ISSN 2278-3091
Volume 10, No.4, July - August 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse351042021.pdf
https://doi.org/10.30534/ijatcse/2021/351042021

Safe Data Transfer Using Logic Gate Based Cryptographic Technique in Wireless Sensor Network

Dinesh Kumar Gupta[1], Dr. Deepika Pathak[2]
[1]Department of Computer Science and Application, Dr. APJ Abdul Kalam University Indore (M.P.) India, dineshgupta1111@gmail.com
[2]Department of Computer Science and Application, Dr. APJ Abdul Kalam University Indore (M.P.) India, deepikapathak23@gmail.com

ABSTRACT

Wireless Sensor Networks consist of independent sensor nodes attached to one base station. In wireless sensor networks, nodes are connected to sensing environment and communicate the data to the base station. As WSNs continues to grow, they become vulnerable to attacks and hence the need for operative security techniques. Applications of wireless sensor networks demands for the well-organized and secure communication. For the solution of well-organized and reliable security, we need cryptography algorithms which provide good solutions. For providing reliable security techniques mainly data confidentiality, key management is used. Identification of suitable cryptographic techniques for WSNs is an important challenge due to limitation of energy, computation capability and memory of the sensor nodes. Symmetric cryptography techniques do not act well when the number of sensor nodes increases. Hence asymmetric key cryptographic techniques are widely used. Here we propose an electronic logic gate based symmetric Cryptographic technique which is more suitable for small and medium WSNs.

Key words : Asymmetric Cryptography, Key management, Logic gates, Symmetric Cryptography, WSN.

1. INTRODUCTION

Wireless Sensor Networks (WSNs)

The WSN is a wide network of wireless sensor nodes which sense the data from external sources. A wireless node contains components like storage, processing, sensing and transmission as their main electronic components. The computational power passed by these electronic components is generally low but these electronic devices are the main contributors for computing. The task of these electronic devices is to collect data in a wireless network and pass the collected data to the network between the connecting nodes which work as collective unit. The WSN is applicable for monitoring human body organs, environmental monitoring, temperature and humidity controlling, vehicle traffic controlling system etc. [1].

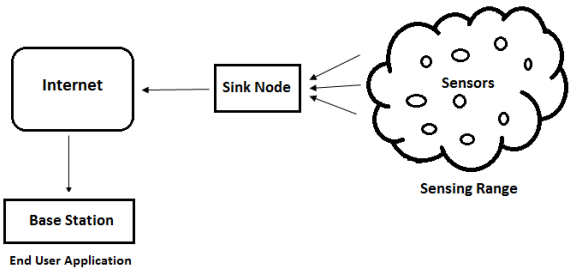

Figure 1: Wireless Sensor Networks

Figure 1 shows the basic setup of wireless sensor network applications. A basic application is used to monitor the environment such as human body organ monitoring, temperature control or any other application by using sensor nodes for proving the desired computational demands. During communicating through the network, a case arises of failure which is solved by using self-configuration and adaptation features of WSN. With grow of WSN, now there are mostly no monitoring stations in the networks to monitor nodes working during the working life of the network, it is being done by sensor nodes by itself [2].

WSN refers to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. These networks will consist of many self-organizing, low-power, low-cost wireless nodes deployed to monitor the environment. WSNs are technically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This indicates to a very demanding environment to provide security [3].

2. ATTACKS ON WSN

In a WSN, the sensor nodes are deployed not in a confirmed area but they are spread over a large area, thus their single controlling and monitoring in a network is mostly not so easy to do task. Hence the unauthorized users provide faults

and errors in the security of these nodes without having any physical access to the sensor nodes [4].

There are following steps possible for attack.

- Sender S wishes to send a message to Receiver R.
- S asks R for its encryption key.
- When R returns key, then that key is intercepted by the attacker and who substitutes his/her key.
- Sender encrypts message using this bogus key and returns it.
- Since the attacker is the owner of this bogus key, the attacker can read the message.

3. SECURITY REQUIREMENTS

A WSN is a special type of network. It shares some similarities with a classic computer network, but it also shows many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes.
General computer network basic concepts are used for working of WSN. Security requirements are the additional feature of WSN which included some certain and important terms such as confidentiality, authenticity, integrity, availability, Non-repudiation and freshness.

The Security requirements in WSN include:

3.1. Confidentiality

Confidentiality means the security process which ensure message share between user and recipient is not understood by anyone in the network. Data confidentiality is obtained in WSN with the help of the following statements.

- Data should be restricted within the network.
- Secure Connection with key management.
- Keys should be convertible with respect to the layered attacks.

An unauthorized user in a network is not allowed to access information in a network.

3.2. Authenticity

Authenticity allows the receiver to maintain the originality of data which involves more than one proof of identity. It may be a in the form of password or a key known only the user. A secret message authentication code called MAC is shared between the nodes communicating in a network to achieve secure data communication in a network, providing reliable communication of data form source to destination.

3.3. Integrity

Integrity means trusting the data resources. Date integrity means that the data is not altered by an accident or any malicious activity and source integrity means data is only originated form the trusted person or source. An unauthorized user in a communicating network is not permitted to transform the information being transferred in a network.

3.4. Availability

Availability means to ensure that the data resource is available for authentic user. It says that data should be available always to the legal users throughout the network even if internal or external failures, faults, errors or attacks are occur. In WSNs, certain services are needed on demand and certain are fixed. Like node connectivity is sometimes fixed service or is on demand service to provide such services and demands needs in a network at any time, for this availability parameter is used in a network.

3.5. Non-Repudiation

Non-repudiation means to ensure that the message transferred has been sent and received by the users claiming to have sent and received the message.

3.6. Freshness

Data freshness assures that the data received during exchange is fresh without any trace of reused data. In WSN, the data may be transferred within the given time interval, so we must guarantee that it is fresh. To achieve this, time stamp are used. It consists of two types such as Weak freshness provides a little order for the data's so delay cannot be calculated, whereas Strong freshness provides a general order and allows the calculation of delays [5].

4. CRYPTOGRAPHIC TECHNIQUES

To avoid above explained attacked and to achieve security of data in WSNs, mostly cryptographic techniques are being used as an important part of the WSNs security architecture.
Cryptography is basically encryption techniques used to encrypt our basic data packets into some secured data packets of coded data words that are being transferred over the network instead of direct original data packets transmission as shown in Figure 2.

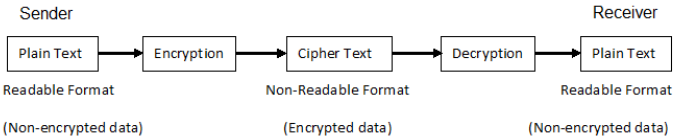

Figure 2: Cryptographic technique

During transmission encrypted data is basically a set of some extra bits along with the data bits for securing the original data from being accessed by the attackers. It is secured and

compatible to the existing protocols over the network operating system as a layered model of network.

After observing the constraints and limitations of sensor networks, it is clear that these kinds of network environment need light-weight cryptography to achieving high level of security. For a practical security solution, each sensor must have a balance between cost, performance and security level but it is very difficult to obtain all these design goals at the same time. It is observed that in such situations developers sacrifice the security level by using cost-effective key solutions without any proper mechanisms for key distributions. Thus WSN requires more flexible methods for key distribution in the network, which is similar to the techniques used in traditional fixed networks.

Cryptography techniques are provided to meet the basic security requirements of confidentiality and integrity in networks basically there are two cryptographic algorithms Symmetric Cryptography (Secret Key) and Asymmetrical Cryptography (Public Key).

4.1 Symmetric Cryptography

It uses a single secret key for both encryption and decryption of the data packets in a communicating network which is kept as secret in a network as shown in Figure 3.

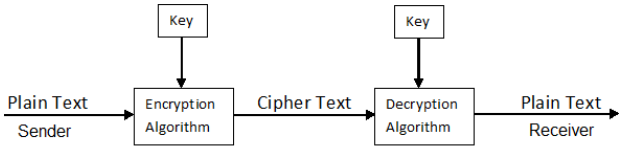

Figure 3: Symmetric Key Cryptography

In Symmetric Key Cryptography, a single key is used for both functions encryption and decryption. For symmetric key encryption to work, two nodes share same secret key which has to be protected from access by others. But the process for installation of key in the system is an important issue to solve by using only symmetric key. The main challenge is in the case of wide distributed area like WSN. Frequent change of key is required in unprotected area where chance of attack on the key is high.

Consider a small sensor network that has pair-wise secret keys pre-loaded in the memory before the development phase. Each sensor node has a list of n keys, one for self and n-1 for others in an n-node network. After deployment phase, nodes can exchange the secret keys for encryption. The network administrator can also manually update the keys whenever it is required. But the problem arises when new node is added then it will need a new key. Such systems can be used for small network but are not practical for large networks.

Let's consider Key Distribution Center (KDC) which distributes keys to the pair of nodes whenever communication has to be established. Every node would have to share a unique symmetric key with the KDC for the purpose of key distribution and authentication. This can leads to increase in the number of packets flowing between nodes and KDC should be well protected and it also requires fixed infrastructure with trusted server. But this method is not prevalent for many sensor network deployments.

The above method shows how limited is KDC in case of WSN. The WSN requires more flexible method for key distribution in the network. So, other method is used.
Keeping the key secreted in the network in the most difficult task in the network.

4.2 Asymmetric Cryptography

It uses two keys public and private keys for data encryption and decryption which avoids the treat of key sharing in a network to implement reliable security needs as shown in Figure 4.

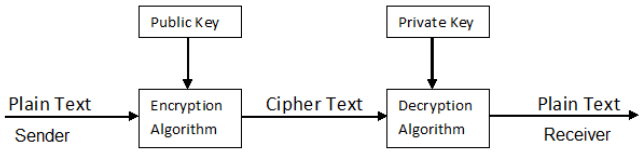

Figure 4: Asymmetric Key Cryptography

The keys are used as two ways security providers. Public key encrypt the data and private key decrypt the encrypted data. Private Key is only provided to the authorized users for accessing the data. A user can decrypt the data at the destination end comparing its public key.

Public key systems are the alternative techniques used in place of symmetric keys. It simplifies the key management and offer additional functionality that was not available in symmetric systems. Public key cryptography is a fundamental and widely used technology that secures the communication both in private networks and across the public network like Internet.

Public key cryptography uses a pair of key names as secret private key and published public key. Here, the key used for encryption is not same as the key for decryption. This type of security technique is called asymmetric cryptography.

4.3 RSA

A method to implement a public key cryptosystem whose security based on the difficulty of factoring large prime numbers was proposed. RSA stands for Ron-**R**ivest, Adi-**S**hamir and Leonard-**A**dleman who first publicly described the algorithm in 1977. In this technique, it is possible to

encrypt data and create digital signatures. It was so successful that today RSA public key algorithm is the most widely used in the world [6].
It is not suitable for WSN security because sensor node has less power and memory. It takes more time for calculations.

4.4 Elliptic Curve Cryptography (ECC)

This method is mainly depending on the algebraic structure of elliptic curves. The difficulty in problem is the size of the elliptic curve. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements such as an elliptic curve group could provide the same level of security afforded by an RSA based system with a large modulus and correspondingly larger key such as 256 bit ECC public key should provide comparable security to a 3072 bit RSA public key. For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation $y^2=x^3+ax+b$. [7]

Elliptical Curve Cryptography is a proven technology that is used in many different commercial products such as mobile phones, smart cards, email systems and many others. Cryptographic security of system is depends upon mathematical complexity. As complexity increases processor's work at the same time and performance of the system also improve. If we compare the security level of ECC then it is much lower than that of RSA.

4.5 TinyECC

TinyECC provides simple, configurable, flexible and ready-to-use software for developing WSN based applications with ECC at its core. All the ECC operations including point addition, point doubling and point multiplications are supported by TinyECC [8].

Compared to RSA, ECC has small key size, low memory usages etc. Hence it has attracted attention as a security solution for wireless networks.

5. DESIGN OF ASYMMETRIC KEY CRYPTOGRAPHY

An asymmetric key cryptography is generally used as implemented technique as a security more efficiently than symmetric cryptography. As the basic principle of public key says it consists of a pair of related and different keys

- Public Key: Provided to any one publically
- Private Key: Provided to authentic user privately

These keys are related to each other but computationally different; also we cannot determine our private key using our public key as shown in Figure 5.

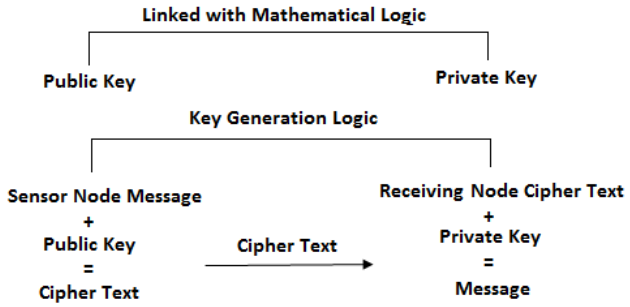

Figure 5: Design of Asymmetric Key Cryptography

Asymmetric encryption uses two related keys (public and private) for data encryption and decryption and takes away the security risk of key sharing. The private key is never visible. A message that is encrypted by using the public key can only be decrypted by applying same algorithm and using the matching private key. Examples are RSA, ECC etc.

Thus higher level attacks are avoided using such cryptographic algorithms and reduces security complexities also by avoiding known key in a network. Therefore, it is mostly applicable in the general public network for data communication. Asymmetric public key cryptosystems such as the RSA or ECC are usually usable in WSN [1].

5.1 Encryption

The encryption can be given by following equation.
C = E (M, Ke)
where
E = Encryption Algorithm
M = Message (Plain Text)
Ke = Encryption Key
C = Cypher Text

5.2 Decryption

The decryption can be given by following equation.
M = D (C, Kd)
where
D = Decryption Algorithm
Kd = Decryption Key

5.3 General Principle

A principle of asymmetric key cryptography can be given by points.

- Any Receiver A uses an algorithm to calculate an encryption key KEa and a decryption key KDa.
- Then the receiver publicizes KEa to anyone who cares to hear, but the receiver keeps secret the decryption key KDa.

- User B sends a message to A by first encrypting that message using the publicized key for that receiver A, KEa.
- Since only A knows how to decrypt the message, so it's secure.

The Public Key Cryptography (PKC) is used presently for solving security issues of WSN currently. Mostly ECC, RSA, LPKC (Large size PKC) are used along with key generation techniques either using static key generation or by using group key generation providing number of WSN applications successful implementations.

In addition to key management and security, public-key cryptography can be the efficient and reliable scheme for number of WSN applications. Public key cryptography provides more advantages because of its low memory usage, low CPU consumption and shorter key size over symmetric cryptography. The asymmetric algorithms are more reliable with variable key management generation techniques providing efficient security goals as the key size is equal and varied at each step without being in need to make them known to all nodes in a network. Private Key is not computed by public key of the network provided as a security feature of asymmetrical cryptosystems. The asymmetric cryptosystems are more efficient in security goals achievement as compared to symmetric cryptosystems. Public key based cryptographic techniques are introduced to remove the drawbacks of symmetric approaches.

6. HYBRID CRYPTOGRAPHY

Symmetric key algorithm has a disadvantage of key distribution and asymmetric algorithm need much computation, so the power of the sensor is wasted in it and it is not feasible to use as power is wasted then sensor will be of no use. Thus the algorithm which combines both the algorithms asymmetric and symmetric; so the advantages of both the algorithms can be utilized in it.

A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to its best advantage. One common approach is to generate a random secret key for a symmetric cipher and then encrypt this key via an asymmetric cipher using the recipient's public key. Then the message itself is encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key and then uses that key to decrypt the message. This is basically the approach used in some applications.The study of these key management schemes are based on the review of some research papers defining some works done on cryptography for solving security issues on data transmission over the network [3].

7. PROPOSED CRYPTOGRAPHIC TECHNIQUE FOR WSN

This proposed method is based on symmetric cryptography with some small hardware or Software implementation. Here we use some electronic logic gates such as OR, AND, XOR and XNOR gates. So it is logic gate based cryptography. This technique required an IC Chip with logic gates on each node in WSNs. A KDC (Key distribution Center) on base station is also required for generating keys at every data transmission.

7.1. Logic gate based symmetric cryptography

We have following points in mind during this:

- Involves a random key that has the same length as the message (plain text) to be encrypted.
- The key is used once and then discarded.
- The Symbols are kept in mind shows in Table 1.
- Key is also coded by OR or AND gate with message using Table 2.
- The Key is exclusively OR or exclusively NOR with the message to produce the cipher using Table 2.
- Given the key and the cypher, the receiver uses the same method to reproduce the message.

Table 1: Abbreviations used in method

Symbols	**Meanings**
S	Sender
R	Receiver
REQ	Request for data
ACK	Acknowledgement
K	Key
M	Message
Ck	Key Cypher
Cm	Message Cypher

Table 2: Truth table for used logic gates

Input		Output			
A	B	OR Gate	AND Gate	XOR Gate	XNOR Gate
		Y = A+B	Y = A.B	Y = A'B+AB'	Y = A'B'+AB
0	0	0	0	0	1
0	1	1	0	1	0
1	0	1	0	1	0
1	1	1	1	0	1

7.2 Sender side Request

If sender S sends the data to receiver R then first S send request to R for sending data as shows in Figure 6.

- Receiver R accepts the request and Check S is authentic node in network.
- The R send acknowledgement ACK to sender S of this request.
- After receiving ACK, sender S sends the data in coded form.
- The receiver R receives data in coded form and decodes it.
- The receiver sends the ACK to sender S for successfully receiving of data.

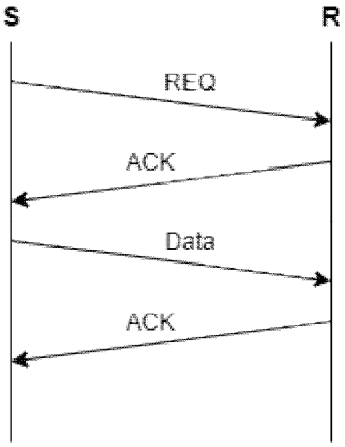

Figure 6: Sender side request

7.3 Receiver side Request

If receiver R wants the data from sender S then R send request to S for sending data as shown in Figure 7.

- Sender S receives the request for data and check R is authentic node in network.
- Then send ACK for this request.
- Sender S send wait signal for waiting some time because sender search the data for sending.
- Sender S send the data to receiver R in coded form
- Receiver R accepts the data in coded form and decodes it.
- Then R sends ACK for successfully receiving of data.

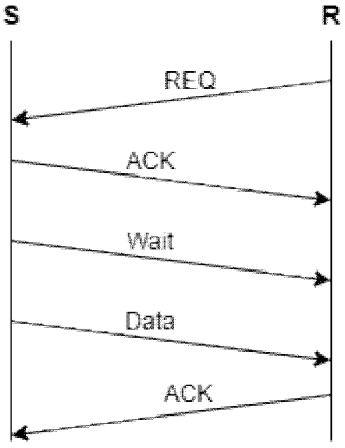

Figure 7: Receiver side request

7.4 Encryption-Decryption

Here, we used electronic logic gates for encryption and decryption. We use same size of key with message. It means the size of key is same as the size of message.

7.4.1 Sender Side

- The Key K and Message M is passed through OR gate (or AND gate) to get the Key cypher Ck as shown in Figure 8 and 9.
- The Key K and Message M is passed through XOR gate (or XNOR gate) to get the Message cypher Cm.
- Same key K is used by Sender and Receiver for only one time. After that key is discarded.
- New key is used for any new data transmission.
- Key Cypher Ck and Message Cypher Cm are sent to Receiver R.

7.4.2 Receiver Side

- The receiver R accepts the both cyphers and decodes it as shown in Figure 8 and 9.
- Key K and Key Cypher Ck is passed through the AND gate (or OR gate) to get the original Key.
- This key is matched with his key, if it is matched then message is authenticate.
- Assure that no attack on cyphers.
- Then Key K and Message Cypher Cm is passed through the XOR gate (or XNOR gate) to get the original Message.

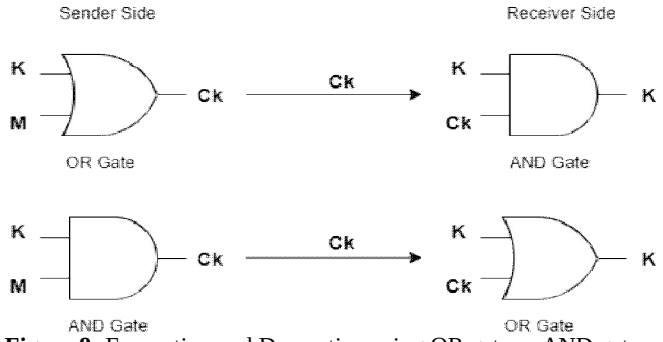

Figure 8: Encryption and Decryption using OR gate or AND gate of Key with message

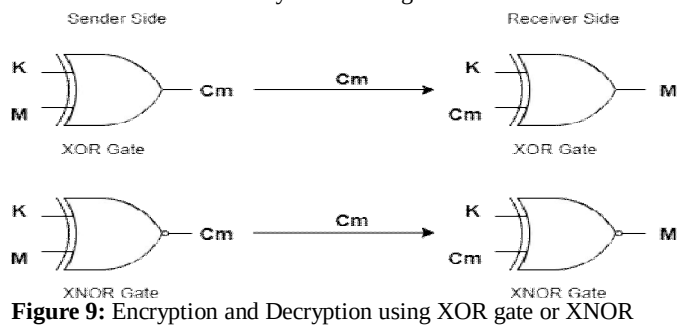

Figure 9: Encryption and Decryption using XOR gate or XNOR gate of Message with key

8. RESULT AND DISCUSSION

We can implement this proposed method in any wireless sensor network and get better results compare to other cryptographic techniques. Because it is electronic logic gates based technique and small battery power required for encryption and decryption. There is no mathematical calculation required compare to other cryptographic techniques.
Here we discuss some examples.

8.1 Data transmission in 4-bit system

Here we discuss 4-bit data transmission.

Suppose K = 0101 and M = 1100 then Key Cypher Ck is produced by OR or AND gate at sender side. This Ck is transmitting to receiver side. After that message cypher Cm is produced by XOR or XNOR gate at sender side and this Cm is transfer to Receiver side as shown in Figure 10.

The Receiver produce the Key K using AND or OR gate by Ck. This Key K is matched with his own key by receiver, if it is matched then receiver produce the original message M using XOR or XNOR gate by message cypher Cm as shown in Figure 11.

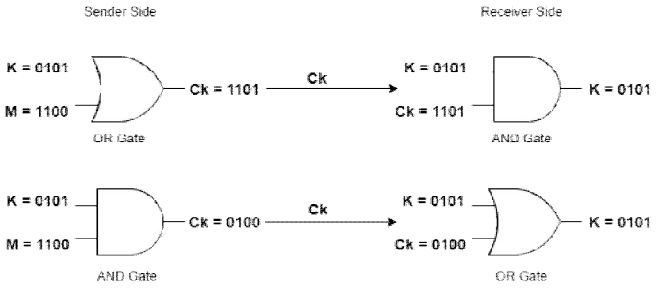

Figure 10: Key Cypher for 4-Bit System

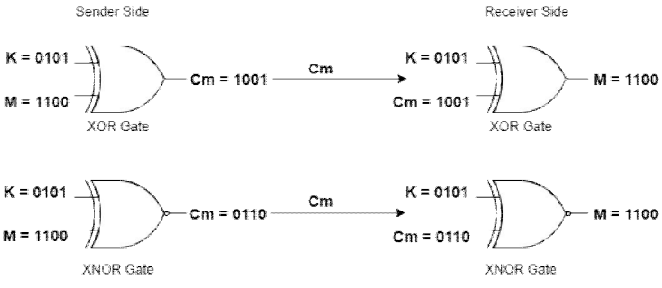

Figure 11: Message Cypher for 4-Bit System

Receiver gets the original message and assures that it is secure.

8.2 Data transmission in 8-bit system

Here we discuss 8-bit data transmission

Suppose K = 10101100 and M = 11110000 then follow same process as above. See Figure 12 for Key Cypher and Figure 13 for Message Cypher.

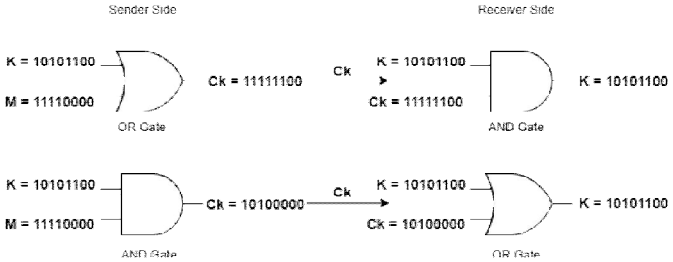

Figure 12: Key Cypher for 8-Bit System

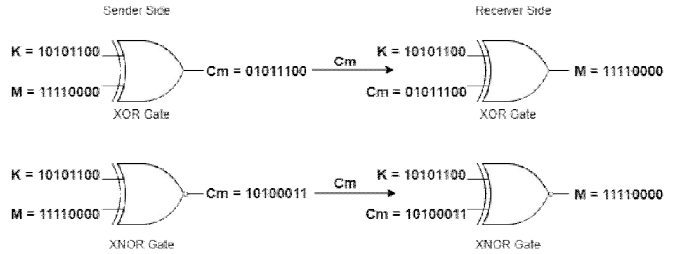

Figure 13: Message Cypher for 8-Bit System

Receiver gets the original message and assures that it is secure.
Similarly, we can design this for 16-Bits, 32-Bits and 64-Bits System.

9. ADVANTAGES OF PROPOSED LOGIC GATE BASED SYMMETRIC CRYPTOGRAPHY

- Small electronic circuit is required on an IC chip.
- Logic gates based encryption and decryption.
- No overloading on processor.
- No mathematical calculation required.
- Very Small battery power is required.
- Possibility of attack on message is very less because extra hardware is required to attack.

10. COMPARISON TO OTHER CRYPTOGRAPHIC TECHNIQUES

We can compare this proposed method to other available cryptographic method as shown in Table 3.

Table 3: Comparison to other methods

Base	**Symmetric Cryptography**	**Asymmetric Cryptography**	**RSA Cryptography**	**ECC Cryptography**	**Proposed Logic gates based Symmetric Cryptography**
Software/Hardware Required (Extra)	Software based	Software based	Software based	Software based	Software and Hardware based
Mathematical Calculation Required	Yes	Yes	Yes	Yes	No
Battery Power Consumption	Low	High	Very High	Very High	Very Low
Possibility of Attack	High	Medium	Low	Low	Very Low
Processor Overload	Low	High	Very High	Very High	Very Low

11. CONCLUSION

The WSNs continues to grow and become widely used in many applications. So the need for security becomes dynamic. However, the WSN suffers from many constraints such as limited energy, processing capacity and storage capacity. The Cryptography is one of the ways for providing security. Selecting the appropriate cryptography method for sensor nodes is important to provide security services in WSNs. The proposed logic gate based symmetrical cryptography is well suited for WSNs as compared to asymmetrical cryptography. This proposed technique is comparatively well suited for small and medium WSNs because of its low energy consumptions.

REFERENCES

1. H. Dogra & J. Kohli. **Secure Data Transmission using Cryptography Techniques in Wireless Sensor Networks: A Survey**, *Indian Journal of Science and Technology*, Vol. 9(47), pp. 1-5, 2016.
2. E. Shi & A. Perrig. **Designing secure sensor networks**, *Wireless communication magazine*, Vol. 11(6), pp. 37-43, 2004.
3. M. Panda. **Security in Wireless Sensor Networks using Cryptographic Techniques**, *American Journal of Engineering Research (AJER)*, Vol. 03, Issue 01, pp. 50-56, 2014.
4. Y. Wang, G. Attebeery & B. Ramamurthy. **A survey of security issues in Wireless Sensor Networks**, *IEEE Communication Surveys and Tutorials*, Vol. 8(2), pp. 02-23, 2006.
5. A. Faquihand & P. Kadam. **Cryptographic Techniques for Wireless Sensor Network Security – A Survey**, *International Journal of Advanced Computational Engineering and Networking*, Vol. 3, Issue 6, pp. 106-110, 2015.
6. R. L. Rivest, A. Shamir & L. Adleman. **A method for obtaining digital signatures and public key cryptosystems**, *Communications of the ACM*, Vol. 21(2), pp. 120-126, 1978.
7. K. Lauter. **The advantages of Elliptic Curve Cryptography for Wireless Security**, *IEEE Wireless Communications*, Vol. 3, pp. 22-25, 2004.
8. N. Saqiband & S. S. Shekhawat. **Securing Wireless Sensor Networks using Elliptical Curve Cryptography**, *International Journal of Engineering Trends and Technology (IJETT)*, Vol. 56(1), pp. 07-11, 2018.