International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Framework for Intrusion Prevention Based on Block Chain in IoT Environment

Thamraj Narendra Ghorsad*[1], Dr. Amol Zade [2]

Submitted: 27/01/2024 **Revised**: 05/03/2024 **Accepted**: 13/03/2024

Abstract: The Internet of Things works by helping different network devices connect via wireless and wired media. There has been a lot of research in IoT over the last few decades and millions of devices have been connected. In the development of IoT technology, security-related challenges have started to arise as well as in the expanded volume of data, a large amount of additional data is generated by IoT so the combination of different things and classes in data has changed. This has paved the way for the handling of large amounts of information and the creation of different applications to provide strong security of data. However, most research has focused on designing and building the stable topology of networks, as well as the dynamic structure of wireless sensor nodes. Given the limited difficulties of sensor nodes, it is necessary to redesign with minimal network overhead, providing strong protection against malicious actions. Therefore, in this study, we focused on proposing a framework for intrusion prevention and intrusion identification integrated into the WSN for IoT devices to provide strong security with high network distribution ratios . The proposed scheme is classified into two sections in the first section; autonomously organized clusters provide better stability to clusters based on the principle of uncertainty. And in the second section, developed an end-to-end secure and multi-hop path based using the blockchain technique. The parameters of different network metrics have shown good improvement in the results of our simulations in terms of existing solutions.

Keywords: *Internet of Things, Wireless Sensor Network, Blockchain, Intrusion Prevention, Sensor Nodes*

1. Introduction

Over the past few decades, WSN has been playing a key role in a variety of areas. A large number of sensor nodes are made to store a large amount of real-time data and forward it to the base station [1]-[2]. When data arrives near a base station, that data is processed and transferred to users. The sensors nodes are battery operated and operate randomly in the monitoring area [3]-[4].Because of problems in sensor nodes and communication overhead, many researchers have focused on network stability and efficient routing [5]-[6] .Data stored in static WSN may not be accurate, which may reduce network reliability. Nor is it able to change static WSN status to obtain information.In IoT systems, entire devices are interconnected to collect and transfer information using hardware, software, and mobile sensors.The nodes are movable in the network field and use a variety of carriers to capture information. And can be connected to different systems, and complete information can be sent via BS.Nowadays, various researchers aim to integrate the field of WSN with IoT for strong network coverage and growth of network development [.[13]-[12

Applications based on IoT require reliable data exchange to provide strong data security between sensor nodes.In existing systems, a lot of work has been done in cluster-based network infrastructure on strengthening routineaccomplishedbased onthe network life cycle and network throughput improvement .[18]-[16] Stabilizing clusters with reliable data routing in sensor nodes is a big problem .[20]-[19] Sensor nodes are neglected without any fixed infrastructure after the erection of wireless sensor networks, so optimizing the energy routing process by optimizing the energy between the nodes and BS/RSU is themainissue. [.[23]-[21]-[11 This research proposes an intrusion prevention framework, the function of which is based on WSN and is to extend the network life cycle with safe data routing between various devices in IoT.Based on some of the previous solutions our proposed system divides IoT objects into different clusters and selects the cluster head on the concept of uncertainty.Also, the network measurement and analysis parameters were used to determine the position of the cluster head.Furthermore, in previous solutions, it is difficult to guarantee that data transmission will be secure until the end due to constraints in the IoT nodes.Our proposed system operates from a robust and reliable end-to-end secure approach based on blockchain technology.Accordingly, our suggested system works to increase the routing performance of IoT nodes in terms of data security and energy optimization.

The organization of paperare as follows:Section 2 discussed the background details of the problem in the existing system. Section 3, presents the details of the suggested intrusion detection and preventive model for preventing routing in an IoT environment. Section 4 presents the numerical analysis of the framework. In

[1] *Research Scholar, G.H.Raisoni University, Amravati –Maharashtra, INDIA*
[2] *Professor,G.H.Raisoni University, Amravati –Maharashtra, INDIA*
** Corresponding Author Email: raj.ghorsad@gmail.com*

thelast Section 5, presented theconclusion and discussion of research.

2. Background Details

Typically, wireless sensor networks have limitations on some parameters like energy, memory, processing, etc. All nodes in the WSN are interconnected from a dynamic and ad-hoc approach using wireless transmission. The main function of wireless sensor nodes is simply to collect information and transfer it to the end-point through intermediate devices. For Routing performance; if want to extend the network lifetime and provide strong security to data then the limited constraints of the sensor nodes cannot be ignored.The network is more prone to malicious threats. IoT devices collect large amounts of data in real-time. If such data goes to malicious nodes, the privacy of the data will be lost.Therefore, end-to-end routing channels need to be installed if you want to strengthen routing functionality with data security in mind, and only authenticated IoT devices in the network will exchange information.

In [27], proposed LEACH algorithm for designing various clusters. Each cluster has one cluster head that choosethe preset of several nodes. All other common nodes remain stationery and network data has been sent to the CH BS using a one-hop transmission.

In [28], proposed a mobile LEACH protocol for improving the energy utilization with static nodes and Base stations. Cluster heads are selected based on the probability model. The proposed approach is used for routing complexity and minimizes the network overhead.

In [29], suggested a system for extending the network lifespan based on cluster network and cluster mobility. Initially, all the sensors and sink nodes are static and CH is dynamic. The purpose of the proposed system is to minimize network delay.

In [30], proposed the system for improvement in energy utilization based on distance-aware routing protocol using various sink nodes. If the nodes are in the same network area, then the proposed system used one-to-one transmission (direct) using the sink node. During the data transmission, If the node is away from the sink, then the transmission is done by the multi-hop routing technique.

3. Proposed System

Use The main purpose of the proposed system is to create a network with various clusters and provide security for routing.In the first step, primarily network routing structures are carried out, each node has its routing table that can store the information of neighboring nodes.The purpose of these steps isto develop energy optimization clustering techniques based on cluster heads. The second step is a strong security framework to prevent potential intrusion attacks and enhance network reliability using blockchain architecture. In blockchaining, complete data is divided into a data chunk, and each data blockis connected using a cryptographic technique.

Each block is protected using an asymmetric hash function and a hashtag is placed behind each block. The use of this technique helps to track compassionate data blocks and secure the network.In addition, the proposed technique has taken forward the performance and effectiveness of the network in terms of different measurement parameters. Cluster head and base station as shown in Figure 1.

3.1 Network settingand Clusters Management

Initially,the base station used beacon messages to locate the node, then the source nodes expand the packet counter and transfer the data by storing all the data received from one-hop neighbors to the base station in routing tables.A node will receive a base station message from several neighboring nodes .And base station will store the entire information in a routing table by choosing the route with the least number of hops.In this way, the nodes in all networks create and update their routing tables based on short distances. After creating a routing table, direct transmission can only be done through nodes whose values base station is set to 1.

Subsequently, the network field was subdivided into different cells using the Voronoi architecture in the proposed system. Each node in the network corresponds to a specific cell with some of its values. Also,everyVoronoi cell is selected as a cluster in the network model. Furthermore, to recognize the node, the threshold values at some distance is set and it is slightly increase without finding any node within the boundary of the Voronoi cell.

It takes any node in the network and assigns it as a cluster head. Setting threshold value with preset distance may have more than one node selected. The principle of uncertainty [43] is used in the proposed technique to decide the position of nodes with the minimum changes shown in Equation 1.

$$\Delta p \, \Delta q \approx \frac{h}{2} \qquad (1)$$

Where,

Δp - node position,

Δq-node speed

h- constant.

Using the equation 1, node goes nearer to cluster head that determine the actual position of node. After selecting the cluster head, information is provided to the cluster head as well as updating the routing table based on the information of general nodes, and the specific ID of the node is defined as the CH.In our suggested technique, supdate their routing

table when select the cluster head. The main aim of the network node is used as cluster heads for delivering the data on time and improve network connectivity.In addition, the network has gained stability by reducing the amount of energy used in sensor nodes.

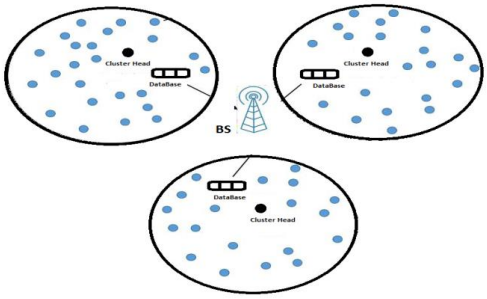

Fig 1: WSN with Cluster and Cluster Head, and BS

When the network node selects as a CH the initial process getsstarts with constructing the point-to-point routing sequence to the base station. The CH transmits the route discovery packet (RDP) to the next CH based on their radius.After receiving the route discovery packet, the CH checks the total residual energy of the node, if the total is not less than the threshold value then CH is the part of the routing sequence. If the total energy is less than the threshold value then CH neglects the RDP.

3.2 Data Security

The last few years have seen remarkable revolutions in all areas and researchers are making extensive use of blockchain techniques in their research. Blockchain systems can be used to provide reliability and secure access to data in network nodes [26]-[44].

The architecture is structured in a decentralized manner, providing strong security to the data in the network, and blockchain techniques have been used in some parts of the network where peer-to-peer communication is taking place between nodes.

In the proposed technique, a robust and secure model has been developed to prevent attacks in the network as well as provide more security to the routing data between nodes, CH, and BS in the network using blockchain techniques. It includesa hash function for encrypting data in the network.Each cluster head in the network has a private key that is used to communicate between the sensor and BS and to create a secure data path between them.A hash function is assigned to each message in the network in which the output value is obtained according to Equation 2 after the input process.

$$f(n) = p \qquad 2$$

Where n-data packet

p -hash value.

In the proposed technique, the use of the Bitwise XOR operator in the hash function because Bitwise XOR has less time and higher efficiency.In the proposed technique, the main activity of the base station is to process and respond to the data generated by the sensors. The database of the base station records each data packet containing all the information i.e., location ID, cluster head ID, sensor ID, etc.Each CH checks the reliability of packets depending on the authorized private key.The proposed technique uses blockchain architecture to encrypt information from the cluster and BS to avoid malicious threatsshown in figure 2.BS is an important part of WSN which monitors the functioning of CH and sensor nodes. The proposed technique gives BS full control over the operation of the entire network and can remove some cluster heads from the network if they become abnormal or dead.

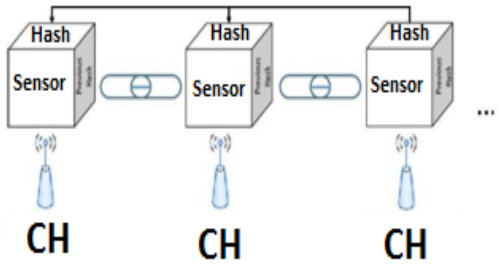

Fig 2: Hash algorithm computational using the blockchain technology

4. Simulation and Parameters

This partrepresents the simulation parameter of the wireless sensor networks based on the IoT environment as shown in table 1. The proposed technique contains various sensor nodes and transmission rates to evaluate simulation results. The total number of nodes used for simulation is 120 to 600 and set the data transmission rate 1-to-5seconds.Set the velocity of CH is 1-to-12 m/s. Furthermore, set the transmission ranges from 20 m to 25 m. To analyze performance evaluation, NS2 has been used.For the performance analysis, using the three parameters of network lifetime, Energy Utilization, packet drop ratio, Routing Overhead and compare the final result of the proposed technique with existing approach.

Table 1: Simulation parameter

Parameter	***Value***
Monitoring area	210m X 210m
Deployment	Random
Packet size, k	52-bits

Payload Size	512-Bytes
MAC layer	IEEE 802.15.4
Control Messages	20-bits
Node's TransmissionRange	20meters to 25meters
Simulation time	2200sec
Network interface type	Wireless

4.1 Mathematical Approach

In this part, we examine the proposed techniquewith various methods such as effective distance-aware routing protocol, LEACH Distance-M, and MECA.

4.1.1 Network Lifetime

Figure 3 presents a comparison of the suggested framework with the existing methods formaximum network life cycle with 24%, 27%, and 32% respectively. In particular, the instability of the network in earlier systems reduces the lifetime of the network. But in the existing system, the routing decision is non-optimal and strong, and in any case, the lifetime of the network is extended.In this proposed technique we have focused on making the energy of the network more efficient by using Voronoi cells as well as the load balancing between the sensor nodes in the network.Also, the proposed technique works by tracking the position closest to the cluster head and minimizing communication overhead. So, the result is that the lifetime of different network nodes has improved over the previously proposed technique.

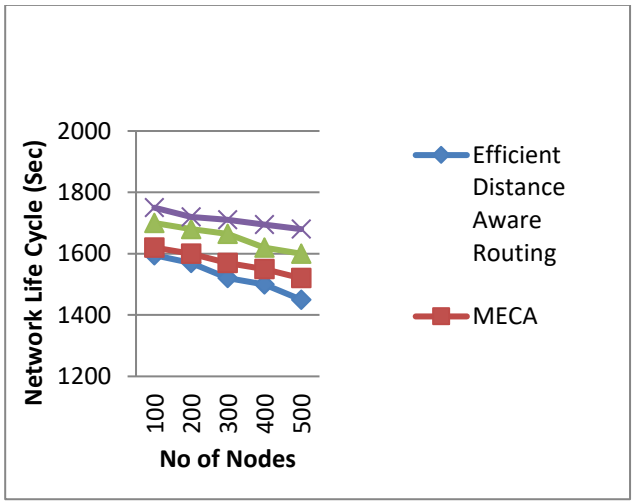

Fig 3: Representation of Network Life cycle and Network Nodes

Figure 4 shows the network lifetime in terms of the rate of sending different data between 1 to 3 seconds. The results of the research show that the lifetime of the network in the suggested technique has increased by 27%, 32%, and 36%, respectively, compared to the existing techniques.This suggested technique builds a lightweight and robust data security system using the XOR function. In addition, in existing systems the paths are updated frequently rather than resolved, but, in our proposed technique, the paths are re-adjusted based on the position of nodes with minimum difference.

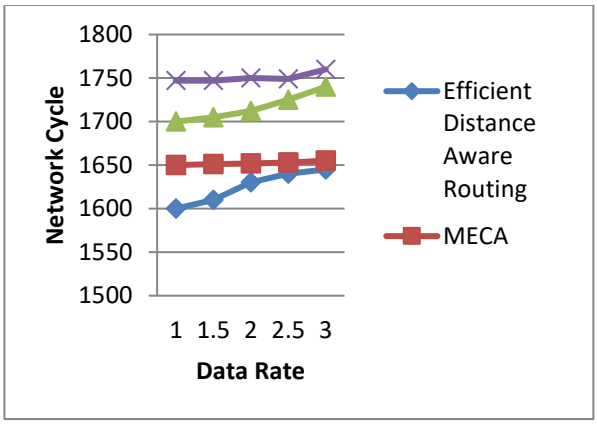

Fig 4: Data transfer Rate

4.1.2 Energy Utilization

Figure 5 compares the behaviour of the suggested method to the existing solution of the system when considering various nodes in the network. The results demonstrates that the suggested method has increased the performance of the network over the existing technique, as it has seen a 27%, 30%, and 34% increase in energy utilization.After analyzing the network, it was found that the routes are updated from the demand of the node. In addition, the proposed technique allows for efficient use of energy required for multi-hop data transmission and sensor nodes, as the cluster head rotates in the Voronoi cells based on the information.Also, the Cluster head rearranges the shortest route to BS that preventing unnecessary energy consumption in the network area. Thus, at least cluster heads are selected to send complete data to BS.

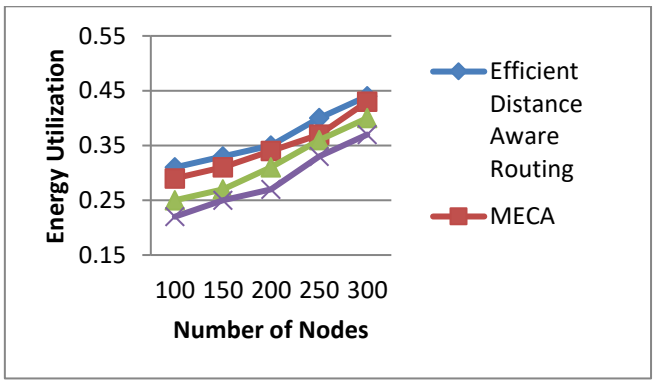

Fig 5: Energy Utilization of Network Node

4.1.3 Packet Drop Ratio

Figure 6 shows the behavior of our suggested techniques as compared with existing solutions for several network nodes. It was found that our suggested technique reduces the packet drop ratio by 27%, 30%, and 35% as compared to existing approach. Due to the instability and congestion in the network, existing solutions cannot transmit the data more efficiently. Our proposed technique uses a multi-hop approach to transmit data in energy-efficient ways, thus reducing packet drop.Also, the proposed technique does not select the next hop that is out of reach, thus reducing the time required for route adjustment. Thus, the use of distance parameters reduces data latency and increasethe data transmission effectiveness.The suggested technique provides strong security for data based on the blockchain technique, thatencrypt the data using the XOR hash function. The proposed security technique helps to reduce the possibility of packet drop by identifying abnormal activity occurring in the nodes.

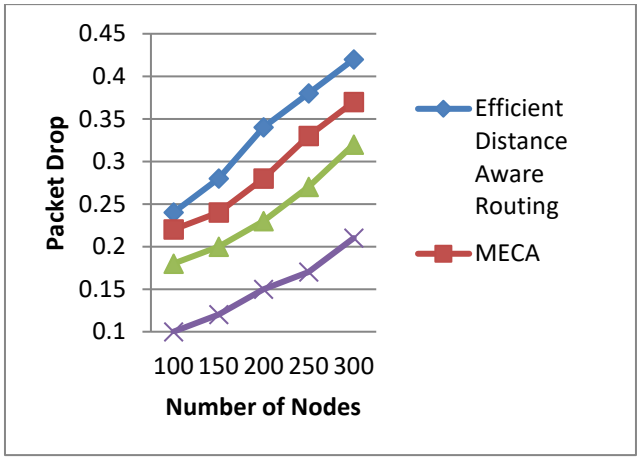

Fig 6: Packet Drop Ratio

4.1.4 Routing Overheads

A comparative analysis of the existing solution and the proposed technique is shown in Figure 7.The proposed technique reduces the network overhead by 27%, 31%, and 37% as compared to the existing system. Properly implementing blockchain encryption has reduced the time required for data transmission, reduced routing overhead, and improved network performance.In addition, cluster heads are placed close to the nodes to reduce routing overhead to retrieve data from the network.

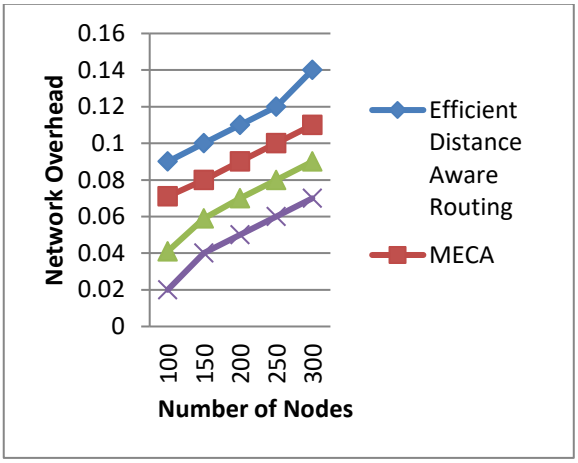

Fig 7: Routing Overhead

5. Conclusion

In this paper, introducing techniques to protect routing in the environment of the Internet of Things using wireless sensor networks. The main purpose of this proposed technique is to extend network life, provide strong security to data, and prevent the network from malicious threats. The proposed technique involves different cluster heads and Voronoi cells. In addition, the proposed technique works on minimal energy consumption and minimal routing overhead. The speed of the cluster heads in the network is selected based on the principle of uncertainty with minimal variation. Using such a scheme reduces routing overhead and communication costs of the network. Furthermore, with the help of the blockchain technique, robust security is achieved using the hash function. In the future, the results will be analyzed by implementing the proposed technique on the hardware platform.

Conflicts of interest

The authors declare that they have no potential conflict of interest.

References

[1] Yetgin, H., et al., A survey of network lifetime maximization techniques in wireless sensor networks. IEEE Communications Surveys & Tutorials, 2017. 19(2): p. 828-854.

[2] Abuarqoub, A., et al., Dynamic clustering and management of mobile wireless sensor networks. Computer Networks, 2017. 117: p. 62-75.

[3] Anisi, M.H., et al., Energy harvesting and battery power-based routing in wireless sensor networks. Wireless Networks, 2017. 23(1): p. 249-266.

[4] Ahmad, M., et al., A Novel Connectivity-Based LEACH-MEEC Routing Protocol for Mobile Wireless Sensor Network. Sensors, 2018. 18(12): p. 4278.

[5] Bellavista, P., et al., Convergence of MANET and WSN in IoT urban scenarios. IEEE Sensors Journal, 2013. 13(10): p. 3558-3567.
[6] Banerjee, T., et al., an Increasing lifetime of wireless sensor networks using controllable mobile cluster heads. Wireless Communications and Mobile Computing, 2010. 10(3): p. 313-336.
[7] Busch, P., T. Heinonen, and P. Lahti, Heisenberg's uncertainty principle. Physics Reports, 2007. 452(6): p. 155-176.
[8] Chernyshev, M., et al., Internet of Things (IoT): Research, simulators, and testbeds. IEEE Internet of Things Journal, 2017. 5(3): p. 1637-1647.
[9] Cardei, M., Y. Yang, and J. Wu. Non-uniform sensor deployment in mobile wireless sensor networks. in 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks. 2008. IEEE.
[10] Dantu, K., et al. Robomote: enabling mobility in sensor networks. in Proceedings of the 4th international symposium on Information processing in sensor networks. 2005. IEEE Press.
[11] Din, I., et al., Information-centric network-based vehicular communications: overview and research opportunities. Sensors, 2018. 18(11): p. 3957.
[12] Din, I.U., H. Asmat, and M. Guizani, A review of information-centric network-based internet of things: communication architectures, design issues, and research opportunities. Multimedia Tools and Applications, 2019. 78(21): p. 30241-30256.
[13] Din, I.U., et al., Trust management techniques for the Internet of Things: A survey. IEEE Access, 2018. 7: p. 29763-29787.
[14] Din, I.U., et al., The Internet of Things: A review of enabling technologies and future challenges. IEEE Access, 2018. 7: p. 7606-7640.
[15] Dvir, A., et al., STWSN: A novel secure distributed transport protocol for wireless sensor networks. International Journal of Communication Systems, 2018. 31(18): p. e3827.
[16] Din, I.U., et al., Machine learning in the Internet of Things: Designed techniques for smart cities. Future Generation Computer Systems, 2019.
[17] Elhoseny, M. and A.E. Hassanien, Expand mobile WSN coverage in harsh environments, in Dynamic Wireless Sensor Networks. 2019, Springer. p. 29-52.
[18] Gope, P., et al., Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE transactions on industrial informatics, 2019.
[19] Heinzelman, W.R., A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wireless microsensor networks. in System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference. 2000. Maui: IEEE.
[20] Haseeb, K., et al., Secret sharing-based energy- aware and multi-hop routing protocol for IoT based WSNs. IEEE Access, 2019. 7: p. 79980-79988.
[21] Jiang, Q., et al., Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. IEEE Access, 2017. 5: p. 3376-3392.
[22] Khattak, H.A., et al., Toward integrating vehicular clouds with IoT for smart city services. IEEE Network, 2019. 33(2): p. 65-71.
[23] Khan, M.A., and K. Salah, IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 2018. 82: p. 395- 411.
[24] Khandnor, P. and T. Aseri, Threshold distance-based cluster routing protocols for static and mobile wireless sensor networks. Turkish Journal of Electrical Engineering & Computer Sciences, 2017. 25(2): p. 1448-1459.
[25] Krishnan, A.M. and P.G. Kumar, An effective clustering approach with data aggregation using multiple mobile sinks for heterogeneous WSN. Wireless Personal Communications, 2016. 90(2): p. 423-434.
[26] Khattak, H.A., et al., Integrating fog computing with VANETs: A consumer perspective. IEEE Communications Standards Magazine, 2019. 3(1): p. 19-25.
[27] Mehra, P.S., M.N. Doja, and B. Alam, Fuzzy based enhanced cluster head selection (FBECS) for WSN. Journal of King Saud University-Science, 2018.
[28] Mezghani, O. and M. Abdellaoui. Improving network lifetime with mobile LEACH protocol for Wireless Sensors Network. in 2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA). 2014. IEEE.
[29] Morris, D.Z., Leaderless, blockchain-based venture capital fundraises $100 million and counting. Fortune (magazine), 2016: p. 05-23.
[30] Noel, A.B., et al., Structural health monitoring using wireless sensor networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2017. 19(3): p. 1403-1423.
[31] Pirbhulal, S., et al., A novel secure IoT-based smart home automation system using a wireless sensor network. Sensors, 2017. 17(1): p. 69.
[32] Popper, N., A venture fund with plenty of virtual capital, but no capitalist. New York Times, 2016. 21.
[33] [33] Regis, A.W. and E.B. Rajsingh, Mobile entities in wireless sensor networks: comparative study and performance analysis. International Journal of Information and Communication Technology, 2017. 11(3): p. 301-324.

[34] [34] Reyna, A., et al., On blockchain and its integration with IoT.
[35] Challenges and opportunities. Future Generation Computer Systems, 2018. 88: p. 173- 190.
[36] Singh, S.P. and S. Sharma, A survey on cluster-based routing protocols in wireless sensor networks. Procedia computer science, 2015. 45: p. 687-695.
[37] Tsitsiroudi, N., et al. EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs. in 2016 9th IFIP Wireless and Mobile Networking Conference (WMNC). 2016. IEEE.
[38] Wang, J., et al., Energy-efficient cluster-based dynamic routes adjustment approach for wireless sensor networks with mobile sinks. The Journal of Supercomputing, 2017. 73(7): p. 3277-3290.
[39] Wen, W., et al., EAPC: Energy-aware path construction for data collection using the mobile sink in wireless sensor networks. IEEE Sensors Journal, 2017. 18(2): p. 890-901.
[40] Wang, J., et al., An energy-efficient distance-aware routing algorithm with multiple mobile sinks for wireless sensor networks. Sensors, 2014. 14(8): p. 15163-15181.
[41] Wang, J., et al. A mobile-sink based energy-efficient clustering algorithm for wireless sensor networks. in Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. 2012. IEEE.
[42] Yang, Y., M.I. Fonoage, and M. Cardei, Improving network lifetime with mobile wireless sensor networks. Computer communications, 2010. 33(4): p. 409-419.
[43] Yuan, X., et al., A genetic algorithm-based, dynamic clustering method towards improved WSN longevity. Journal of Network and Systems Management, 2017. 25(1): p. 21-46.
[44] Yang, Y. and M. Cardei. Movement-assisted sensor redeployment scheme for network lifetime increase. in Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems. 2007. ACM.
[45] Zhang, J., et al., Energy-efficient data-gathering rendezvous algorithms with mobile sinks for wireless sensor networks. International Journal of Sensor Networks, 2017. 23(4): p. 248-257.