Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 11, November 2022, pg.165 – 176

Monitoring, Detecting and Early Warning of Forest Fires using Blockchain in Wireless Sensor Network

Long Tran Huy[1*]; Chinh Tran Thien[1]; Hoai Trung Tran[2]; Quynh Le Chi[3]
[1]Research Institute of Posts and Telecommunications, Vietnam
[2]University of Transport and Communications, Vietnam
[3]Electric Power University, Vietnam
[1*] huylong.ript@gmail.com; [1] trthchinh@gmail.com; [2] hoaitrunggt@yahoo.com; [3] quynh.lechi@gmail.com

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i11.013

Abstract— Forest fires cause economic and material losses and destroy the environment, causing many negative impacts on human habitats and forest ecosystems. The unpredictable threat of wildfires leads to climate change and the greenhouse effect. It is worth noting that up to 90% of forest fires occur mainly due to human activities [1], even due to tampering, vandalism, and hostile actions. Therefore, to minimize the destruction caused by forest fires as well as accurately identify the area where forest fires occur and support government agencies, forest rangers, and search and disaster relief forces, ... it is necessary to monitor, detect and warn of forest fires right from the early stage (early warning). This paper proposes to use static sensor nodes combined with mobile in wireless sensor network (WSN) to Forest fire Monitoring, Detection, and Early Warning - FMDW. At the same time, integrating Blockchain technology (BC) in WSN solves the problem of secure routing, and distributed data storage, and prevents destructive and tampering attacks. This also suggests new research directions on monitoring, detecting, warning, and protecting forests in countries using Blockchain security technology in WSN.

Keywords— WSN, blockchain, cluster head, routing, sensor node, security.

I. INTRODUCTION

Forest fire is a disaster that causes great damage to countries, regions, and the whole world in terms of socioeconomic, ecological, and environmental aspects. Wildfires can be caused by natural causes, such as high temperatures or thunderstorms that can produce spontaneous combustion of dry fuels such as sawdust, leaves, etc. [2], or by activities subjective human activity, such as unextinguished campfires, slash-and-burn farming, improperly burned debris, or destructive activities, such as forging forest management data, burning forests to clear traces of illegal logging, destroying forests by hostile forces, reactionaries, etc. In the past, detecting forest fires using watchtowers was often ineffective because they were based on human observations. Nowadays, thanks to the progress of 4G,5G…and satellite image processing methods, and especially the blockchain technique (BC) Many remarkable progresses have been made.

The paper is organizes as follows:

In the next section, section II-A the structure of WSN is reviewed. In section II-B a short analysis of existing WSN is given. In section 3 some proposals for including block chain concept for existing WSN are mentioned. Taking the constrains and the challenges facing the modern WSN in 4G,5G ecosystem we address briefly the lightweight block chain in Section 4..

II. MODEL OF MONITORING, DETECTION, AND EARLY WARNING OF FOREST FIRES USED IN WSN

A. Wireless Sensor Network Architectures

A WSN usually consists of a large number of SNs densely deployed in a sensor area and one or more sink nodes (Sink) or base stations (BS) containing data located near or within the sensor area such as in Figure 1. Sinks/BS sends queries or commands to SNs in the sensor area, and SNs collaborate to complete the detection task and send sensor data to the Sink/BS. While, Sink/BS also acts as a gateway to external networks, such as the Internet. It collects data from SNs, performs simple processing on the collected data, and then sends the relevant information (or processed data) over the Internet to the requested user [9].

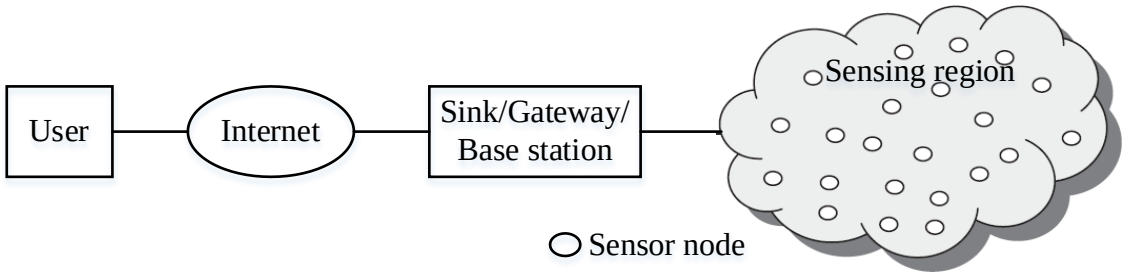

Fig. 1 Sensor network architecture

According to [9], to send data to the Sink/BS, each SN can use a hop-long link, resulting in a single-hop network architecture. However, long-distance transmission is very expensive in terms of energy consumption. Therefore, it is necessary to reduce traffic and transmission distance to increase energy savings and prolong network life. Therefore, multi-hop short-distance communication is preferred. In multi-hop communication, a sensor node transmits its sensor data toward the Sink/BS through one or more intermediate nodes, which can reduce the energy consumption for communication. The architecture of multi-hop networks can be organized into two types: flat and hierarchical. In a flat network organization, each node plays an equal role in performing the sensing task, and all sensor nodes are peers. In a hierarchical network organization, sensor nodes are organized into clusters, where cluster members send their data to cluster heads (CHs), while CHs act as switches next to transmit data to the sink node (Sink). Data aggregation can be performed at CHs to reduce the amount of data transmitted to the Sink/BS and improve the energy efficiency of the network [10]. With the above proposal to use WSN for FMDW, hereafter we choose the WSN organization architecture in the form of multi-tier clustering architecture [9]. There, in the direction from the sensor node to Sink/BS, the lowest layer is a "Tier 0 cluster member", we call it a "Normal Sensor Node (NSN)" with SNs considered as members of the cluster. The next layer is "Tier 1 cluster head (T1CH)" and we call it the "Base sensor cluster". The next floor is "Tier 2 cluster head (T2CH)" and we call it "Advanced Sensor Cluster". Finally, "Sink/BS Sensor Cluster". Sinks/BSs in the WSN are linked together on the basis of the Internet, through wired transmission lines, such as fiber optic cables, and/or 3G/4G/5G mobile radio links, and/or lines of satellite transmission.

B. Analysis of some well-known WSN model for monitoring, detecting, and early warning of forest fires

According to Udaya Dampage et al [1], the authors proposed a forest fire detection system based on wireless SNs deployed in a cellular architecture to cover the entire area. The proposed mobile architecture is in situations where the forest fire detection system is not feasible. Because, SNs can hardly be mobile in forest conditions, only maybe with SNs (using PDA devices) of forest rangers or forces responsible for field patrol. Therefore, we propose an FMDW system as a Static Wireless Sensor Network (SWSN) or a fixed sensor node, combined with a mobile architecture based on sensor devices handheld (PDA, mobile phone) of the rangers or authorized forces in the responsible units. In which, the static architecture is the main one, the mobile architecture only supports the connection for the static architecture in each situation. The fixed network architecture we propose is also suitable for [8], where applying the on-demand k coverage technique provides event detection using static nodes with variable sensor coverage change. This technique utilizes maximum detection performance with minimal event power consumption.

Also as suggested by [1], WSN is organized according to network architecture, and based on clusters, clusters are arranged according to mobile architecture. This is even more difficult to do because the closer the SNs are to the CH, the higher the energy consumption. Because it has to provide power for the data collection and

transmission of the SN itself, it also has to transmit the data of neighboring SNs to its CH. Thus, the SNs near the CH will soon run out of energy and will die, which makes the sensor network/cluster appear vulnerable to data collection. Therefore, with the SWSN that we proposed above, in the T1CH cluster sensor network cell architecture, we choose the NSN sensor node to be located outside the edge/edge of the T1CH sensor cluster and the sensor node. The Effort Sensor Node (ESN) is placed between the NSN and T1CH as shown in Figure 2. In essence, the ESN node is still the NSN node but is enhanced with additional power to ensure that it can both collect and transmit its sensor data and perform the task of relaying the data of other nodes. NSN is adjacent to T1CH.

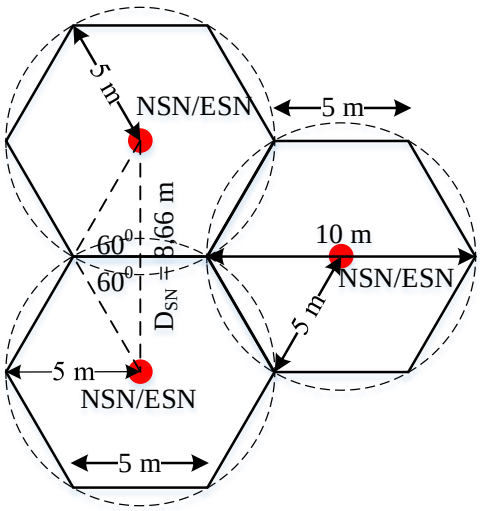

Fig.2 Sensor node structure (NSN, ESN)

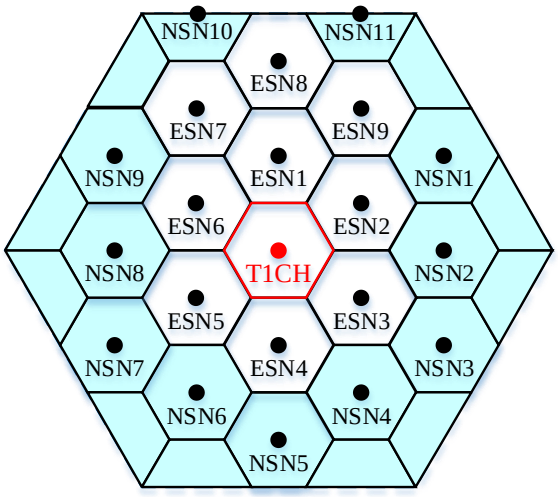

Fig.3 T1CH sensor cluster organization architecture

The organizational architecture of the base sensor cluster T1CH: As shown in Figure 3, the organizational architecture will consist of sensor nodes or NSN sensor network cells located at the edge/edge of the cluster, and sensor network cells. ESN variables are located around the cluster center T1CH (between the NSN and T1CH). Accordingly, at the edge/edge of cluster T1CH, there are 9 NSNs network cells (symbols from NSN-1 to NSN-9), and each NSN network cell has an RNSN sensor area radius = 4.33 m. At 6 adjacent edges of the T1CH with neighboring T1CHs, there will be 12 empty SNS halves. To fill this gap, it will only be necessary to arrange 2 more NSN cells in each T1CH (symbols NSN-10 and NSN-11), where half the area of NSN-10, NSN-11 will fill space at one edge of the T1CH, while the remaining half of the NSN grid cell fills the space for the adjacent edge of the neighboring T1CH. Similarly, the half-cell gaps at the remaining edges of the T1CH will be filled by the NSNs of neighboring T1CHs. On the other hand, around the center of the T1CH cluster, 6 ESNs will be arranged (symbols from ESN1 to ESN6), and each ESN network cell also has a radius of RESN = 5 m. At the same time, using 3 sensor nodes ESN-7, ESN-8, and ESN-9 to both collect and transmit sensor data of that same network cell, and perform data forwarding of NSN-10 and NSN-11 to T1CH.

The organizational architecture of the T2CH advanced sensor cluster is shown in Figure 4, the organizational architecture will have 18 clusters of T1CHs (symbols from T1CH-1 to T1CH-18), and each cluster has a radius of sensor area RT1CH = 21.65 m, the T1CHs are arranged adjacently around the center of the T2CH cluster. However, similar to the above, at the six adjacent edges of the T2CH with neighboring T2CHs, there will be 12 empty halves of the T1CH cluster. To fill this gap, it will only be necessary to arrange in each T2CH 2 more T1CH clusters (symbols T1CH-19 and T1CH-20), where half the area of T1CH-19, T1CH-20 will fill the gap at one edge of the T2CH, while the remaining half of the area of the T1CH fills the space for the adjacent edge of the neighboring T2CH. Similarly, the half-cluster gaps at the remaining edges of the T2CH will be filled by the T1CHs of the neighboring T2CHs.

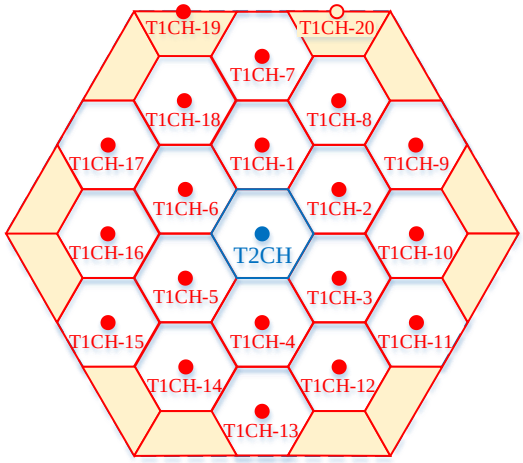

Fig.4 T2CH sensor cluster organization architecture

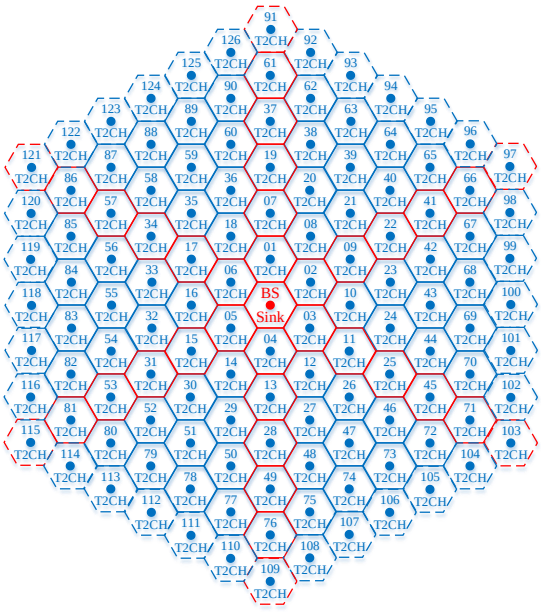

Fig.5 Sink/BS sensor cluster organization architecture

The organizational architecture of the Sink/BS sensor cluster is shown in Figure 5, each T2CH has a radius of the sensor area RT2CH = 108.25 m, is arranged adjacently around the Sink/BS, the T2CHs communicate with the Sink/BS directly. or indirectly through neighboring T2CHs. Sink/BS organizational architecture depends on actual requirements, in the organization architecture Figure 5, suppose there are 126 clusters of T2CHs (symbols T2CH-1 to T2CH-126).

Sinks/BSs are considered reliable and unrestricted in terms of resources (such as communication, Internet connection, power supply, computing power, data processing, ...) and are linked with each other through the Internet to transmit sensor data in the area of responsibility to the centralized data storage and processing center of the FMDW system, as shown in Figure 6. The number of Sinks/BSs in the SWSN network is calculated accurately and determined based on the specific forest area where an FMDW sensor is required.

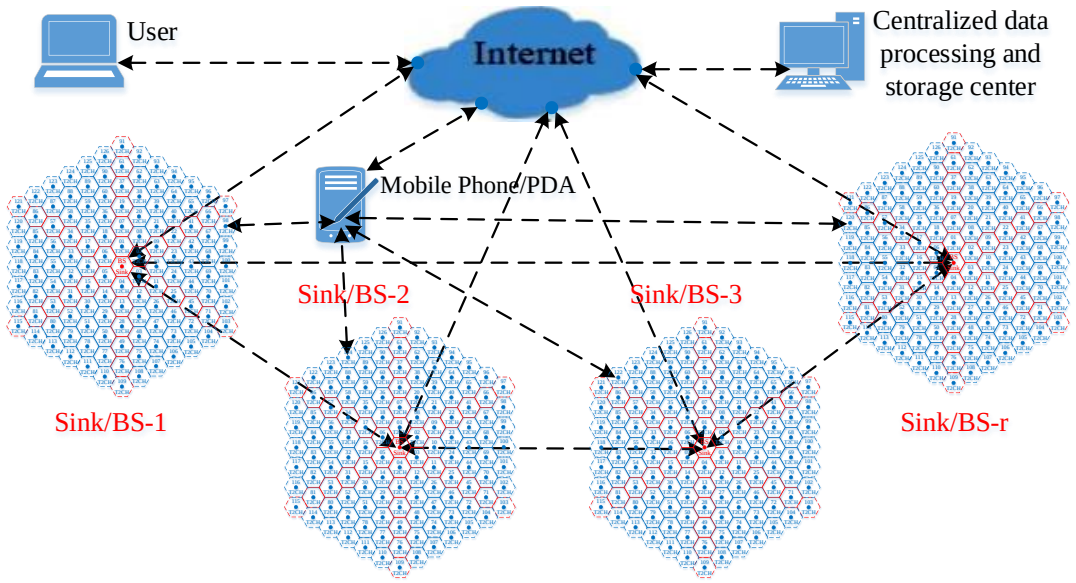

Fig.6 WSN model used for forest fire monitoring, detection and early warning

C. Determination of the range of FMDW

Normally, the SN consists of a microcontroller (Memory Central Unit - MCU) that consumes 7.5 mW of power and that in standby mode consumes 1.8 mW, the sensor module consumes 0. 16 mW, the radio transceiver has the highest power consumption of 24 mW, and the power supply uses a Lithium battery with a capacity of 4,800 mAh [1], [11]. The SN is designed to be spherical to withstand external forces and has features that prevent damage from the harsh conditions common in tropical forests. To monitor temperature and relative humidity, a DHT22 sensor is used, while an LDR sensor and an MQ9 sensor are used to monitor light intensity and CO levels, respectively. The Arduino Nano board was chosen as a microcontroller device, which is small in size and flexible for a variety of applications. The nrf24L01 module is used as a transceiver on NSNs and ESNs to communicate with each other [1] and with the cluster head node T1CH. In the calculation of FMDW range determination, similar to [1], we assume that the maximum sensing range of an NSN called a sensor network cell is defined with a radius of the transceiver area of the NSN of RTxRx = 5 m. For ESNs, each ESN will be responsible for forwarding data to 2 neighboring NSNs, so the power supply for the ESN is determined to be doubled, meaning a capacity of 9,600 mAh and the same radius of the transceiver area. of the ESN is still 5 m. At the same time, the NSN/ESN button is mounted on the trunk of the tree 1m above the ground to effectively conduct the first-stage surface fire detection test [1]. According to Figure 2, the effective sensing area radius of the NSN/ESN network cell is as follows:

$$R_{NSN/ESN} = R_{TxRx} \times \sin(60^0) = 5 \times \sin(60^0) = 4.33\ \text{m} \qquad (1)$$

Where R_{TxRx} is the radius of the transceiver area of the NSN/ESN node. The effective sensing area of an NSN/ESN node, also known as the effective sensing area of the NSN/ESN network cell, is equal to:

$$S_{NSN/ESN} = 6 \times \frac{1}{2} \times R_{TxRx} \times R_{NSN/ESN} = 6 \times \frac{1}{2} \times 5 \times 4.33 = 64.95\ \text{m}^2 \qquad (2)$$

Where $S_{NSN/ESN}$ is the effective sensing area of the NSN or ESN cell.

For the T1CH sensor cluster, we also use the Arduino nano module and the nrf24L01 module which has a maximum transmission range of 100 m in the forest environment to transmit data between T1CH clusters and between T1CH to T2CH, equipped with a lithium-ion battery and enhanced with a 5W solar battery, 12 V output voltage [1]. According to Figure 3, with an effective sensing area radius of NSN/ESN network cells of 4.33 m, each T1CH will have an effective sensing area radius and effective sensing area determined as follows:

$$R_{T1CH} = R_{NSN/ESN} \times 5 = 4.33 \times 5 = 21.65\ \text{m} \qquad (3)$$

$$S_{T1CH} = S_{CH-T1CH} + \sum_{i=1}^{9} S_{ESNi} + \sum_{j=1}^{9} S_{NSNj} + \sum_{k=1}^{12} \frac{S_{NSNk}}{2} = 64.95 \times (1 + 9 + 9 + 6) = 1{,}623.75\ \text{m}^2 \qquad (4)$$

Where R_{T1CH} is the effective sensing area radius of T1CH, S_{T1CH} is the effective sensing area of T1CH, $S_{CH-T1CH}$ is the effective sensing area of the central network cell T1CH, S_{NSNi} is the effective sensing area of the ith NSN network cell, S_{ESNj} is the effective sensing area of the j^{th} ESN network cell, $\frac{S_{NSNk}}{2}$ is the effective sensing area of the k^{th} NSN half-cell

For T2CH, we use an Arduino nano module, nrf24L01 module, and 433MHz RF wireless multi-duplex transceiver module (UART) -1,000 m (HC-12) to transmit data between T2CHs and T2CHs. between T2CH and Sink/BS, equipped with a lithium-ion battery and enhanced with a 10 W – 20 W solar battery, with a voltage

output of 12 V [1], [11]. According to Figure 4, with an effective sensing area radius of the T1CH of 21.65 m, each T2CH will have an effective sensing area radius and effective sensing area defined:

$$R_{T2CH} = R_{T1CH} \times 5 = 21.65 \times 5 = 108.25\ \text{m} \qquad (5)$$

$$S_{T2CH} = S_{CH-T2CH} + \sum_{l=1}^{18} S_{T1CHl} + \sum_{m=1}^{12} \frac{S_{T2CHm}}{2} = 1{,}623.75 \times (1 + 18 + 6) = 40{,}593.75\ \text{m}^2 \qquad (6)$$

Where R_{T2CH} is the effective sensing area radius of T2CH, S_{T2CH} is the effective sensing area of T2CH, $S_{CH-T2CH}$ is the effective sensing area of the center T2CH, S_{T1CHl} is the effective sensing area of the first T1CH, $\frac{S_{T1CHm}}{2}$ is the effective sensing area of the mth T1CH half.

Thus, the farthest transmission distance of T1CH to the cluster head center T2CH is $4 \times R_{T1CH} = 4 \times 21.65 =$ 86.60 m, with the maximum transmission range of 100 m of the nrf24L01 module selected above, the T1CH is guaranteed to stay within the transmission range directly to the T2CH without having to forward the data through any intermediate T1CH hops any. This will allow to minimize the number of hops and respectively minimize the end-to-end latency (D_{e2e}), because the power supply for T1CH has been supplemented by solar cells.

For Sink/BS, according to Figure 5, with an effective sensing area radius of T2CH of 108.25 m, each Sink/BS will have an effective sensing area radius and effective sensing area as follows:

$$R_{Sink/BS} = R_{T2CH} \times 9 = 108.25 \times 9 = 974.28\ \text{m} \qquad (7)$$

$$S_{Sink/BS} = S_{CH-Sink/BS} + \sum_{n=1}^{126} S_{T2CHn} = 40{,}593.75 \times (1 + 126) = 5{,}155{,}406.25\ \text{m}^2 \qquad (8)$$

In which $R_{Sink/BS}$ is the effective sensing area radius of Sink/BS, $S_{Sink/BS}$ is the effective sensing area of Sink/BS, $S_{CH-Sink/BS}$ is the effective sensing area of the cluster center Sink/BS, S_{T2CHn} is the effective sensing area of the nth T2CH, $\frac{S_{T1CHo}}{2}$ is the effective sensing area of the oth half T2CH, $\frac{S_{T1CHp}}{3}$ is the effective sensing area of the pth T2CH one third..

Similar to T1CH, the farthest transmission distance of T2CH to the Sink/BS center is $8 \times R_{T2CH} = 8 \times 180.25$ = 866.03 m, with a maximum transmission range of 1,000 m (according to the 433MHz RF module (UART) selected above), there will be 4 T2CH layers around the center of the Sink/BS cluster that will remain within transmission range directly to the Sink/BS, while the T2CHs from Layer 5 to Layer 8 need to forward data through an intermediate T2CH burst (e.g. Layer 5 T2CH has a T2CH-61 burst that will forward data to Sink/ The BS through the T2CH-01 cluster, similarly the 6th T2CH layer with T2CH-91 will forward data to the Sink/BS through the T2CH-07 burst, etc.). This will minimize the number of hops and respectively minimize the end-to-end latency (D_{e2e}).

III. PROPOSAL TO INTEGRATE BLOCKCHAIN TECHNOLOGY IN EXISTING WSN

A. Proposed system model and Blockchain structure for some existing WSNs

Integrating BC technology into the WSN will allow the provision of a secure and permanent database that stores transactions in the form of a digital ledger, distributed among all nodes in the network. Transactions are encapsulated in blocks that are added to the chain in chronological order. A large number of connections between sensor devices will be handled thanks to the distributed nature of BC [4]-[7]. This will greatly reduce the cost of installing and maintaining large centralized data centers. Besides, when BC technology is integrated into WSNs, it will eliminate the centralized architecture of WSNs [12]. With our proposed SWSN-based FMDW application above, the size of a Sink/BS that can include the number of nodes or cells of the defined NSN/ESN sensor network can be up to $25 \times 25 \times 127 = 79{,}375$ sensor network node/cell and capable of covering up to 5.155 km2. Thus, when the forest area needs to be monitored and detected, hundreds of km2, the number of sensor nodes is also up to millions of nodes. Therefore, the traditional WSN network with centralized data access will be difficult to meet the requirements. The integration of BC technology in WSNs will ensure monitoring of a large number of devices in the network, especially in the case of WSNs with application expansion needs (eg, increasing the number of Sink/BS). At this time, the WSN system can coordinate the handling of connections between devices, evaluate the reliability of the SN, secure routing, authenticate the SN, etc., at the same time, the security and reliability of the system. enhanced [4] - [7]. The presence of a large number of malicious nodes in the WSN has negative effects on routing, such as modifying data and broadcasting false route information that affects the performance of the network. Accordingly, attacks in WSN occur in two ways, namely data attacks and routing attacks. In data attack, adversary nodes perform data spoofing. During a routing attack, malicious nodes choose a route with the least power draining the energy of the NSN/ESN. Network efficiency suffers due to high latency and low packet delivery rate [7].

Similar to [6], [7], our proposed BC system model is shown in Figure 7 as follows: i) A SWSN includes NSNs, ESNs, T1CHs, T2CHs, Sinks/BSs, and others. end users (Users); ii) To prevent the participation of malicious nodes in the network, the registration of nodes is done by the Certificate Authority Node (CAN); iii)

Each sensor node participating in the routing process is authenticated by the Sink/BS and performs mutual authentication, thereby using the private BC to authenticate the NSNs, ESNs in T1CH, T2CH and using the BC. public to authenticate T1CHs, T2CHs in Sink/BS; iv) T1CH gathers data from NSNs/ESNs, processes and sends data directly to T2CH, while T2CH sends data to Sink/BS by selecting relay T2CH node based on remaining energy and distance minimum from Sink/BS; v) The NSNs/ESNs and T1CHs, T2CHs are static, randomly deployed and guarantee sensor coverage for a large area as required; vi) Sink/BS has high compute and storage capacity, it implements BC based on proof of authority and is responsible for validating nodes and storing sensor data; vii) T1CH, T2CH have lower computing and storage capacity than Sink/BS and are also equipped with sufficient power supply for data aggregation, computation, processing, storage, and forwarding operations.

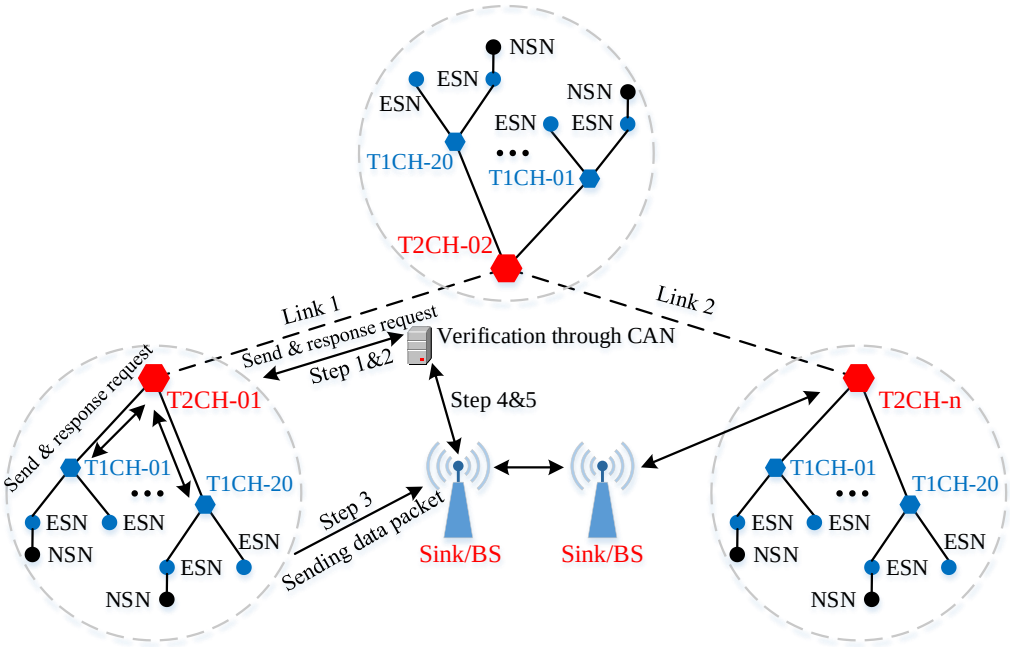

Fig.7 Our proposed BC system model

According to the model proposed above, the steps in the authentication scheme are initialization, registration, and authentication. During initialization, Sinks/BSs initialize all the NSNs/ESNs contained in the SWSN. Sink/BS generates public keys for itself, T1CHs, T2CHs, and private keys for NSNs, and ESNs. The keys are used to verify the integrity of the message. Each node has its unique MAC (Media Access Control) address. Identity of Sink/BS, T1CH, T2CH, and NSN, ESN is marked as SinkID/BSID, T1CHID, T2CHID, and NSNID, ESNID. T1CHs and T2CHs are registered using smart agreements implemented on public BC. The identity information of the T1CH and T2CH is stored in the public BC. Smart agreement verifies whether T1CH or T2CH node already exists or not. Furthermore, the validity of the MAC address of T1CH, T2CH, and the correctness of their identity will be checked. When these steps are done successfully, the public BC will record the identity of T1CHs and T2CHs. If identity verification fails, an error message is returned. In contrast, NSN, and ESN registration is done on private BC. NSNs and ESNs are allowed to join the BC network after registration. The process of registering NSNs and ESNs is the same as that of T1CHs and T2CHs. Identity information of NSN and ESN is stored on private BC. NSNs and ESNs are associated with their T1CH after deployment. In addition, when two T1CHs/T2CHs communicate, mutual authentication of T1CHs/T2CHs is performed. Both T1CHs/T2CHs send requests to Sink/BS for authentication. Because SWSN is vulnerable to two types of external and internal attacks. Therefore, the registration and authentication of NSNs, ESNs, T1CHs, and T2CHs will reduce outside attacks. Intruders will not be allowed to penetrate the network. However, internal nodes can act maliciously and broadcast false information into the network.

According to Sung-Jung Hsiao and Wen-Tsai Sung [5], by applying BC encryption, the security of sensor data can be effectively improved. BC is a cryptographically protected compound cryptographic transaction record. Each section contains the encrypted hash of the previous part, the corresponding timestamp, and the transaction data. Transaction data represents SWSN sensor data, where BC transaction records are modified into sensor data records and stored in data blocks. Each BC data block usually contains two parts, a header, and a body. The block header is a block header that encapsulates the current version number, previous block address, timestamp, random number (nonce), target block value of the current block (bits), and a Merkle tree, such as the root value (Merkle-root). The block body mainly contains the data quantity and details of the data obtained, each piece of data is permanently recorded in a data block and can be queried later. According to our suggestion, given the characteristics of the FMDW application, it is necessary to add parameters to the block header such as

"End-to-End Delay (EED) and geographical location (GL)" as shown in Figure 8, these proposed parameters are also consistent with [13], [14]. The EED parameter represents the network performance, this parameter is as minimal as possible. The GL parameter helps forest rangers, search and disaster relief forces to determine the exact location of the node, where the disaster occurred (such as the location of the fire, the location of the node/hole loss. sensor, the location of the node being tampered with/hacked, etc.). B. Prathusha Laxmi, A. Chilambuchelvan [13] proposed a Geographic Secured Routing (GSR) protocol to provide security by using both node and message authentication with a computing power low algorithm and uses the standard SHA-3 algorithm for authentication instead of user-defined authentication methods. However, the GSR algorithm consists of 3 stages: (i) network setup; (ii) discovering safe 1-hop nodes; (iii) secure communication through 1-hop nodes. But with Blockchain, all 3 stages of GSR are implicitly satisfied. Because SHA applied in BC will allow the data processed by a hash function to be one-way and it is almost impossible to compute the initial input values from the processed output values [5], [6]. Furthermore, BC transmits data that is not rewritable and, therefore, its security level is very high. This security is particularly beneficial when applied to WSNs built using the latest BC configuration [15]-[17]. Each NSN, ESN master node is connected to some sensor device and has a serial number to understand BC link order. In addition to collecting its sensor data, each BC also collects measurement data from the nodes of the other blocks. That is, when a new BC is created for a node block, the master node also acquires sensor data. Therefore, every node keeps its sensor data and for other nodes, no node is the central node, which proves the application of decentralization. All BC nodes are connected through a peer-to-peer (P2P) network and have the most secure encryption determined based on network cryptographic calculations [5].

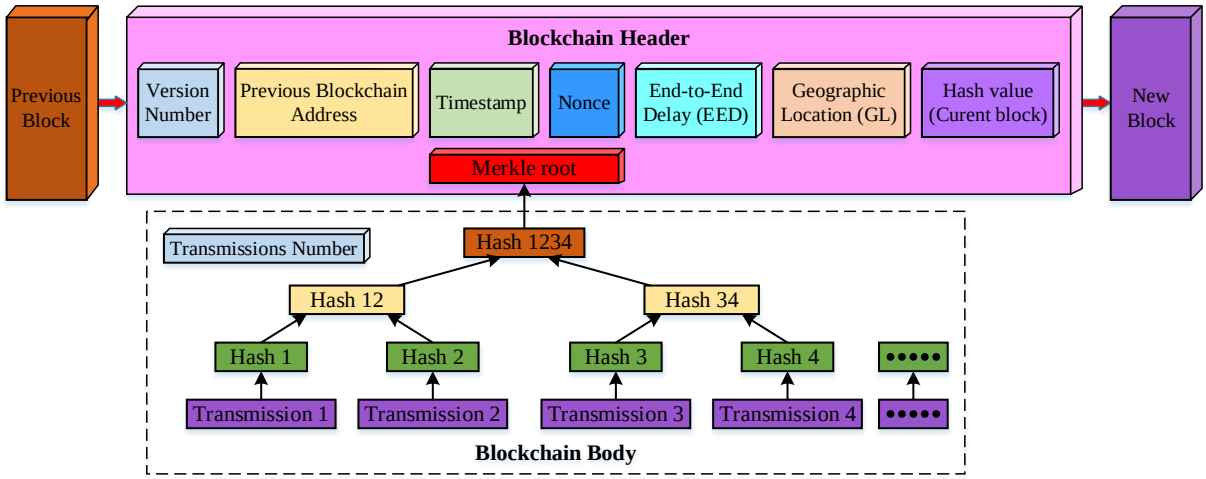

Fig.8 Our Proposed Blockchain Structure

B. Define end-to-end delay

By definition [13], it is the time required to transmit information from the source sensor node to the Sink/BS. From the above proposed network architecture according to Figure 3, Figure 4, Figure 5, the end-to-end delay (D_{e2e}) is determined as follows:

$$D_{e2e} = k_{T1CH} \times \left(D_{NSN/ESN} + D_{Other-T1CH}\right) + k_{T2CH} \times \left(D_{T2CH} + D_{Other-T2CH}\right) + \left(D_{Sink/BS} + D_{Other-Sink/BS}\right) \quad (9)$$

In there: k_{T1CH} is the number of hops transmitted from NSNs, ESNs to the beginning of the burst T1CH (k_{T1CH} = 0 ÷ 3, k_{T1CH} = 0 when the sensor node is in the cluster center T1CH, k_{T1CH} = 3 when the NSN lies at the edge/edge of T1CH); $D_{NSN/ESN}$ is the transmission delay of the NSN, ESN to another ESN, or T1CH; $D_{Other-T1CH}$ is the delay based on other factors of T1CH (such as block packing delay, processing delay, computation, etc.), note that in NSNs, ESNs have no delay component based on other factors, since at these nodes there is no processing or calculation; k_{T2CH} is the number of hops transmitted from T2CHs to Sink/BS (k_{T2CH} = 0 ÷ 5 on request, k_{T2CH} = 0 when the sensor assembly is in the center Sink/BS, k_{T2CH} = 2 When the transmission distance from T2CH to Sink/BS is through an intermediate T2CH, in our proposed model we will only choose k_{T2CH} = 2 to minimize transmission delay; D_{T2CH} is the transmission delay of T1CH to T2CH; $D_{Other-T2CH}$ is the delay based on other factors of T2CH (such as block packing delay, processing delay, computation, etc.); $D_{Sink/BS}$ is the transmission delay of the T2CH to the Sink/BS; $D_{Other-Sink/BS}$ is the delay based on other factors of the Sink/BS (such as block packing delay, processing delay, computation, etc.).

C. Determine the geolocation of the sensor node

According to Tian He et al. [18], WSN has been proposed for various applications including search and disaster relief, target tracking, and intelligent environment. Therefore, the geographic location (GL) of sensor nodes has become an important part of their state. Many localization algorithms for sensor networks have been proposed to provide location information for each node. The authors [18] divided localization protocols into two categories: range-based localization protocols, which are more expensive due to hardware dependence, and local protocols. range-free localization protocols are more cost-effective. There are many existing systems and protocols that attempt to solve the problem of determining the location of the sensor node. The approaches are taken to deal with this localization also differ in their respective device and network capabilities. Such as device hardware assumptions, signal transmission model, time and power requirements, network texture (homogeneous versus heterogeneous), nature of the environment (indoor vs. outdoor), node or beacon density (Beacons), device time synchronization, communication costs, failure requirements, and device portability. The authors [18] proposed a new range-free algorithm, called Approximate Point-In-Triangulation Test (APIT), with improved performance. in actual system configurations. Accordingly, APIT requires a heterogeneous network of sensor devices and our sensor system proposed above meets this requirement (with different nodes such as NSN, ESN, T1CH, T2CH, and Sink/BS). Where a small percentage of these devices (percentage varies depending on network and node density) are equipped with high-power transmitters and location information obtained via GPS, which are also T2CHs. and Sink/BS as our recommendation, devices equipped with this position as anchors. Using beacons from these anchors, APIT performs position estimation by isolating the environment into triangular regions between signaling nodes. The presence of a node inside or outside of these triangle regions allows a node to reduce the diameter of the estimated area in which a node resides, to provide a good location estimate, which has been proved in [18].

D. Efficient, secure and reliable routing mechanism based on conventional Blockchain for WSN

In an insider attack, nodes behave selfishly in the network. It is important to identify and remove malicious nodes after registration. The trust value of the nodes is calculated to remove the malicious nodes. The following steps involve assessing the reliability of the nodes.

1) Step 1: T1CH checks the status of NSNs, and ESNs or they are alive or not.

2) Step 2: Information about transmission time, forwarding rate, and delayed response time (also known as end-to-end delay parameter De2e) is collected for the surviving nodes and calculates the communication quality.

3) Step 3: The confidence value η is calculated based on the communication quality of the nodes.

4) Step 4: If η is greater than a defined threshold value, it is considered a legitimate node, otherwise it will be identified as a malicious node and removed from the network.

5) Step 5: The η of each node is between 0 and 1. After evaluating the reliability, the T1CHs will send a η of the node to its T2CH, and then the T2CH again forwards this η to the Sink/BS. The smart agreement will detect malicious nodes deployed at Sink/BS.

6) Step 6: Nodes with high η transmit the packet to their associated T1CHs. After receiving packets from NSNs, and ESNs, T1CHs forward to T2CH and continue forwarding to nearby Sink/BS.

Before going into lightweight WSNs we will summarize the differences between the two data flow processes in BC-integrated WSNs and existing WSNs [4]. The data in WSNs with Blockchain does not use centralized data centers. In WSNs integrated BC technology the data will go through the distributed Blockchain because the centralized server has been eliminated. Thanks to the distributed ledger in the blockchain, data authentication, and data tampering have become better. The data flow will also become more reliable and secure with the application of BC technology (see table 1).

TABLE I
COMPARISION BETWEEN TYPES OF WSNs

WSNs with Blockchain	**WSNs without Blockchain**
Decentralized	Centralized
Distributed ledger	Client- server architecture
High power consumption	Low power consumption
High security	Low security
Requires a device with a large processing speed and storage capacity	WSN devices have limited processing speed and storage capacity
More difficult to implement and maintain	Simple to implement and maintain

IV. LIGHTWEIGHT BLOCK CHAIN FOR WSN

A. Constrains of IOT blockchains and challenges facing them

Current IoT ecosystems have been put into service decades ago and rely on that time standard: centralized, brokered communication models, otherwise known as the server/client paradigm. All devices are identified, authenticated, and connected through cloud servers that sport huge processing and storage capacities but no adequate measure against insider attacks, and malicious insiders. Connections between devices have to exclusively go through the internet, even if they happen to be a few feet apart (no other choice)

While this model has connected generic computing devices for decades and will continue to support small-scale IoT networks as we see them today, it will not be able to respond to the growing needs of the huge IoT ecosystems of 4G,5G, and beyond.

Existing IoT solutions are expensive because of the high infrastructure and maintenance costs associated with centralized clouds, large server farms, and networking equipment. The sheer amount of communications that will have to be handled when there are tens of billions of IoT devices will increase those costs substantially. Furthermore [19] communicating a single bit of data consumes several orders of magnitude more power than computing a basic 32-bit arithmetic instruction [20].

Wireless transmission of a single bit can require over 1000 times more energy than a single computation. It can therefore be beneficial to perform the additional computation to reduce the number of bits transmitted. If the energy required to compress data is less than the energy required to send it, there is a net energy saving and an increase in battery life for portable computers. However, it is not al easy to perform such an additional computation. Some measures that need to be taken to meet these demands will be mentioned briefly. Such as:

- A framework of energy-efficient methods utilizing compressed sensing (CS) to send data via IoT systems is proposed to reduce significantly power consumption for transmitting data [21].
- CRC HASH FUNCTION: The main advantage of the proposed CRCs is that the irreducibility testing, which is either time or memory-consuming, can be omitted. It takes only O(n) time to generate a random polynomial of degree n. In contrast, it takes Ω(n3) time to generate a random irreducible polynomial of degree n. A detailed quantitative analysis of the achieved security as a function of message and CRC sizes is given and shows that the presented authentication scheme might be useful for low-cost resource-constrained devices [22].
- H. Krawczyk [23] presented a proposal to reduce sequence's key length significantly so that transmission time is shortened. Dajiang Chen et al [24] pointed out that using LFSR (linear feedback shift register) along with polar code will reduce time cost significantly and give hardware simplicity.
- Especially, one needs many special and efficient algorithms to create the IoT blockchain:
  - ✓ 1st: the closed ring connecting the intended nodes so that no other element can enter without being detected. Using trace function over finite field brings a new nice advantage, namely: easy to prove the secured reconstructions properties of a secret sharing scheme [25]. This closed ring possess the following properties:
    - All participants are connected in a logic ring initially
    - Two different pairwise shared keys between participants Ui and Uj can be computed using their shares.

In our scheme, we use the finite field F defined by a primitive polynomial. The definition of this field is tighter than a polynomial ring. So A is surely satisfied and easily checked.

If a and b are two elements in F, then a+b=c is also an element in F, and furthermore: a+c=b and b+c=a. In other words c, the pairwise common key does exist for any pair! B is thus satisfied also. We state that our schemes are secure reconstruction secret sharing.

- ✓ 2nd: the order number of these nodes needs to be pseudo-randomly rearranged so that it is difficult for the adversary to make the correct guess of the node name. The probability of that correct guess will be 1/N (with N the length of the ring) [26].
- ✓ 3rd: the hop-count(decimation step) algorithm to carry out the successive checking see [27], [28].

Due to the limited scope of this review, we cannot go further in detail.

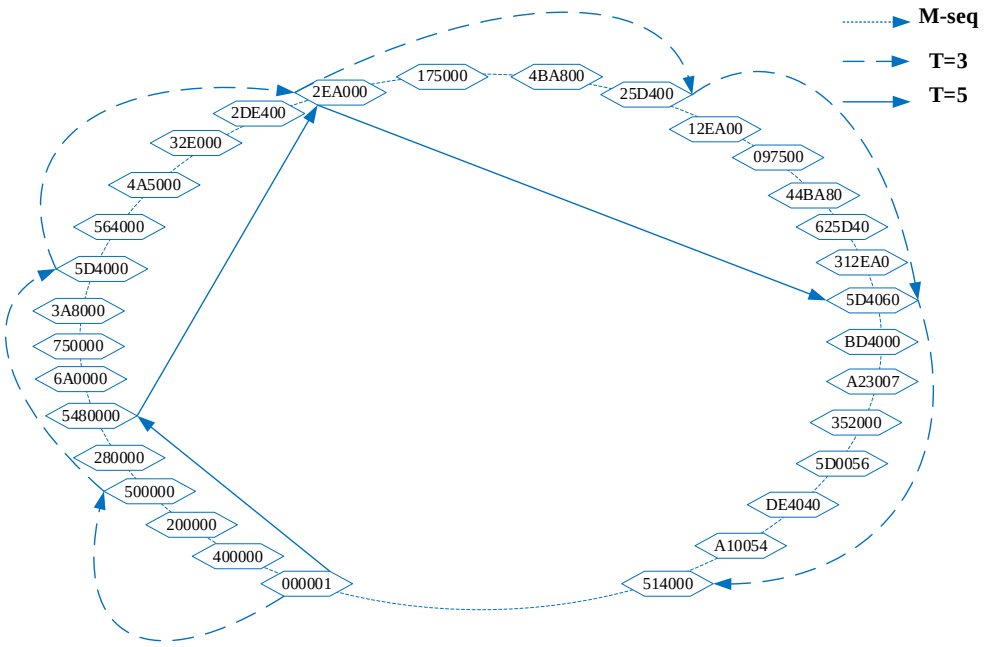

Fig.9 intrusion detection and prevention by identity and hop-count check (with 31 node)

V. CONCLUSION AND FURTHER WORKS

In this paper, we first review the structures of the traditional WSNs, since they continue to work for many years to come. Some proposals to integrate blockchain technology into the typical traditional WSN have been made.

Taking the perspective of 4G, and 5G into account we mention some new suggestions based on our work. In the coming contributions we hope to go further in details, which are challenging and interesting.

REFERENCES

[1] Udaya Dampage, Lumini Bandaranayake, Ridma Wanasinghe, Kishanga Kottahachchi & Bathiya Jayasanka, *Forest fire detection system using wireless sensor networks and machine learning*, Scientific Reports, 2022, nature portfolio, www.nature.com/scientificreports.

[2] Nelson, R. (2020) Untamedscience.com. April 2019. [Online]. Available: https:// untam edsci ence. com/ blog/ the- envir onmen talimpact-of-forest-fires/. Accessed 30 December 2020.

[3] Vikash Kumar, Anshu Jain and P N Barwal, *Wireless Sensor Networks: Security Issues, Challenges and Solutions*, International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 859-868.

[4] Cuong V Nguyen, Minh T Nguyen, Trang T.H Le, Thang A Tran, Duy T Nguyen, *Blockchain technology in wireless sensor network: benefits and challenges*, ICSES Transactions on Computer Networks and Communications, Vol. X, No. Y, December 2021, ISSN: 2588-5847.

[5] Sung-Jung Hsiao, Wen-Tsai Sung, *Utilizing blockchain technology to improve WSN security for sensor data transmission*, Tech Science Press, CMC, 2021, vol.68, no.2, pp. 1899-1918.

[6] Usman Aziz, Muhammad Usman Gurmani, Saba Awan, Maimoona Bint E Sajid, Sana Amjad, and Nadeem Javaid, *A Blockchain Based Secure Authentication and Routing Mechanism for Wireless Sensor Networks*, IMIS 2021, LNNS 279, Volume 279, pp 87-95.

[7] Saba Awan, Maimoona Bint E. Sajid, Sana Amjad, Usman Aziz, Usman Gurmani, and Nadeem Javaid, *Blockchain Based Authentication and Trust Evaluation Mechanism for Secure Routing in Wireless Sensor Networks*, Proceedings of the 15th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2021, LNNS 279, Volume 279, pp 96-107.

[8] Alam, K. M., Kamruzzaman, J., Karmakar, G. & Murshed, M. *Dynamic adjustment of sensing range for event coverage in wireless sensor networks*. J. Netw. Comput. Appl. 46, 139–153 (2014).

[9] Edited by Jun Zheng, John Wiley & Sons, Inc., Hoboken, New Jersey, *Wireless sensor networks*, Copyright © 2009 by Institute of Electrical and Electronics Engineers, ISBN: 978-0-470-16763-2.

[10] *R. Rajagopalan and P. Varshney, "Data-aggregation techniques in sensor networks: A survey", IEEE Communications and Surveys and Tutorials, vol. 8, no. 4, 4th Quarter 2006, pp. 48 – 63.*
[11] Ali M. Abdal-Kadhim & Kok S. Leong, *Investigation of Wireless Sensor Node Power Consumption Profile Powered by Heterogeneous Hybrid Energy Harvesters with EPDD Management Algorithm*, International Journal of Electronics, Volume 106, 2019 - Issue 8, pp. 1264 – 1280, ISSN: 0020-7217 (Print) 1362-3060 (Online).
[12] A. Banafa, "*Iot and blockchain convergence: benefits and challenges,*" IEEE Internet of Things, 2017.
[13] B. Prathusha Laxmi, A. Chilambuchelvan, *GSR: Geographic Secured Routing using SHA-3 algorithm for node and message authentication in wireless sensor networks*, Future Generation Computer Systems 76 (2017), pp 98–105.
[14] *B. Prathusha Laxmi, A. Chilambuchelvan, GSTP: Geographic Secured Two Phase Routing Using MD5 Algorithm, Circuits and Systems, 2016, 7, 1845-1855, Published Online June 2016 in SciRes.*
[15] Q. Lu and X. Xu, "*Adaptable blockchain-based systems: A case study for product traceability*," IEEE Software, vol. 34, no. 6, pp. 21–27, 2017.
[16] W. Meng, E. W. Tischhauser, Q. Wang, Y. Wang and J. Han, "*When intrusion detection meets blockchain technology: A review*," IEEE Access, vol. 6, pp. 10179–10188, 2018.
[17] Y. Zhao, Y. Li, Q. Mu, B. Yang and Y. Yu, "*Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems*," IEEE Access, vol. 6, pp. 12295–12303, 2018.
[18] Tian He, Chengdu Huang, Brian M. Blum, John A. Stankovic, Tarek Abdelzaher, *Range-Free Localization Schemes for Large Scale Sensor Networks*, MobiCom '03, September 14-19, 2003, San Diego, California, USA Copyright 2003 ACM 1-58113-753-2/03/0009.
[19] Zheng Gong, Zheng Huang, Weidong Qiu And Kefei Chen, *Transitive Signature Scheme from LFSR**, Journal Of Information Science And Engineering 26, 131-143 (2010).
[20] Kenneth C. Barr And Krste AsanoviC, *Energy-Aware Lossless Data Compression*, ACM Transactions on Computer Systems, Vol. 24, No. 3, August 2006, Pages 250–291.
[21] Minh T. Nguyen, *An energy-efficient framework for multimedia data routing in Internet of Things (IoTs)*, (2019) Industrial Networks and Intelligent Systems 6(19):159120.
[22] Elena Dubrova, Mats N¨aslund, G¨oran Selander, and Fredrik Lindqvist, *Lightweight CRC-based Message Authentication*, *Royal Institute of Technology*, Stockholm, Sweden 2015 pp1-18.
[23] Hugo Krawczyk, *LFSR-based Hashing and Authentication*, CRYPTO 1994: Advances in Cryptology — CRYPTO '94 pp 129–139.
[24] Dajiang Chen, Ning Zhang, Nan Cheng, Kuan Zhang, Zhiguang Qin, Xuemin Shen, *Physical Layer based Message Authentication with Secure Channel Codes*, IEEE Transactions on Dependable and Secure Computing 2018.
[25] LeinHarn, ZheXia, ChingfangHsu, YiningLiu, *Secret sharing with secure secret reconstruction*, Information Sciences 519 (2020) pp 1-8.
[26] Son Nguyen Van, Le Chi Quynh, Giang Nguyen Hoai, Bui Lai An,Tran Canh Duong, *Generating The Interleave Division Multiple Access (Idma) Used In 5g Mobile Communication System*, Journal of Xidian University 15 issue12-2021 pp 1-11.
[27] Perumal Raghavan Kavitha, Rajeswari Mukesh, *Detection of Impersonation Attack in MANET Using Polynomial Reduction Algorithm*, International Journal of Network Security, Vol.20, No.2, PP.381-389, Mar. 2018 (DOI: 10.6633/IJNS.201803.20(2).19).
[28] Dang Van Truong, Le Chi Quynh, *Applying M-sequences Decimation to Generate Interleaved Sequence*, Journal of Science and Technology on Information security No 2.CS (14) 2021.

