REVIEW ON DYNAMIC KEY SECURITY PROTOCOLS IN WIRELESS SENSOR NETWORK USING PSEUDORANDOM NUMBER GENERATOR

Shrivastava N.P., Bansal D.
E-mail id: npshrivastava80@gmail.com
Anand International College of Engineering, Jaipur

Abstract-In the current scenario, Wireless Sensor Network (WSN) is also playing an important role in research field because it provides so many surveillance applications such as in military, environmental monitoring, battlefield strategy planning, industrial monitoring and many more. Wireless sensor network are self configurable wireless network that tends to major requirement of security. Data would be transferred from one sensor node to another node in open environment. Distributed nature, restricted computing power needs algorithms that require less complex algorithms. To overcome this problem light weight security protocol is used in WSN Classical Security algorithms cannot be easily applied to Wireless Sensor Networks. In this paper a survey of security protocols proposed for wireless sensor is provided, the paper also provides a comparison for the same.

Security plays an important part in wireless network. In the Present work, secure key management for providing security is play a vital role over wireless sensor network. In the present scenario, because of less computing power and memory space Conventional public key system is not worth full . In the research work the author has used random number to form the key which is a method to increase the security. Main advantage of the present work is that it is tuff to break a pair because a new random key generated each time.

Keywords: Wireless sensor Network, Light weight security protocols, Random number generator.

1. INTRODUCTION

A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensor nodes to monitor physical or environmental situations. A WSN system associate a gateway that gives wireless connectivity back to the wired world and distributed nodes. Generally a wireless sensor network (WSN) consist thousands of sensor nodes.[1]These sensor nodes can interact with other sensor nodes using radio signals. Wireless sensor network (WSN) have many resource necessity like limited processing speed, storage capacity, and communication bandwidth. When the sensor nodes are organised, they establish a convenient network framework for providing a multi-hop communication between them. After that, sensors can start collecting the data or information. Base station is the central node for providing and receiving all the information to all the sensor nodes. To perform some specific instruction wireless sensor device acknowledge to the queries sent by a “control site” and also provides sensing samples.[2]

1.1 Security Requirements in WSN

1.1.1 Confidentiality

Message Confidentiality is one of the major concerns in wireless sensor network because it is used to keep the information safe from unauthorized access. In WSN, information collected from the sensor node is very sensitive, so for transferring these data, security between them is essential. For this, a safe communication channel has been established. Encryption technique is a standard approach to provide confidentiality in wireless sensor network using a secret key.

1.1.2 Integrity

Data privacy of data by malicious nodes can be prevented by using data confidentiality but the data being changed by malicious node cannot be stopped. Message integrity ensures that the data or message cannot be altered by other party during transmission. The communication network can work in-appropriately by disrupting the message due to a malignant node. Message authentication code (MAC) or cyclic code plays a vital role in message integrity to prevent the access by an unauthorised person. At the sender side MAC is calculated over the packet using their secret key, then at the receiver side re-computation is performed for performing message integrity.

1.1.3 Authentication

Message authentication is a process used to ensure that the receiver is capable to analyze the authenticity of the message. Since wireless sensor networks use public wireless environment, so there is a need to provide authenticity against the message coming from malicious nodes. If no certification is there, a malicious node can behave as a different node, and some sensitive data may be acquired and also impede the proper operation of other nodes. Since an opponent can easily inject a message, the receiver comes to know about the authenticity of

DOI Number: https://doi.org/10.30780/specialissue-ICRDET-2019/003

the message used for decision control. In this communication, Message Authentication Code (MAC) is used to provide authenticity. Symmetric key cryptography is also used to provide message authentication.

1.1.4 Freshness

In wireless sensor networks, sensor transmits the information to other nodes through specific time intervals but what should be taken care of is the delivery of the measurement times. There is a possibility; an attacker can retransmit the same copy of old measurement value. Now, there is a need to analyze that the data is new.[6] For preserving the data freshness, a counter value or any other random number is added with the message during the encryption procedure. This is necessary for sensor network in symmetric key cryptography.

1.1.5 Availability

To ensure more availability of services, the security protocol uses less communication power and less processing. But in large WSN,the DOS attack and node compromise gives data availability. So ,there should be methods ,to counter the interference of malicious nodes .Certain ways like,en-route filtering ,in network processing can be used to regulate and lower the impact of unavailability of series.

1.1.6 Secure Localization

Sensor node location information is important to recognize when the identification is required. In addition, location information can prevent large-scale attacks.

1.1.7 Time Synchronization

These protocols should not be controlled to produce incorrect data.

1.1.8 Robustness

When some nodes are compromised the entire network should not be compromised.

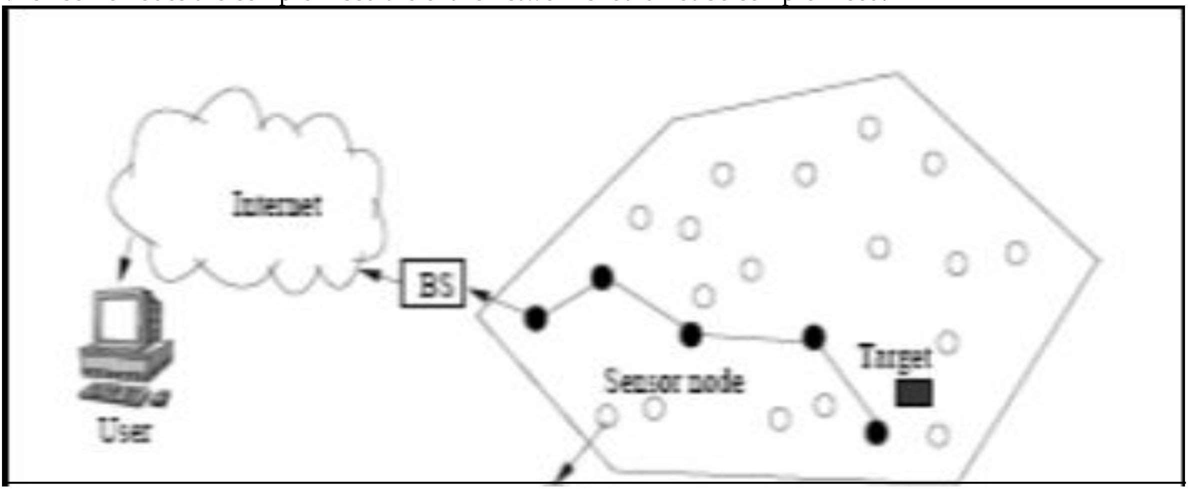

Fig. 1.1 Wireless Sensor Network

2. SECURITY PROTOCOLS

In this chapter,TinySec, SPINS, LLSP and LISP are described.

2.1 LiSP (Light Weight Security Protocol)

LiSP is a light weight security protocol for a broad –level network in WSN. Lisp divides the entire network into sensing groups or clusters and a group header (GH) is elected for each group. Lightweight security protocol (LiSP) provides a feature of rekeying which makes a settlement between security and resource consumption. With the novel rekeying protocolLiSPperiodically renews the shared key. [12]This method is used to solve the key[10] stream-reuse problem and maximize the scalability/energy efficiency.According to Park and shin large number of nodes is divided into small cluster, and a head for each cluster is selected and a key server also.LiSP is used to provide key management of small network along with large network environment. LiSP are having some characteristics which are:

- ➢ Ack need not to be sent since it uses an effective key to broadcast.
- ➢ In key broadcasting implicit authentication is provided by LiSP.
- ➢ In this it is possible to restore the lost keys.
- ➢ In this key is changed without need of recreating them during transmission.

Lisp uses cryptographic algorithm for key renewable application and stream cipher rather than block cipher technique for efficient/ fast processing.[10] Lisp can work in minimal broadcast media so it needs very less time synchronization and thus this is very flexible. To find petty movements in the network Lisp uses intrusion detection system (IDS).

2.2. TinySec (Link Layer Protocol)

TinySec protocol comes in the link layer security architecture that has been combined with the Tiny OS version which is developed by the University of Berkeley.[4] Due to broadcast nature, wireless network become insecure so TinySec maintain a network which provides a way for secure communication. Link layer architecture disclose "bad" data packets directly and „Save resources. TinySec Provides security in two ways first is encryption with identity authentication and other is only authentication.[7] In identity authentication method data is encrypted and a message authentication code (MAC) is added to the data package. While in only authentication method encryption on data does not performed but using MAC, [11]data package is realized. In Tiny Sec security protocol, authentication of data package is must but encryption of package is not mandatory because it depends on the running application. In the encryption method of data, Skipjack block encryption, code block chaining (CBC) and 8-bit initialization vector (IV) are needed.[6]

2.3 SPINS

SPINS the security protocol, developed by Berkeley University contains two secure protocols: SNEP and µTESLA. SNEP protocol provides Data authentication between two party, data confidentiality and data freshness. µTESLA is used to provide identity authentication broadcasting. [9]
SNEP contains the below properties:

2.3.1 Semantic Security

In semantic security during the information transmission in wireless environment message is encrypted each time when it is send to other node but attacker cannot steal the information whether it has obtain the same encrypted copy of message multiple times.

2.3.2 Identity/Data Authentication

The receiver can assure that the message has come from the authenticated sender verifying the Message authentication code (MAC).

2.3.3 Replay Protection

BY using counter value in MAC stops old message to be sent again.

2.3.4 Low Communication Overhead

The counter is set at sender and receiver side. There is no need of adding the counter in the message, which provides low communication overhead. In this only 8 bytes, is added to the message.
In RF channels more energy is needed for sending data so SNEP contain another ccryptographic method to provide semantic security without additional transmission overhead. Using MAC two way authentications and data integrity approaches are achieved.

2.3.5 µTESLA

In conventional methods of security, asymmetrical approach is used for identity authentication. Here at the sender side message package have sent with MAC address by using a key, which is only known by it-self and one way function is also used for broadcasting. The key to thismessage is sent after a certain time Broadcast. So there is no possibility of data package modification. At the receiver end, by using same key data is authenticated and kept into the buffer memory. In this process for encrypting the data package, RC5 is used. This recognition for the certification process,[9] Tesla required synchronization between sender and receiver, even if it is free. Adrian Perrig et al. proposed µTESLA to overcome some efficiency of TESLA in sensor network, some of which are present below-

- µTESLA requires symmetric mechanisms for authentication while TESLA verifies the data packages with Digital signature but for sensor nodes digital signature is more costly.
- Too much energy is required for sending and receiving to disclose a key in each packet. µTESLA discloses the key once per epoch.
- To store a one way key chain is expensive in a sensor node. µTESLA helps to restrict the number of authenticated senders.

2.4 LEAP (Localized Encryption and Authentication Protocol)

LEAP is proposed by Sencun Zhu, which is a key management protocol used in sensor network. Since LEAP gives the basic security services like authentication and confidentiality. So it provides a secure communication in sensor network. To meet the different performance requirements and security levels LEAP can be used to meet the difficulties of sensor networks.[8]
Characteristics of LEAP:

- Leap predicted about single keying mechanism and concludes that, it is not convenient to provide a secure communication in wireless network. So LEAP creates four types of keys for each sensor node.
  - **Individual key**-The Individual key which is a unique key shared between a node and its correlative base station to provide security.
  - **Group Key**–This key is also known as the global key. Group key is mutual for all the sensor nodes within the network. Group key is used to encrypt the data that is broadcast to all the nodes.

- **Pair wise key**- Key which is common for a node and its neighbour sensor nodes.
- **Cluster Key-** Key which is common for a node and its multiple neighbour sensor nodes.

➢ LEAP can prohibit security attacks on sensor networks. Key establishment feature of LEAP makes it more efficient and storage requirement are also decreased. LEAP is feasible for the current generation sensor nodes.

➢ LEAP adds an efficient protocol for local broadcast authentication based on the use of one-way key chains.

2.5 LLSP (Energy Efficient Link Layer Security Protocol)

LLSP is link layer security protocol provides message authentication, access control, message confidentiality, and replay protection. LLSP follow the concept of Tiny Sec. LLSP have capacity of early rejection and provides low performance overhead.

Table-2.1 Comparison of Different Security Protocols

Features/ Protocol	Key Management	Overhead	MAC Used	Security Requirement			Application
				Encryption	Authentication	Integration	
LISP	Symmetric	Variable	YES	Stream Cipher	MAC	MAC	Used when security is required between node to group head.
SPING	Symmetric	8 bytes	YES	--	CBC-MAC/Hash function	MAC	Small size Network. µTESLA used to made authenticated routing between node to base station
TinySec	Any	4 bytes	YES	CBC-RC5	CBC-MAC	CBC-MAC	In network processing and local broadcast
LEAP	Pre-deployed	Variable	YES	MAC	MAC	MAC	End to End application, Prevent from attacks.
LLSP	Any	-	YES	AES-CBC	MAC	CBC-MAC	In n/w processing and local broadcast. Resource constraint environment can be combined with higher level security

3. DIFFERENT PSEUDO RANDOM NUMBER GENERATOR ALGORITHM

Security is wireless sensor network bound with its resource scare nature. For dynamic key generation pseudo random generators are used. In the following section some mostly used pseudo number generators are discussed and a comparison for the same is also presented in table.

3.1 Park – Miller Algorithm

Park-Miller the random generator algorithm is employed to supply 32-bit sequences of key. The Park-Miller having these three subsequent criteria to supply smart pseudo random numbers-
Sequence full amount, sequence is satisfactorily Random, efficient Implementation with 32-bit arithmetic. 32 – bit sequence key plays an important role in stream cipher encryption and decryption. "In cryptography, a stream cipher is asymmetric key cipher wherever plaintext digits are connected with a pseudo random cipher digit [2] Stream (key stream). In an exceedingly stream cipher every plaintext digit is encrypted one at a time.

3.2 Blum Blum Shub Algorithm

This algorithmic program is additionally used to produce the pseudo number generator[2].This algorithmic program planned by Lenore Blum, Manuel Blum and Michael Shub therefore it named as Blum BlumShubrandom number generator.
This algorithmic program uses 2 large prime numbers. The generator isn't applicable to be used in simulation as a result of its takes time when large amount of information are here.
This algorithm is provably secure because using

➢ Euler's criterion
➢ Legendre symbol

- Jacobi symbol,
- Composite quadratic residues

The basic concern of this algorithm is used in probabilistic public key encryption. It essentially produces the key stream during encryption and decryption process.

3.3 RC4 Algorithm

RC4 random number generator generates a pseudo random key stream that's accustomed generate the cipher text. This formula referred to as pseudo random number generator as a result of it generates a sequence of numbers that satisfy the properties of random numbers.
RC4 algorithm having two components-

- Key scheduling algorithm.
- Pseudo random number generation algorithm.

The key stream contains 256 bytes array. Once array has been initialized and shuffled with the key scheduling algorithm, it's used and changed within the pseudo random generation formula to come up with the key stream. Symmetric key encryption method is used in RC4 which is a stream cipher. This formula utilized in SSL and TLS between internet browsers and servers. key scheduling algorithm is generally used to produce the state array. In this 256 bytes array is used,value of array area is same as their index.

3.4 Wichman Algorithm

Wichman Hill. Security could be a huge issue in wireless network in WSN device nodes are Communicate through wireless medium, it has the distributed nature of these reason and preparation in remote space these networks are susceptible to security attacks that have an effect on the correct functionality of the device network. Major application of device network is in military and civilian application that contains some sensitive data if correct security algorithmic program isn't applied over it than certified knowledge is accessed by intruders and attackers. Any algorithmic program that is a part of any security technique contains two elements. one is the message given by user and second one is the key. Key plays a vital act in secret writing. pseudo random number is used to generate the key.

CONCLUSION

Wireless sensor Network is a new technology used for surveillance in different areas. They are resource scare networks with highly venerable to security due to using less secured wireless medium. A Lightweight Security protocols are used for wireless sensor network. These protocols use dynamic key and random number generator also used to generate the random number for the dynamic key. In this paper a survey of lightweight protocol is discussed and a random number generator process is also discussed.

REFERENCES

[1] Sen J, Security in wireless sensor network, in wireless Sensor Networks: Current Status and FutureTrends,2012.

[2] Stallings W., Cryptography and Network Security, Prentice Hall, 4th edition, 2005.

[3] AkyildizI. F., SuW. SankarasubramaniamY., and Cayirci E. Wireless sensor networks: A survey, Computer Networks Journal, Elsevier Science, Vol. 38, No. 4, pp 393– 422, March 2002

[4] LighfootL. E.,Ren J., and Li .T, : An energy efficient link-layer security protocol for wireless sensor networks, in Proceedings of the IEEE International Conference on Electro/Information Technology (EIT ’07), pp. 233–238, Chicago, Ill, USA, May 2007.

[5] Sun Bo, Li Chung-Chih, Kui Wu, Xiao Y.: A lightweight secure protocol for wireless sensor networks, ELSEVIER, computer communication, 29 (2006) 2556–2568.

[6] D. Alsoufi, E. Khaled, A. Tariq and N. Ahmad: Security in wireless Sensor Network, International journal of computer Science and Engineering Survey, vol 3, no. 3, June 2012.

[7] C. Karlof, N. Sastry, and D. Wagner,: Tiny Sec: a link layer security architecture for wireless sensor networks, in 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, 162 – 175.

[8] S. Zhu, S. Setia, and S. Jajodia.: Leap: efficient security mechanisms for largescale distributed sensor networks, In CCS ’03: Proceedings of the 10th ACM conference on Computer and communications security, New York, USA, 2003, 62–72.

[9] Perrig A., Szewczyk R., Wen V., Culler D., and J. D. Tygar. SPINS: Security protocols for sensor networks. In Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001), July 2001.

[10] T. Park and K. G. Shin: LiSP: a lightweight security protocol for wireless sensor networks, ACM Transactions on Embedded Computing Systems, vol. 3, no. 3, pp. 634–660, 2004.

[11] Ojha A., jainK.: A Survey on Lightweight Security protocol using Dynamic Key for Wireless Sensor Network, International journal of advance research in computer science and communication engineering, vol. 3, Issue 9, September 2014.

[12] Ojha A., jain K.: Implementation of LiSP using Park – Miller for Wireless Sensor Network, International journal of Computer Applications, vol. 110, No. 8, January 2015.

DOI Number: https://doi.org/10.30780/specialissue-ICRDET-2019/003