Secure Group key authentication using Advance Multiple Encryption standard in Social Internet of things (SIoT)

S.Jayasri[1]
Research Scholar, Department of Computer Science, School of Computing Sciences,
Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, 600 117

Dr. R.Parameswari[2]
Professor, Department of Computer Science, School of Computing Sciences,
Vels Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai, 600 117

Abstract*— The Social Internet of Things (SIoT), a rapidly developing technology, is a result of the Internet of Things. The Internet of Things (IoT) has become the subject of numerous sophisticated research initiatives in recent years. To address issues with the Internet of Things (IoT) like scalability, trust, and resource discovery from social computing, the Social Internet of Things (SIoT) was developed. Due to the restricted resources of users in major task utilising SIoT systems, Cloud and WSN is most important for storage of service provisioning. In order to get to a destination with protected authentication and key generation in WSN, research has been done to study the SIoT realisation issues utilising the clustering approach. With a better clustering method and greater node density to improve energy efficiency, protocols are categorised based on single hop and multiple hop clustering approaches and the energy distribution depending on distance from source to destination. when the SIoT environment's heterogeneous node density increases. In this work, we emphasise the necessity of creating authentication solutions using lightweight cryptographic algorithms and protocols.

Keywords*— Social Internet of Things (SIoT),Wireless Sensor Network (WSN), MQTT Protocol, AMES(Advanced Multiple Encryption System).

1. INTRODUCTION

The Social Internet of Things is a cutting-edge IoT platform that enables diverse IoT devices to connect and establish relationships. WSN and IoT are study areas that have their roots in computer networks and machine to machine (M2M). A wireless sensor network (WSN) uses thousands of sensor nodes (SNs) to send and perceive the gathered data to the base station (BS). Target tracking, disaster detection, healthcare monitoring, military surveillance [15], and environmental monitoring are just a few of the real-time uses for WSN. Unfortunately, it is unable to replace the battery of SNs that aren't functioning due to the limited energy resources and remote deployment of WSNs. These restrictions had a bigger influence on numerous researchers and businesspeople, motivating them to produce low-power hardware systems and implement energy-efficient protocols[1]. Moreover, energy-efficient routing algorithms have been used in the ongoing study to allow for a beneficial use of the battery-power required for the extension of WSNs' lifetimes. As a result, clustering-based routing protocols, or CBR, have achieved superior network lifetime augmentation results than non-clustering protocols. Typically, in a clustering scenario, SNs are piled up into clusters, and each cluster has a node known as the cluster head (CH). The CHS will designate a specific time slot for data transmission for each SN. The primary responsibility of the CH is to collect data felt from SNs. The gathered data will then be directly aggregated with packets through CHs or BS [2].

2. LITERATURE REVIEW

The following sections explain the privacy techniques used in wireless routing protocols as well as the existing system aspects.

In [8], WSN - WINCH - Wirelessly energy-charged which is a practical framework has been utilized in the research for battery maintenance that includes sensor batteries and these will be operated utilizing mobile robots. Therefore, this technique incorporates a routing process, where the CH is chosen optimally while executing the LEACH-C protocol - low-energy adaptive clustering hierarchy-centralized. To check and position the appropriate CH, the robots are used to do the work. Certainly, this

utilized technique minimizes overhead issues when compared with existing techniques. Further, an empirical model has been employed for sensor nodes that focuses on energy charging rates. This method has been utilized to calculate the energy acquired by every sensor in the mobile charger proximity. Nevertheless, due to the usage of the robot, the total expense was high, and the energy level emitted from every robot will take the same period which indicates the emission is maximum (3 times more) compared to the cluster case.

In [12], GDTMS - Gaussian distribution-based comprehensive trust management system has been used in the research doe F-IWSN - Fog-computer, an industrial WSN. Therefore, the trade-off amidst energy consumption, transmission performance, and security has been initiated with the grey decision-making method. This proposed trade-off method has been effectively used by choosing a suitable trust-management-based-secure routing scheme. Further, the simulation results exhibited that the GDTMS performance has procured better results compared to similar techniques and prevents the occurrence of network holes that helps in network load balance and promote network survivability. Nevertheless, these techniques are only suitable for external attacks and not for internal attacks.

The review expanded on the cluster-based and clustering methods in WSN for energy consumption minimization in [7]. As a result, these techniques enable various aspects such as unequal clustering, security, reliability, routing, cluster formation, and CH-cluster head selection. Furthermore, various strategies in terms of optimization, ML-machine learning methods, and classical concepts have been investigated. With the respective tables, the in-depth view of the reliable parameters has been considered. As a result, this survey aids in the identification of reliable information on WSN, and the existing research clearly mentions open issues, challenges, and research findings.

In [9], NEHCP - novel energy harvesting clustering protocol - is a clustering protocol that was used in the study to reduce energy consumption, particularly in WSNs. Furthermore, various clustering-routing protocols have been used in WSN to extend network lifetime. To address the energy-consuming issues, the NEHCP method employs a novel clustering method. Because of the use of solar energy, this process differed greatly from other existing clustering techniques. The main advantages of solar energy are that it extends the lifetime of sensor networks and overcomes issues that plague other clustering protocols. NEHCP has been divided into three phases: the transfer phase, the set-up phase, and the initial phase. In the lifetime performance evaluation, the used technique received 71.8%. However, the harvesting device used in energy Harvesting - EH-WSNs should be thoroughly researched.

In the study, the E2 S-DRL - energy-efficient sleep scheduling method utilising DRL - Deep Reinforcement Learning method was used with three significant phases including routing, duty cycling, and clustering. To begin, the clustering operation was carried out using the ZbC - Zone-based clustering scheme, which was processed using a hybrid technique combining AP - Affinity Propagation and PSO - Particle Swarm Optimization to reduce energy consumption through data aggregation. In this study, PSO was used to select the best exemplar for creating the AP clusters. Finally, this technique reduces delay by 40% while increasing energy consumption by 35% in the evaluation of throughput and network lifetime compared to existing methods.

According to [11], C-DTB-CHR-ADD - centralised density-and-threshold-based cluster head replacement - adaptive data distribution and C-DTB-CHR is an energy-efficient clustering protocol that has been used in research to reduce clustering operations, long-distance communication, and preventing CH's nodes. Essentially, the C-DTB-CHR protocol process is based on dense clusters that occur in the sleeping mode and are dependent on node-active probability, thereby minimising communication with the CHs and assisting in network lifetime extension.

The TLHA - two-Layer Hierarchical Aggregation protocol was used in the research in [13] to filter out redundant information in data traffic. In order to process the data filtration effectively, simple-aggregation techniques are used in sensed data-based classification with the normalised standard deviation. The study also employs k-means-based reclassification models to improve algorithm efficiency and a two-layered redundant data filtration method for data classification. In most cases, the aggregation protocol in the process helps to reduce data traffic in the upper and lower layers of the hierarchy. This method uses 13% and 51% less energy than DAWF and STCA methods, respectively, and produced superior results when compared to the existing method.

In WSN [6], the wireless receiver can be accessed by others in order to monitor and interrupt network communications. Therefore, these networks can be used in various safety-critical applications including fire detection [14], health-care monitoring, radiation, and military. Certainly, it is significant to ensure the privacy of the location in both source and destination of the field networks. Typically, the sensor nodes consist of various networks that have the capability to transmit and sense the data-sinking process. To utilize the information collected from the nodes, it is important that the sink should send the information to the server with the trusted routes and the selected routing path transmitted from source to destination prone to various security attacks. And this scenario will create a path for the intruders to predict the location of the source and interrupt the services which results in a high delay in energy efficiency. The transmitter path network has been operated and the data packets are routed from source to destination via multi-hop communication and with various topologies. At the same time, various topology structure indicates the multi-hop communication and location-aware mechanism, these will resolves the network issues that persist on hot-spot. In order to avoid the problems that arise on the energy-hole, the next and present location data of the sink node are utilized in packet forwarding in the internal structure [5].

3. PROPOSED METHODOLOGY

In this paper, we propose a secure group key authentication method in the Social Internet of Things based on the Advance Multiple Encryption standard. Initially, the network was created using nodes and network primitives. Following that, a novel authenticated group key agreement for IoT is created with key generation using Advanced Multiple Encryption Systems (AMES) based on the MQTT protocol and the Hardy Wall Algorithm. The scalability of the authentication models was determined using the secured routing protocol and the agglomerative hierarchical clustering approach in the following step. Finally, the computation cost, communication cost, key generation time, session time, and key verification time were used to evaluate the proposed method's performance.

Initially, the social IoT deployment was done based on the circumstances. If a user registers with a key authentication function, they can log in using the provided key and share videos, manage posts, and connect users. Following that, the sensor communication data stored in the IoT server is processed using the AMES and MQTT protocols, as well as the Hardy algorithm. If the condition is not met, users are not permitted to access the network. Finally, the data sharing and results are analysed based on the security techniques used.

3.1. **IoT Applications**

IoT - The Internet of Things indicates an ecosystem for different devices including wearable devices, sensors, and smartphones that are deployed with intelligence networking that have the capability to exchange millions of information over the internet. Basically, the connectivity of IoT devices is considered an important advancement in the evolutionary world. Therefore, every day millions of users who uses smart devices access application such as social media in order to retrieve relevant information based on their geographical locations and interests [3]. Further, user information including locations, posts, and interests is acquired according to the information collected from GPS. Hence, this user information will be frequently analyzed by AI-enabled IoT devices that are executed by social-media applications to enable advertisements and recommendations and this helps to enhance user engagement.

3.2 Clustering Methods

Most of the existing research has used clustering methods in order to reduce the network traffic that comes to the BS and enhance the network lifespan. Normally, cluster networks are categorized into two types such as heterogeneous sensor networks and homogeneous sensor networks. In a heterogeneous network, every node is allocated by initial energy that is varied from each other, and a homogeneous sensor network defines the nodes every node will be allocated by a similar initial-energy value and the CH remains static once it got chosen. Therefore, these CH will be operational for the rest of the period of the network. These sensor networks have their own limitations such as instability of the network and it is significant to resolve these issues and enhance the network stability, lifetime, and efficiency [4].

3.3 Enhance Reliable communication using MQTT Protocol in Social Internet of things

In the current study, the MQTT - Message Queuing Telemetry Transport Protocol - was used in social IoT - Internet of things to improve communication reliability. This protocol was created in order to connect physical devices with appropriate applications used in web development. During the preceding generations, IoT played a significant role in Networking through the use of published IoT protocols such as MQTT; however, each protocol used does not have similar features that are required for IoT. The current study contributes to the identification of an effective protocol in IoT through efficient use cases.

To determine the effectiveness of the proposed system, statistical measurements should be analysed and processed in real-world applications. In this study, we used MQTT and the Hardy wall to advance multiple encryption standards. As a result, MQTT has become widely used in IoT. Typically, the MQTT protocol has been used to publish and subscribe in the evaluation of the presented use cases, which defines the message transmission speed and throughput.

Certainly, the use cases are used in networking or web applications with a large number of resources, such as sensors that aid in data collection. The current study concentrated on MQTT protocol use cases in IoT. The main reason for the protocol's development is to reduce battery failure and increase bandwidth capability for message communication via satellite. For vital message transport, MQTT has considered a lightweight standard focused on subscribe structure. The primary application of MQTT in the study is also aimed at unreliable systems, high dormancy, low data transmission, and limited gadgets. The main purpose of using these kinds of standards is to maximise data broadcast reliability.

Furthermore, the use of the MQTT protocol in the study is significant because it not only improves reliable communication but also supports monitoring and controlling the IoT environment. MQTT implementation increases the level of hardware support. It typically accepts and handles user requests, and appropriate information is delivered to the appropriate receivers. MQTT's main significant features are classified according to parameters such as lightweight, secure, low operating cost, subscribe/publish elements, centralised broker, simple conference standard, and information gathering.

3.4 Secure group key authentication using Advance Multiple Encryption standard in Social Internet of things

In the experimentation process, the current study employs the secure group key authentication method, which is a novel technique that employs advanced multiple encryption standards - AEMS in social IoT. As a result, the developed IoT-based method with encryption technique is used for the module's connectivity speed, communication security, and device management. Typically, this technique uses the hardy wall encryption method to protect the user device as well as the id of the IoT devices. As a result, these methods are used to reduce bandwidth and memory consumption. This algorithm is also used in the IoT environment for secure message transmission, ensuring that data breaches and leaks are avoided. Messages from the user will be securely transmitted using the MQTT protocol. This protocol will consume less network bandwidth, be more scalable, be extremely lightweight, and keep the flag in its current state. The main advantage of this technique is that it can transmit data over long distances without requiring any changes to network routes. This is why these techniques are suitable for the IoT environment. When compared to other protocols, such as HTTP, MQTT is considered the fastest protocol because the small data packet utilisation allows for faster communication with the server while maintaining the connection active.

For secure communication, an advanced multiple encryption system was used in this study. In this case, the advanced constrained devices were represented in an IoT environment, and the connected devices are essentially managed by IoT. The devices are immersed in an IoT environment during the communication process. AMES has undoubtedly demonstrated that the security of the system processed in an IoT environment has been maximised. Secure keys and

protocols are used to protect network connectivity. During the initialization, an encryption method was used for user authentication, and this process was carried out using the hardy-wall encryption mechanism.

4. RESULTS AND DISCUSSION

We have provided detailed information on the results obtained from the execution process in the result analysis and comparison section, as follows:

The result analysis of MQTT, GKAMES, and HWAMES with certain metrics such as Packet Delivery Ratio, Throughput, Delay, and Computation Time has been defined in the study. Therefore, these are evaluated with the Number of IoT Nodes, PDR without Authentication, and PDR MQTT authentication. The result analysis of MQTT, GKAMES, and HWAMES has been represented in Table 4.1 4.2, and 4.3.

4.1 PACKET DELIVERY RATIO

In this case, packet delivery is accomplished by separating the data packets attained at a specific destination from the total data packets received from sources. Furthermore, the packet delivery ratio is simply the ratio of total received packets in the destination portion to total packets sent from the origin or source.

Table 4.1 Packet Delivery Ratio

Packet Delivery Ratio(%)		
Number of IOT Nodes	**PDR without authentication**	**PDR GKAMES authentication**
1	86	93
2	87	94
3	89	95
4	88	95
5	92	92
6	89	94
7	90	97
8	91	98
9	92	96

4.2 THROUGHPUT

Here, throughput is the evaluation of units of system information that are processed in a provided time. Therefore, it is employed in the systems measured from different aspects of network and computer systems to organizations.

Table 4.2 Throughput

Throughput(kbps)		
Number of Nodes	**Throughput without authentication**	**Throughput GKAMES authentication**
1	3072	3863
2	3178	3673
3	3170	3869
4	3164	3856
5	3187	3866
6	3194	3859
7	3165	3858
8	3159	3775
9	3484	3898

4.3 DELAY

The amount of delay has been calculated based on the time interval between the initial experiment and the induction. Furthermore, measurements are performed multiple times in some cases; for example, there is the possibility of subsequent and post-tests following a communication delay.

Table 4.3 Delay

Delay(seconds)		
Number of IOT Nodes	**Delay without authentication**	**Delay GKAMES authentication**
1	0.124	0.113
2	0.144	0.145
3	0.155	0.136

4	0.156	0.127
5	0.166	0.127
6	0.167	0.138
7	0.158	0.139
8	0.149	0.139
9	0.151	0.130

4.4. COMPUTATION TIME

Computation time is also known as running time which considers the time length needed for the computational process performance. The procured computation time is proportional to the rule applications

Computation time(seconds)		
Number of IOT Nodes	**Delay without authentication**	**Delay GKAMES authentication**
1	9.672	16.062
2	9.376	14.065
3	9.377	15.068
4	9.778	13.069
5	9.678	16.069
6	9.778	14.07
7	9.579	14.071
8	9.580	15.072
9	10.381	16.073

In the GKAMES Result Analysis, based on the certain aspects with the evlaution of number of IoT nodes, when compared to the PDR without authetication, PDR GKAMES authentication procured better results on node 1, node 2, node 3, node 4, node 5, node 6, node 7, node 8, and node 9 with 83%, 84%, 85%, 86%, 86%, 87%, 87%, 88%, and 89%. Throughput on kbps procured 3103, 3103, 3109, 3106, 3106, 3109, 3108, 3115, and 3119.. Delay on seconds procured 0.153, 0.155, 0.156, 0.157, 0.157, 0.158, 0.159, 0.159, and 0.160. computation time on seconds procured 10.062, 10.065, 10.068, 10.069, 10.069, 10.070, 10.071, 10.072, and 10.073.

5 . Comparison of the Proposed Methods with the existing Algorithms

In this section, we have compared the proposed method with the existing algorithms with certain metrics and comparison results as follows:

5.1 PACKET DELIVERY RATIO

In Figure 1 graph, the number of social media IoT nodes Vs. PDR has been compared and analyzed with the novel hash authentication based Hardy wall algorithms with AMES that are based on IoT MQTT protocol and AMES. The procures simulation results mentioned that NHHWAMES acquired high PDR than MQTT_IoT. The comparison table defines the PDR of MQTT_IoT and NHHWAMES with the Number of IoT nodes.

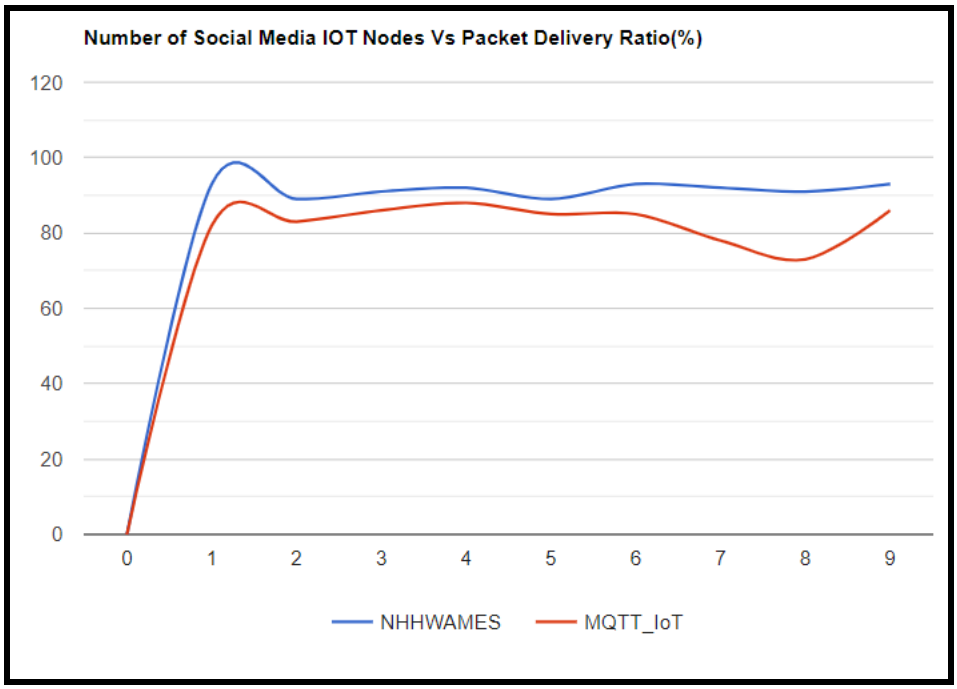

Figure 1 Number of Social Media IoT Nodes Vs PDR

5.2 THROUGHPUT

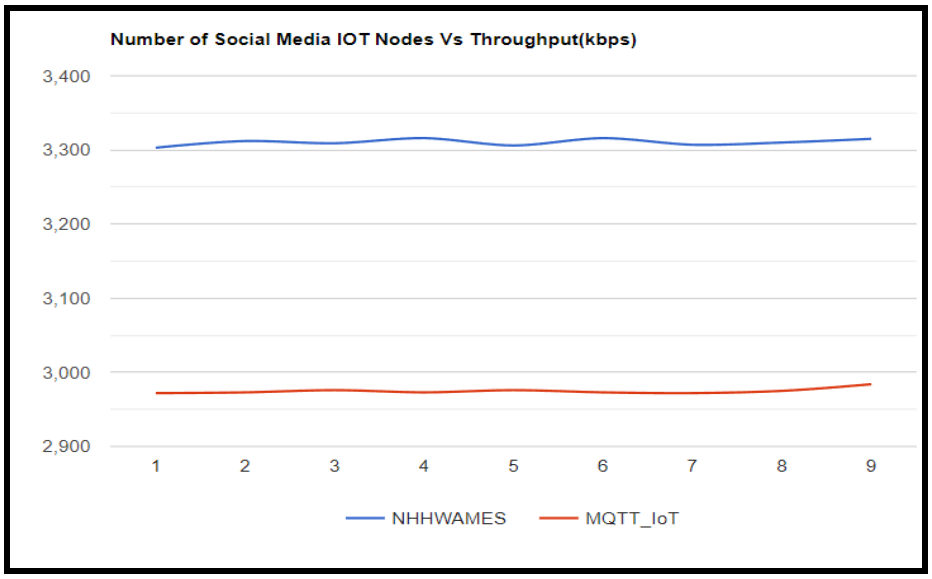

Figure 2- Number of Social Media IoT Nodes Vs Throughput

In Figure 2 graph, the number of social media IoT nodes Vs. throughput has been compared and analyzed with the novel hash authentication based Hardy wall algorithms with AMES that are based on IoT MQTT protocol and AMES. The procures simulation results mentioned that NHHWAMES acquired high throughput than MQTT_IoT

6. CONCLUSION

In the Social Internet of Things, the current study proposed a secure group key authentication method based on the Advance Multiple Encryption standard. Initially, the network was created using nodes and network primitives. Following that, a novel authenticated group key agreement for IoT is created with key generation using Advanced Multiple Encryption Systems (AMES) based on the MQTT protocol and the Hardy Wall Algorithm. The scalability of the authentication models was determined using the secured routing protocol and the agglomerative hierarchical clustering approach in the following step. Finally, the proposed method's performance was evaluated using computation cost, communication cost, key generation time, session time, and key verification time, and it outperformed existing methods.

REFERENCES

[1]Singh, H., & Singh, D. (2021). Hierarchical clustering and routing protocol to ensure scalability and reliability in large-scale wireless sensor networks. *The Journal of Supercomputing*, *77*(9), 10165-10183.

[2] Sabor, N., Ahmed, S. M., Abo-Zahhad, M., & Sasaki, S. (2018). ARBIC: An adjustable range based immune hierarchy clustering protocol supporting mobility of wireless sensor networks. *Pervasive and Mobile Computing*, *43*, 27-48.

[3] Shuja, J., Humayun, M. A., Alasmary, W., Sinky, H., Alanazi, E., & Khan, M. K. (2021). Resource efficient geo-textual hierarchical clustering framework for social IoT applications. *IEEE Sensors Journal*, *21*(22), 25114-25122.

[4] Nurlan, Z., Zhukabayeva, T., & Othman, M. (2021). EZ-SEP: Extended Z-SEP routing protocol with hierarchical clustering approach for wireless heterogeneous sensor network. *Sensors*, *21*(4), 1021.

[5] Christopher, V. B., & Jasper, J. (2021). Jellyfish dynamic routing protocol with mobile sink for location privacy and congestion avoidance in wireless sensor networks. *Journal of Systems Architecture*, *112*, 101840.

[6] Kirton, J., Bradbury, M., & Jhumka, A. (2018). Towards optimal source location privacy-aware TDMA schedules in wireless sensor networks. *Computer Networks*, *146*, 125-137.

[7] Amutha, J., Sharma, S., & Sharma, S. K. (2021). Strategies based on various aspects of clustering in wireless sensor networks using classical, optimization and machine learning techniques: Review, taxonomy, research findings, challenges and future directions. *Computer Science Review*, *40*, 100376.

[8] Baroudi, U. (2017). Robot-assisted maintenance of wireless sensor networks using wireless energy transfer. *IEEE Sensors Journal*, *17*(14), 4661-4671.

[9] Sah, D. K., & Amgoth, T. (2020). A novel efficient clustering protocol for energy harvesting in wireless sensor networks. *Wireless Networks*, *26*(6), 4723-4737.

[10] Sinde, R., Begum, F., Njau, K., & Kaijage, S. (2020). Refining network lifetime of wireless sensor network using energy-efficient clustering and DRL-based sleep scheduling. *Sensors*, *20*(5), 1540.

[11] Darabkh, K. A., Al-Rawashdeh, W. A. S., Al-Zubi, R. T., & Alnabelsi, S. H. (2017). C-DTB-CHR: centralized density- and threshold-based cluster head replacement protocols for wireless sensor networks. *The Journal of Supercomputing*, *73*(12), 5332-5353.

[12] Fang, W., Zhang, W., Chen, W., Liu, Y., & Tang, C. (2020). TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing. *wireless networks*, *26*(5), 3169-3182.

[13] Tolani, M., & Singh, R. K. (2019). Lifetime improvement of wireless sensor network by information sensitive aggregation method for railway condition monitoring. *Ad Hoc Networks*, *87*, 128-145.

[14] Xu, Y. H., Sun, Q. Y., & Xiao, Y. T. (2018). An environmentally aware scheme of wireless sensor networks for forest fire monitoring and detection. *Future Internet*, *10*(10), 102.

[15] Zawaideh, F., & Salamah, M. (2019). An efficient weighted trust-based malicious node detection scheme for wireless sensor networks. *International Journal of Communication Systems*, *32*(3), e3878.