Atlantis Highlights in Computer Sciences, volume 4
Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021)

Study on Security Improvement with Transmission of Aggregated Data Through Hamilton Clustering Protocol

M. Bobby[1,*] D. Usha[2]

[1,2] *Department of Computer Science, Mother Teresa Women's University, Kodaikanal, India.*
[*] *Corresponding author. Email: upmbobby@gmail.com*

ABSTRACT
WSN (Wireless Sensor Network) is a network of devices that can perform data transmission from an analyzed field via wireless links. Thus, secure data transfer is needed to ensure correct data transmission from source nodes to the destination node as data passes via numerous intermediate nodes. It is significant to confirm that the network is free from malicious nodes to securely transfer the data in WSN, thereby achieving a reliable transmission. This study aims to form a cluster-based topology and then perform energy-based clustering by the proposed Hamilton Theory-based Clustering (HTC). As security is in WSN, Multicast Asymmetric Encryption (MAE) and decryption are employed. The high density of nodes makes it sense the same data repeatedly, leading to energy loss and minimized network lifetime. To solve this issue, the study introduced Algebraic Model-based Data Aggregation (AM-DA). Performance analysis is also assumed to assess the efficiency of the proposed methods.

Keywords: *Algebraic Model-based Data Aggregation, Hamilton Theory-based Clustering, Multicast Asymmetric Encryption, Wireless Sensor Network, Security.*

1. INTRODUCTION

WSN, expanded as Wireless Sensor Network, is a network of devices that communicate all the information collected from an observed area via wireless links. The data delivers over multiple nodes, and with a gateway, the data connection to other networks [1]. A WSN can also be named a distributed network as it consists of many self-directed, tiny, low-powered, and distributed devices called motes or sensor nodes. The data delivery occurs over various nodes in the network. The data carry from source to destination. Several intermediary nodes are responsible for delivering the data to the sink (destination) node. The wireless network is the more popular service utilized in industrial and commercial applications because of its technological advancement in processor, communication, and usage of low-power embedded computing devices. The main issue in WSNs is to accomplish secure data transfer. The security necessities in WSNs include data confidentiality, node authentication, resilience in contradiction of traffic analysis, and anti-compromise.

Hence, the study [2] proposed a Key Chain of Multiple Asymmetric techniques for asymmetrical algorithm key generation. The keys have been generated from two algorithms and then integrated with XOR and SHA2 (hash functions). Subsequently, a diehard test is applied to test this process. The outcomes exhibited that the randomness enhanced while using SHA2.

Thus, the system is secure and confidential. In addition, the paper [3] designed a Data Aggregation (DA) protocol that is trust-based by the use of integrity verification and data validation in WSN. The data sensed is encrypted by this protocol through the use of the shared symmetric key. Subsequently, the Homomorphic MAC tag is to sign the encrypted data, followed by fragmentation. After receiving the signed blocks, the aggregator carries out the SUM aggregation after assessing the data correctness and conforming to the individual block's integrity. Then, the aggregated blocks have transferred to the destination. Here, the sink performs second-time verification. Each sensor reiterates this process to attain the sensed outcomes. The simulation outcomes are analyzed. It is initiate that the recommended method enhances the correctness of data.

The article [4] presented a strategy named Mutual Exclusive Sleep Awake Distributed Data Aggregation

(MESA2DA), which can gather and classical data into an efficiently minimized data recurrence and packet size. The introduced strategy is operative and, then a comparison is completed with the HEED protocol. The study also discussed the energy restrictions in WSN.

Replacing the strength of nodes in the WSN is an issue. It is because they cannot be physically recycled once deployed. When there is more data transmission, the nodes lose power. Hence, Energy must be made less consumed. The simulation outcomes of this study are energy efficient to the HEED method for enhancing the network lifetime.

Likewise, the paper [5] is mentioned routing based on the cluster is one of the effective techniques for data accumulation and aggregation. It also exposed that the non-centralized strategies for data forwarding and path selection remove the single-point failure and confirm correct routing decisions. Consequently, a cluster-based routing enhances the Packet Delivery Ratio (PDR), network lifetime and assists scalability in Mobile WSN. Thus, the present study aims to perform secure data transmission in WSN by the proposed Cluster-based Topology Formation, Distributed Asymmetric Encryption, and Data Aggregation for Encrypted Data.

2. RELATED WORKS

Various techniques used by the traditional studies for secure data transmission in Wireless Sensor Networks have conversed in this section.

Sensors are susceptible to numerous attacks due to their cost. In addition, these WSNs can access as it is typically situated nearer to the source. It is also possible for any device to access the information transferred in WSN. That is because the communication channel is unrestricted. The study [6] proposed a lightweight and secure key agreement and authentication protocol for the Internet of Things (IoT) relied on WSNs. The proposed protocol's security verification is explored by the widely accepted and well-known Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. An analysis started, and the outcomes showed that the introduced protocol is efficient and suitable for IoT-WSN.

Moreover, secured data aggregation and authentication mechanisms had introduced to enhance Quality of Service (QoS) in a survivable and scalable cluster built Underwater WSN. The cluster head in each cluster is authenticated by the gateway to ensure that all the clusters are being handled by valid nodes. Also, the data being communicated in the network will be securely handled to ensure that it will not get compromised during network operations. This functions in two modules as data aggregation and authentication [7].

The proposed system is analyzed to evaluate its efficiency concerning a packet drop, data reliability ratio, end-to-end delay, and average energy consumption in this particular WSN. The analysis has carried out by comparing with the traditional methods. The results have represented in the graphical form stating the performance of the proposed Secure Authentication with Protected Data Aggregation (SAPDA) than the existing systems. A one-way hash function has also been used in the article [8] to afford security between WSN nodes so that communication can happen through a trustworthy link. All the nodes in the WSN have two keys named pairwise and local keys. Here, the generation of pairwise key occurs external to the cluster for multi-hop nodes, whereas this key generation occurs interior to the cluster for single-hop nodes. On the inverse, the local key has generated to the individual nodes through the coordinator node. This introduced methodology had assessed by comparing it with the key management scheme (one-hop). The results revealed the efficiency of this proposed methodology. Data Aggregation (DA) is a needed method in WSN.

The article [9] proposed a threefold homogeneous method that supervises secure neighbor selection, energy-efficient routing, and data aggregation. This greedy approach provides Trust Assisted Global and Greedy Congestion-aware Data Aggregation for (TAG–GCDA) secured WSN with reduced energy consumption and improved reliability. The method enhances global aggregation precision with finite restrictions in neighbor reliability and aggregation.

The paper [10] explored that the DA strategies lower the data redundancy and assure security. Thus, it has gained the attention of investigators. Various secured aggregation strategies had introduced by researchers. This paper surveyed existing solutions. In addition, an effort had made to perform classification based on the employed mechanisms and node topology to assure privacy. This analysis exposed that the node topology has an impact on the DA strategy's performance. As the WSN nodes applied to the human inaccessible and hostile environment, these are highly susceptible to security threats. The survey also spots different security attacks like node compromising, eavesdropping, collusion, byzantine attack, and coalition. Besides, solutions had also examined.

The study [11] presented a hybrid energy-efficient dynamic arranging strategy for flexible WSN with the aid of examined Time Division Multiple Access (TDMA) and Carrier Sense Multiple Access (CSMA). Moreover, a Variable Step Size Firefly Algorithm (VSSFFA) has been introduced in cluster formation to generate clusters. They are energy aware by optimal Cluster Head (CH) selection.

A simulation had undertaken using the NS-2 simulation tool results showed the outstanding

performance of the proposed method than the conventional strategies. Accordingly, a protected data transmission method had introduced that used chaotic compressed sensing that relies on the T-way Bernoulli [12]. This method possesses inherent encryption characteristics and does not require any additional cost. The proposed methodology is efficient for long-term and large-scale data transmission with robust security, long transmission, and high energy efficacy, which is through simulation.

Additionally, the article [13] employed a Feistel structure to propose a symmetric encryption method for WSNs. A theoretical analysis had carried out to assess the algorithm's security. The empirical outcomes showed the efficiency of the proposed algorithm in terms of memory size, energy consumption, and computation cost. Besides diffusion and confusion of data, ULEA assumes minor encryption rounds with simplified transformations and functions to complex the cipher. The security analysis and experimental results suggest that the ULEA algorithm is an appropriate, low storage space, energy-efficient encryption process with high security for WSNs.

Moreover, a key distribution protocol has been utilized in the paper [14] for securing the resource-constrained WSNs. The results exhibited that the used protocol is secure and effective than the traditional methods.

Similarly, key management and dynamic authentication scheme had recommended for WSN in the study [15]. And it provides a single lightweight protocol for both authentication and key establishment while optimizing the security level. The key distribution algorithm is based on pre-existing information to generate dynamic keys and does not require any secure channel sharing phase which improves the security, energy efficiency, and reduced memory consumption.

The genetic algorithm had used for determining the cluster heads and the artificial bee colony algorithm had used for determining member nodes in each cluster. It intended to afford a lightweight protocol to establish key and perform authentication, thereby optimizing security. About the four key parameters (i.e. the remaining energy, density, centrality, and distance) the cluster heads are chosen. After determining the cluster heads, the bee colony algorithm has applied by determining the range for each cluster head, the member nodes in each cluster head selected. The experimental outcomes proved the efficacy of the proposed method [16].

3. SECURITY ISSUES

The various problems identified from the above existing studies are presented here.

The study proposed a lightweight authenticated key agreement method to secure a WSN. Though efficient outcomes had been obtained, the security has further enhanced the system performance [6]. The present study proposed multicast asymmetric encryption to increase system security. Also introduced is Hamilton Theory-based Clustering (HTC) as it has various merits such as energy efficiency, topology management, effective network communication, and minimize the delay. These merits of the proposed cluster-based strategy enhance the efficiency of the system.

Symmetric encryption has been employed in the study [13] to secure WSN. However, the present study uses multicast asymmetric encryption (MAE) as it can enhance data security. It is a highly secured encryption scheme than symmetric encryption. That is more suitable when there is an involvement of many endpoints. It makes key distribution easier. All these advantages make it effective than traditional symmetric encryption.

The conventional system [14] has a drawback in terms of energy consumption in WSN. The minimum resources in Base Station (BS) and WSN lead to more energy consumption. As a result, there is a reduction in the network's lifetime. To solve this, the present study proposed Algebraic Model-based Data Aggregation (AM-DA), which is an energy-effective methodology in WSN that eliminates redundancy (i.e., it removes sensing identical data by numerous nodes) thereby enhancing the network lifetime.

The main discussions of this study are specified here.

1. To perform cluster-based topology formation and energy-based clustering using the proposed Hamilton Theory-based Clustering (HTC) [18].
2. To secure the data transmission by the proposed Multicast Asymmetric Encryption (MAE) [19] and decryption.
3. To avoid redundancy by eliminating the sensing of the same data by numerous nodes in WSN by the introduced Algebraic Model-based Data Aggregation (AM-DA) [20].
4. To analyze the performance of the proposed methodologies for significant parameters like network lifetime, throughput, Packet Delivery Ratio (PDR), Residual energy, and security analysis like a man-in-the-middle attack, replay attack [21]. This analysis had performed to evaluate the efficiency of the proposed system.

The identified research gaps are discussed below.

1. The study has to be implemented in real-time [12]. This indicates that simulation is carried out and real-time implementation had not been performed.
2. The existing study [3] intends to propose watermarking for increasing data aggregation

security. Though there exist various methods, this particular technique is not introduced.

4. DISCUSSION & ANALYSIS

The study focuses on various methodologies to increase security during data transmission in WSN. Hamilton Theory-based Clustering (HTC) brings together to perform clustering, Multicast Asymmetric Encryption (MAE), and decryption are planned to enhance the security during data transfer in WSN and Algebraic Model-based Data Aggregation (AM-DA) is wished-for to eliminate redundancy and improvise the network lifetime [22-27]. Various steps are involved in securing the data transmission in WSN. The overall view of it is shown in the below figure.1.

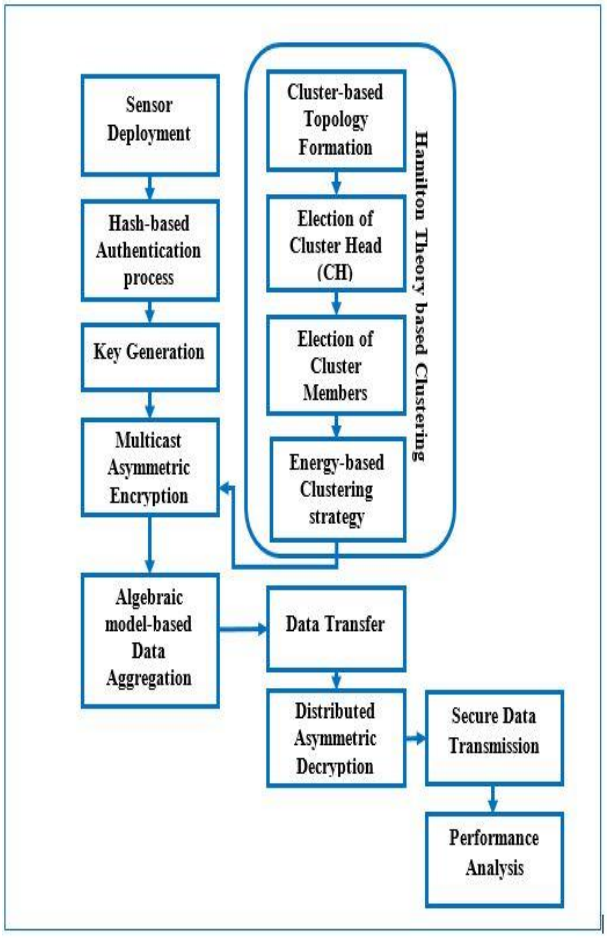

Figure 1 Overall view of the proposed system

Initially, the sensors are deployed in the network area. Then, the hash-based authentication process is performed and keys are generated. The cluster-based topology is formed to elect the Cluster Heads (CHs) and cluster members. Subsequently, energy-based clustering is performed using the HTC [28]. This is fed to the MAE (Multicast Asymmetric Encryption). Followed by this, Data Aggregation is performed by AM-DA. In this way, the data transfer occurs between source and destination. Once the data reaches the destination, the Distributed Asymmetric Decryption (DAD) is performed, thereby performing secure data transmission. Finally, the performance analysis is undertaken to assess the system's efficacy.

4.1. Hamilton Theory-based Clustering (HTC)

HTC is an automated method where data is grouped and sorted into clusters. Various clustering algorithms rely on the concept of Euclidean Distance (ED). On the other hand, HTC intends to utilize level curves for defining the boundary of the cluster. Hence, these boundaries are found to be the Hamiltonian system's solution. The main significant merit of this technique is no need of knowing the cluster counters a priori, not like other clustering methods. Not only has this, the Hamiltonian dynamics and algorithm's geometric nature permitted to merit from various geometric information such as geometric moments for classifying and clustering and also modeling the time-altering clusters [29-31].

In this methodology, data had termed as elements in space (x, p). For instance, a two-dimensional image pixel is a point denoted by (x, p). Figure. 2. Shows the clustering of the flock-of-birds based on Hamiltonian.

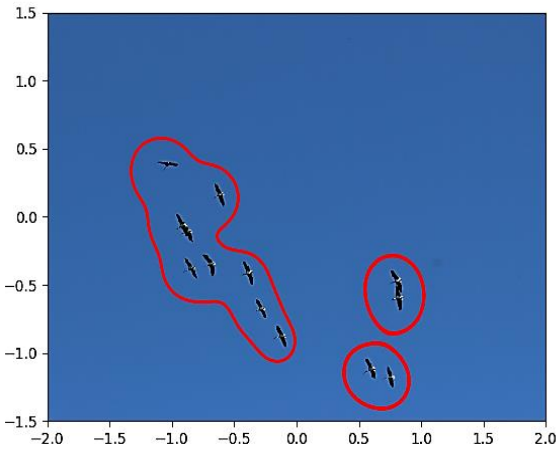

Figure 2 Clustering – Birds [17]

In the above figure 2, the birds had clustered and grouped into three varied groups by the proposed Hamiltonian Theory-based Clustering (HTC).

4.2. Multicast Asymmetric Encryption (MAE)

The typical idea of not distinguishing by itself confirms that no information bit had disclosed when putting the related message encryptions under various public keys. The proposed MAE provides robust security by affording the opposition the capability to select two plaintext vectors. Their coordinates are messages (plaintext) possibly associated or even similar. Subsequently, anyone vector had chosen among the two

at random. Followed by this, encryption is performed coordinate-wise with varied public keys. The ultimate aim of the opposition is to find the encrypted one. That had accomplished easily when a Boolean function differentiates the two plaintext vectors and is also quantifiable from the data is encrypted.

4.3. Algebraic model-based Data Aggregation (AM-DA)

WSN comprises many sensor nodes of small size whose job is to sense the preferred occurrence in a specific area. These networks possess numerous applications like disaster management, military, security, habitat monitoring, and so on. The sensor nodes are generally small and have minimum processing ability due to reduced battery power. This power constraint makes these networks susceptible to failure. Thus, the study proposed AM-DA, which is an energy-effective methodology in WSNs. The node's high density in WSN makes it sense the same data many times, resulting in redundancy. This redundancy minimizes the power and decreases the network lifetime. Consequently, the introduced AM-DA eliminates redundancy during the transfer of data packets from the source to the destination.

5. CONCLUSION

The study focuses on Hamilton Theory-based Clustering (HTC), Multicast Asymmetric Encryption (MAE), and Algebraic model-based Data Aggregation (AM-DA) to cluster, enhance the system security, and eliminate redundancy during transmission of data from source to destination in WSN. That increases the network lifetime and minimizes the vitality of the node. Thus, secure data transmission may be accomplished.

AUTHORS' CONTRIBUTIONS

M.Bobby and D.Usha developed the formalism, performed the analytical process, and contributed to the final version of the manuscript.

REFERENCES

[1] E. K. Kaur, M. Kaur, and D. Saghotra, "Analysis a Performance Metrics of WSN."

[2] A. H. Hamza and S. M. K. Al-Alak, "Evaluation key generator of Multiple Asymmetric methods in Wireless Sensor Network (WSNs)," in Journal of Physics: Conference Series, 2021, p. 012096.

[3] S. E. Roslin, "Data validation and integrity verification for trust based data aggregation protocol in WSN," Microprocessors and Microsystems, vol. 80, p. 103354, 2021.

[4] B. Gupta, S. Rana, and A. Sharma, "An Efficient Data Aggregation Approach for Prolonging Lifetime of Wireless Sensor Network," in International Conference on Innovative Computing and Communications, 2020, pp. 137-147.

[5] J. Sumathi and R. L. Velusamy, "A review on distributed cluster based routing approaches in mobile wireless sensor networks," Journal of Ambient Intelligence and Humanized Computing, pp. 1-15, 2020.

[6] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," Future Generation Computer Systems, vol. 100, pp. 882-892, 2019.

[7] N. Goyal, M. Dave, and A. K. Verma, "SAPDA: secure authentication with protected data aggregation scheme for improving QoS in scalable and survivable UWSNs," Wireless Personal Communications, pp. 1-15, 2020.

[8] A. F. Khan and G. Anandharaj, "Ahkm: an improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in iot," Egyptian Informatics Journal, 2020.

[9] Uvarajan, K.P., Gowri Shankar, C, "An Integrated Trust Assisted Energy Efficient Greedy Data Aggregation for Wireless Sensor Networks." *Wireless Pers Commun* 114**,** 813–833 (2020).

[10] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," IEEE transactions on Dependable and Secure Computing, vol. 12, pp. 98-110, 2014.

[11] V. Sundararaj, S. Muthukumar, and R. Kumar, "An optimal cluster formation based energy efficient dynamic scheduling hybrid MAC protocol for heavy traffic load in wireless sensor networks," Computers & Security, vol. 77, pp. 277-288, 2018.

[12] H. Gan, S. Xiao, and Y. Zhao, "A novel secure data transmission scheme using chaotic compressed sensing," IEEE Access, vol. 6, pp. 4587-4598, 2017.

[13] H. Hayouni and M. Hamdi, "A novel energy-efficient encryption algorithm for secure data in WSNs," The Journal of Supercomputing, vol. 77, pp. 4754-4777, 2021.

[14] M. R. Alshammari and K. M. Elleithy, "Efficient and Secure Key Distribution Protocol for Wireless Sensor Networks," Sensors, vol. 18, p. 3569, 2018.

[15] S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: An efficient dynamic authentication and key management mechanism for heterogeneous WSNs," Future Generation Computer Systems, vol. 92, pp. 789-799, 2019.

[16] M. A. Zangeneh and M. Ghazvini, "An energy-based clustering method for WSNs using artificial bee colony and genetic algorithm," in 2017 2nd Conference on Swarm Intelligence and Evolutionary Computation (CSIEC), 2017, pp. 35-41.

[17] D. Casagrande, M. Sassano, and A. Astolfi, "Hamiltonian-based clustering: Algorithms for static and dynamic clustering in data mining and image processing," IEEE Control Systems Magazine, vol. 32, pp. 74-91, 2012.

[18] Z. Guo, K. Yu, Y. Li, G. Srivastava, and J. C. -W. Lin, "Deep Learning-Embedded Social Internet of Things for Ambiguity-Aware Social Recommendations", IEEE Transactions on Network Science and Engineering, doi: 10.1109/TNSE.2021.3049262.

[19] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-Enhanced Data Sharing with Traceable and Direct Revocation in IIoT", IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3049141.

[20] K. Yu, L. Lin, M. Alazab, L. Tan, B. Gu, "Deep Learning-Based Traffic Safety Solution for a Mixture of Autonomous and Manual Vehicles in a 5G-Enabled Intelligent Transportation System", IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3042504.

[21] Puttamadappa, C., and B. D. Parameshachari. "Demand side management of small scale loads in a smart grid using glow-worm swarm optimization technique." *Microprocessors and Microsystems* 71 (2019): 102886.

[22] Bhuvaneswary, N., S. Prabu, S. Karthikeyan, R. Kathirvel, and T. Saraswathi. "Low Power Reversible Parallel and Serial Binary Adder/Subtractor." *Further Advances in Internet of Things in Biomedical and Cyber Physical Systems* (2021): 151.

[23] Prabu, S., Balamurugan Velan, F. V. Jayasudha, P. Visu, and K. Janarthanan. "Mobile technologies for contact tracing and prevention of COVID-19 positive cases: a cross-sectional study." *International Journal of Pervasive Computing and Communications* (2020).

[24] Parameshachari, B. D., H. T. Panduranga, and Silvia liberata Ullo. "Analysis and computation of encryption technique to enhance security of medical images." In *IOP Conference Series: Materials Science and Engineering*, vol. 925, no. 1, p. 012028. IOP Publishing, 2020.

[25] Hu, Liwen, Ngoc-Tu Nguyen, Wenjin Tao, Ming C. Leu, Xiaoqing Frank Liu, Md Rakib Shahriar, and SM Nahian Al Sunny. "Modeling of cloud-based digital twins for smart manufacturing with MT connect." *Procedia manufacturing* 26 (2018): 1193-1203.

[26] Seyhan, Kübra, Tu N. Nguyen, Sedat Akleylek, Korhan Cengiz, and SK Hafızul Islam. "Bi-GISIS KE: Modified key exchange protocol with reusable keys for IoT security." *Journal of Information Security and Applications* 58 (2021): 102788.

[27] Nguyen, Tu N., Bing-Hong Liu, Nam P. Nguyen, and Jung-Te Chou. "Cyber security of smart grid: attacks and defenses." In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2020.

[28] Rajendran, Ganesh B., Uma M. Kumarasamy, Chiara Zarro, Parameshachari B. Divakarachari, and Silvia L. Ullo. "Land-use and land-cover classification using a human group-based particle swarm optimization algorithm with an LSTM Classifier on hybrid pre-processing remote-sensing images." *Remote Sensing* 12, no. 24 (2020): 4135.

[29] L. Tan, H. Xiao, K. Yu, M. Aloqaily, Y. Jararweh, "A Blockchain-empowered Crowdsourcing System for 5G-enabled Smart Cities", Computer Standards &Interfaces, https://doi.org/10.1016/j.csi.2021.103517.

[30] C. Feng et al., "Efficient and Secure Data Sharing for 5G Flying Drones: A Blockchain-Enabled Approach," IEEE Network, vol. 35, no. 1, pp. 130-137, January/February 2021, doi: 10.1109/MNET.011.2000223.

[31] N. Shi, L. Tan, W. Li, X. Qi, K. Yu, "A Blockchain-Empowered AAA Scheme in the Large-Scale HetNet", Digital Communications and Networks, https://doi.org/10.1016/j.dcan.2020.10.002.