ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Pattern Viable Restoration (PVR) Technique with Novel Viable Key (VK) Script for Secured Data Transmission in WSN

A. Vijayalakshmi and P. Vanaja Ranjan

Department of Electrical And Electronics Engineering, Embedded System Technology Division, College of Engineering, Anna University, Chennai, India

ARTICLE INFO

Article history:
Received 10 October 2015
Accepted 30 November 2015
Available online 24 December 2015

Keywords:
Data confidentiality, Data security, Encryption, Viable Key, Wireless Sensor Network

ABSTRACT

The Data confidentiality and security are the two most important design goals for efficient energy utilization in data collection. This is a significant research concern in the wireless sensor networks. Multipath routing protocol is observed to provide efficient energy utilization by balancing the traffic among multiple paths. This paper proposes a pattern based Viable Key (VK) encryption technique for Secured Data Communication (SDC) to achieve data confidentiality and security in wireless sensor networks. The main objective of the proposed technique is to improve the security, confidentiality of data transmission and to enhance the network lifetime of the wireless sensor networks. This paper presents the novel Pattern Viable Restoration (PVR) with Viable Key (VK) script technique for secured data communication and also discusses on the unique encryption and decryption algorithm for data restoration. The method is observed to be adaptable for secure data transfer with multipath routing design with improved network life time. The results show that the data confidentiality has improved by the appropriate design of cipher text using VK encryption suitable for multipath routing protocols. The power consumption of the proposed PVR with VK technique is analysed through TINY-OS based IRIS motes and performance characteristics are compared with the standard encryption algorithms.

To Cite This Article: A. Vijayalakshmi and P. Vanaja Ranjan., Pattern Viable Restoration (PVR) Technique with Novel Viable Key (VK) Script for Secured Data Transmission in WSN. ***Aust. J. Basic & Appl. Sci.,*** *9(35), 291-299, 2015*

INTRODUCTION

Wireless sensor network (WSN) is collection of a large number of nodes deployed as a protocol support network using processors that includes sensing device, power source such as battery, and transceiver with radio for communication discussed by Akyildiz et al. (2002). These small, smart nodes of low cost sensing and computing devices motivated researchers and engineers to use them to observe and monitor physical phenomenon. WSNs are used for distributed and cooperative sensing of physical phenomena and events of interest. These networks have applicability in areas like habitat monitoring, medical care, military surveillance traffic control and more system health monitoring applications. Sensor nodes communicate the occurrence of an event to a sink node that acts as a base station (Vijayalakshmi and Vanajaranjan, 2013). Sink node then transmits the data network layer to the user for online monitoring. However, data communication layer sometimes face some potential safety risks which was discussed by Villas et al (2013), Artigas (2005) et al.

Designing secure routing protocol is one of the effective methods for addressing secure data transfer issues. Data reliability, confidentiality discussed by Alwan and Agarwal (2013) and secure data transfer (Liu et al 2012) are the major issues that have attracted great amount of research, and a number of secured data transfer approaches have been proposed. Previous research works mainly concentrate on delivering packets along disjoint multipath routes, which can be generally summarized as follows: deterministic disjoint multipath routing and randomly disjoint multipath routing discussed by Villas et al (2013). Both routing protocol focuses on transmitting copies of packets along the disjoint routes. Random disjoint multipath routing does not have a fixed candidate route for selection. Therefore, it is able to ensure that adversaries cannot know the routes, even if they obtain the routing algorithms in advance. The dynamic key management based secret sharing was discussed by Lan et al. (2013). However, most previous works do not consider the network lifetime of WSNs, which may lead to a high probability of sensor node outage and cause an ending of normal operations. Reed Solomon (RS) codeword encryption strategy was discussed in Wang et al. (2012). Forward error correction (FEC) code is one of the technique to provide reliability and confidentiality in WSNs. This FEC proposed by Aggarwal et al.

Corresponding Author: A. Vijayalakshmi, Department of Electrical And Electronics Engineering, Embedded System Technology Division, College of Engineering, Anna University, Chennai, India
E-mail: vkk3101@gmail.com

(2012)16] increase the data transmission reliability and decrease the energy consumption. The enhancement of the network security and lifetime by exploiting an effective randomly disjoint multipath routing scheme with secret sharing was also discussed. However, most previous works consider encryption or cryptography algorithm for security. Designing of key management algorithm and development of secure routing protocol are two issues that have focused by large amount of research. Most researchers have proposed various security schemes such as the design of secure and efficient routing protocol discussed by Alwan and Agarwal (2013), the design of secure data aggregation protocol (Estrin et al 1999), (Bhoopathy, V. and Parvathi, R.M.S., 2012) and key management algorithms by Pietro et al (2003). This paper has focused to protect the data by developing an encryption algorithm based on patterns.

The sensed data routing from the source to sink node in secured manner in a Wireless Sensor Network (WSN), is still a challenge. There are many research on data security algorithm using cryptography discussed by Stallings, used for secure and reliable transmission of data. Designing of secured routing protocols are to fulfil different performance demands such as data transfer with less power consumption, packet delivery ratio, packet loss, throughput, data reliability etc., which are important issues in wireless sensor networking. Existing secured routing protocols in wireless sensor networks are designed based on the mathematical modelled data encryption or decryption algorithms. Most literatures discussed the cryptography based data security for various applications. This paper proposes pattern based Viable Key (VK) technique for secured and confidential data transmission.

The rest part of the paper is organized as follows. The related work in the area of secure data transfer communication schemes is discussed in Section 2. The Viable Key Technique is discussed in Section 3. The design of VK script based Viable Key is presented in Section 4. Section 5 discusses the experimental explanation of PVR with VK technique. The performance analysis of the proposed technique is discussed in Section 6. Finally Section 7 concludes the Pattern Viable restoration Key based encryption technique..

1. Related Works:

The secure Energy Efficient Node Disjoint Multipath Routing Protocol (EENDMRP) was proposed by Murthy et al. (2012). It is a sink initiated proactive multipath protocol. Some of the security threats like spoofing, sinkhole attack, etc., are addressed. This protocol used the digital signature based cryptosystem for security aspects. In this paper, MD5 hash function and RSA algorithm are used for security. The asymmetric (public) key crypto system is used for designing the security in EENDMRP.

The Hybrid Multipath Scheme for Secure and Reliable Data Collection (H_SPREAD) protocol proposed by Wenjing et al (2006) has some advantages and drawbacks. This H-SPREAD protocol had been developed based on the N-to-1 multipath routing protocol. It first finds the multiple node disjoint paths. 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, the H-SPREAD is a secured protocol. Even though it is a secured protocol, the maximum security can be achieved by compromising M paths for transmission. When there is any node failure or path failure, there may be a packet loss. Thus, there is a difficulty to achieve better data reliability by this protocol. It mainly concentrates on the routing protocol based security, therefore no data encryption or decryption algorithm was proposed. The proposed VK technique proposes the data encryption and decryption algorithm for data security and confidentiality.

The homophonic substitution and error-correction coding were proposed by Oggier and Mihaljevic (2014) for achieving the cryptographic security. The main focus of this work is the transmission of the encrypted data over a noisy channel. 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 also been addressed.

2. Viable Key (VK) Technique:

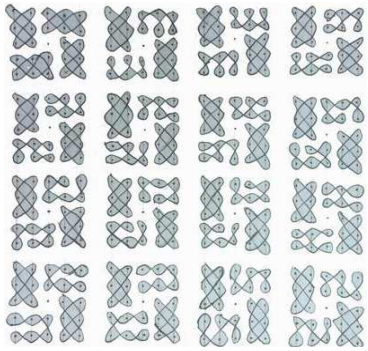
The various types of sensor nodes such as source node, destination node router node etc. are deployed on the network field for different purposes. The main goal of this paper is to transfer the sensed data to the base station (BS) in secured manner. For secured data transfer, this paper proposes the Pattern Viable Restoration (PVR) technique for encrypting the sensed data at source (Cluster Member - CM) node and decrypting the encrypted data at the destination (BS) node. The VK constructs used for PVR encryption technique is shown Figure 1. It shows the 16 different VK constructs which are named with natural numbers from 1 to 16. These 16 VK constructs are formulated from the VK script ‘O’. This VK construct formation has one symmetric VK construct ‘O+O’ and fifteen asymmetric VK constructs. The asymmetric VK constructs are numbered as VK construct 2 through VK construct 16. Similar to this VK constructs formation, there are 16 different symmetric VK constructs and 240 different asymmetric VK constructs can be postulated in a similar way.

The proposed VK 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 can be possible to form the derived VK script. This paper

proposes the derived VK script 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' does not have any derived VK script. Each VK script follows either 2x3 array or 3x2 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 forms its original symmetric VK constructs called 'O+O' is denoted as number 1 in Figure 1. The VK script 'O' is combined with other VK script 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 script 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 remaining 240 are called as asymmetrical VK constructs.

The proposed PVR technique with novel VK uses the time slot based scheduling for encryption and decryption of the data using 256 different Viable Keys. When an event occurs for time 'T', the source node senses the event-data and encrypts data packets using VK1 during time T1 and VK2 during time 'T2' and VK3 during time 'T3' and so on. The data encryption can be done using 256 VKs which are VK1, VK2, VK3, … , VK256. This paper explains the proposed PVR technique with VK uses time scheduling based encryption of the data packets using 16 VKs. The design of VK constructs using VK script 'O' is explained in the following section. It can be possible to extend upto 256 Viable Keys for encryption.

The Viable Key (VK) for data encryption is designed based on the symmetrical and asymmetrical VK constructs. The VK is generated based on the symmetrical VK constructs which is named as "Pattern Viable Recurrent (PVR) Key" and the asymmetrical VK constructs based VK is named as "Pattern Viable Asymmetric (PVA) Key". Some example of VK constructs used for PVR key and PVA key are given in the Figure 2 and Figure 3 respectively.



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. 1: Formation of VK constructs using VK script 'O'.

These VK constructs can be represented by 5x5 array and is shown in Figure 4. R11, R12 … R55 are the variables to indicate the bit position of the sensed data during encryption and decryption. For example R23 means the position of the bit is second row third column. Figure 5 shows the bit representation of the pattern used for encryption and decryption. Using bit representation, the corresponding bit in the 'R23' is 'b7'.

4.1. Design of VK script based Viable Key:

4.2. Design of Viable Key:

The sensors placed on the sensor nodes are continuously senses the data such as temperature, current, voltage acceleration etc of the electrical system. These sensors transmit the data only when an event is occurred, 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

$$Plaintext = D(s) = b_0 | b_1 | b_2 | b_3 | b_4 | b_5 | \ldots . | b_{20} | b_{21} | b_{22} | b_{23} | b_{24} \quad (1)$$

The Recurrent Check Bit (RCB) b_{24} is used to identify whether the encryption is done based on the symmetrical VK constructs or asymmetrical VK

constructs. If it is identified, then it can easy to identify the secret key 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. Otherwise the encryption VK constructs is asymmetrical the PVA key is the suitable for decryption.

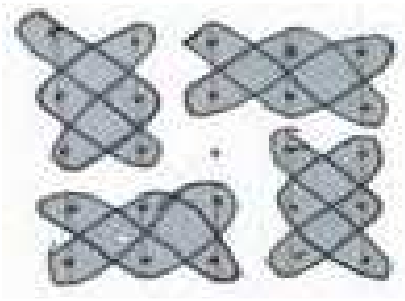


Fig. 2a: 'O+O' VK constructs.

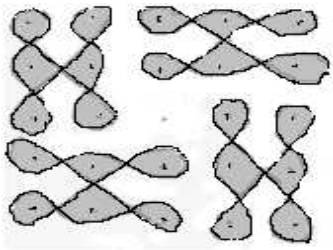


Fig. 2b: "H+H" VK constructs.

Figure 2 Symmetrical VK constructs used for PVR key

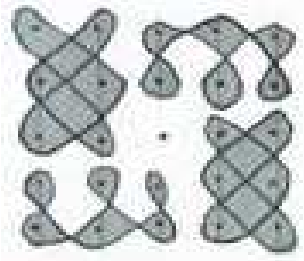


Fig. 3a: "O+E1" VK constructs.

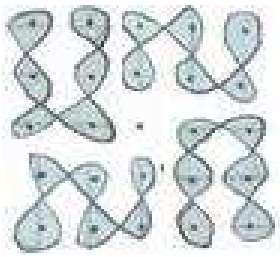


Fig. 3b: "U+S" VK constructs.

Fig. 3 Asymmetrical VK constructs used for PVA key.

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 place 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 is having the b_{24} called RCB bit. Then 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

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

The symmetrical VK constructs used for the secret key PVR(S) is given by

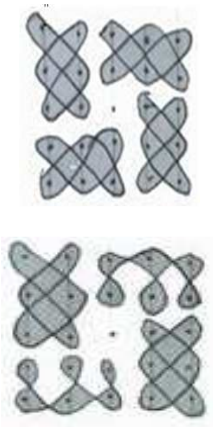
$$PVR(S) = \text{'}O+O\text{'} = \quad (3)$$

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

Fig. 4: Form of 'O+O' using 5x5 array.

$$\begin{matrix} b_0 & b_1 & b_2 & b_3 & b_4 \\ b_5 & b_6 & b_7 & b_8 & b_9 \\ b_{10} & b_{11} & b_{24} & b_{12} & b_{13} \\ b_{14} & b_{15} & b_{16} & b_{17} & b_{18} \\ b_{19} & b_{20} & b_{21} & b_{22} & b_{23} \end{matrix}$$

Fig. 5: Bit pattern Representation



$$PVA(S) = \text{'}O+E1\text{'} = \quad (5)$$

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

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

4.3. PVR Key for Encryption/Decryption:

The PVR key is designed based on the symmetrical VK constructs. There are 16 symmetrical VK constructs which are formed based on the VK scripts. The PVR key generates 16 different encryption/decryption key format using 16 symmetrical VK constructs for assembling data in the payload field. Among these 16 different PVR key, the following section explains design of one PVR key based on the symmetrical VK constructs 'O+O'. The PVR key designed from the 'O+O' symmetrical VK constructs for assembling data into payload field is shown in Figure 6.

The generated PVR key using equation (5.12) is given by

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

Similarly, asymmetrical VK constructs used for the secret key PVA(S) is given by

Bits	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}
Position	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_{33}
Position	R_{43}	R_{52}	R_{41}	R_{53}	R_{42}	R_{51}	R_{55}	R_{44}	R_{35}	R_{54}	R_{45}	R_{34}	
Bits	b_{12}	b_{13}	b_{14}	b_{15}	b_{16}	b_{17}	b_{18}	b_{19}	b_{20}	b_{21}	b_{22}	b_{23}	

Fig. 6: Format for PVR Key.

It shows the payload field of the data packet format for the sensed data. The sensed data is first obtained from the sensor and RCB is added and is converted to the 25-bit format. In this 25 bit, first 24-bit from 1 to 24 indicates the payload reading of the sensor and the last bit (25th bit) indicates the Recurrent Check Bit (RCB).

4.4. PVA Key for Encryption / Decryption:

The PVA Key based Encryption method is suitable for asymmetrical VK constructs. The proposed algorithm can generate 240 asymmetric VK constructs. Thus this key can generate 240 different PVA key. From these 240 PVA key this section explains design of one PVA using asymmetrical VK constructs 'O+E1' is shown in Figure 7. Similar to the PVR key, PVA key is also having 25-bit including RCB. In PVA key RCB is the last bit like PVR key.

Bits	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}
Position	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_{33}
Position	R_{53}	R_{43}	R_{52}	R_{41}	R_{51}	R_{42}	R_{55}	R_{44}	R_{35}	R_{54}	R_{45}	R_{34}	
Bits	b_{12}	b_{13}	b_{14}	b_{15}	b_{16}	b_{17}	b_{18}	b_{19}	b_{20}	b_{21}	b_{22}	b_{23}	

Fig. 7: Format for PVA key.

3. Secured Data Communication (SDC) Scheme:

5.1. Assumptions:

The following assumptions are made for the system model:

- Model is the homogeneous system model which means nodes which are within communication range. Radio transmission range of each sensor node is same.
- All the nodes in the network that contain the same initial energy. The nodes are battery powered and are comprised of sufficient memory capacity to execute communication and computation capabilities.
- The sensor nodes are randomly deployed in the network area. They are static in nature and every node has a unique node-ID.
- Whenever an event occurs the source (Cluster Member-CM) node encrypts and transmits the data to Base Station.
- The source node and the destination node only know the VK constructs based secret key.

5.1.1. Secured Data Packet Format:

The source node transmits the secured data packet which includes Node-id, Length which is equal to the number of bytes between the Length and hash sum, Encrypted Pay Load, RCB is the Recurrent Check Bit which is used to identify the VK construct type, Hash Sum for error detecting byte and Pattern Viable Restore field is used to identify the VK constructs. The format of the secured data packet is shown in Figure 9.

Fig. 8: Experimental Testbed using IRIS mote.

Node-id 2 bytes	Length 2 bytes	Pay Load 3 bytes	RCB 1bit	Hash Sum 2 bytes	Pattern Viable Restore 4 bits

Fig. 9: Secured Data Packet Format.

5.1.2. Recurrent Check Bit (RCB):

The data packet transmitted by any sensor node has payload field. The payload field of the data packet carries the sensed data. In this technique, the VK based encrypted data is included in the payload field of the packet before the data transmission starts. The length of the payload field is defined as 3 bytes which includes 24 bit VK based encrypted payload data. One bit is defined for Recurrent Check Bit (RCB). The VK technique uses PVR key and PVA Key for encryption or decryption. 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. It means that the PVR key is used. When RCB is '0', the asymmetric VK constructs based PVA key is used for encryption or decryption

.

5.1.3. 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 equation (16)

$$Hash\,Sum = FF - \left[Lower\ 8\text{-}bit\ of\ \left(LP_i + RP_i + RCB_i\right)\right] \quad (7)$$

where LP_i indicates the Left Part bits (b_0-b_{11}) of the packet 'i' and RP_i Right Part bits (b_{12}-b_{23}) of the packet 'i'.

The calculated Hash sum is included in the data packet format before transmitting. At the receiver end the Lower 8-bit of (LP_i+RP_i+RCB) and the Hash Sum is added and check 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-(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 otherwise there is an error. In this case the sum of 03, 18, A5, 01 and 3B is equal to FF. This means that the data is received without any transmission error.

5.1.4. Pattern Viable Restore:

It is the last field in the packet format. It has 1 byte length having a value ranges from 00000000 to 11111111 (0 to 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 construct for their convenience. This means that the VK constructs-id differ from one user and another user. This paper 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 the 'O+F' VK constructs.

The transmitter transmits the secured data packets with value 0011 (3) in the Pattern Viable Restore field and the RCB bit is set to 0. At the receiver end the data is decrypted using the 3rd VK construct in the Asymmetric form (O+F) and PVA key. In contrast, if it transmits the encrypted data with RCB bit is 1, the receiver uses the 3rd VK construct of the Symmetric form 'F+F' and PVR key to decrypt the data. The 3rd VK constructs of symmetric form represents the 'F+F' and the 3rd VK constructs of asymmetric form follow '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 algorithm done in this paper is 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.

4. Experimental Testbed for VK:

The Pattern Viable Restoration technique is implemented on the TINY-OS based cross-bow IRIS motes (Vijayalakshmi and Vanajaranjan, 2013) to make the transmission is secured and the performance of the Pattern Viable Restoration based VK technique is compared with the standard encryption algorithms such as DES, AES and SHA algorithms. The prototype test bed for VK technique is shown in Figure 8. In this test bed, one IRIS mote is configured as Base Station (BS), one mote is configured as transmitter (source node) and two as routers. The change in potentiometer is sensed by the transmitter node. When event (change) occurs, the event information is communicated to the BS through the routers. In this experiment the sensed data (potentiometer reading) is encrypted by VK technique before it is transmitted to the BS.

The transmitter and the BS motes only know the PVR/PVA key. The router does not have the knowledge about the data and encryption techniques. The performance analysis of the various standard encryption algorithms using IRIS motes has also done.

5. Performance Analysis:

The impact of message length on total energy consumption for four different encryption schemes is shown in Figure 10. The result shows that the SHA (Secure Hash Algorithm) algorithm consumes more energy than other three algorithms because the computation of this security algorithm is more

complex. The proposed VK technique consumes 2.6 times less than AES, 1.2 times less than DES and nearly 6 to 7 times less than SHA. This analysis shows that the VK technique consumes comparatively very less energy due to its less complex design. The processor energy consumption analysis has done for various message lengths. Since SHA and AES algorithms have constant step length (64 byte and 124 bytes) and does not depend on the length of the message, these algorithms maintains same energy consumption even though the message length increases. Moreover the VK technique follows DES but consumes less energy than DES. The energy consumption of these algorithms increases linearly as the length of the message increase. For the messages with four different message lengths, the average processor energy consumption for DES and VK algorithms are 123μJ and 98μJ respectively.

Figure 11 shows the Radio Transmission (RF) energy consumption for the four different encryption algorithms. The AES and DES algorithms have more or less equal RF energy consumption for various message lengths. The RF energy consumption increases linearly with the increase in message length. The VK technique follows the DES algorithm but consumes comparatively less energy. In WSN node, more energy is consumed during packet transmission state than other states such as sensing, listening etc. Since there is no additional bytes are added to the message in VK technique, it consumes less energy. The AES and DES algorithms consume 1.2 times more than VK and SHA consumes 2.2 times more than VK. This higher RF energy consumption is mainly happened because SHA algorithm adds nearly 20 bytes to the message after encryption.

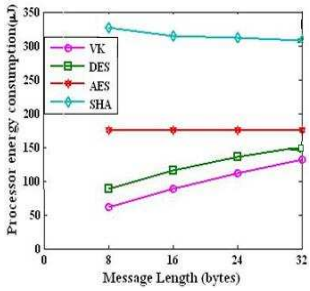


Fig. 10: Processor Energy consumption.

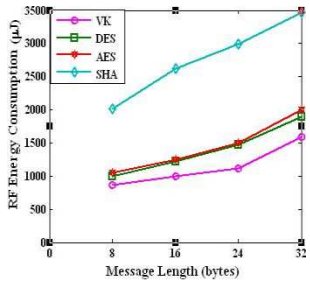


Fig. 11: RF Energy Consumption.

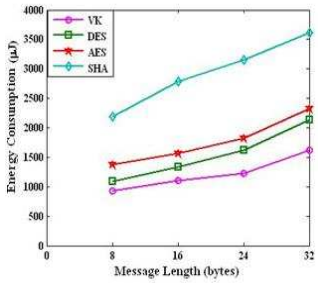


Fig. 12: Total Energy Consumption.

The impact of message length on total energy consumption for four different encryption schemes is shown in Figure 12. The result shows that the total energy consumption increases with increase in message length in all four algorithms. The SHA has more energy consumption due to its more complex encryption algorithms and the proposed PVR using VK technique has less energy consumption because of its simple VK script based encryption algorithm. AES and DES have relatively more energy

consumption than proposed technique. The total energy consumption of DES and AES have1.2 times higher and SHA has 2.2 times higher than the proposed technique.

6. Conclusion:

This paper has proposed a new model with pattern based data encryption key called Viable Key. It is designed specifically for resource constrained devices like wireless sensor nodes. The proposed VK technique has mainly concentrated on data security and highlighted the protected data transmission. In this security technique the data is encrypted only by source node and is decrypted only by destination node. The proposed technique can incorporate various keys from among the 256 patterns to encrypt data because of which the proposed PVR with VK data security technique provides higher security strength. The proposed SDC Scheme with VK technique is seen to enhance the lifetime of the network. The VK technique is designed in this paper for the 5x5 array pattern and as a future work this design is been extended to 10x10 array patterns, though its performance analysis is still to be analysed.

ACKNOWLEDGMENT

The authors gratefully acknowledge UGC for Meritorious for Sciences, New Delhi for providing financial support to carry out this research work under the UGC scheme.

REFERENCES

Akyildiz, F., W. Su, Y. Sankarasubramaniam, E. Cayirci, 2002, "Wireless Sensor Networks: A survey", *Computer Networks*, 38(4): 393–422.

Wenjing Lou and Younggoo Kwon, 2006. "H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks", *IEEE Transactions on Vehicular Technology*, 55(4): 1320-133.

Hind Alwan And Anjali Agarwal, 2013. "A Multipath Routing Approach for Secure and Reliable Data Delivery in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, 1-10.

Anfeng Liu, Zhongming Zheng and Chao Zhang, 2012. "Secure and Energy-Efficient Disjoint Multipath Routing for WSNs", *IEEE Transactions on Vehicular Technology*, 61(7): 3255-3265.

Shiva Murthy, G., Robert John D'souza, Golla Varaprasad, 2012. "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", *IEEE Sensors Journal*, 12(10): 2941-2949.

William Stallings, "Cryptography and Network Security Principles and practices", 3rd Edition, Pearson Education Prentice Hall.

Frederique Oggier and Miodrag J. Mihaljevic, 2014. "An Information-Theoretic Security Evaluation of a Class of Randomized Encryption Schemes", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 158-168.

Vijayalakshmi, A., P. Vanaja Ranjan, 2013 "Code Strategy Algorithm for Online Power Quality Monitoring of Electrical Equipment using WSN under Tiny-Os Environment", *Journal of Theoretical and Applied Information Technology*, 57(3): 465-473.

Estrin, D., R. Govindan, J.S. Heidemann, S. Kumar, 1999. "Next century challenges: Scalable coordination in sensor networks", *Mobile Computing and Networking*, 263-270.

Bhoopathy, V. and R.M.S. Parvathi, 2012, "Secure Authentication Technique for Data Aggregation in Wireless Sensor Networks", *Journal of Computer Science*, 8(2): 232-238.

Leandro Aparecido Villas, Azzedine Boukerche, Heitor Soares Ramos, Horacio A.B. Fernandes De Oliveira, Regina Borges De Araujo, and Antonio Alfredo Ferreira Loureiro, 2013. "DRINA: A Lightweight and Reliable Routing Approach for In-Network Aggregation in Wireless Sensor Networks", *IEEE Transactions on Computers*, 62(4): 676-689.

Marc Sanchez Artigas, Pedro García López, Antonio F. Gomez Skarmeta, 2005, "A Novel Methodology for Constructing Secure Multipath Overlays", *IEEE Journal On Internet Computing*, 9(6): 50-57.

Di Pietro, R., L.V. Mancini, Y.W. Law, S. Etalle, P. Havinga, 2003. "LKHW: A directed diffusion-based secure multi-cast scheme for wireless sensor networks", *Proc. of 32nd International Conference on Parallel Processing Workshops (ICPPW'03)*, 397- 406.

Yun Lan, Chunying Wu And Yiying Zhang, 2013. "A secret-sharing-based key management in Wireless Sensor Network", *IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 676 – 679.

Honggang Wang, Liudong Xing, E. Howard and Michel, " Reed–Solomon Code based Green & Survivable Communications Using Selective Encryption", *International Journal of Performability Engineering*, 6(3): 297 – 299.

Aanchal Aggarwal, Sunita Sangwan and Simerpreet Kaur, 2012. "Enhancing Robustness of EC Cryptic Data using Forward Error Correction", *International Journal of Engineering and Innovative Technology (IJEIT*), 2(1): 133-138.

Meikang Qiu, Wenzhong Gao, Min Chen, Jian-Wei Niu, and Lei Zhang, 2011. "Energy Efficient Security Algorithm for Power Grid Wide Area Monitoring System",. IEEE Transactions on Smart Grid, 2(4): 715-723.