Asian Journal of Information Technology 15 (11): 1746-1757, 2016
ISSN: 1682-3915

Fuzzy Logic Based CH Selection for Secured Data Communication with PVR Encryption Using VK-Constructs

A. Vijayalakshmi and P. Vanaja Ranjan
Department of Electrical and Electronics Engineering, College of Engineering,
Anna University, 600025 Chennai, Tamil Nadu, India

Abstract: The security and energy efficient data collection is crucial in Wireless Sensor network because of the limited energy storage capability of sensor nodes. The encryption algorithms available in cryptography can be exploited to provide data security. The standard encryption algorithms can have major impact on data security which use analytical model for encryption and consume power. This study presents an improved fuzzy logic based cluster formation and cluster head selection based data collection algorithm with enhanced network lifetime for multi-cluster topology achievable with using the Pattern Viable Restoration (PVR) algorithm based on Viable Key (VK) scripts. This new method is proposed for secure data communication with minimal energy consumption in sensor nodes. The presented study has two folds: cluster formation and Cluster Head (CH) selection algorithm. Secured data communication based on VK Scripts. The extensive simulation results and experimental analysis using TINYOS based IRIS motes prove on the proposed algorithm of longer network lifetime.

Key words: Cluster head selection, data security, encryption, energy efficiency, fuzzy logic, wireless sensor networks

INTRODUCTION

Wireless Sensor Networks (WSNs) typically have no fixed infrastructure like wired network and wireless sensor nodes have constrained resources and limited amount of energy (Akyildiz *et al*., 2002). Thus, the main constraint of designing communication algorithm is to minimize the energy consumption of a node and to enhance the network lifetime. To achieve these goals, most researchers had designed energy efficient protocols and algorithms. One of the most popular strategy used for this purpose is clustering. The various clustering algorithms were presented by Abbasi andYounis (2007).

Clustering in WSNs can be considered as the actual partitioning of dynamic nodes in the distributed sensor network structure into several clusters discussed by Chinara and Rath (2009) and energy efficient routing protocol for WSN based on fuzzy logic was discussed by Momani and Saadeh (2011). Clusters of the nodes in the distributed sensor network structure are formed with respect to their distance between each other. These nodes which are located within their radio transmission range, setup a bidirectional communication link between them. Typical clustering algorithms are known as single-hop clustering algorithms presented by Chinara and Rath (2009) and multi-hop clustering algorithms presented by Ohta *et al.* (2003).

The role of WPANs in system health monitoring of electrical grid is sensor signal-based machine signature analysis, remote energy monitoring, power theft monitoring and fault diagnostics of the equipment in the grid. Due to this reason, wireless sensor nodes need to be configured with security mechanism to shield the data or plain text over the wireless medium.

Designing of key management algorithm and development of secure routing protocol are two issues that have been focused by large amount of research. For secure and reliable data transmission, most researchers had developed various encryption algorithms based on crypt analysis. For example, the Reed Solomon (RS) code based security algorithms have been proposed by Wang *et al.* (2010) and key management algorithms (Pietro *et al*., 2003; Jankowski and Laurent, 2011). The various security schemes have been proposed in literature such as the design of secure and efficient routing protocol by Alwan and Agarwal (2013) and Chinara and Rath (2009) the design of secure data aggregation protocol by Estrin *et al.* (1999), Bhoopathy and Parvathi (2012) and Roy *et al.* (2012).

Corresponding Author: A. Vijayalakshm, Department of Electrical and Electronics Engineering, College of Engineering, Anna University, 600025 Chennai, Tamil Nadu, India

The elliptic curve cryptography for multimedia compression was proposed by Tawalbeh *et al.* (2013). The selective encryption algorithm was used during compression and perceptual encryption has been achieved by using selective bit-plane encryption which was used in multimedia before the compression process.

The design of clustering protocol has two main parts: cluster formation and Cluster Head (CH) selection. This study proposes a Fuzzy Logic based Cluster Head selection algorithm (FLCS) for Cluster formation and Cluster Head selection. The main focus of FLCS is to form an optimal number of clusters and to develop the best CH selection algorithm, thereby, increase the life time of the network. This study also discusses a novel technique to build secured data transmission using pattern viable restoration of data while transmission and while reception. The patterns are specifically formulated using English alphabet script and termed herein as Viable Key (VK) script. The VK array is formulated as pattern viable restorations based on recurrent keys or on asymmetric keys.

Literature review: Performance analysis of cluster based wireless sensor networks was presented by Malik *et al.* (2009). The researcher analyzed the performance of the adaptive clustering protocol called Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for the increased network lifetime and balanced energy among the nodes. The performance analysis of the LEACH protocol had been done by Malik *et al.* (2009) and Heinzelman *et al.* (2002). The CHs were elected only based on the residual energy and CH position was rotated among the nodes in random manner.

The Balanced Cost Cluster-Heads Selection Algorithm (BCSA) proposed by Zytoune *et al.* (2009) is the modified LEACH clustering algorithm. This algorithm considered the remoteness of the nodes to the sink and nodes residual energy were the main criteria for the cluster head selection. As compared to LEACH, the BCSA has very less performance improvement.

The Fuzzy Relevance-based Cluster head selection Algorithm (FRCA) for mobile ad hoc networks was developed by Lee and Jeong (2011). In this algorithm, the fuzzy relevance was used to select a node as CH. The Fuzzy Relevance Degree (FRD) was included in the packet structure and these packets were transmitted by the nodes in the network with FRD for CH selection. The fuzzy value used for FRD was determined by the available power, distance and mobility and ranges between 0 and 1 ($0\leq\mu\leq1$). The FRD was calculated based on energy of a node in the network. The number of CH obtained in FRCA was higher and the analysis was compared with CBRP-Cluster Based Routing Protocol. The main drawback of FRCA is more CH overhead maintenance cost. This is due to the higher number of CH selection.

The Fuzzy-logic-based clustering algorithm for WSN using energy predication approach called LEACH-ERE was proposed by Lee and Cheng (2012). The criteria for the selection of cluster head was based on two parameters such as Residual Energy (RE) and expected Residual Energy (ERE). The selection of a node to act as a CH candidate had been done only when it had more RE and more ERE.

The Hybrid Multipath Scheme for Secure and Reliable Data Collection (H_SPREAD) protocol proposed by Lou and Kwon (2006) had been developed based on the N-to-1 multipath routing protocol. The multiple node disjoint paths were found first. Among these paths M disjoint paths were selected for delivering the message at the BS. In this protocol the message is first divided into shares and each share has N packets. These shares were transmitted over M paths. Due to the use of N shares among M paths, H-SPREAD was discussed as a secured protocol. Even though, it is a secured protocol, the maximum security can be achieved by compromising M paths for transmission.

Reed-Solomon Forward Error Correction (RS-FEC) based selective encryption approach for secure and reliable wireless communication was discussed by Wang *et al.* (2010). This algorithm first divide the original data into number of frames and each frame has K symbols and sequence number. Then the original symbol was encoded by RS code, during encryption the K original symbols were encoded into N codeword symbols. In Mode 1, only $N\text{-}K\text{+}b_1$ symbols were encrypted by the sender, in Mode 2, $K\text{+}b_2$ symbol had been encrypted. The b_1 and b_2 were predefined values defined by the users. From the original data only 'w' symbols were encrypted and transmitted. At the receiver end only 'w' symbols were decrypted and decoded. The algorithm discussed in this literature is based on the code theory algorithm and it consumes more power for encoding and decoding.

Hybrid key management based security mechanism was discussed by Pan *et al.* (2012) for health care monitoring of elderly people using WSN. Two modified algorithms based on Feistel cipher structure were proposed. This algorithm generated the random 128 bits key for four round functions whereas in Feistel cipher 16 round functions were used. Four keys were generated by dividing 128 bits into four 32 bits sub-keys named as K_1, K_2, K_3, K_4. The plain text of 64 bit was equally divided into two parts. Each part is 32 bit long. The encryption and decryption were done using these four sub-keys and the round function F. The 64 bit plain text was encrypted by using $K_1K_2K_3K_4$ and decrypted by using $K\ K_4\ K_3\ K_2$. $_1$ This algorithm used the same concept of Feistel cipher structure with reduced number of sub-keys.

Secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) was presented by Souza and Varaprasad (2012) and Alwan and Agarwal (2013). The security provided by this protocol was designed using digital signature based crypto system which used the MD5 hash function and RSA algorithm. In this protocol the source node selected the node-disjoint path and M messages are transmitted through the selected path. Encryption of these messages had been done by using MD5 hash function. The digital signature was used by source node to encrypt message digest H(M) with its private key.

The homophonic substitution and error-correction coding were proposed by Oggier and Mihaljevic (2014) for achieving the cryptographic security. The performance analysis of the transmission of the encrypted data over a noisy channel was analyzed. The data was encoded by the encoder before encryption. The modulo2 addition had been used for encrypting the data. The extra randomness was achieved by using wire-tap channel coding combined with channel noise. The security analysis for passive advisory and active advisory have also been addressed.

This study proposes pattern based encryption algorithm for encrypting the sensed data which does not require any logical or mathematical based processing. The proposed Pattern Viable Restoration (PVR) technique with Viable Key (VK) Script in this study consumes very less energy because it uses script based encryption technique. The PVR technique with VK script uses only the scripts for encrypting the source node data in which there is only the replacement of the bits and does not require any complex computation. The advantage of the proposed technique is encryption and decryption which is done only one time by the source node and destination node respectively. The intermediate node in the routing path does not have/need the knowledge about the data. Thus, the router nodes consume lesser energy. The proposed data security algorithm is applied to the cluster based network. The FLCS algorithm discussed in this study select the most appropriate node in the network as the Cluster Head (CH) for secured data communication.

MATERIALS AND METHODS

Fuzzy logic based cluster head selection input/output membership function for FLCS: The proposed algorithm has used three input membership functions and one output membership function for selecting a node being a Cluster Head (CH). The input membership functions are Residual Energy (RE), Least Recently Selected (LRS) Number of Neighbours (NN) and Criticality of the Event (Event) and the output membership function is Probability (P). Triangular membership functions are used for input and output variables and are shown in Fig. 1 and 2, respectively.

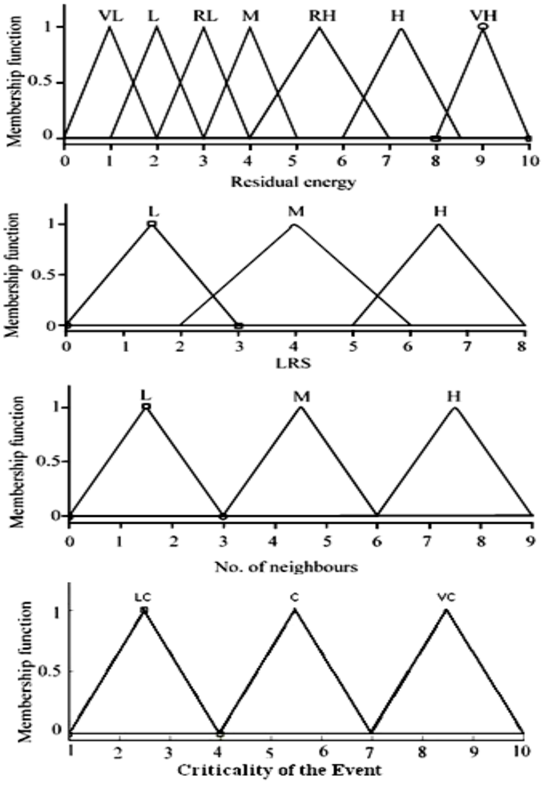


Fig. 1: Membership function for input variables

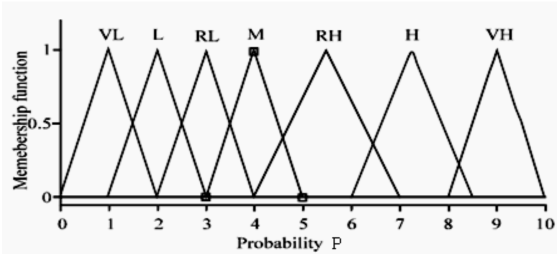


Fig. 2: Membership function for probability of node being a cluster head

This algorithm concentrates on the selection of the appropriate node as CH for event driven applications. For event based applications, it considers criticality of the Event (Event) which is also one of the input criteria in addition to the RE and LRS. Criticality implies on how emergency is an Event and hence gets higher priority for CH selection. The linguistic variable used for Criticality of the event is Very Critical (VC), Critical (C), Less Critical (LC), for RE is given by Very High (VH), High (H), rather high (RH), medium (M), rather low (RL), low (L) and very low *(VL)* and the linguistic variables used for the other two input variables LRS(n) and NN(n) are High (H), Medium (M) and Low (L), respectively. The only fuzzy output variable is the probability of a CH candidate P. The linguistic variables used for the output variable P is given by Very High (VH), High (H), Rather High (RH), Medium (M), Rather Low (RL), Low (L) and Very Low (VL). Based on these linguistic variables, the proposed algorithm selects the best CH candidate. The higher the probability shows the more chance for the node being a CH.

Fuzzy Logic based Cluster head Selection algorithm (FLCS): The pseudo code of the improved clustering method is described as Fuzzy Logic based Cluster Head Selection algorithm (FLCS). In every clustering round, each sensor node generates a random number between 0 and 1. If the random number for a particular node is bigger than the pre-de?ned threshold T which is the percentage of the desired tentative CHs, the node becomes a CH candidate. Every node in the network broadcasts its Residual Energy (RE). Then, all the nodes calculate the Probability using the Fuzzy Inference System based on RE, LRS, NN and criticality of the event and FLCS value is calculated using its probability and its neighbours' residual energy.

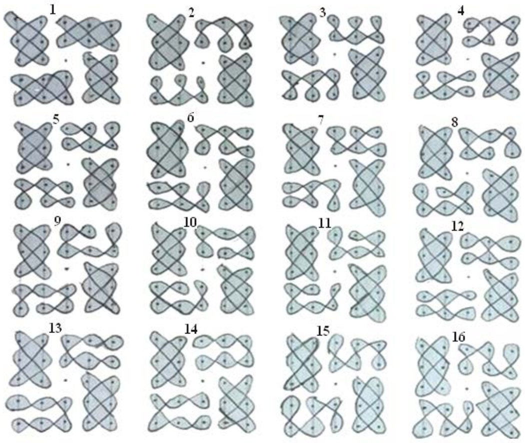
Fuzzy Logic based Cluster head Selection algorithm (FLCS)

```
Input:
N- Network
T-Threshold value to become a cluster head
n-Node
m-Number of nodes in the network
Cost(n)-Probability of a node being a cluster head
C-Number of clusters
$CH_{MAX}$- Maximum number of times a node ‘n’ has a chance of being a CH
Output: CH node
1.  Begin
2.  CH(i)_count=0
3.  if (rand(0,1) > T )
4.  Broadcast energy of a node $n_i$ $E_{RE}$
5.  Calculate $\varphi(n_i)$ using FIS based on RE, LRS, NN and Criticality
6.  For ( i=1-m)
7.  $FLCS(n_i) = \frac{E_{RE}(n_i(t))}{\sum_{j=1}^{k} E_{RE}(n_j(t))} \times \varphi(n_i)$
8.  End
9.  Broadcast the CH_CAND($n_i$) with FLCS($n_i$) value
10. If (FLCS($n_i$) == max(FLSC($n_i$)| j=1,2,...... , m)) then begin
11. Broadcast CH_ADV($n_i$)
12. Receive REQ_JOIN ($n_i$ , $n_j$)
13. CH(i) = CH(i)$\cup${$n_i$}
14. CH(i)_count+=1
15. Calculate available power
16. Cost ($n_i$) = RE($n_i$)+LRS($n_i$)
17. If ((Cost($n_{(i)}$ = min Cost ($n_{(j)}$))&&($CH_{(MAX)}$ = = CH(i)$_{count}$))
18. Send NOT_CH
19. End
20. Else
21. Goto step 10
22. End
23. End
24. End
```

Once FLCS is calculated, the node broadcasts a Candidate-Message with FLCS value. This message means that the sensor node is a candidate for CH. Once a node advertises a candidate-message, it waits for candidate-messages from other nodes. After receiving the candidate messages from other nodes, the FLCS value of all the candidates are compared with each other. If FLCS value of itself is bigger than every FLCS values from other nodes, the sensor node broadcasts a CH-Message which means that the sensor node itself is elected as CH. If a node which is not a CH receives the CH-Message, the node selects the closest cluster head as its CH and sends a JOIN-REQ request to the cluster head. Thus, clusters are formed with CHs.

Viable Key (VK) constructs based on VK script: The various types of sensor nodes such as source node, destination node router node, etc., are deployed on the network field for different purposes as routing, communication of sensed data from any equipment for health/performance monitoring of these apparatus in the power grid. The main goal of this study is to communicate the sensed (events as fault/malfunctions/disturbances while in operation in the grid) information of electrical data observed from the electrical system by the sensor node/end device to the Base Station (BS) in a secured manner. Secured data transfer demands newer algorithmic approaches for encryption that addresses security, lower power consumption in coding the encryption, intelligence in decryption etc. This study proposes the Pattern Viable Restoration (PVR) technique for encrypting the sensed (event) data of the electrical system at source node (cluster member or end device) and novel method for decrypting the encrypted data at the destination (BS) node that should be deployed at the electrical substation.

The VK-constructs used are a new proposal used for PVR encryption technique as presented in this study and as is shown Fig. 3. It shows the 16 different VK-constructs which are named herein with natural numbers from 1-16. These 16 VK-constructs are formulated from the VK script ‘O’. This VK-constructs formation has one symmetric VK-constructs ‘O+O’ and fifteen asymmetric VK-constructs.



First Row : 'O+O', 'O+E', 'O+E1', 'O+F'; Second Row : 'O+F1', 'O+F2', 'O+F3', 'O+G' Third Row: 'O+G1', 'O+G2', 'O+G3', 'O+H'; Fourth Row : 'O+U', 'O+U1', 'O+S', 'O+S1'

Fig. 3: Formulation of VK-constructs using VK Script 'O' for pattern viable restoration technique

The asymmetric VK-constructs are numbered as VK-constructs 2 through VK-constructs 16. Similar to this VK-constructs formation; there are 16 different symmetric VK-constructs and 240 different asymmetric VK-constructs which can be postulated in a similar way. Some of the symmetric and asymmetric VK-constructs are shown in Fig. 4.

The proposed technique has 256 different VK-constructs. These VK-constructs are framed using English alphabets E, F, G, H, U, S and O. These alphabets are used as basic shapes to form the original VK-constructs for encryption. From these basic alphabets called Viable Key (VK) scripts, it is possible to form the derived VK scripts. This study proposes the derived VK scripts for 'E' is 'E1'; 'F' is 'F1' 'F2', 'F3'. Similarly, for other VK scripts G, U and S is given by 'G1', 'G2', 'G3'; 'U1'; 'S1', respectively. The remaining VK scripts 'O' and 'U' do not have any derived VK script. Each VK script follows either 2×3 array or 3×2 array.

The various combinations of these VK scripts are used to form the different VK-constructs which are unique for data encryption. For example, the VK-constructs formation using VK script 'O' is explained as follows: The VK script 'O' itself form its original symmetric VK-constructs called 'O+O' which is denoted as number 1 in Fig. 4. The VK script 'O' is combined with other VK scripts E, F, G, H, U and S form the VK-constructs like O+E, O+F, O+G, O+H, O+U and O+S and are denoted as 2, 4, 8, 12, 13 and 15. Similarly, the derived VK-constructs are obtained using the derived VK scripts E1, F1, F2, F3, G1, G2, G3, U1 and S1 are O+E1, O+F1, O+F2, O+F3, O+G1, O+G2, O+G3, O+U1 and O+S1 and are denoted as 3, 5, 6, 7, 9, 10, 11, 14 and 16. Therefore, 16 different VK-constructs are obtained from a single VK script 'O'. Similarly the remaining VK scripts E, F, G, H, U, S, E1, F1, F2, F3, G1, G2, G3, U1 and S1 can be used to form rest of 240 different VK-constructs. Among these 256 VK-constructs 16 VK-constructs in the combination of E+E, E1+E1, O+O, etc., are called as symmetrical VK-constructs and the remaining 240 are called as asymmetrical VK-constructs.

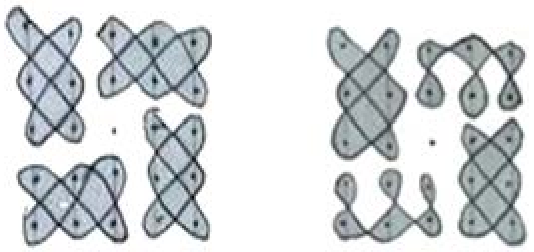
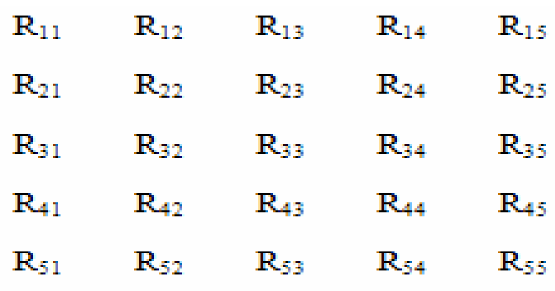


Fig. 4: Symmetrical 'O+O', asymmetrical 'O+E1' VK-constructs



R_{11}	R_{12}	R_{13}	R_{14}	R_{15}
R_{21}	R_{22}	R_{23}	R_{24}	R_{25}
R_{31}	R_{32}	R_{33}	R_{34}	R_{35}
R_{41}	R_{42}	R_{43}	R_{44}	R_{45}
R_{51}	R_{52}	R_{53}	R_{54}	R_{55}

Fig. 5: Formulation of 'O+O' using 5×5 Array

The Viable Key (VK) for data encryption is designed based on the symmetrical and asymmetrical VK-constructs. The secret key is generated based on the symmetrical VK-constructs which is named as "Pattern Viable Recurrent (PVR) Key" and the asymmetrical VK-constructs named as "Pattern Viable Asymmetric (PVA) Key". The VK-constructs used for PVR key and PVA key are given in Fig. 4. The VK-constructs of these keys can be represented by 5×5 array and is shown in Fig. 5. R_{11}, R_{12} … R_{55} are the variables to indicate the bit position of the sensed data during encryption and decryption. For example, R_{23} means the position of the bit is second row third column.

Design of VK script based viable key: The Viable keys are designed using VK-constructs. Different VK scripts are combined to form VK-constructs. The design of Viable Keys (PVR/ PVA) is explained in the next section using one symmetrical VK-construct 'O+O' for PVR key and one asymmetrical VK-constructs 'O+E1' for PVA key.

Design of viable key based restoration technique: The sensors placed on the sensor nodes which are connected to the electrical system continuously monitor the system health by sensing the parameters of the system such as temperature, current, voltage and acceleration, etc., of the electrical system. These sensors transmit the data only when an event (abnormality in system) occurs, the sensed data is first converted into 25-bit data. This means that the first 24 bits represent the 3-Byte payload bit and the last bit b_{24} represents the Recurrent Check Bit. The 25-bit representation of the plain text is the sensed data D(S) and is given by Eq. 1:

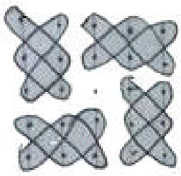
$$\begin{aligned}\text{Plain text} = D(s) &= b_0|\, b_1|\, b_2|\, b_3|\, b_4|\, b_5| \\ &\ldots\ldots|\, b_{20}|\, b_{21}|b_{22}|b_{23}\,|\, b_{24}\end{aligned} \qquad (1)$$

The Recurrent Check Bit (RCB) b_{24} is used to identify whether the encryption is done based on symmetrical VK-constructs or asymmetrical VK-constructs. If it is identified, then it can easily identify the secret key which is used for encryption at the transmitter. The secret key is either Pattern Viable Recurrent (PVR) key or Pattern Viable Asymmetric (PVA) key. If the VK-constructs used for encryption is symmetrical, the decryption can be done using PVR key and otherwise if asymmetrical the PVA key would be the suitable key for decryption.

During encryption at the transmitter end, the D(s) is converted to the array. The first five bits b_0, b_1, b_2, b_3, b_4 are placed in the first row of the array and next five bits b_5, b_6,b_7, b_8, b_9 are placed in the second row. The middle row consists of the b_{10}, b_{11} in the first two columns and b_{12}, b_{13} are in the last two columns. The third column of the middle row has the bit b_{24} called RCB bit. The remaining bits b_{14}-b_{23} are placed in the last two rows. Therefore the bit formation of the array BM(S) is given by Eq. 2:

$$BM(S) = \begin{bmatrix} b_0 & b_1 & b_2 & b_3 & b_4 \\ b_5 & b_6 & b_7 & b_8 & b_9 \\ b_{10} & b_{11} & b_{24} & b_{12} & b_{13} \\ b_{14} & b_{15} & b_{16} & b_{17} & b_{18} \\ b_{19} & b_{20} & b_{21} & b_{22} & b_{23} \end{bmatrix} \qquad (2)$$

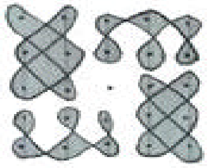
The symmetrical VK-constructs used for the secret key PVR(S) is given by Eq. 3:

PVR(S) = 'O+O' =  (3)

The dot (.) at the center bit is called Recurrent Check Bit (RCB). The generated PVR key using Equation (3) is given by Eq. 4:

$$\begin{aligned}PVR(S) \;=\; & R_{11}|R_{22}|R_{31}|R_{12}|R_{21}|R_{32}|R_{23}|R_{14}| \\ & R_{25}|R_{13}|R_{24}|R_{15}|R_{43}\,|\,R_{52}|R_{41}|R_{53}\,| \\ & |R_{42}|R_{51}|R_{55}|R_{44}|R_{35}|R_{54}|R_{45}|R_{34}\end{aligned} \qquad (4)$$

Similarly, asymmetrical VK-constructs used for the secret key PVA(S) is given by Eq. 5:

PVA(S) = 'O+EI' =  (5)

The asymmetrical VK-constructs based crypto key is known as PVA key and is given by

$$\begin{aligned}PVA(S) = & R_{11}\,|\,R_{22}\,|\,R_{31}\,|\,R_{12}\,|\,R_{21}\,|\,R_{32}\,|\,R_{13}\,| \\ & R_{23}\,|\,R_{14}\,|\,R_{25}\,|\,R_{15}\,|\,R_{24}\,||\,R_{53}\,|\,R_{43}\,| \\ & R_{52}\,|\,R_{41}\,|\,R_{51}\,|\,R_{42}\,|\,R_{55}\,|\,R_{44}\,|\,R_{35}\,|\,R_{54}\,|\,R_{45}\,|\,R_{34}\end{aligned} \qquad (6)$$

Implementation of PVR technique using VK-constructs with iris motes: The Pattern Viable Restoration technique is implemented on the TINY-OS based cross-bow IRIS motes to make the transmission is secured and the performance of Pattern Viable Restoration (PVR) technique is compared with standard encryption algorithms such as DES, AES and SHA algorithms.

Configuration of IRIS MOTE-XM2110: The IRIS-XM2110 (IRIS Data Sheet information) is the sensor board which is used as wireless sensor node or mote. The XM2110 is developed based on the Atmel ATmega1281 micro controller. It includes a processor that operates on Tiny-OS operating system environment. The ATMEGA 1281 is a low-power microcontroller which executes the designed technique from its internal flash memory. It has ZigBee protocol based RF 230 transceiver for wireless communications. It uses IEEE 802.15.4 protocol standard and operates on 2.4 GHz frequency band. The single XM2110 board can be configured to perform various sensor applications, processing of the sensed data and the network/radio communications, etc.

The prototype test bed for PVR technique is shown in Fig. 6. In this test bed, one IRIS mote is configured as Base Station (BS), one mote is configured as source node that acts as transmitter. The router nodes are deployed

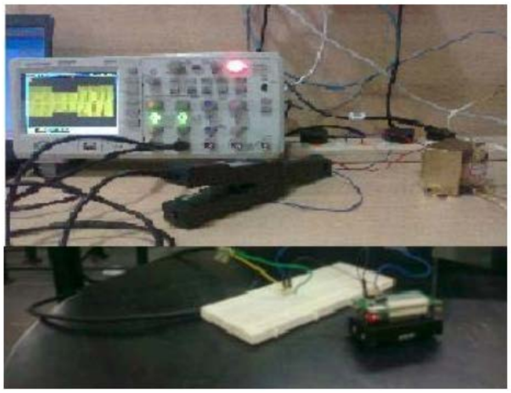


Fig. 6: Experimental setup for voltage sag event of equipment with detection and transmission by end device

between BS and source node. The Hall Effect sensor probe is connected to the transformer for health monitoring. The disturbances or abnormalities occurred in the transformer like voltage sag and voltage swell are detected as events (Vijayalakshmi and Ranjan, 2013) by the sensor. When an event (sag/swell) occurs, the event information is communicated to the BS through the routers.

In this experiment the sensed data (event information) is encrypted by PVR technique before the data or event transmission starts. It means that the encryption is done by the transmitter or source node. In the proposed PVR technique, the PVR/PVA key is only known to the transmitter and BS motes. The IRIS motes are configured to perform as source node, router, Base Station and are deployed on the network field to identify the electrical disturbances. The router nodes do not have the knowledge about the data and encryption techniques. The performance analysis of the various standard encryption algorithms using IRIS motes also has been done. The graphical observation of the electrical disturbance is shown in Fig. 7.

Secured Data (SD) packet format: The source node transmits the secured data packet which includes Node-id, length which is equal to the number of bytes between length and hash sum, encrypted pay load. The payload field of the data packet carries the sensed data (event information) of the electrical system. The length of the payload is variable. In PVR technique, the Viable Key (VK) based encrypted event information is included in the payload field of the packet before the data transmission starts. This study considers the length of the payload field which is defined as 3 bytes which includes 24 bit PVR technique with VK based encrypted payload data.

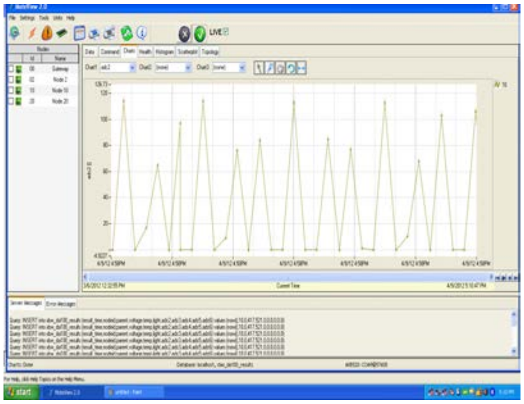


Fig. 7: Graphical observations of electrical disturbances

Node-id (2 bytes)	Length (2 bytes)	Encrypted pay load (Variable)	RCB (1bit)	Hash sum (2 bytes)	Pattern viable Restore (4 bits)

Fig. 8: Secured Data (SD) packet format

The next field is Recurrent Check Bit (RCB) which is used to identify the VK-constructs type (symmetrical and asymmetrical). The last two fields are Hash Sum for error detection and Pattern Viable Restore field which is used to identify the VK-constructs like O+O', 'E+E' or 'S+O', etc. The format of the secured data packet is shown in Fig. 8.

Recurrent Check Bit (RCB): One bit field in SD packet is Recurrent Check Bit (RCB). The Pattern Viable Restoration (PVR) technique uses PVR key and PVA Key for encryption or decryption depending on the type of VK-constructs used. The RCB bit is the bit which is used to identify the type of key used for encryption or decryption. This bit has the value either '0' or '1'. When RCB is '1', the sensed data is encrypted or decrypted based on the symmetric VK-constructs and uses the PVR key of the corresponding VK-constructs. When RCB is '0', the asymmetric VK-constructs based PVA key is used for encryption or decryption.

Hash sum: The next field of the packet format is 'Hash Sum'. This field is used for detecting transmission errors in transmitted data. The source node calculates the Hash Sum using Eq. 7:

$$\text{Hash sum} = \text{FF} - \left[\begin{matrix}\text{Lower } 8-\text{bit of} \\ \left(\text{LP}_i + \text{RP}_i + \text{RCB}_i\right)\end{matrix}\right] \tag{7}$$

Where, Lp_i indicates the left part of payload bits (b_0-b_{11}) of the packet 'I' and

Rp_i right part of payload bits (b_{12}-b_{23}) of the packet ‘i’ and RCB is the recurrent check Bit.

The calculated Hash sum is included in the SD packet format before transmitting. At the receiver end the lower 8-bit of (LP_i+RP_i+RCB) and the hash sum are added and checkd whether the sum is equal to ‘FF’. If it is ‘FF’, the receiver decides that there is no transmission error in the received data. For example, if the sensed data has three bytes of 03H, 18H, A5H and RCB bit is 1 means the calculated hash sum is 3EH [FF-lower 8 bit of (03H+18H+A5H+01H)]. These values are included in the secured data packet format and are transmitted to the receiver. At the receiver end the values 03H, 18H, A5H, 01H and 3EH are added. If the sum is equal to FF then the received data has no transmission error or else there is an error. In this case the sum of lower 8 bit of (03H, 18H, A5H, 01H) and 3EH is equal to FFH. This means that the data is received without any transmission error.

Pattern viable restore: It is the last field in the SD packet format. It has 1 byte length having a value which ranges from 00000000 to 11111111 (0-256). The value included in this field can be used to identify the VK-constructs-id for decryption at the receiver end. Generally, user can name the VK-constructs with unique VK-constructs-id like 1, 2, 3,…, 16 for symmetrical VK-constructs and 1, 2, 3,…, 240 for asymmetrical VK-constructs with unique VK-constructs-id assignment during encryption process. The user can give any VK-constructs-id for any VK-constructs for their convenience. This means that the VK-constructs-id differ from one user to another user. This study has designed the encryption technique for one symmetrical VK-constructs ‘O+O’ with VK-constructs-id assigned 0001 (1) and fifteen asymmetrical VK-constructs ‘O+E’ to ‘O+S1’ with assigning VK-constructs-id 0001 (1) to 1111 (15). For example, the encryption done in the transmitter end is based on ‘E+F1’ VK-constructs. The transmitter transmits the SD packets with value 0011 (3) in the Pattern Viable Restore field and the RCB bit is set to 0. This ‘0’ indicates the asymmetrical VK-constructs.

At the receiver end the data is decrypted using the 3rd VK-constructs in the asymmetric form (E+F1) and PVA key is used because of the asymmetric form. In contrast, if it transmits the encrypted data with RCB bit is 1, the receiver uses the 3rd VK-constructs of the Symmetric form ‘F+F’ and PVR key is used to decrypt the data. The 3rd VK-constructs of symmetric form represents the ‘F+F’ and the 3rd VK-constructs of asymmetric form follows ‘O+F’. In this way, the data can be encrypted and decrypted using 16 symmetrical VK-constructs and 240 asymmetrical VK-constructs. The encryption and decryption technique done in this study are only for 16 VK-constructs. The acquired data is encrypted by inserting a new key for, every time slot. The key is known only to the source and the destination. The pattern viable key encryption technique is adaptable for 256 VK-constructs.

RESULTS AND DISCUSSION

Probability of CH selection based on criticality of the event: Figure 9 shows the surface view output of the probability of the node being elected as CH when the occurred event is very critical. The crisp value of the criticality of the event for very critical event used in FLCS algorithm is 9. When, there is an occurrence of very critical event, the result shows that the probability of node being CH is less. This means that there is the possibility of more number of nodes in the network which becomes CH since the probability value required for node being CH is less for very critical event. In Fig. 9, the yellow region shows the fuzzified probability of CH selection. The performance of the network is analyzed based on the simulation parameters listed Table 1.

Figure 10 shows the surface view output of the probability of the node being selected as CH when the occurred event is less critical. The crisp value used for less critical event is 2. The output infers that more probability is required for a node to act as CH when there is less critical event. The yellow region of Fig. 9 and 10 indicate the fuzzified probability value of

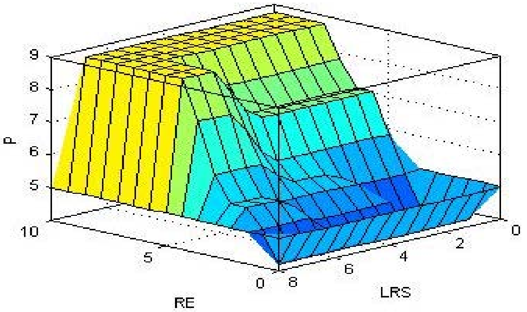


Fig. 9: probability of CH selection for very critical event

Table 1: Simulation parameters

Parameter	Values
Topographical Area (m)	300×300
Sink location (m)	Center of the area
Number of nodes	100, 400
Transmission range	40 m(133 ft)
Packet size	100 bytes
Initial battery level	1 Joule
Energy for data aggregation	2 μJ/packet
Energy consumption for radio E_e	20μJ/packet
Energy consumption for amplifier	5nJ/packet
MAC Protocol	IEEE 802.15.4

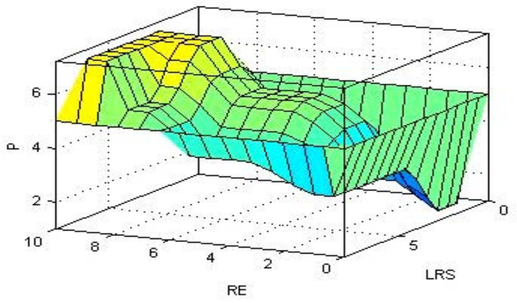


Fig. 10: Probability of CH selection for less critical event

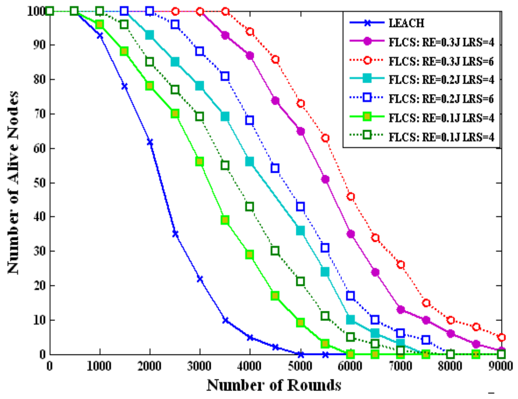


Fig. 11: No. of alive nodes increases with static sink for LRS = 4 and LRS = 6

CH selection for very critical and less critical event. From these output, it can be observed that the increase in yellow region indicates that the increase in the level of criticality of the event.

Effect of static sink on network lifetime: The energy consumption rate can directly influence the life-time of the sensor nodes as the depletion of battery resources which will eventually cause failure of the nodes. The number of alive nodes as a function of level of participation in packet forwarding by changing the value of Residual Energy (RE) between 0.1 and 0.3J and the value of Least Recently Selected (LRS) is 4 and 6 with the constant value of the Number of Neighbours (NN) which is 5 and the sink is static as shown in Fig. 11.

The performance of the FLCS algorithm is compared with LEACH protocol which is the standard clustering protocol. From the results, it can be seen that in LEACH protocol, the number of nodes that are alive are almost equal to 100 which means the whole network is alive till 694th round butin FLCS scheme it is found that, the whole network is alive till 1256th round, 2352nd round and 3597th round for RE = 0.1, 0.2 and 0.3J with static sink,

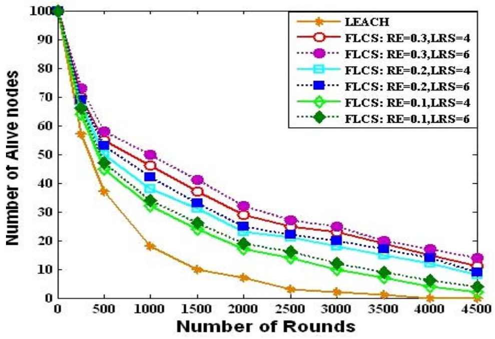


Fig. 12: No. of alive nodes decreases with mobile sink (LRS = 4 and LRS = 6)

respectively. This performance improvement is achieved only due to the selection criteria of FLCS. The FLCS algorithm uses three parameters such as RE, LRS, NN for cluster head selection. In FLCS, there is a threshold limit for Residual Energy (RE). Thereby, the elected CH node does not drain out butit loses its CH position when it has the RE less than the threshold limit. Similarly, FLCS has threshold limit for the other two parameters also. Selected CH in FLCS does not drain out earlier than LEACH because it has residual energy even if it loses its CH position and it lives for longer time than LEACH.

Effect of mobile sink on network lifetime: The performance of the FLCS algorithm is also analyzed with mobile sink. The number of alive nodes using mobile sink with FLCS algorithm is shown in Fig. 12. The FLCS algorithm with mobile sink is also simulated with RE = 0.3, 0.2 and 0.1J. The result shows that the whole network is alive only when number of rounds is <100 in all methods. The number of alive nodes decrease with very fast rate when the number of rounds increase. This happens due to the mobility of the sink, eventhough the result shows that the FLCS algorithm with RE = 0.3J, LRS = 6 perform well as compared to other cases of FLCS and LEACH. Moreover, the mobile sink is also not suitable for event driven monitoring applications because of its mobility.

Network lifetime enhancement by FLCS algorithm: Energy is the most important issue in WSN and the most important metric for measuring WSN is the network life time. Network lifetime is the time recorded when the first node of the network completely drains out of battery resource. The comparative results of FLCS algorithm with mobile sink and LEACH are presented in Fig. 13. Figure 14 shows the comparison of simulation results of network lifetime of the standard LEACH protocol and FLCS algorithm with static sink.

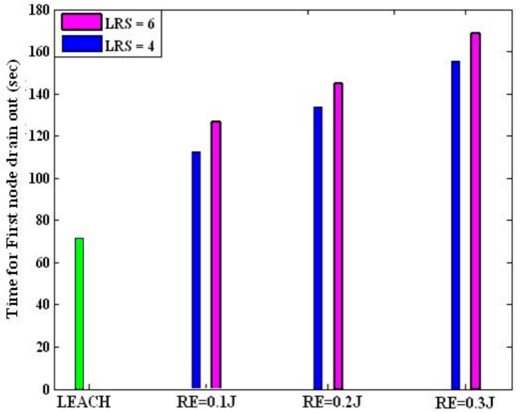


Fig. 13: Network lifetime with flcs increases for mobile sink for LRS = 6 than LRS = 4

From the presented results, the time for drain out of battery of the first node is earlier in LEACH protocol than the FLCS with static sink. The time for first node to drain out its battery in FLCS algorithm with static sink occurs at 1234 seconds with RE = 0.3J and LRS = 6, at 1095 sec with RE = 0.3J and LRS = 4, if a node is having initial energy of 1J but in real time the energy storage in AA battery is 9360 J. But in LEACH it occurs nearly 1026 sec earlier and in FLCS with mobile sink of 1013 sec earlier. Therefore, FLCS algorithm with static sink achieves increased network life time than LEACH protocol and FLCS algorithm with static sink.

From the presented results, the time for drain out of battery of the first node is earlier in LEACH protocol than the FLCS with static sink. The time for first node to drain out its battery in FLCS algorithm with static sink occurs at 1234 seconds with RE = 0.3J and LRS = 6, at 1095 sec with RE = 0.3J and LRS = 4, if a node is having initial energy of 1J but in real time the energy storage in AA battery is 9360 J. But, in LEACH it occurs nearly 1026 sec earlier and in FLCS with mobile sink of 1013 sec earlier. Therefore, FLCS algorithm with static sink achieves increased network life time than LEACH. The network lifetime achieved by the FLCS scheme using static sink shown in Fig. 14 is nearly 86% more than that can be obtained by the standard algorithm and also nearly 84% more than FLCS with mobile sink as shown in Fig. 13. This shows that the use of FLCS algorithm can improve energy efficiency and prolong the lifetime of the network.

Impact of message length on energy consumption: The impact of message length on processor energy consumption for four different encryption schemes is shown in Fig. 15. The result shows that the processor energy consumption increases with the increase in message length in all four algorithms. The SHA has maintained constant processor energy consumption with the increase in message length but it is high energy consumption due to its more complex encryption algorithms.

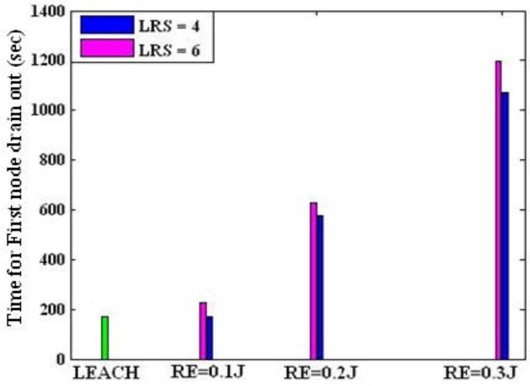


Fig. 14: Network lifetime with FLCS increases more for static sink for LRS = 4 and LRS = 6

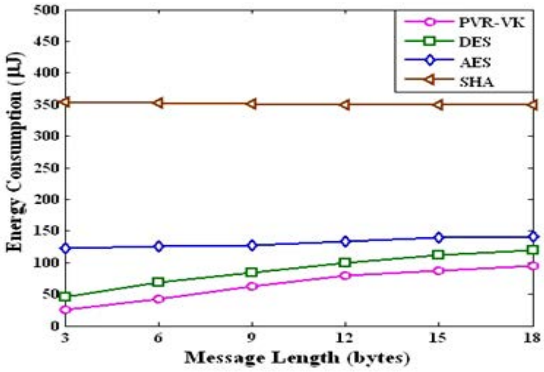


Fig. 15: Impact of message length on energy consumption

The standard encryption algorithms AES and DES have relatively more energy consumption than the proposed technique. These standard encryption algorithms use ten times and sixteen times permutation respectively. Therefore, these algorithms consume more energy than the proposed technique. As compared to the other three encryption algorithms, the energy consumption of the proposed PVR technique has 2 times lesser than DES, 5 times lesser than AES and 14 times lesser than SHA algorithm. This improved performance is obtained by using PVR technique because of its simple VK script based encryption technique and its concept does not require complex computation calculation.

CONCLUSION

The deployment of the proposed WPAN is applicable for a large scale system as the Power Grid that uses cluster based sensor network developed with maximum coverage of the transmission range. The cluster based multi-cluster topology with appropriate CH selection algorithm and PVR with VK based security algorithm discussed in this study considers the more secured data collection with less energy consumption. This algorithm is comparatively simpler as it does not require any formal mathematical based processing. The FLCS always has optimal number CH for various values of probability of CH selection. The proposed FLCS algorithm is capable of adapting the selection criteria for Cluster Head selection dynamically also based on the criticality of the event in the network. The simulation and experimental results demonstrate the effectiveness of the proposed approach with regards to transmission of secured data with enhanced network lifetime of wireless sensor networks deployed with randomly scattered nodes. The future work is in progress towards developing energy efficient sensor fusion with secured data communication for multi-cluster mobile network.

ACKNOWLEDGEMENTS

The researchers gratefully acknowledge UGC for meritorious for sciences, New Delhi for providing financial support to carry out this research work under the UGC scheme.

REFERENCES

Abbasi, A.A. and M. Younis, 2007. A survey on clustering algorithms for wireless sensor networks. Comput. Commun., 30: 2826-2841.

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. A survey on sensor networks. Commun. Mag. IEEE., 40: 102-114.

Alwan, H. and A. Agarwal, 2013. A multipath routing approach for secure and reliable data delivery in wireless sensor networks. Int. J. Distrib. Sens. Networks, 13: 1-1.

Bhoopathy, V. and R.M.S. Parvathi, 2012. Secure authentication technique for data aggregation in wireless sensor networks. J. Comput. Sci., 8: 232-238.

Chinara, S. and S.K. Rath, 2009. A survey on one-hop clustering algorithms in mobile ad hoc networks. J. Network Syst. Manage., 17: 183-207.

Estrin, D., R. Govindan, J. Heidemann and S. Kumar, 1999. Next century challenges: Scalable coordination in sensor networks. Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 15-19, 1999, Seattle, Washington, USA., pp: 263-270.

Heinzelman, W.B., A.P. Chandrakasan and H. Balakrishnan, 2002. An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wireless Commun., 1: 660-670.

Jankowski, K. and P. Laurent, 2011. Packed AES-GCM algorithm suitable for AES/PCLMULQDQ instructions. Comput. IEEE. Trans., 60: 135-138.

Lee, C. and T. Jeong, 2011. FRCA: A fuzzy relevance-based cluster head selection algorithm for wireless mobile Ad-Hoc sensor networks. Sensors, 11: 5383-5401.

Lee, J.S. and W.L. Cheng, 2012. Fuzzy-logic-based clustering approach for wireless sensor networks using energy predication. IEEE Sens. J., 12: 2891-2897.

Lou, W. and Y. Kwon, 2006. H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks. IEEE Transact. Vehicular Technol., 55: 1320-1330.

Malik, A.S., J. Kuang, J. Liu and C. Wang, 2009. Performance analysis of cluster-based wireless sensor networks with application constraints. Int. J. Comput. Network Inf. Secur., 1: 16-23.

Oggier, F. and M.J. Mihaljevic, 2014. An information-theoretic security evaluation of a class of randomized encryption schemes. Inf. Forensics Secur. IEEE. Trans., 9: 158-168.

Ohta, T., S. Inoue and Y. Kakuda, 2003. An adaptive multihop clustering scheme for highly mobile Ad hoc networks. Proceedings of the 6th International Symposium on Autonomous Decentralized Systems, April 9-11, 2003, IEEE Computer Society, Washington, DC, USA., pp: 293-300.

Pan, J.S., Li, S. and Z. Xu, 2012. Security mechanism for a wireless-sensor-networkbased healthcare monitoring system. Commun. IET., 6: 3274-3280.

Pietro, R.D., L.V. Mancini, Y.W. Law, S. Etall and P. Havinga, 2003. LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks. Proceedings of the International Conference on Parallel Processing Workshops 2003, October 6-9, 2003, IEEE, New York, USA., ISBN: 0-7695-2018-9, pp: 397-406.

Roy, S., M. Conti, S. Setia and S. Jajodia, 2012. Secure data aggregation in wireless sensor networks. Inf. Forensics Secur. IEEE. Trans., 7: 1040-1052.

Souza, R.J.D. and G. Varaprasad, 2012. Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks. Sens. J. IEEE., 12: 2941-2949.

Tawalbeh, L., M. Mowafi and W. Aljoby, 2013. Use of elliptic curve cryptography for multimedia encryption. Inf. Secur. IET., 7: 67-74.

Vijayalakshmi, A. and P.V. Ranjan, 2013. Code strategy algorithm for online power quality monitoring of electrical equipment using wsn under tiny-os environment. J. Theor. Appl. Inf. Technol., 57: 465-473.

Wang, H., L. Xing and H.E. Michel, 2010. Reed solomon code based green & survivable communications using selective encryption. Int. J. Performability Eng., 6: 297-299.

Zytoune, O., Y. Fakhri and D. Aboutajdine, 2009. A balanced cost cluster-heads selection algorithm for wireless sensor networks. Int. J. Comput. Sci., 4: 21-24.