TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

Secure Data for Wireless Sensor Network using Detection Malcious Node Method

Oudani Hassan[1], Krit Salahddine[1], Karimi khaoula[1] and Elmaimouni Lahoucine[2]
[1]*Laboratory of Engineering Sciences and Energy, Polydisciplinary Faculty of Ouarzazate, Ibn Zohr University, Agadir, Morocco*
[2] *Laboratory of Energies Renouvelables, Microsystèmes Acoustiques et Mécaniques Polydisciplinary Faculty of Ouarzazate, Ibn Zohr University, Agadir, Morocco*
hassan.oudani@gmail.com , salahddine.krit@gmail.com, karimi.khaoula92@gmail.com, la_elmaimouni@yahoo.fr

Article Info
Volume 82
Page Number: 4968 - 4982
Publication Issue:
January-February 2020

Article History
Article Received: *18 May 2019*
Revised: *14 July 2019*
Accepted: *22 December 2019*
Publication: *25 January 2020*

Abstract:
Wireless sensor network (WSN) is a network containing of extensive autonomous hundreds of thousands of devices. These sensors are used to monitor physical and environmental conditions. The trusted routing novel protocol is designed and is reliable and installs a secure network with power management. Based on conditions, hierarchy clustering is selected to use the cluster head system. The problematic of energy and safety in WSN is a huge drawback. All This constraint are used to overcome the correct routing protocol. Recent studies shown that the usage of a period and calculation efficient system of cryptography in conjunction including improved routing protocol is able to confirm energy-efficient and secure interaction on WSNs. In this paper we familiarize a novel strategy LSBEE (Loop Secure Based on Energy Efficient) which is secure and energy efficient able to detect a malicious node in WSN. Trial results display that our proposed method routing protocol accomplishes improvement than the already existing state-of-the-art protocols in the form of number of live nods during number of rounds, stability period, and detection a malicious nodes in WSN using Simulink Matlab 2013.

Keywords: *WSN, Routing Protocol; Secure network; Energy Efficient; Malicious Node; cryptography; Safety ; LSBEE; Matlab 2013.*

1 Introduction

Wireless Sensor Networks (WSNs) utilization increased by the spontaneous improvements in MEMS (Micro Electro-Mechanical-Systems). WSNs are consisting a several nodes that perform with each other to complete action of sensing. These sensors work with each other information delivery from network towards sink. All these information are the units concerned in observing the interesting areas[1]. A wireless sensor network gives various and unforeseen uses like.

Health care, battle field surveillance, intensive care habitat and Atmosphere monitoring[2], and actually uncountable uses. Since the nodes require to be unobtrusive, they can carry only a little battery because they consist a little form-factor[3]. Due to this they do low-power operation and they have supply limited energy[4]. Sensor limitations cannot be done here. Memory, bandwidth and the computational ability are the resources which are inhibited in the nodes. In application of WSN and development of protocol, Power maintenance is the one main discussed and significant matter [5].

From few days, for data communication the utility of WSNs is maximum. Usually, in order to get sensory data infrastructure of WSN establishes a various self-dependent sensor nodes spreaded upon network and frontward to base station where sink is the base station [6]. In repetition, these

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

nodes of sensor can be of various kinds like visual, acoustic, magnetic, thermal, and infrared sensors [6]. These sensors are have capacity for identifying the actions needed to be observed, controlled and assessed [7]. These nodes of sensor are reinforced with the little battery resources. Non-deniably, action and the period of life of WSN mainly based on reliable transmission, power utility etc. Although, WSN is a paradigm of vital interaction and it stays in suspicion and therefore needs reliable method. The incompetent routing or transmission might proceed the dropping of data and thus, till successful delivery network undertake retransmission. This yields exhaustion of energy. On the other side, in WSN the malicious nodes probability is not able to be avoided universally. In those conditions, WSN with outdated organization needs mistake flexibility and safety in contradiction of any probable eavesdropping and message distribution. The large space is provided by the architecture which is multi-layered for vulnerabilities and operation [8].A complete information of protection threats and attack probability is able to see in [8]. According to literature, shared wireless medium and the spontaneous featured makes WSN get acquire more vulnerably [8]. The good idealized utility of laptops and adaptor of wireless network might give a permits for listeners to acquire the network. This causes retransmission which forces system to undertake retransmission and therefore maximum delay and power utilization. These all boundaries disrupt distribution of QoS. An optimal solution to alleviate these issues is the routing protocol is firming with improved safety methods. Non-deniably, formation of information and network system requires key factor where security standard represents key factor. The three key dimensions of security data are as follows: data availability, integrity, confidentiality. The WSN depend on several factors like mankind and an atmospheric situation has attracted Academia-industries. Majority of safety breaches of both sensor networks and wired networks are same; therefore, sensor networks attacks due to deployment of nodes in unsafe areas even in usual mutual atmosphere [9]. To discuss with such oppositions, cryptography methods have been considered which allows safe data communication in wireless network. Mainly two kinds of cryptography methodologies; they are symmetric and asymmetric key. Both transmitter and receiver perform decryption and encryption of data by using same key in case of symmetric key encryption. In asymmetric key dimensions keys used are different, and the private decryption key is obtained to only at the recipient, mainly the key of encryption is familiar to all the participants or linked nodes. Because of overheads in signalling, energy consumption and higher computational difficulties local cryptosystems those are key encryption is not suitable to WSNs. Consequently, to get a correct security solution based on the WSNs behaviour requires a trade-off among changed encryption methodologies.

Four types of routing algorithms classifications for WSNs are as follows: Hierarchical Algorithms, Information Centric Algorithms, Location Dependent Algorithms, Flow of Network and Aware Algorithms of QoS [10, 11]. For minimizing the count of transmitted information to the sink, routing algorithms works fusion and data aggregation and effectively keeping the power utilization sensor nodes and undertaking them in multi-hop interaction in certain cluster. The cluster creation is dependent its locality to the head of cluster and on the sensor energy reservation [12]. The cluster heads are needed for BS top stage communication and minimize the directly above traffic. For that a novel loop secure based energy efficient routing protocol (LSBEE) is introduced.

Other parts of the offered document are classified as below: Section 2 tells the study of dissimilar writings relating to WSN energy effectiveness, safety and protocols of safe interaction for WSNs. Section 3 represents the

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

proposed methodology and algorithm steps of LBSEE protocol. Results of simulation are showed in part 4 and conclusion is represented in part 5.

2 SECURITY IN WSN

2.1 Security

Typically, safety in WSNs represents the examination of linked routing and safe communication upon wireless media [13]. Yuan et al. [14] researched several safety plan model upon spread networks of sensor. Including to allow energy efficient routing, authors originate that including changing supply voltages is able to be a potential methodology; however it is not able applicable in main uses because of dependency on hardware. Hemalatha et al. [15] was improved security unit, here authors demoralised the earlier Indian Vedic mathematics. In their methodology, at the region of point multiplication, features of the cross multiplication can be used. Thus, using this methodology they got a cost effective message safety unit. The operation of their introduced unit upon for WSN was originating good enough to the local messages safety methodologies.

To secure the transmission Furtak et al. [16] used cryptographic units at the data link layer to safe broadcast. Their methodology was known effective to confirm safety for information collection also. In [17], authors implemented a modern node construction that services Trusted Platform Module (TPM) to display cryptography. TPM spread on a sequence of trust that purposes to include trustability between the constituents of the spread nodes of sensor. This method imposes the system to function only if software and hardware performing formations is confirmed over and done with particular cryptographic operations. Authors specified that the usage of tamper resistant hardware is able to confirm that the keys of cryptographic would not leave of absence of a safe perimeter. Tellez et al. [18] implemented a protocol of safe interactions for surrounding observing upon WSNs. Recognizing the flow of safety in safe MSP430 microcontroller units (MCUs), authors implemented bootstrap loader (BSL) secret code showed acceptable to prevent exposure of difficult safety data, certainly the encryption keys. To meet it, authors repaired the poor BSL secret code. Jasmin et al. [19] used Advanced Encryption Standard (AES) technic to confirm safety for dissimilar facilities. The necessity of its introduced RCON and S-Box was to provide facility to a materially commanding cryptosystem to WSNs. Their improved non-linear organisation of the safety system supported the obtaining of private and public key for every custom, dependent on which the autograph confirmation was finished. The major role of their non-linear organization methodology was the highest range of safety for information spreading upon WSNs. Mengyao et al. [20] improved a lightweight trust calculation unit applying ring-dependent clustering methodology. Authors improved a safe power effective cluster-routing protocol by using the inter clusters routing algorithm. Authors create that their introduced unit not only enables robustness in contradiction of malicious and egotistic nodes to confirm dependable statistics distribution, but also balances the entire delay and power utilization. Oreku [21] implemented a mathematical unit dependent WSN dependability model that gives insight of the several issues disturbing dependability of the WSN interaction and information collection. Ji et al. [22] combined uncertainty test methodology with conformance justification to allow challenging of the WSNs safety operations. A same determination was prepared by Qi et al. [23] that measured dissimilar safety pressures in WSNs. To meet it authors used the information of Finite State Machine (FSM). In their investigation authors know that protocol of Tiny PK is not able to satisfactory to struggle Sybil attack. Also the writers specified that the unawareness of those methodologies might cause violation of QoS and power utilization. Hu et al. [24] implemented a safe

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

unit of clustering that confirms the identification of node interaction when adding in and leaving from network safely (NJQS). Zhang. [25] Researched WSNs safety preparing during pointing on power efficient routing to have maximum life-period of network. Mainly, they concentrated on reaching safe communication upon restricted atmosphere of manufacturing model.

Fouchal et al. [26] implemented a spread unit to guarantee node identification by including a confirmation element. In this unit, Trusted Platform Module (TPM) fitted out with every node that collect keys of encryption. TPM of the every node owns their personal unrestricted and also public and private keys (pair) key documentation. Therefore the utility of documentation creates system restricted as in real-time interaction wishes many extra nodes as a network section. Nakamura et al. [27] implemented a rule dependent organization middleware which provide facility to updatable WSN atmosphere for information safety. The middleware is dependent on LINC, a rule-dependent organisation middleware. Its introduced LINK dependent safety unit allowed WSN nodes to assign or separate in safe way according to necessity. Jokhio et al. [28] implemented a novel safety unit to confirm node region needed to safety-smooth interaction upon WSNs. Cumulatively, they pointed on reaching safety, flexibility, and scalability including the optimal power utilization. Their introduced unit involving a double-way identification unit and a light-weight encryption method for safe key establishment. Karapistoli et al. [29] concentrated over evaluating dissimilar message imagining and pictorial analytics dependent methodologies for safe interaction upon WSNs. Kannan et al. [30] implemented a adoptable and measurable safety unit during managing least idleness for protocol of WSN. The base of its unit was dependent on a source viewpoint, in which unit was implemented to safe every source in the WSN atmosphere, other than protect from attacks.

2.2 Security Techniques of Routing-based Security

Typically, routing dependent safety methodology put on the safety characteristics during working routing upon WSN. In these methodologies, the at-hand routing methods are improved effectively to confirm safe interaction upon network. From few years, Das et al. [31] resulting a safe routing unit in which authors concentrated on repelling occurrences such as wormhole attack and overflowing attack in WSN. To reach it, authors used medium access control (MAC) improvement. Henze et al. [32] introduced a safe contact unit to confirm difficult information safety upon network of sensor and raised area of cloud. Therefore, authors know to confirm well-organized presentation the tradeoff between safety and exchange time of key must be reduced. To reach it, authors used RSA and AES encryption with key size of 128 bit and 2048 bit, particularly. For increasing safety characteristics of the WSNs, Chen et al. [33] resulting an improved LEACH protocol. According to dynamic mobility circumstances performance of LEACH protocol could improve the cluster.

Methodologies created by authors are good enough compare to the routing protocol of traditional LEACH, mainly in the form of strength and memory feeding. Tang et al. [34] introduced a routing unit called Cost-Aware Secure Routing (CASR) to WSNs, here they subjugated possibility theoretical information to put on random walking unit and stability factor of energy. Obaidat et al. [35] resulting a safety unit for safe over heterogeneous network of sensor. To reach it, authors implemented a methodology of trust element that uses connection excellence and characteristics of node excellence to measure whether the connection is effective to confirm safe communication.

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

2.3 Cryptographic-dependent Methodologies

Cryptographic technics are important applied techniques for communication safety or network. This technic usually displays encryption upon vulnerable connections or nodes to prevent any safety breaches. Therefore, irrefutably, maximum of the current protocols of cryptography are cold and therefore needs additional optimization to reach both time and computational effective operation. In Recent, Shankar et al. [36] did determination to deed cryptography public-key method called Elliptical Curve Cryptography (ECC) to allow safe interaction upon WSNs. Kodali et al. [37] also used ECC in addition of Diffie- Hellman key interchange unit for safety of WSN interaction. Xu et al. [38] resulting a cryptosystem was particularly structured to repel attacks of DoS in WSN. The main uniqueness in its unit was the apply of ECC with a numerical sign to reach safe interaction upon network of sensor. Munivel et al. [39] also used public key infrastructure (PKI) to do encryption and maintaining of key for safe WSN interaction. Soosahabi et al. [40] implemented a probabilistic cryptographic unit by manipulating the level of real-time communication. Al-Haija et al. [41] used encryption of RSA to confirm safety upon WSN. Yan et al. [42] used cryptosystem of AES to reach strengthen and effective interaction in WSN. Jeon et al. [43] implemented an encryption dependent safety unit which is subjugated unrestricted adjoining sources encryption performance. This method was create effective in the form of improved modulation and minimum difficulty.

Huang et al. [44] used unit of cryptosystem to secure information accumulation in WSNs, here they used cryptographic methods to execute shared identification among nodes of sensor. In view of the toughness of the initials dependent safety unit, Liu et al. [45] resulting a sign unit by using node recognize message. They used investigational idea by applying node message to result a sign technic. Panda et al. [46], used Advanced Encryption Standard (AES) encryption unit to confirm information concealment in WSN interaction. In this methodology, they uses AES dependent similar key unit that segments the unique key for both decryption and encryption among transmit and recipient. Sekhar et al. [47] used community key cryptography unit to result a safety unit to execute peripheral representative identification and development of assembly key. In this unit, the peripheral representative interconnects along the base station utilizing encryption of public key, and additional interconnects with nodes of WSN by usage secret key distribution unit. In real, their unit included three successive stages; identification, registration and development of assembly key. Therefore, authors are not able to report the matters of period and computational difficulty, which is compulsory for transmission of QoS upon WSNs.

Praveena et al. [48] implemented a technic of cryptography known as Modern Encryption Standard Version-II (MES-V-II), this deeds encryption of symmetric key methodology to do information safety above WSNs. Yu [49] also used cryptography of public-key to originate a PKI for WSNs. Writers used encryption of RSA to confirm WSN safety. The entire safety unit including two sequential stages; the node of sensor achieve greetings with base station in first stage, in which sensor node and base station implement a assembly key to confirm end to end connection safety. In the next stage of their safety unit, writers used the resulting assembly key to encrypt information to manage confidentiality for the period of communication upon WSN. Salam et al. [50] resulting a key pre-spreading unit that uses cryptography of public key to allow safe key settlement between nodes of sensor.

Authors know that the pre-spreading unit dependent on public key cryptography provides improved action, especially in terms of source feeding, node repetition attack, attack-resiliency etc. Botta et al. [51] notices the matter of vitality

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

effective even though using cryptographic methods upon WSN connections. To reach optimum resolution, authors use accelerators of hardware cryptographic in aggregation with micro-controller. Writers realized that apply of hardware accelerator able to considerably create well-organized calculation and therefore is able give improved power effectiveness. Landstra et al. [52] recommended a key maintenance unit mainly for unrelated WSNs. In their introduced unit nodes of sensor put on earlier keys create trust between nodes. Predominantly, it exists in a well-defined secure time that prevents any run-time attack. Poornima et al. [53] proposed to create most cultured safety unit to direct the necessity of non-group confidentiality, frontward concealment and retrograde concealment. The key role was the facility of key generation, key cancelation and interchange.

2.4 Safety demands in WSNs

Few key safety requirements in WSNs are detailed below [54]:

2.4.1 Information Confidentiality

In WSNs, node is needed conceal any important information to neighbouring nodes. In repetition, there are several application situations in that nodes may deliver difficult information and therefore promising a safe transceiver channel is compulsorily provided. Allowing safe data mainly linked to nodes of sensor (i.e., region of node, importance of node, etc.) and connected public keys data is compulsory. In main routing protocols of WSN, symmetric encryption along a private key delivery is favoured to reach message Concealment. For instance, system of encryption of RC5 has been originate well-organized to simplify information of WSN confidentiality. Other algorithms like DES need maximum remembrance area, calculations and energy utilization and therefore not able to be favoured for WSNs.

2.4.2 Information Integrity

Declaring information concealment, the robbery of the information is able to be avoided expressively. Therefore, it doesn't confirm safety of the message components. Opponents on network might proceed variation in the information that finally may bring network indiscretion. Information reliability confirms unified transmission on network by preventing other fake operations from the hateful node. Else, the probability of information alteration is not able to unnoticed even in the absence of hateful nodes, mainly in the time of information interchange between neighbouring nodes. In those situations, confirming information reliability come to be unavoidable by improving medium access control (MAC) of the stack of the protocol.

2.4.3 Information Authentication

As a wireless communication methodology, WSN needs significant destination and source to confirm flawless information interchange through the network. It is able to prevent the probability of information interchange with unlicensed nodes, also known as hateful node. Information identification confirms transmitter and receiver that the delivery of information meets to the legal recipient. In the double way interaction, information identification able to worked by applying symmetric method. In this way, both the source and destination can segment the private key to evaluate data confirmation code (MAC) for entire message.

2.4.4 Information Freshness

In WSN communication, including the information concealment and honesty, the freshness of information is compulsory to create in time judgement. When the mutual key plans are applied it converts inevitable in the sensor network. However, united key circulation turn into time feeding, mutual keys needed to be altered. Furthermore, if the node is conscious of the phase

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

of key variation, it turn to be adoptable to carry on normal interaction. To allow information freshness, a sequence of time is able to be included in every packet.

2.4.5 Accessibility

Accessibility indicates the delivery of facilities of WSN at Denial of Service (DoS) attacks. In repetition, DOS attacks may directs each and every films of the protocol stack of WSN which finally might incapacitate nodes to operate additional interaction. Depletion of battery and retransmission might be occurred by DoS attack by forcing the network. It can minimize the life period of the network meaningfully. Classically, to provide approachability in networks of sensor, the idleness of sensor nodes are considered. Few of the basis safety methodologies used in WSNs are conferred in the part 3.5 below.

2.5 Basic Safety Models for WSNs

Below part details on the few key safety methods applied in networks of sensor.

2.5.1 Cryptography

Classically, WSNs include several small sensors which frequently go through opponents because of deficiency of energy, handling ability and time, and availability of memory. In other side, the usage of encryption method needs extra bits transmission that needs more dealing out time, power and memory. Definitely, the usage of typical encryption methods might maximize packet loss, delay and jitter in WSNs[55][56].

2.5.2 Steganography

Distinct cryptosystems that aims to secreting the concept of data, steganography directs at hiding the appearance of the data. Actually, steganography implants data as particular audio-visual aid information (picture, video, voice, etc.) in this way that it keep safe the existence of extra message in stego message. Where, the main detached to operate the carrier in this way the information stays unnoticeable to the others by keeping unique appearance. Therefore, this is source comprehensive technic that is able to guide only for message hiding intension. As a non-specific safety unit it doesn't reflects difficulties on WSN transmission and chiefly energy restraints. In view of above conversation, it is able to be imagined that the information safety and confirmation are linked to the lifetime or energy effectiveness of the WSNs. The safety breaches (leading information damages because of malicious node attacks) yields as undesirable retransmission that leads exhaustion of energy. Along with the exhaustion of energy it air force network to undertake overdue delivery and therefore interrupts setting up standard of QoS. Hence, to improve such matters allowing safe interaction among sensor nodes is compulsory. Here is the necessity to build an optimum resolution to build up WSNs by that prevent node or information conciliation for the duration of interchange amongst the nodes of sensor. Considering, in this survey paper few of new writings directing safety in WSN, and energy effective of safe interaction upon WSNs are conversed and particular strong point and boundaries are evaluated [56].

3 Proposed Looping Method of security in WSN

3.1 Loop Construction Process for WSN

In the real-time WSN has energy restriction and security difficult, to develop the life time of network, it is needed every node must pass less strength for the period of routing the packet. The following figure 1. a, b, c, d, e and flow chart below in figure 2 Shows the flow and working of the looping strategy proposed LSBEE algorithm to formed the loop between all nodes in WSN[2].

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

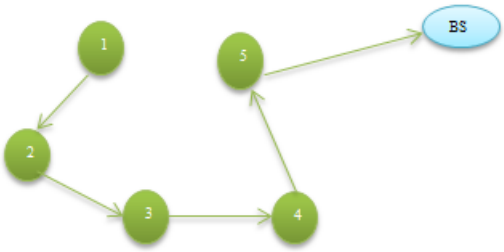


Figure 1. a: Step 1 of LSBEE

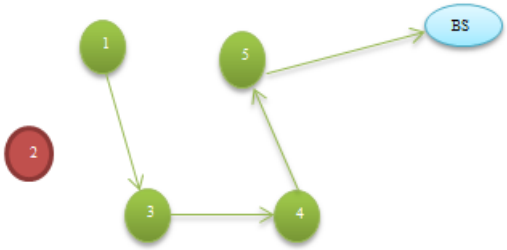


Figure 1. b: Step 2 of LSBEE

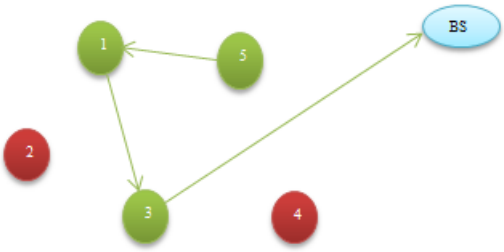


Figure 1. c: Step 3 of LSBEE

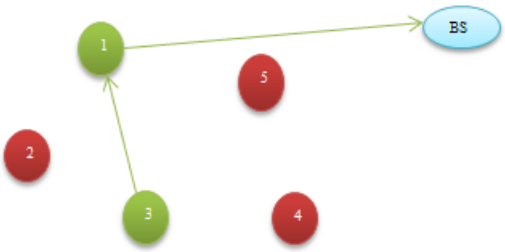


Figure 1. d : Step 4 of LSBEE

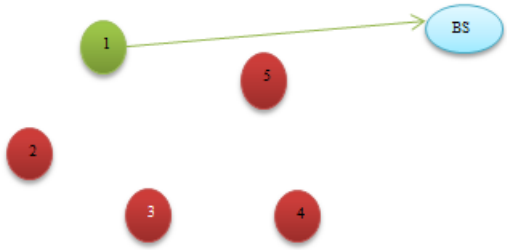


Figure 1. e : Step 5 of LSBEE

3.2 Algorithm Steps of Loop Construction Process for WSN

The following step shows the LSBEE Algorithm:

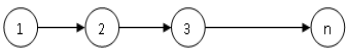
Algorithm Steps:

1. A set of WSN nodes randomly distributed in an area.
2. Each node is labelled by its name a storage memory in each node holds the information of its name and the names of the other nodes in its network along with other information such as

- Distance with other nodes in WSN and distance to base station.
- Present status of the energy.
- The neighbour name presently to whom it is linked in the loop.

3. A single loop of all nodes in the WSN is formed as shown in the figure(a)
4. The first node passes the sensed information to the next node along its other pre-stored status and additional information. i. e

5. Node (2) passes its sensed information to node (3) along with the information of node (1) i e. so on till the last node of the loop.



January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

6. The last node (n) containing all other nodes information communicates with the base station. In such method the WSN works for first round.
7. Node (1) before starting its work i.e. passing its sensed information to node (3) it generates a random number from the alive nodes , excluding the dead ones. The random numbered nodes act as the initiator to form the loop in the next round of message transmission to base station. In this way the different rounds of data transfer from WSN to BS takes place.
8. When any of the nodes gets dead or if its energy is below 10% of its total energy those nodes will be removed and a new loop of alive nodes will be formed which work will accordingly from steps (1) – (7) until the entire nodes die in the WSN.

3.3 Flow chart Algorithm of Loop Construction Process for WSN

The figure 2 represents the flow chart of the LSBEE algorithm steps for the communication process at the data transfer rounds from WSN to the base station during its operation.

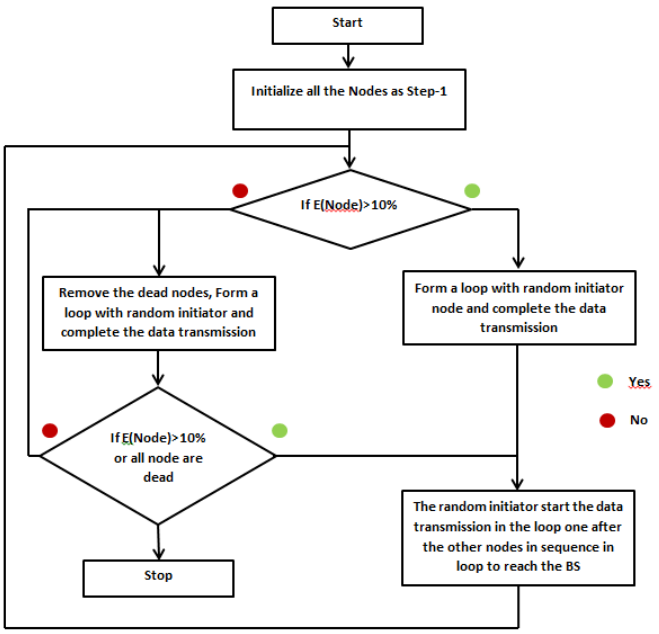


Figure 2: flow chart Algorithm LSBEE Energy

3.4 Process of Security Encryption and Authentication for WSN

The following step shows the LSBEE Algorithm for security:

Algorithm Steps:

1. All nodes are initialized with their names i.e. a numerical node number pre assigned for every node and stored inside their storage memories.
2. All nodes initially have a common secret number stored in their memories which is used for authentication to verify the node belongs to the same network or it is an outside node.
3. The first node encrypts the sensed data using a randomly generated symmetric key using AES encryption standard then transmits the data along with the key in the address (Node number) of the data packet were the receiving node uses the key for decryption process.
4. The common secret key of the node is added with the node number and placed in next address to the encryption key stored address.
5. The node number of the node is put in every first byte location of the sensed data packet which is to be transmitted to the next nodes.
6. The second node after receiving the packets from first node. Extracts the node number of first node then goes to that address extracts the encryption key to decrypt the data and also collects the secret authorization code from the next location of key which will be subtracted from the node number and compared with the secret code pre-stored in it to authorizers the node is valid or invalid. If the node is valid it will accept the data else it will reject the data.

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

7. Similar process is repeated from steps (3)-(6) for the subsequent nodes in the loop were every node generates a random encryption symmetric key while passing data between nodes.

8. Random encryption key every time for securing the data between nodes and base station is generated. Due to random selection of encryption key in every round of transmission provides more robust and strong security with simple computation power at each node and also prevents unauthorized addition of any new nodes in the network.

3.5 Flow chart of process Security Encryption and Authentication for WSN

The figure 3 represents the flow chart of the LSBEE algorithm steps for the security encryption and authentication process at the data transfer rounds from WSN to the base station during its operation.

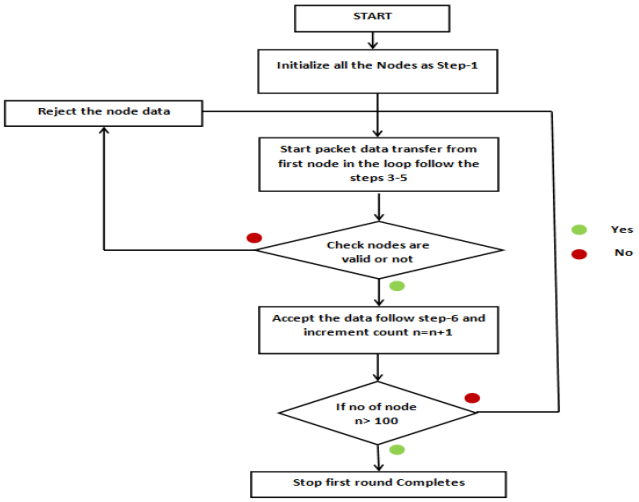


Figure 3: flow chart Algorithm LSBEE Security

3.6 Example of Authentication process used LSBEE Protocol

The following example shows the security and authentication process used LSBEE protocol between the nodes during data exchange in the WSN. In this example the keys are taken as byte size just to illustrate.

Ex:

Let the authentication secret key (ID-key) =80.

- **Data packet from node-1**

Node No.	Enc-key	ID-key						
1	34	80+1						
Addr-0	Addr-1	Addr-2	Addr-3	Addr-4	Addr-5	Addr-6		Addr-n

- **Data packet from node-2**

Node No.		Enc-key	ID-key					
2		49	80+2					
Addr-0	Addr-1	Addr-2	Addr-3	Addr-4	Addr-5	Addr-6		Addr-n

- **Data packet from node-3**

Node No.			Enc-key	ID-key				
3			57	80+3				
Addr-0	Addr-1	Addr-2	Addr-3	Addr-4	Addr-5	Addr-6		Addr-n

TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

4 ANALYSIS AND RESULTS SIMULATION OF LSBEE Protocol

4.1 Parameters of simulation

In our example of test, we let the authentication secret key (ID-key) =80, and insert 5 malicious nodes in original with same key as original nodes in WSN.

The introduced method is replicated with broadly assumed simulation atmosphere, MATLAB 2013. The WSN is denoted by 100 nodes of sensor they are set up in 100 x 100 meter square areas. Position of the base station fixed exactly at centre of carefully chosen square area. The primary strength is 1J for every node of sensor; Table 1 defined others parameters simulation of LBSEE protocol:

Table 1: Simulation parameters

Number of nodes	100
Simulation Surface (m^2)	(100,100)
Initial Energy(j)	1
Energy Transmission (j)	$50*10^{-9}$
Energy Reception(j)	$50*10^{-9}$
Simulator	Matlab 2013
number of rounds	13000
Number of malicious nodes insert	5
(ID-key) of nodes	80
(ID-key) of malicious nodes	80

4.2 Results simulation

The execution of our security algorithm LSBEE gives us the results illustrated in the figure1, figure2, figure 4, 5, 6 and figure 7 below:

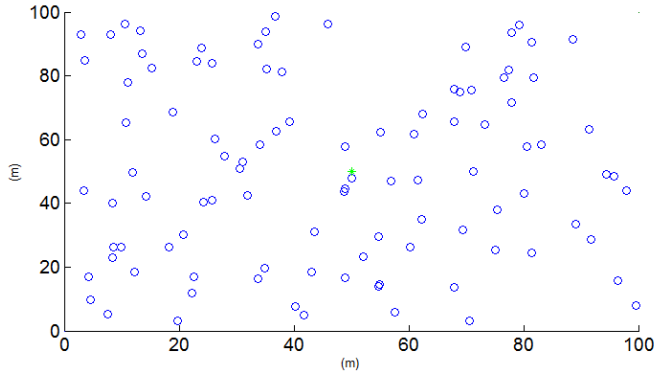


Figure 4: Original distributed nodes in WSN

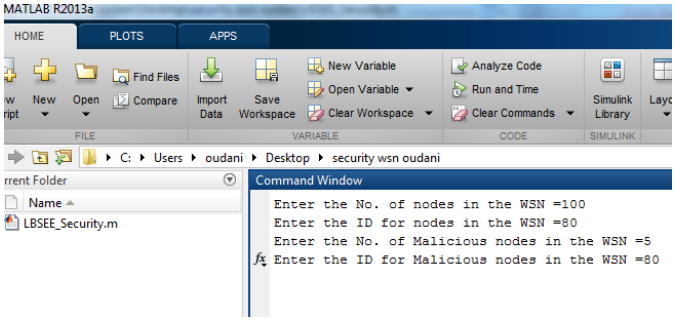


Figure 5: Execution Parameters Algorithm LSBEE

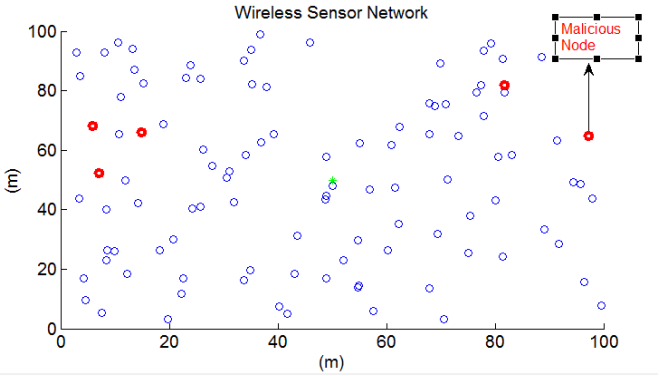


Figure 6: Original distributed nodes with indicate 5 malicious nodes in WSN using LBSEE protocol

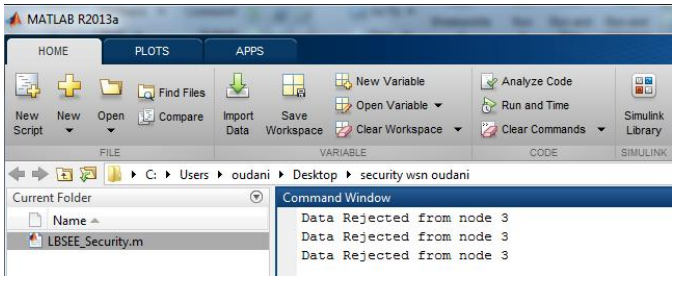


Figure 7: Reject data of all malicious nodes

4.3 Analysis Results simulation

After insert (n=5) malicious node in the original architecture (Figure 4), and after distribution key, the execution of LBSEE protocol show that our algorithm determines the malicious node, and

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

indicates it in red color(Figure 6). On the other hand our algorithm refuses exchanged the data with the malicious nodes as shown in figure 7 above.

5 CONCLUSION

In the proposed method LSBEE the nodes connected in the loop require less energy to transmit and receive from its neighbours which will save lots of energy of the WSN in the networks helping to improve network life time. In every round only one node spends energy to communicate with base station. Overall lifetime of the WSN network gets improved. The random numbered nodes acts as the initiator to form the loop in the next round of data transmission to base station and the random number is used as encryption key every time for securing the data between nodes and base station. Due to random selection of encryption key in every round of transmission provides more robust and strong security with simple computation power at each node. Hence the results of simulation reveals that the introduced technic LSBEE is outperforming the other methods in life time stability and security as discussed above.

REFERENCES

1. Hassan Oudani , Salah-Ddine Krit , Lahoucine El Maimouni " combining leach, pegasis hierarchical protocol and constraint distance to increase the lifetime of wireless sensor networks", International Journal of Mechanical and Production Engineering Research and Development (IJMPERD) ISSN (P): 2249-6890; ISSN (E): 2249-8001 Vol. 8, Issue 4, Aug 2018, 571-581
2. Hassan Oudani , Salah-Ddine Krit , Khaoula Karimi and Lahoucine El Maimouni, "A New Approach Looping Protocol Efficient in Energy for Wireless Sensors Network "Jour of Adv Research in Dynamical & Control Systems, Vol. 11, 04-Special Issue, 2019
3. W.R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks", in IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000, vol. 8, pp. 8020.
4. A. Manjeshwar and D. P. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," Proceedings of 15th IEEE International Parallel and Distributed Processing Symposium, San Francisco, 23-27 April 2001, pp. 2009-2015.
5. V. Loscri, G. Morabito and S. Marano, "A Two-Levels Hierarchy for Low-Energy Adaptive Clustering Hierarchy (TL-LEACH)," Proceedings of IEEE Vehicular Technology Conference, Dallas, 25-28 September 2005, pp. 1809-1813.
6. Kifayat, K., et al, "Information and Communication Security, Security in wireless sensor networks, , Springer, 2010, p. 513-552.
7. Sekhar, V.C. and M. Sarvabhatla. "Security in wireless sensor networks with public key techniques". In Computer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.
8. K. Sharma, M. K. Ghose, D. Kumar, "A comparative study of various security approaches used in wireless sensor networks", Int. J. Adv. Sci.Technol., vol. 17, pp. 31–44, 2010.
9. Panda, M. Data security in wireless sensor networks via AES algorithm. In Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on. 2015. IEEE.
10. S. Varshney, C. Kumar and A. Swaroop, "A comparative study of hierarchical routing algorithms in wireless sensor networks," Computing for Sustainable Global Development (INDIACom), 2nd

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

International,Conference on, New Delhi, 2015, pp. 1018-1023.
11. J.M.Corchado, J.Bajo, D.I.Tapia and A.Abraham, "Using heterogeneous wireless sensor networks in a telemonitoring system for healthcare", IEEE transactions on information technology in biomedicine, vol.14, no.2, pp.234-240, 2010.
12. K.Patel, T.Sanjay and J.Pradeep, "Energy Efficient Hierarchical Routing Algorithm in Wireless Sensor Network.", International Journal of Advanced Research in Science,Engineering and Technology, vol.1, no.3, pp.103-109, 2014.
13. Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.
14. Yuan, L. and Qu, G., "Design space exploration for energy-efficient secure sensor network", Proc. The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 17-19 July 2002, pp.88 – 97.
15. S. Hemalatha and V. Rajamani, "VMIS: An improved security mechanism for WSN applications," 2014 International Conference on Science Engineering and Management Research (ICSEMR), Chennai, 2014, pp. 1- 3.
16. J. Furtak, Z. Zieliński and J. Chudzikiewicz, "Security techniques for the WSN link layer within military IoT," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 233-238.
17. M. Barbareschi, E. Battista, A. Mazzeo and S. Venkatesan, "Advancing WSN physical security adopting TPM-based architectures," Proceedings of the 2014 IEEE 15th International Conference on Information Reuse and Integration (IEEE IRI 2014), Redwood City, CA, 2014, pp. 394-399.
18. M. Tellez, S. El-Tawab and M. H. Heydari, "IoT security attacks using reverse engineering methods on WSN applications," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 182-187.
19. U. Jasmin and R. Velayutham, "Enhancing the security in signature verification for WSN with cryptographic algorithm," 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT- 2014], Nagercoil, 2014, pp. 1584-1588.
20. L. Mengyao, Y. Zhang and X. Li, "Ring-based security energy-efficient routing protocol for WSN," The 26th Chinese Control and Decision Conference (2014 CCDC), Changsha, 2014, pp. 1892-1897.
21. G. S. Oreku, "Reliability in WSN for security: Mathematical approach," 2013 International Conference on Computer Applications Technology (ICCAT), Sousse, 2013, pp. 1-6.
22. S. Ji, Q. Pei, Y. Zeng, C. Yang and S. p. Bu, "An Automated Black-box Testing Approach for WSN Security Protocols," 2011 Seventh International Conference on Computational Intelligence and Security, Hainan, 2011, pp. 693-697.
23. Y. Qi, Q. Pei, Y. Zeng, C. Yang and S. p. Bu, "A security testing approach for WSN protocols based on object-oriented attack model," 2011 Seventh International Conference on Computational Intelligence and Security, Hainan, 2011, pp. 517-520.
24. X. Hu and Y. Zhang, "Research on Security Mechanism of Nodes Joining in and Quitting from WSN," 2011 Third Pacific-Asia Conference on Circuits, Communications and System (PACCS), Wuhan, 2011, pp. 1-4.
25. G. Zhang, "Aviation manufacturing equipment based WSN security monitoring system," The Proceedings of 2011 9th International Conference on Reliability, Maintainability and Safety, Guiyang, 2011, pp. 499-503.

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

26. H. Fouchal, J. Biesa, E. Romero, A. Araujo and O. N. Taladrez, "A Security Scheme for Wireless Sensor Networks," 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, pp. 1-5.
27. Y. Nakamura, M. Louvel and H. Nishi, "Coordination middleware for secure wireless sensor networks," IECON 2016 - 42nd Annual Conference of the IEEE Industrial Electronics Society, Florence, 2016, pp. 6931-6936.
28. S. H. Jokhio, I. A. Jokhio and A. H. Kemp, "Light-weight framework for security-sensitive wireless sensor networks applications," in IET Wireless Sensor Systems, vol. 3, no. 4, pp. 298-306, December 2013.
29. E. Karapistoli and A. A. Economides, "Wireless sensor network security visualization," 2012 IV International Congress on Ultra-Modern Telecommunications and Control Systems, St. Petersburg, 2012, pp. 850-856.
30. V. Kannan and S. Ahmed, "A Resource Perspective to Wireless Sensor Network Security," 2011 Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Seoul, 2011, pp. 94-99.
31. A.K.Das, R.Chaki, and K.N.Dey, "Secure energy efficient routing protocol for wireless sensor network", Foundations of Computing and Decision Sciences, Vol. 41, No. 1, pp.3-7,2016.
32. M. Henze, S. Bereda, R. Hummen, and K. Wehrle, "SCSlib: Transparently accessing protected sensor data in the cloud. Procedia Computer Science, Vol.37, pp.370-375, 2014.
33. L. Chen, "An Improved Secure Routing Protocol Based on Clustering for Wireless Sensor Networks", InMechatronics and Automatic Control Systems, pp. 995-1001, 2014 Publishing.
34. D. Tang, T.Li, J. Ren, and J. Wu, "Cost-Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks", Parallel and Distributed Systems, IEEE Transactions, Vol. 26(4), pp.960-973, 2015
35. M.S. Obaidat, S.K. Dhurandher, D. Gupta, N. Gupta, and A. Asthana, "DEESR: dynamic energy efficient and secure routing protocol for wireless sensor networks in urban environments",Journal of Information Processing Systems, Vol.6(3), pp.269-294, 2010
36. S.K. Shankar, A.S. Tomar, and G.K. Tak, "Secure Medical Data Transmission by Using ECC with Mutual Authentication in WSNs", Procedia Computer Science, Vol. 70, pp.455-61,2015
37. E. Munivel, and G. M. Ajit, "Efficient public key infrastructure implementation in wireless sensor networks", In Wireless Communication and Sensor Computing, ICWCSC, InternationalConference, pp. 1-6. IEEE, 2010.
38. R. Soosahabi, Naraghi-Pour, D. Perkins, and M.A. Bayoumi, "Optimal probabilistic encryption for secure detection in wireless sensor networks. Information Forensics and Security",IEEE Transactions on, 9(3), pp.375, 2014
39. Q.A. A-Haija, A. Tarayrah, H. A-Qadeeb, and A. Al-Lwaimi, "A tiny RSA cryptosystem based on Arduino microcontroller useful for small scale networks. Procedia Computer Science, Vol.34,pp.639-646,2014
40. R.K. Kodali, and N.N. Sarma, "Energy efficient ECC encryption using ECDH", In Emerging Research in Electronics, Computer Science and Technology Springer, pp. 471-478, 2014
41. J. Xu, and L. Dang, "Multi-User Broadcast Authentication Protocol in Wireless Sensor Networks against DoS Attack", Open Cybernetics & Systemics Journal, Vol.8, pp.944-950, 2014
42. Y. Yan, T. Shu, "Energy-efficient In-network encryption/decryption for wireless body area sensor networks", InGlobal Communications

January - February 2020
ISSN: 0193 - 4120 Page No. 4968 - 4982

Conference (GLOBECOM), IEEE 2014,pp. 2442-2447, 2014
43. H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks", Information Forensics and Security, IEEE Transactions, Vol.8, No. 4, pp.619-625, 2013
44. S.I. Huang, S. Shieh, and J.D. Tygar, "Secure encrypted-data aggregation for wireless sensor networks. Wireless Networks, 16(4), pp.915-927, 2010
45. J.K. Liu, J. Baek, J. Zhou, Y. Yang, and J.W. Wong, "Efficient online/offline identity-based signature for wireless sensor network. International Journal of Information Security, vol.9(4), pp.287-296, 2010
46. Panda, M. Data security in wireless sensor networks via AES algorithm. In Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on. 2015. IEEE.
47. Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques. In Computer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.
48. Praveena, A. and S. Smys. Efficient cryptographic approach for data security in wireless sensor networks using MES VU. in Intelligent Systems and Control (ISCO), 2016 10th International Conference on. 2016. IEEE.
49. Zhang Yu, "The scheme of public key infrastructure for improving wireless sensor networks security," 2012 IEEE International Conference on Computer Science and Automation Engineering, Beijing, 2012, pp. 527-530.
50. M. Iftekhar Salam, P. Kumar and HoonJae Lee, "An efficient key predistribution scheme for wireless sensor network using public key cryptography," The 6th International Conference on Networked Computing and Advanced Information Management, Seoul, 2010, pp. 402-407.
51. M. Botta, M. Simek and N. Mitton, "Comparison of hardware and software based encryption for secure communication in wireless sensor networks,"2013 36th International Conference on Telecommunications, and Signal Processing (TSP), Rome, 2013, pp. 6-10.
52. T. Landstra, M. Zawodniok, and S. Jagannathan, "Energy-efficient hybrid key management protocol for wireless sensor networks," in IEEE Conference on Local Computer Networks (LCN), 2007. 14
53. A. Poornima and B. Amberker, "Key Management Schemes for Secure Communication in Heterogeneous Sensor Networks," in International Journal of Recent Trends in Engineering, 2009.
54. Héctor KASCHEL, José MARDONES, Gustavo QUEZADA," Safety in Wireless Sensor Networks: Types of Attacks and Solutions",Studies in Informatics and Control, 22(3):323329· September2013,DOI:10.24846/v22i3y20139, https://www.researchgate.net/publication/269398801
55. Madhumita Panda, " Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-03, 2014, Issue-01, pp-50-56.
56. Ouafaa IBRIHICH, thesis 2017 '' Security protocols for wireless sensor networks '' ,2017