ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

A Survey on Lightweight Protocol Using Dynamic Key for Wireless Sensor Network

Kusumlata Jain[1], Ankita Ojha[2]

Department of Computer Science, Banasthali University, Jaipur, India[1]

Department of Information Technology, Banasthali University, Jaipur, India[2]

Abstract: Wireless sensor networks have lots of interest in research department. Wireless sensor networks of thousand of minute devices capable of computation, communication and sensing. Security is a major concern over wireless network. The present work deal with a secure key management which provide the security for wireless sensor network. Conventional public key system may not be applicable because of restricted computing power and memory space. To s this problem a lightweight protocol is used. The present work the author has used random number to form the key .The key management method take part in an important task in security. The reward of present work is that for each pair new key is generated so it is very difficult to break. In the present work, for encryption and decryption, block cipher and dynamic key techniques is used. In this work dynamic key is generated using linear congruential generator. Most important advantage is that after encryption and decryption key is leftover. The result shows that our scheme provides better security connectivity in minor storage cost and in less time. In the recent year for security of data another technique is used known as key management. Another approach is used for data security is using the hash function. Wireless sensor network has the limited computing power and storage space due to this we create a lightweight protocol which contain the one-way hash function and XOR operations so that the production does not require high storage space and computing power.

Keywords: wireless sensor networks, dynamic key, LCG, encryption, decryption, hash function, lightweight protocol, Key distribution.

I. INTRODUCTION

Cryptography is the practice and study of hiding information. Cryptography is the art and science of transforming message to make them secure and immune to attack. In cryptography original message is converted into another message at encryption side and converted into original message at receiver side. Cryptography use mainly two cipher: stream and block cipher. In stream cipher convert plain text into cipher text bit by bit or byte by byte. In block cipher it converts whole plaintext into cipher text block of same length.

The paper [2] proposed a new way for security in which this scheme using blocks cipher. The paper proposed algorithm in which plain text is divided into block of 49 bits and key size of 196 bits .The rest paper contained as follow: section 2 contains brief introduction of concepts used in cryptography, section 3 contained classified method for generating dynamic key. Section 4 contains conclusion and future scope. The paper [4] also presents a key management and key distribution scheme. In which key is distributed among the nodes of network. Many methods are use for key distribution like pair-wise key management, which mainly used for the unicast communication. Another scheme is used known as group-wise key distribution in which it is used for multicast network. Another scheme is used which is mainly for the broadcast network means all the nodes can access the key for secure communication.

The paper [3] also presents the working of hash function we can use the hash function with the key distribution. The hash function plays an important role in the cryptographic methods. It is an important tool which provides the data integrity.

Input for the hash functions are a block of data then it produces a hash value as an output. A hash function takes a variable length data as input and produces a predetermined length output.[11]

II. BASIC CONCEPTS FOR CRYPTOGRAPHY

A. Basic Terms

- Cryptanalysis is a science of analysing cipher text to decrypt it and extract hidden information without the knowledge of encryption mechanism.
- Cryptography is a mechanism to provide the secure communication between two parties in the presence of third Party. Cryptography uses the modern mathematical theory and computer science approaches.
- Cryptology is the mathematics, such as number theory, application of formulas and algorithm that underpin cryptography and cryptanalysis.
- Plaintext: This is the original message file. All the encryption technique is applied over it.
- Cipher text: It is the encoded message of the original message. It is an unreadable form of the original message.
- Encryption: Encryption is the way to convert plaintext into ciphertext. It take the two parameter one is key and another one is plaintext.
- Decryption: It is the way to convert ciphertext into the original form of the message. It the two parameter one

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

is the input key and another one is ciphertext which we want to convert it into the original message.[1]

- Symmetric key: Only one key is used by sender and receiver for both encryption and decryption operation.
- Asymmetric key: In this two keys are used one for encryption and another is for the decryption. In this sender use one to perform encryption and another key is used for decryption.[1]
- Key: Key is mainly used to provide the secure communication between two communication parties.

B. Security Services

- Authentication: This service provides authentication between the communications parties means only authenticate person can access the access.
- Access Control: This service provides protection against unauthorized access to data.
- Data confidentiality: This service is used to protect the data from any intermediate disclosure
- Data Integrity: This service ensures to design the system to defend data from modification, insertion and deletion.
- Nonrepudiation: This service protects the data against repudiation or negation by either the sender or receiver.

C. Symmetric Key Encipherment

In this method an entity can transmit a message over a communication channel by using a single secret key for both encryption and decryption.

D. Asymmetric Key Encipherment

In asymmetric method key two keys is used for encryption and decryption. One key is used for encryption and another key is used for decryption.

III. CLASSIFIED METHODS FOR GENERATING DYNAMIC KEY

A. *Linear Congruential Generator (LCG)*

In the present work [13] author proposed a method based on the symmetric key encryption suggests the name "Lightweight protocol using dynamic key for wireless sensor network. In the proposed work every message is encrypted and decrypted by using the dynamic key than key is discarded after performing the encryption operation. A key discarding function is called after every decryption function and a new key is generated to perform the encryption and decryption. This concept is based on one time pad. The proposed algorithm is implemented on MATLAB 7.0 [12, 13, 14].

1) Why LCG is Best

This is an oldest pseudorandom number generator algorithm. LCG fast and require minimal memory to preserve state. This makes them valuable for simulating several independent streams. [13]

B. *Dynamic Key*

Dynamic mean which is changed every time. It is new and an advanced concept. These keys are used for each pair of encryption and decryption and after decryption these are discarded so name is dynamic key. Whole keys are not shared between the parties but little bit information are shared between two parties so on the basic of these information both parties produce the dynamic key. In this key is applied over the different part of the message. [2]

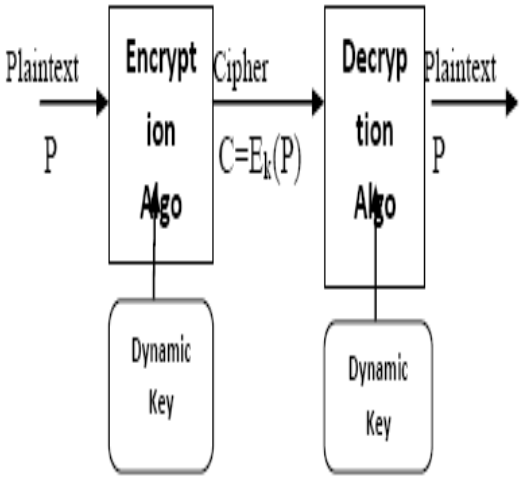

Fig. 1 Cryptography using Dynamic key mechanism

C. *One Tine Pad*

In the paper [2] dynamic key generation is similar to one time paid because in dynamic key, key is used for encryption and decryption after that it is discarded.

The same processor is used in one time pad, it is implemented using a random set of non repeating character as input. The most striking feature is that once the key is used for transposition it is never used again. It is unbreakable if it is used in a right direction and it produces the output which has no relationship to the original message. The security of one time pad is depends on randomness of the key. [2]

Problems	Dynamic Key	Session Key
Key use	once	Every session
Life of key	Within a message	Within a session
Reusability	NO	YES
Man-in-middle attacks	NO	YES
Key can do	Decrypt all message	Decrypt all message in session

Fig. 2 Differences between the types of the key

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

D. *Linear Congruential generator using security protocol*
Linear congruential generator is mainly used to produce the random number. The equation which is used to produce the random number is as follow:

$X_{n+1} = aX_n + b \bmod m$, n = 1, 2, 3..... And (n > 0)

Where
a = multiplier, 0 < a < m
b= increment, 0 < c < m
m = modules, m > 0
X_0 = Starting value, 0 < X_0 <m
Parameter of LCG are = (X_0, m, a, b)

If m, a, b, X_0 are integer than it produce the result in the range of 0 < X_n < m. Here m to be very large so it produce a large number of random number.

LCG is the simplest form to generate the pseudo random number. The reason that we select the random number, because it is simple, more efficient and well known pseudo random number. [2]

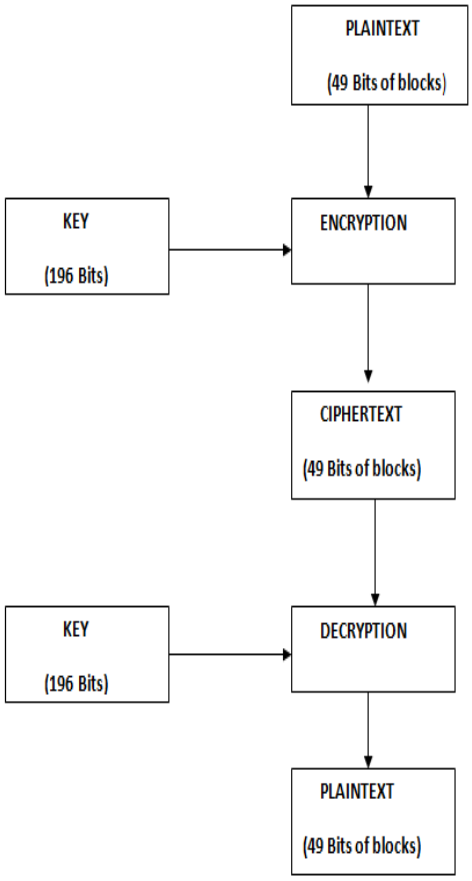

Fig. 3 Present method flowchart

E. Dynamic Key Generation
In the planned work like the one time pad or we can say that dynamic key is generated by using linear congruential generator (LCG). In planned work user enter a key 'EK'. The size of the input key is between 6 bits to 14 bits means minimum size is 6 bits and maximum size is 14 bits. Depending upon enter key length a base value (X_0) is determined from a pre defined table so that table 1. An inbuilt key 'ibk' is concatenated with the key which is entered by user to creating a matrix of 14X14. A random function (FR_r) is used to produce the key. A random function contains various matrix operations like addition, multiplication, shifting etc. In which the random number X is added to the final matrix to produce the dynamic key. [2]

F. Key Distribution Method
This method is more efficient method of encrypting large message. Symmetric key distribution is use the common secret key between two communication parties. It is also useful to produce the lightweight protocol. Key distribution method and other rules are backbone for the security between the sensor nodes and between sensor nodes and base stations. Key management scheme provide the security for unicast, multicast, and broadcast network. Unicast mean sender sends data it is received by only one receiver, in multicast sender sends data it is received by multiple receivers, in broadcast sender sends data which is received by all other receivers.[9]

In key distribution method KDC (Key distribution centre) is used by using this it reduce the number of keys which are shared between the two communication parties.

(1) Classified Key Management method
There are many methods in which many classified schemes are used for key distribution method. Key distribution scheme for wireless sensor network can be divided into two parts: dynamic key and static key. Dynamic key which is changed every time mean this key is used only one time after that it is discarded. In static key only one is used for every encryption and decryption process means it remain fix for every encryption and decryption. [4]

- Pair-wise key distribution: This type of key management scheme is mainly used for unicast communication between the network nodes. If there are m nodes in the network than there are (n-1) pairs of key. This allows each node to communicate with the all other node in the network with different pair of keys. [4]
- Group-wise key distribution: These key are mainly used for multicast communication. In pair-wise key distribution two nodes share the one key, for the next two another paired key is used, due to this group-wise key distribution scheme is used in which one sender can communicate with multiple node or to single node with a single pair of key. [4]
- Centralized key based key distribution: In this scheme only one key is loaded into the process to perform encryption and decryption means all nodes can access the same key to convert the original message into unreadable format or again convert unreadable form of the message into the original one. This technique is mainly used for the broadcast communication. In this scheme base station share a key with each sensor node so base station involved in each establishment of key. Due to this it increases overheads and limited the scalability and flexibility. [4]
- Randomize key pre-distribution: In this key pre-distribution a set of keys is preloaded before key

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

distribution or management. In this scheme nodes extract a random key from a large set of keys. After that two sensor node can communicate via this key. This key distribution schemes provides better scalability, flexibility and reduce the unnecessary overhead. [4]

KDC	Key distribution center
HASH	Hash functions
PRF	Pseudo random number
DAG	Directed a cyclic graph
MAC	Message authentication code
WSN	Wireless sensor network

Fig. 4 Key Distribution Methods

(2) Key Distribution Based on network architecture

- Hierarchical Wireless Sensor Network: This type of WSN contains three types of nodes- base station node, cluster node, sensor node. In this type of WSN key distribution centre is used for distribution of the key. It use pair-wise key distribution, group-wise key distribution, network based key distribution between the nodes of the sensor nodes. [5]

Problem	Solution based on key approach
Group-wise key distribution	Symmetric key Asymmetric key
Pair-wise key distribution	Master key
Grid-wise key distribution	Master key

Fig. 5 Key Distribution in Hierarchical WSN

- Distributed Wireless Sensor Network: Distributed sensor network [15] are scattered randomly over the network area. The working of distributed wireless sensor network is similar to the hierarchical network but only difference is that distributed wireless sensor network use the broadcast key distribution but distributed network uses only the unicast and multicast key schemes. [5][10]

Problem	Key style to solve problem
Pair-wise key distribution	-Pair-wise key -Master key -Polynomial based key
Group-wise key distribution	-Dynamic key -Polynomial key -Key matrix

Fig. 6 Key Distribution in Distributed WSN

(1) Advantage and disadvantage of key managements schemes

KEY SCHEME	ADVANTAGE	DISADVANTAGE
Lightweight key distribution	-Low memory and computation cost -Low key setup overhead -Self-management	Low resilience
Pair-Wise key distribution	-node-to-node authentication -High network connectivity	-limited scalability -less resilient -additional overhead for each node to maintain and store distinct pair-wise keys
Grid-Based Key Pre-Distribution	-low communication overhead -low computation overhead -total connected graph	-storage overhead; as each node share the polynomial keys and the ID's
Master key distribution	-Better security than the random key pre-distribution or the Q-Composite scheme -improved resilience	-creates communication overhead -depleted node battery life

Fig. 7 Comparisons of Key Distribution Methods

G. Hash Function to increase message authentication

The paper [14] a hash function is mainly used to convert the input into another form and in the hash function it is difficult to reproduce the input from the hash value. Hash function based MAC protocols are used to provide the security.

Small data blocks of cryptographic checksum produced from the input message by using a key by sender and receiver known as message authentication code. Then it is attached to the original message before sending to the receiver. After that receiver receive that message, calculate his own MAC, compare with it to the receiving one and authenticate the message.[14]

MAC provides the data integrity and authentication. The basic approach is to creating MAC is the concentration of key (K) and input message (M). After that the output

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 9, September 2014

produce by concentration of key and message is given to hash function. The output MAC is appended with message when it is send over the network.[11]

Input key = K
Input message = M
Hash function = H (K, M)
MAC produces the output = [M, H (K, M)]

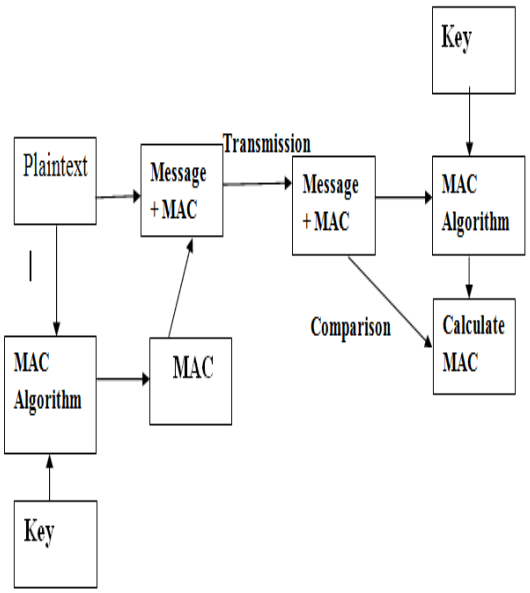

Fig. 8 Authentication using MAC code

IV. CONCLUSION

The paper presented brief survey on lightweight protocol using dynamic key, key distribution mechanisms and hash function for wireless sensor network. Lightweight protocols which create by using one way hash function based MAC protocol. By using this it produce the effective authentication and key exchange mechanisms. Hash function contains the lightweight operation. This survey contains the multiple key distribution approaches using the symmetric key encryption. This paper also contains the key pre distributions which reduce the cost of the key organization Dynamic key is generated by using the LCG which is mainly produced by pseudo random number. It uses the random number numbers so it is very difficult for attacks. By using this it decrease the storage cost and computational time so it is suitable for large scale sensor network. More research is necessary to deal with the challenges so that wireless sensor network provide efficient outcome.

REFERENCES

[1] William Stalling, "Applied Cryptography" 4th Ed.
[2] Zeenat mahmood, Anurag jain, Chetan agrawal," Hybridize Dynamic Symmetric Key Cryptography using LCG", In International Journal of Computer Applications (0975 – 8887) , vol. 60-no. 17 ,December 2012.
[3] Richa Purohit, Yogendra Singh, Dr. Upendra Mishra, Dr. Abhay Bansal," Integrtation of Encryption and Hash Function for Improved Message Authenticity", International Journal of Engineering Research and Applications (IJERA).Vol. 2, September- October 2012, pp.2137-2142.
[4] Che-Chens Lin, Shiuhyng Shieh, Jia-Chun Lin, Lightweight "Distributed Key Agreement Protocol for Wireless Sensor Network", The Second International Conference on Secure System Integration and Reliability Improvement.
[5] SEYIT A. C¸AMTEPE, B¨ ULENT YENER, "Key Distribution mechanism for wireless sensor network: a survey",
[6] Suman Bala, Gaurav Sharma and Anil K. Verma, "Classification of Symmetric Key Management Schemes for Wireless Sensor Network", International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013.
[7] M. Eltoweissy, H. Heydari, L. Morales and H. Sudborough, "Combinatorial Optimization of Group Key Management", J Network and System Management, vol. 1, no. 12, **(2004)**.
[8] D. Liu, P. Ning, and W. Du, "Group-Based Key Pre-Distribution in wireless sensor network", IEEE International Conference on computer and communication socities, 2005, pp. 11.20.
[9] Chi-Yuan Chen, Han-Chieh Chao, "A survey of key distribution in wireless sensor networks", Security and Communication Networks, 13 July,(201).
[10] A. Jem ai, A. Mastouri, H. Eleuch, "Study of key pre-distribution schemes in wireless sensor networks: case of BROSK (use of WSNet)", Applied Mathematics & Information Sciences, 5(3)(2011), 655-667.
[11] Umesh Kumar Singh, Kailash Chandra Phuleriya, Lokesh Laddhani, "Study and Analysis of MAC Protocols Design Approach for Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Science and Software Engineering, Apirl (2012).
[12] Bo Sun, Chung-Chih Li, Kui Wu, Yang Xiao, "A LCG Based Secure Protocol for Wireless Sensor Networks", IEEE INTERNATIONAL CONFERENCIE ON COMMUNICATION, 2006.
[13] Bo Sun a, Chung-Chih Li , Kui Wu , Yang Xiao, "A Lightweight Secure Protocol for wireless sensor network", ELSEVIER, Computer Communications 29 (2006) 2556–2568.
[14] Denis trček, "MAC Based Lightweight protocol for Strong Authentication and Key Exchange", JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 21, 753-765 (2005).
[15] Priya L C, Shantal Devi Patil, " A survey on Sensor Aunthication in Dynamic Wireless Sensor Networks ", International Journal of Computer Science and Information Technology Research,Vol. 2, Issue 2, pp: (454-461), Month: April-June 2014.