# Security Enhancement of WSN Data using Symmetric Data Encryption through Tabulation Method of Boolean Function Reduction

Linoy A. Tharakan
Research Scholar
Bharathiyar University
Coimbatore Tamilnadu,
India

R. Dhanasekaran, PhD
Director-Research,
Syed Ammal Engineering College
Ramanadhapuram,
Tamilnadu,India

## ABSTRACT
Data transmitted across the Sensor network requires high confidentiality and integrity . Thus the most important issue in a WSN is security The common approach of imparting security is converting the data into ciphers which almost protect the data from external access. Though security is important the mechanisms for imposing security have sometimes results in an undesirable affect in the overall performance of the network . Thus the protection of data in the networks from external tampering is considered the one of the most important researches at this time. In this paper we proposed an algorithm that encrypt the data using a noble symmetric key encryption based on Boolean Quine-Mc Cluskey (tabulation)method of data manipulation.

## Keywords
Cipher Data, Compression, Data Aggression, Encryption, Privacy, WSN

## 1. INTRODUCTION
Wireless sensor networks (WSNs) may be considered as the third wave of a revolution in wireless technology. It makes the living style of human being more secure, easy and advantageous in various aspects of human being. They sensed data from various environment, process the data locally with some computation and communicate the data among the sensor nodes. The main feature of wireless sensor networks (WSNs) is the elimination of wires in communication. Without wires, they can be spread in a remote area for monitoring applications where running wires is not feasible. Nodes are indeed self manageable in terms of sensing, processing, memory and communication abilities are from the start all included [1].But sensor networks also introduce severe resource constraints due to their limited data storage and power[2]. Process of reducing the data that be transmitted without the loss of overall content of information, thereby reducing the size of the data is known as data compression.[13]

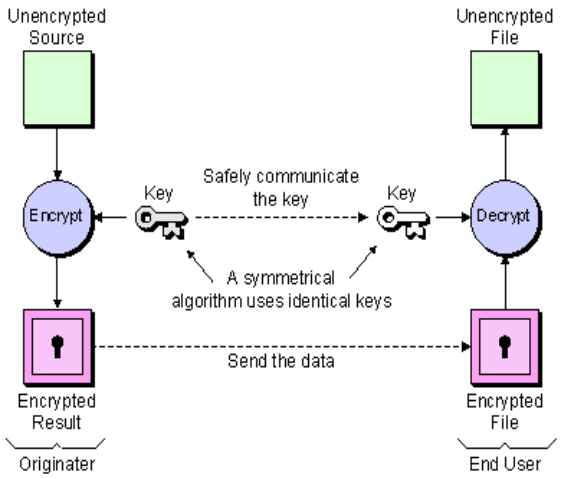
## 2. DATA SECURITY IN WSN
Certainly, unreliable communication is a major factor threat to security in sensor. There are many defied protocols where the security is heavily relies, which in turn depends on communication. WSN usually follows a connectionless routing protocols such as packet based routing protocols which is not so reliable. The channel errors may cause the packets damaged or lost. The result is lost or missing packets. Furthermore, the unreliability in wireless communication channel fallout in errors in data sets. Even if the channel is reliable, communication may unreliable due to the broadcast nature of the wireless sensor network [2]. Conflicts between the data packets will results the transfer itself in failure. The multi-hop routing, node processing, network congestion etc. can lead to greater latency in the network, thus making it difficult to achieve synchronization among nodes.[2] In the case of sensor security the synchronization issues can be critical. The security mechanism is depends critical event reports and cryptographic key distribution. Another most crucial factor in data packet security is confidentiality. Every network with security focus will mainly address confidentiality problem at the most. [2]. A sensor network should not open sensor readings to its neighbor nodes or to any unauthorized elements. Especially in the situation such as military application where the data is very highly sensitive. In many applications nodes transfer sensitive data between neighboring nodes therefore it is so important to build a secure data path in a WSN. All sensing data should be collected by the nodes and forwarded to the base node properly and precisely. Public Sensor information, such as sensor identification address and public keys, should also be encrypted to some extent to protect against traffic analysis attacks [3] [4]. Attacks can be performed in a variety of ways, such as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on.[2]Today's Sensor network technology offers an efficient way of collecting data in an autonomous way through efficient placement of tiny sensor nodes in the area of sensing . In some important application such as military surveillance and various life critical application data transmission, data aggregation, and data reception should be in a secured and energy efficient way [3]. Even if these technologies offer benefits in large extent, they also exhibit lots of unauthorized data exploitation due to lack of security. Main issue raises in the mode of privacy, since sensor networks provide increased data collection facilities from critical sensing environments [5], [6]. Sensor networks aggravate the privacy issues because they produce large volumes of information which is easily available through remote access. They can gather information in an anonymous manner with low risk. Monitor and Eavesdropping is the most obvious attack to privacy. By listening to the data, the opponent could easily identify the communication contents.[2]

## 3. PRIVACY USING ENCRYPTION

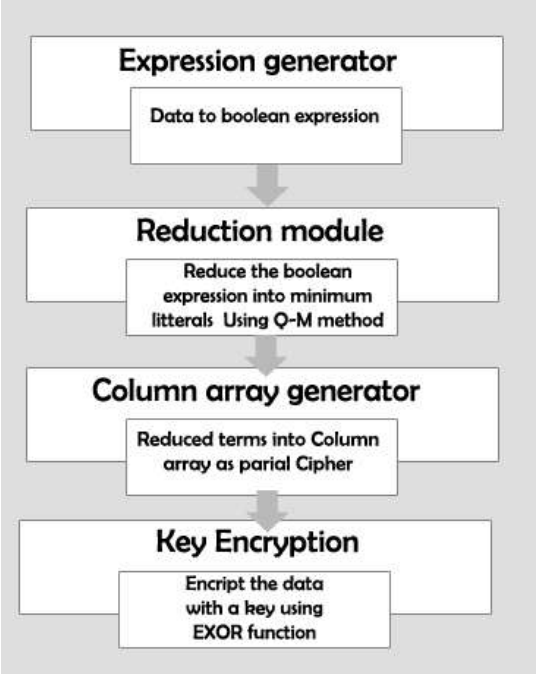
Due to limited energy and restricted computational power, public key cryptographic protocols are costly to implement. Communication topology of sensor networks be at variance from conventional networks. It is required to implement a secret key for sensor nodes with the data aggregation nodes. The vulnerability of this technique is that attackers use large number of nodes that could reconstruct the complete key and crack the security . [7] Due to resources constraints, public key cryptography is not appropriate and apt for the easy implementation most of the sensor networks. Usually a scheme based on Symmetric key cryptography are suitable for sensor networks.However key management problem is the most important insufficiency in symmetric key cryptography. Deploying wireless network in insecure environments, and use of wireless transmission, and the limited resources making the security in WSN is the important issue. Therefore the security needs such as Integrity, Confidentiality Self Organization and Scalability are very important for WSN

## 4. CRYPTOGRAPHIC TECHNIQUES

The improvement of data security by hiding information from unauthorized access makes the data secure. Every node usually communicates confidential data regularly . The sensor network should be secure enough to protect sensed data. Simple method to keep sensitive data secret is to lock the data with a key that only the intended receivers possess, hence achieving confidentiality.[9] Integrity is preventing the information from unauthorized modification. [9]Data authentication can provide data integrity also. Cryptography schemes are often utilized to meet the basic security requirements of confidentiality and integrity in networks. Symmetric Cryptography Symmetric encryption also known as secret-key cryptography, uses a single secret key for both encryption and decryption as shown in Figure 1 A secret key that should be kept in the network., ensuring the data integrity of the network exposed environment where WSNs are used to achieve the security requirements, Several researchers have focused on analysis of cryptographic algorithms in networks and proposing energy aware algorithms for data security for the data transmission . Usually symmetric key methods are faster than asymmetric algorithms as the encryption method is less complex. We first focus on Symmetric Cryptography due to the idea that symmetric algorithm has a greater effectiveness and require less energy consumption, in contrast to public key cryptography.[9]Asymmetric Cryptography is known as public-key encryption, uses two related keys- public and private- for data encryption and decryption, and kept away the risk of key sharing. The private key is never exposed. A message which is encrypted by with the public key can only be decrypted by applying the same method of algorithm and using the similar private key.A message is encrypted by using the private key can only be decrypted by using the pair of public key[9] Public key algorithms are usually omitted in WSN since the larger energy expenditure of battery power and bandwidth was very critical in sensor network. Now a days a node has a powerful CPU and memory. So, now a days a change in the research area from symmetric key cryptography to public key cryptography. And symmetric key does not scale well as the number of nodes increases [10] There is another method of encryption called Homomorphic encryption scheme which allows arithmetic operations on cipher texts, multiplicatively homomorphic approach, where it handles two cipher texts in decryption yields the multiplication of the two corresponding plaintexts.[11], [12]




**The fig1**: Basic architecture of symmetric Key encryption




**The fig 2: Modules of proposed algorithm**

## 5. PROPOSED ALGORITHM

The architecture of proposed algorithm consists of four main module as in figure 2

- Boolean expression generator
- Reduction module
- Column array generator
- Key Encryption

Boolean expression now processed to get a simplified sum of Product (SOP) expression. The reduced Boolean expression may assign variables in complemented and un complemented form. Next each reduced SOP term may now plot it in an array to get converted into a partial cipher data. That data is now encrypted using a same length Binary value (the secret key) using EX-OR function

The figure 3 shows the block diagram of proposed algorithm.

## 6. EXAMPLE FOR ANALYSIS

### 6.1. Encryption

For analysis purpose and explanation sake the data bit is approximated to four bits. Consider the sensed data from four sensor nodes 1011, 1100,0101,1111

**Step 1:** Generate the truth table for the above data for the Boolean function as in the Table 1

**Step 2**: Expression generated from the truth table is shown bellow as equation 1

F(x)=X= A'BC'D +AB'CD+ABC'D' +ABCD -------(1)

**Step 3**: Reduce the expression using Quine-Mc Cluskey method for generating the partial Cipher

| INPUT | OUTPUT |
|---|---|
| ABCD | X |
| 0 0 0 0 | 0 |
| 0 0 0 1 | 0 |
| 0 0 1 0 | 0 |
| 0 0 1 1 | 0 |
| 0 1 0 0 | 0 |
| 0 1 0 1 | 1 |
| 0 1 1 0 | 0 |
| 0 1 1 1 | 0 |
| 1 0 0 0 | 0 |
| 1 0 0 1 | 0 |
| 1 0 1 0 | 0 |
| 1 0 1 1 | 1 |
| 1 1 0 0 | 0 |
| 1 1 0 1 | 1 |
| 1 1 1 0 | 0 |
| 1 1 1 1 | 1 |

**Table 1: The Truth Table**

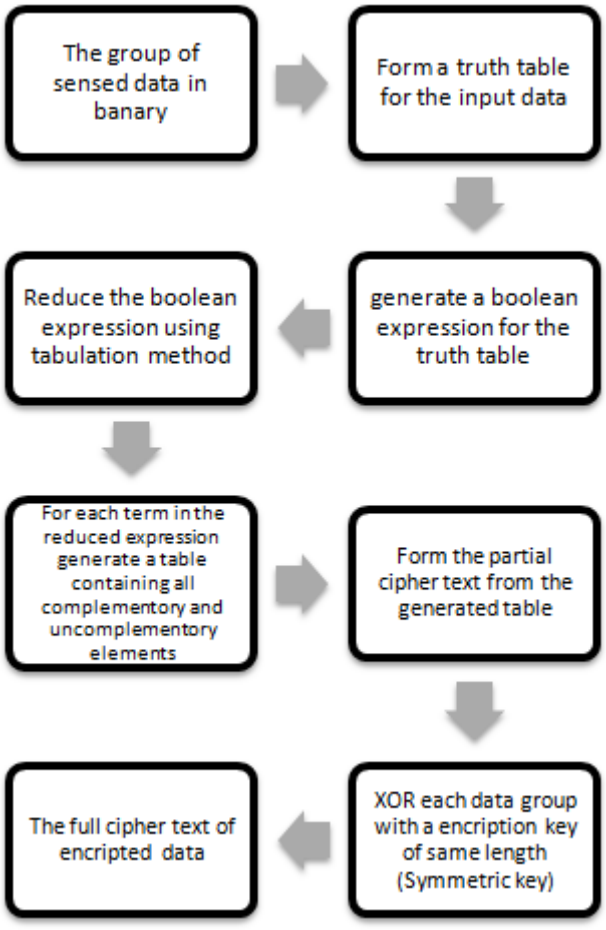



Fig 3: The block diagram (Encryption)

**Table2: Q-A Reduction**

| | | |
|---|---|---|
| 5 | 0101 | (5,13) _ 1 0 1 |
| 11 | 1011 | (11,15) 1 _ 1 1 |
| 13 | 1101 | (13,15) 1 1 _ 1 |
| 15 | 1111 | |

The Table 3 below shows the generation of essential prime implecants(EPI) from prime implecants

**Table 3: Generation of EPI**

| | 5 | 11 | 13 | 15 |
|---|---|---|---|---|
| BC'D * | X | | X | |
| ACD * | | X | | X |
| ABD | | X | X | |
| | * | * | * | * |

The essential prime implecants (EPI) are BC'D and ACD

**Step 4**: Plot the EPI in column array(Table 4A, 4B)

**Table 4a: Column Array For Term 1**

| | | | |
|---|---|---|---|
| A | 0 | 0 | A' |
| B | 1 | 0 | B' |
| C | 0 | 1 | C' |
| D | 1 | 0 | D' |

**Table 4b: Column Array For Term 2**

| | | | |
|---|---|---|---|
| A | 1 | 0 | A' |
| B | 0 | 0 | B' |
| C | 1 | 0 | C' |
| D | 1 | 0 | D' |

**Step 5**: Generate Partial cipher results from the table

**$W_T$=0101, $X_T$= 0010, $Y_T$= 1011, $Z_T$= 0000**

**Step 6**: Produce the final cipher data from the partial cipher using a secret key by EX-OR each terms

Symmetric key: K = 1101

$W_K = W \oplus K = 1000$
$X_K = X \oplus K = 1111$
$Y_K = Y \oplus K = 0110$
$Z_K = Z \oplus K = 1101$

**Step7:** Prepare the cipher text for transmitting

**1000111101101101**

## 6.2 Decryption

The decryption process of this algorithm is not the exact reverse of encryption method. The decryption side doesn't contain the reverse of Quine- Mc Cluskey algorithm that makes this algorithm more interesting and efficient. The data flow diagram of the decryption is shown in the Figure 4

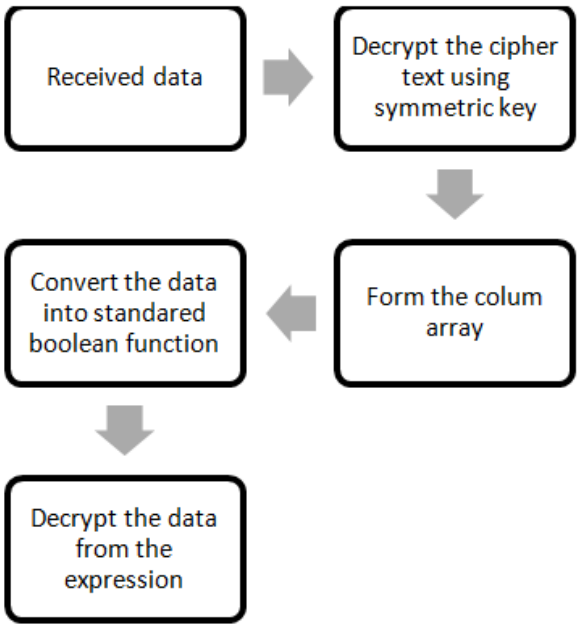



Fig 4: The block diagram ( decryption )

Received data is $R_d$ = 1000 1111 0110 1101

**Step 1**: EX-OR all the received data with same key as in the transmitter side

Decrypt Data =

$R_d$ K= 010⊕010 1011 0000

**Step 2:** Plot the decrypted data in column array (Table 5A, 5B)

TABLE 5A: COLUMN ARRAY FIRST BYTE

| | | | |
|---|---|---|---|
| A | 0 | 0 | A' |
| B | 1 | 0 | B' |
| C | 0 | 1 | C' |
| D | 1 | 0 | D' |

TABLE 5B: COLUMN ARRAY SECOND BYTE

| | | | |
|---|---|---|---|
| A | 1 | 0 | A’ |
| B | 0 | 0 | B’ |
| C | 1 | 0 | C’ |
| D | 1 | 0 | D’ |

**Step 3**: Reproduce the terms of Boolean expression from the column array by taking the 1’s

BC’D , ACD

**Step 4:** Standardize each product term into Standard SOP terms

BC’D(A+A’) & ACD(B+B’)

Standard SOP =

ABC’D +A’BC’D+ABCD+AB’CD --------- (2)

The equations 1 and 2 are same and thus the reproduction of the sensed data is successful.

**Step 5:** 1101,0101, 1011 1111 which is same group of data in the transmitter side

## 7. CONCLUSION

In every wireless data manipulation security is the major issue that to be addressed decently. Data security in WSN is quiet resource killing as it posses lots of computational and procession power consumption. In some important application such as military surveillance and various life critical application data transmission, data aggregation, and data reception should be in a secured and energy efficient way. Here we propose a simple but secure symmetric key encryption algorithm which is well suitable for WSN applications The proposed encryption and decryption algorithm is simple but efficient algorithm for wireless sensor network where the data security is important. Here the data is encrypted using popular Quine Mc Cluskey method of Boolean function simplification and a symmetric key.

## 8. REFERENCES

[1] Frank Schäfer, Martin Kleinsteuber, Hagen Meyer “Wake-Up-Receiver In Energy Efficient Wireless Sensor Networks For Security Applications” Emeric Umbdenstock 2012

[2] John Paul Walters, Zhengqiang Liang “Wireless Sensor Network Security: A Survey security In Distributed, Grid, And Pervasive Computing”. Auerbach Publications, Crc Press 2006

[3] D. W. Carman, P. S. Krus, And B. J. Matt. “Constraints And Approaches For Distributed Sensor Network Security”., Nai Labs, Network Associates, Inc., Glenwood, Md, Technical Report 00-010, 2000.

[4] Linoy A Tharakan ,R Dhanasekaran “SEEMd -Security enabled Energy Efficient Middleware for WSN” ISBN No. 978-1-4799-3914-5/14/ ©2014 IEEEM. Gruteser, G. Schelle, A. Jain, R. Han, And D. Grunwald. “Privacy-Aware Location Sensor Networks”. In 9th Usenix Workshop On Hot Topics In Operating Systems (Hotos Ix), 2003

[5] C. Ozturk, Y. Zhang, And W. Trappe. “ Energy constrained Sensor Network Routing”. In Proceedings of the 2nd Acm Workshop On Security Of Ad Hoc And Sensor Networks, 2004

[6] Anser Ghazzaal Ali Alquraishee And Jayaprakash Kar “A Survey On Security Mechanisms And Attacks In Wireless Sensor Networks” Contemporary Engineering Sciences, 135 – 147 Vol. 7, No. 3, 2014

[7] Dr. Ali Payandeh “Self-Protection Mechanism For Wireless Sensor Networks”, International Journal Of Network Security & Its Applications (Ijnsa), Vol.6, No.3, May 2014

[8] Madhumita Panda “Security In Wireless Sensor Networks Using Cryptographic Techniques”. Aamerican Journal Of Engineering Research (Ajer) 2014

[9] Ian F.Akyildiz, Weilian Su, Yogeshsankara saubramaniam, Ardialcayirci, “A Survey On Sensor Networks” ,IEEE Communications Magazine, Pages 102-114, August 2002.

[10] Priyanka Vasan , Manjit Behniwal “Secure and Reliable Data Transmission Using Homomorphic Encryption in WSN”. International Journal of Advanced Research in Computer Science and Software Engineering . Volume 4, Issue 5, May 2014

[11] Jyoti Rajput, Naveen Garg. “A Survey on Secure Data Aggregation in Wireless Sensor Network” . International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 5, May 2014

[12] Linoy A Tharakan, Dr.R Dhanasekaran Energy Aware Data Compression in Wireless Sensor Network using an advanced RLE method – Matrix RLE (M-RLE) International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 17 (2015)