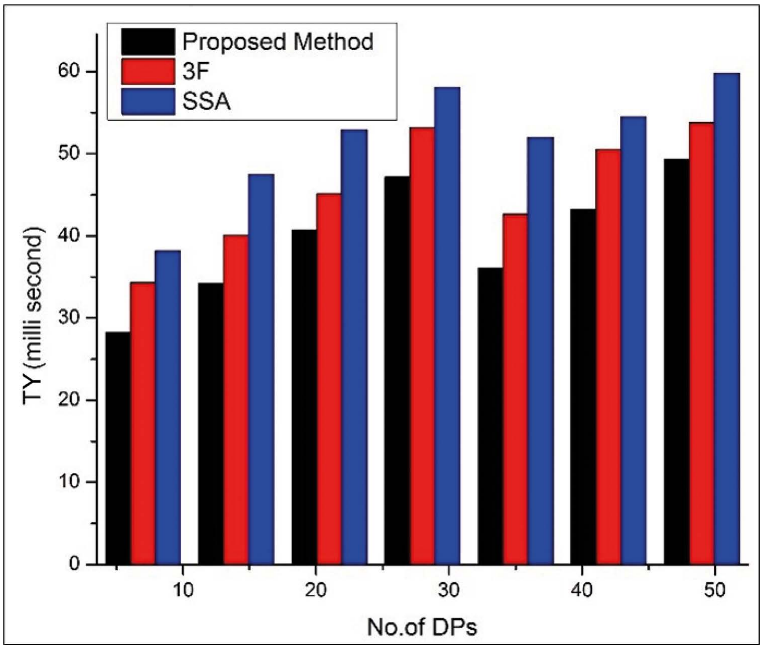

Fig. 4 *Performance assessment using TY.*

distance at various times ensuing reduced or acceptable TY value. After choosing a suitable zone header node, the SN starts transmitting the DPs and subsequently to the DN, thus dropping the TY value. While the conventional data routing methods might transmit the desired DPs through all intermediate SN and thus would raise the TY value of each transmission. By separating the zone header and SNs, the header node can perform optimal data forwarding and also would send the desired data packets to the intended recipient in a WSN. By employing the proposed method, it is possible to reduce the TY value to a certain extent. From the literature survey, we inferred that cryptographic algorithms like the RC4 and message digest version 5 are computationally inexpensive for adaptation in a WSN. They are selectively chosen as they offer service to ensure message integrity and data confidentiality respectively. Tab. VI gives details about analyzing the application of RC4 algorithm and MD version 5 algorithm for data security in WSNs and energy conservation by the nodes.

Algorithm/message (bytes)	Processing time (ms)	Energy utilization (μJ)
MD5 / 16–32	MD: 1.638	43.021
	PP: 0.517	14.236
RC4/ 16	SD: 0.309	2.962

Tab. VI *Analysis of adaptation of suitable cryptographic algorithm.*

Where 'MD' denotes message digest, 'PP' implies pre-processing, and 'SD' represents secure data. Whereas handling messages of 32 bytes in length, the message digest algorithm V5 incurs 1.38 ms and spends energy of 43 μJ. Likewise, for handling messages about 16 bytes in length, the RC4 enciphering process requires 0.43 ms to complete the initialization stage in addition to 0.82 ms for handling the ciphering procedures. The energy utilization of our scheme is validated against the solution proposed in [28]. Tab. VII demonstrates the energy utilization for data transmission between two communicating partners with unusual attacking period.

		Transmission delay (ms)			
Method name	Attacking time (s)	0	1	2	3
EASS	2	39.63	26.54	29.16	31.71
	4	31.35	21.76	23.09	23.70
	6	29.07	17.71	20.38	20.79
Proposed method	2	38.07	25.02	27.98	29.99
	4	31.21	21.05	22.11	23.15
	6	27.19	16.67	18.58	20.31

Tab. VII *Energy utilization of the proposed method against EASS.*

We assume that an SN in a WSN constantly accepts and also forwards desired DPs from neighboring SNs. An eavesdropper may launch an illicit operation after a preset time to meddle with the SN's data. When no attack is considered, the methods including the proposed method almost incur the same energy utilization value. During an attack, the proposed method incurs minimal energy compared to the EASS [29] method.

5. Informal security analysis

The designer provides a unique ID and a network-wide secret key for each SN. The secret key is stored as a hash function $h(K_{\mathrm{SN}})$. Each SN is permitted to generate a random nonce r, which helps to strengthen the enciphering process.

Definition 1 *Attack against the master key and encryption process.* An eavesdropper can try to obtain the master key, nonce, and then try to break the enciphering process. He/she also tries to perform traffic analysis, replay attack, or man-in-the-middle attack. As, the nonce is shared through a secure channel, and the master key is stored as a hash code, the eavesdropper to acquire vital information.

Definition 2 *Anonymity.* In our proposed scheme, all identities and nonce are kept in a write-protected area where only the administrator can access it. And the master key is protected using a hash function. Thus, the adversary to identify the identities of an *SN*. Our proposed scheme satisfies the requirement of anonymity.

Definition 3 *Perfect forward secrecy.* Let an adversary know the SN's secret key K_{SN}. As each SN computes its key $K_{SN_{\mathrm{i}}} = (K_{\mathrm{nk}}, N_{\mathrm{j}})$, the adversary cannot obtain N_{j} due to secure channel protection. Thus, our scheme is robust against perfect forward secrecy.

Theorem 1. *Authentication process is secure against forgery attack.*

Proof. At SN_{i} side:
Step 1: $K_{SN_{\mathrm{i}}} \leftarrow (K_{\mathrm{nk}},\, N_{\mathrm{j}})$
Step 2: $M^{|} \leftarrow h(M) \parallel M$
Step 3: Prepare $Enc(K_{SN_{\mathrm{i}}},\, M^{|} \parallel TS_1)$
It is impossible for the adversary to get the secret key from $h(K_{\mathrm{nk}})$.
At SN_{j}:
Step 1: $K_{SN_{\mathrm{j}}} \leftarrow (K_{\mathrm{nk}}, N_{\mathrm{j}})$
Step 2: Prepare $Dec(K_{SN_{\mathrm{j}}}, M^{|} \parallel TS_1)$
Step 3: If TS_1 is recent copy then compute $h^{|}(M) \leftarrow h(M)$
Step 4: If $h(M) == h^{|}(M)$ then accept SN_{i} as authentic
It is impossible for the adversary to perform a replay attack using a time stamp TS.
Hence, proved. □

6. Discussions

(i) *Authenticity and confidentiality* – The credential information disclose in our method depends only on the nonce and network-wide secret key. In case, an eavesdropper unethically discovers the value of nonce, it is impractical to acquire the network-wide secret key that is kept secure in hash code in SNs at the time of deployment. Moreover, the SN or DN can consider the received message as genuine provided the computed hash value equals the acquired hash value from the SN. Hence, the proposed lightweight and novel security idea can effectively thwart the foe nodes in a WSN from purposefully sending a counterfeit messages to any SN with the intention of compromising or making it a fake node. Besides, data protection, i.e., confidentiality can also be achieved through enciphering the message being sent along with its equivalent hash value. Since the key used for enciphering process is spawned by utilizing both the nonce and network-wide secret key which are dynamically generated, it never gives a chance to a challenger to crack messages whilst transferring them to the intended recipient.

(ii) *Replay attacks* – Since the hash value h and a nonce N are dynamically produced while data transmission, they are unique for each communication. The DN of the current network can confirm and if necessary, reject the current h and N values to evade replay attacks. One of the remarkable advantages of such novel execution is that it authorizes the DN to discover replayed packets with no need of recomputing the hash value. A similar procedure could also be exploited on the DN side.

(iii) *Forward secrecy* – After initiating the proposed authentication procedure randomly at any SN, the shared secret key is utilized only for a particular time before being wrecked by a potential eavesdropper. SNs apply the same secret key to confirm the recipient SN's authentication procedure. This is because the authentication procedure takes place merely one time at the start of the SNs initialization stage. Conversely, if an eavesdropper finds the secret key to break the authentication process, it becomes useless after the preliminary authentication operation. The public key technique is explored to encipher the information during access scheduling.

From the aforesaid discussions and investigational trials, we claim that our proposed access scheduling mechanism is not only improves the lifetime of the WSN but moreover secured it. It helps to improve the data access scheduling operations and performance optimization policy of SNs in a WSN environment. The overall performance of our method outperforms existing solutions and is both sustainable and secure.

7. Conclusions and future

In this paper, we present an authentication-based access scheduling scheme for WSNs. The proposed mechanism comprises two vital stages. The first stage aims to offer a secure lightweight authentication procedure for SNs using a network-wide secret key whereas the second stage optimizes the performance of the underlying network by gathering all necessary information to evade overloading of any SN whilst other SNs are inactive or maintain the light load. In this paper, we devise an access scheduling mechanism that includes only authentic sensor nodes in the underlying network during data processing. Thus, the integration of authentication and access scheduling mechanism helps to improve the performance of the WSN to a certain extent. From the simulation results attained and the assessment, we claim that the proposed method is sustainable and secure. We plan to provide secure end-to-end communication between two authentic nodes. Also, review other attacks that target draining the performance of the WSN and devise a solution to further avoid such attacks as future work.

References

[1] ZHANG J., REN F., GAO S., YANG H., LIN C. Dynamic Routing for Data Integrity and Delay Differentiated Services in Wireless Sensor Networks. *IEEE Transactions on Mobile Computing* . 2015, 14(2), pp. 328–343, doi: 10.1109/TMC.2014.2313576.

[2] DARBY III P. J., TZENG N.-F. Decentralized QoS-Aware Checkpointing Arrangement in Mobile Grid Computing. *IEEE Transactions on Mobile Computing.* 2010, 9(8), pp. 1173–1186, doi: 10.1109/TMC.2010.80.

[3] MEHTA K., LIU D., WRIGHT M. Location Privacy in Sensor Networks Against a Global Eavesdropper. In: *2007 IEEE International Conference on Network Protocols*, Beijing, China, 2007, pp. 314–323.

[4] SIVAKUMAR S., CHELLATAMILAN T., MUTHUMANICKAM K. OTP: Optimal Data Transmission Path Algorithm to Discover Energy Efficient Routes in Mobile Ad-Hoc Networks. *Journal of Electrical Engineering.* 2018, 8, pp. 1–8.

[5] VIJAYALAKSHMI P., SELVI K., GOWSIC K., MUTHUMANICKAM K. A misdirected route avoidance using random waypoint mobility model in wireless sensor network. *Wireless Networks.* 2021, 27, pp. 3845–3856, doi: 10.1007/s11276-021-02703-1.

[6] CHAUDHRY S.A., YAHYA K., AL-TURJMAN F., YANG M.-H. A Secure and Reliable Device Access Control Scheme for IoT Based Sensor Cloud Systems. *IEEE Access.* 2020, 8, pp. 139244–139254, doi: 10.1109/ACCESS.2020.3012121.

[7] CHAUDHRY S.A., YAHYA K., AL-TURJMAN F., YANG M.-H. PFLUA-DIoT: A Pairing Free Lightweight and Unlinkable User Access Control Scheme for Distributed IoT Environments. *IEEE Systems Journal*. 2020, pp. 1–8, doi: 10.1109/JSYST.2020.3036425.

[8] KHAN A.A., KUMAR V., AHMAD M., RANA S., MISHRA D. PALK: Password-based anonymous lightweight key agreement framework for smart grid. *International Journal of Electrical Power and Energy Systems*. 2020, 121, 106121, doi: 10.1016/j.ijepes.2020.106121.

[9] IRSHAD A., USMAN M., CHAUDHRY S.A., NAQVI H., SHAFQ M. A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet-Based Vehicle-to-Grid Technology Framework. *IEEE Transactions on Industry Applications*. 2020, 56(4), pp. 4425–4435, doi: 10.1109/TIA.2020.2966160.

[10] GOPE P., HWANG T. A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks. *IEEE Transactions on Industrial Electronics*. 2016, 63(11), pp. 7124–7132, doi: 10.1109/TIE.2016.2585081.

[11] LUO H., WEN G., SU J. Lightweight three factor scheme for real-time data access in wireless sensor networks. *Wireless Network*. 2020, 26(2), pp. 955–970, doi: 10.1007/s11276-018-1841-x.

[12] WATRO R., KONG D., CUTI S.-F., GARDINER C., LYNN C., KRUUS P. TinyPK: Securing sensor networks with public key technology. In: *2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 2004, pp. 59–64.

[13] DAS M.L. Two-factor user authentication in wireless sensor networks. *IEEE Transaction on Wireless Communication*. 2009, 8(3), pp. 1086–1090, doi: 10.1109/TWC.2008.080128.

[14] KHAN M.K., ALGHATHBAR K. Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks. *Sensors*. 2010, 10(3), pp. 2450–2459, doi: 10.3390/s100302450.

[15] YEH H.L., CHEN T.H., LIU P.C., KIM T.H., WEI H.W. A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Sensors*. 2011, 11(5), pp. 4767–4779, doi: 10.3390/s110504767.

[16] TURKANOVIĆ M., BRUMEN B., HÖLBL M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Networks*. 2014, 20, pp. 96–112, doi: 10.1016/j.adhoc.2014.03.009.

[17] BANERJEE S., CHUNKA C., SEN S., GOSWAMI R.S. An Enhanced and Secure Biometric Based User Authentication Scheme in Wireless Sensor Networks Using Smart Cards. *Wireless Personal Communications*. 2019, 107, pp. 243–270, doi: 10.1007/s11277-019-06252-x.

[18] FENG C., LI Z., JIANG S., JING W. Delay-constrained data aggregation scheduling in wireless sensor networks. *International Journal of Distributed Sensor Networks*. 2017, 13(6), pp. 1–9, doi: 10.1177/1550147717716591.

[19] LU Y., ZHANG T., HE E., COMŞA I.-S. Self-Learning-Based Data Aggregation Scheduling Policy in Wireless Sensor Networks. *Journal of Sensors*. 2018, pp. 1–12, doi: 10.1155/2018/9647593.

[20] NEAMATOLLAHI P., NAGHIBZADEH M., ABRISHAMI S., YAGHMAEE M.-H. Distributed Clustering-Task Scheduling for Wireless Sensor Networks Using Dynamic Hyper Round Policy. *IEEE Transactions on Mobile Computing*. 2018, 17(2), pp. 334–3472, doi: 10.1109/TMC.2017.2710050.

[21] WANG Z., CHEN Y., LIU B., YANG H., SU Z., ZHU Y. A sensor node scheduling algorithm for heterogeneous wireless sensor networks. *International Journal of Distributed Sensor Networks*. 2019, 15(1), pp. 1–11, doi: 10.1177/1550147719826311.

[22] CHEN Q., WANG T., CHENG L., TAO Y., GAO H.Y. Energy-Efficient Broadcast Scheduling Algorithm in Duty-Cycled Multihop Wireless Networks. *Wireless Communications and Mobile Computing*. 2019, Article ID 5064109, pp. 1–14, doi: 10.1155/2019/5064109.

[23] HASAN M.Z., AL-RIZZO H., GÜNAY M. Lifetime maximization by partitioning approach in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking*. 2017, 15, pp. 1–18, doi: 10.1186/s13638-016-0803-1.

[24] LIU W., YU J. Energy efficient clustering and routing scheme for wireless sensor networks. In: *IEEE International Conference on Intelligent Computing and Intelligent Systems*, 2009, Shanghai, China, pp. 612–616.

[25] HAJJI F., LEGHRIS C., DOUZI K. Adaptive Routing Protocol for Lifetime Maximization in Multi-Constraint Wireless Sensor Networks. *Journal of Communications and Information Networks*. 2018, 3(1), pp. 67–83, doi: 10.1007/s41650-018-0008-3.

[26] KUMAR V., KUMAR A. Improving reporting delay and lifetime of a WSN using controlled mobile sinks. *Journal of Ambient Intelligence and Humanized Computing*. 2019, 10, pp. 1433–1441, doi: 10.1007/s12652-018-0901-5.

[27] GANGWAR D.S., TYAGI S., SONI S.K. Improving reporting delay and lifetime of a WSN using controlled mobile sinks. *Network lifetime maximization in wireless sensor network with multiple sink nodes*. 2018, 54(271), pp. 284–290.

[28] IDOUDI H., MABROUK O., MINET P. Cluster-based scheduling for cognitive radio sensor networks. *Journal of Ambient Intelligence and Humanized Computing* . 2019, 10(2), pp. 477–489, doi: 10.1007/s12652-017-0670-6.

[29] MUTHUMANICKAM K., ELANGO S., SENTHIL MAHESH P.C., Vijayalakshmi P. EASS: Encryption and Authentication Based Security Scheme to Prevent Power Exhausting Attacks in Wireless Sensor Networks. *Ad hoc and Wireless Sensor Networks*. 2019, 45(3–4).