IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Volume-3, Issue-9 E-ISSN: 2347-2693

A Study on Security issues in Wireless Sensor Networks

S.Ranjitha[1*] and D. Prabakar[2] and S. Karthik[3]

[1*, 2, 3] *Department of CSE, SNS College of Technology, Coimbatore, India*

www.ijcseonline.org

Received: Aug/22/2015 Revised: Aug/24/2015 Accepted: Sep/23/2015 Published: Sep/30/2015

***Abstract*—** Wireless Sensor Network (WSN) is a technology that shows great promise for various futuristic applications both for public and private sectors. Its shows by few applications like disaster management system, battlefield environment and etc. In this connection many issues are considered among that Security is the main issue in the WSN. Unauthorized access in an entire networks leads to dilute the security. For providing security to this network between the nodes, we need some specialized algorithms. Previously many more algorithms are used to provide either data security or network security. Cryptographic strategies and Secure Algorithms are the key factor to ensuring that either data transmission or data handling between nodes are occurred securely. Id (Identity) Based Cryptography and Public Key Cryptography are the types of cryptography which are used to provide security to the data based on sharing keys between sender and receiver in the network.

***Keywords*—** Cryptography, Id Based Cryptography, Public Key Cryptography, Security, Wireless Sensor Network.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a self organization network and is a collection of number of sensor nodes which are used to collect environmental information and send that information to sink or base station. From the base station user can gather those information for further consideration (Figure 1). In WSN sinks may be static or dynamic. For some applications static sink used as battlefield environment and disaster management system is used as a dynamic sink.

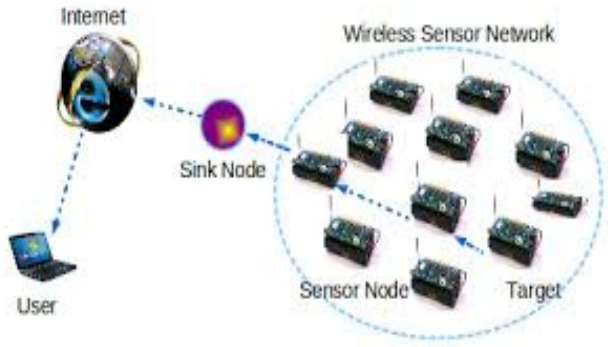

Figure 1: Architecture of WSN

Sensors are inexpensive but those have limited battery power and limited resources. The main characteristics of WSN are Low cost, Ease of use, Scalability, Mobility of nodes, Ability to cope with node failures [5].

Applications of WSN are Forest fire detection, Military, Industrial monitoring, Healthcare monitoring and Vehicle tracking and detection.

Security is one of the issues in WSN. That affects the performance of the network. Without providing security to the data which can be alter or misuse. So security requirements can be affected. The security requirements [10] are listed below,

- Confidentiality
- Integrity
- Authentication
- Availability

- **Confidentiality** means protect the data or information from the unauthorized persons. For example, in military application secret data are transferred between the soldiers. So they keep the data as confidential.
- **Integrity** means ensures that a data is not modified during transmission.
- **Authentication** means ensures the identity of the message or person by its origin. For providing authentication shared key is used.
- **Availability** means ensures that services and information can be accessed at the time they are required. In WSN many risks can be occur due to loss of availability such as denial of service attacks.

Security can be provided to the data by applying cryptography technique. Cryptography contains of two main processes like encryption and decryption. Cryptography is used to hide the original data and transferred to secret data which process can be known as Encryption. The original data is known as plain text and secret data is known as cipher text. Again the cipher text can be transferred to plain text which process is known as Decryption. Keys are used for cryptography process. Based on the keys, the

cryptography technique can be classified. Symmetric key, Asymmetric key and Hash functions cryptography.

- Symmetric Key Cryptography uses same or single key for both Encryption and Decryption.
- Asymmetric Key Cryptography uses different keys which are public and private key.
- Hash functions use mathematical transformations.

II. ISSUES IN WSN

The issues [2] that affect the network design and performance of a wireless sensor network are as follows:

- Architecture
- Localization
- Quality of Service
- Medium Access Schemes
- Data Aggregation and Data Dissemination
- Security

III. SURVEY ON SECURITY ALGORITHMS

There are many algorithms and protocols used to provide security during data transmission. Cryptography techniques are one of the key aspects to provide security. Cryptography is a method of storing and transmitting data in a particular form so that only the known person can read and process it. In that some of the algorithms and protocols are discussed in this survey.

A. RSA ALGORITHMS

In 1977, Ron Rivest, Adi Shamir and Leonard Adleman who first described this algorithm. RSA algorithm is a public key cryptography technique and is an asymmetric cryptography method. Asymmetric cryptosystem use the public key and private key for encryption and decryption for provides security to the data. This method use the key based systems and digital signature also.RSA algorithm key length be not less than 1024bits [4].

The parameters used for RSA and Key generation:

1. Private Key- The two big prime numbers p and q chosen
2. Public Key-Calculate the n value, ie n=pq and calculate φ (n) = (p-1) (q-1)
3. Select public exponent *e* such that 1 < e < φ and gcd (e, φ) = 1
4. Private Key – calculate $d = e^{-1} \bmod \varphi$
5. Public key is (n, e) and private key is d

For Encryption: $c = m^e \pmod n$.
For Decryption: $m = c^d \pmod n$.
For Digital signature: $s = H(m)^d \bmod n$, Verification: $m' = s^e \bmod n$, if m' = H (m) signature is correct. H is a publicly known hash function.

The advantages of RSA algorithm are simpler security architecture and do not require a shared key. The disadvantage is asymmetric cryptosystem is much slower than symmetric cryptosystems.

B. ECC (ELLIPTIC CURVE CRYPTOGRAPHY)

Elliptic Curve Cryptography (ECC) was proposed in 1985 by Neal Koblitz and Victor Miller.ECC is also a public key cryptography technique and is an asymmetric cryptography method. In this method public key is distributed to all and private key is known by particular user only. The mathematical operation of ECC is defined over the elliptic curve $\mathbf{y^2 = x^3 + ax + b}$, where $\mathbf{4a^3 + 27b^2 \neq 0}$.

Each value of the 'a' and 'b' gives a different elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC.

The key length of ECC is 160 bits which gives the same security level of 1024 bits of RSA Algorithm. Symmetric key algorithm provides only confidentiality but the asymmetric key algorithms provide more than that of confidentiality. The security is based on the difficultly of a problem [8].

The advantages of ECC are smaller key size, speed and efficient use of power consumption.

C. OHC (ONE WAY HASH CHAIN)

One Way Hash Chain is one of the cryptography techniques. OHC is used for provide authentication. In OHC, serious of hash functions used. Each data packet contains the unique hash number which is broadening through all over the network for making the data transmission as authenticate. This method is used between the base station and other nodes for provide better security. Control packet is spread over the network from base station. This control packet has the hash number and message authentication code. After creation of hash number and get this number by all the nodes the transmission can take place as secure. OHC is also used for make the data as freshness and increase the security level. This is also used for repair the broken path in the network by using hash number [7].

The advantages of OHC are providing authentication, data freshness and re-initialize the broken path.

D. RING SIGNATURE

Ring signature is used to provide the authentication. Ring is used in this scheme. In the ring pair of public key and private key is used. A signer node produces the signature by them using private key. By using the public key, corresponding ring members can identify the signature of the message. After generation of signature, that can be verified for the message. Ring signature is the strongest unforgeability technique because any non ring member trying to use a ring signature that can be negligible. Ring signature also provides the privacy of the data. Privacy means protect the information from public access [1].

The advantages of ring signature are providing authentication and privacy using signature.

E. SECURE ROUTING PROTOCOLS

There are many numbers of secure routing protocols available. From that Combination of LEACH and ESPDA provide the security to the data. LEACH means Low-Energy Adaptive Clustering Hierarchy protocol which provides the energy efficient. Enhancement work of LEACH is SLEACH, SecLEACH [6]. SLEACH is a Secure LEACH which is the first protocol to add security concept to the LEACH. Symmetric Key is used by this method. SecLEACH is a enhance work of SLEACH which is also provide the efficient security. SecLEACH use the random key pre-distribution scheme.

Energy-efficient and Secure Pattern based Data Aggregation (ESPDA) is a LEACH based secure routing protocol. ESPDA is working in a Cluster based WSN. In this method, sender sends the pattern code first which is the representative of sensed data to the Cluster Head (CH). After collecting the pattern codes, CH compares the codes and identifies the unique one. Then CH sends request to the sender for data. By the combination of LEACH and ESPDA which provide the energy efficiency and security to the data [3].

The advantages of LEACH based security protocol provide lots of energy efficient features and also security to the data.

F. SECURE AND EFFICIENT DATA TRANSMISSION PROTOCOLS

SET-IBS and SET-IBOOS are the secure and efficient data transmission protocols which are used for Clustering based WSN [9]. These two protocols are ID-based cryptography protocols. SET-IBS stands for secure and efficient data transmission – Identity Based digital Signature. This method use the ID as their public key and private key can be created in the data transmission shown in Figure 2. The Signature is generated at sender node and sends that to CH. After receive the signature, the node verify the validity of signature. If it is invalid then reject that message otherwise accept. Online signature is generated by using Offline signature when the message has been known. SET-IBOOS is faster compare to the IBS method.

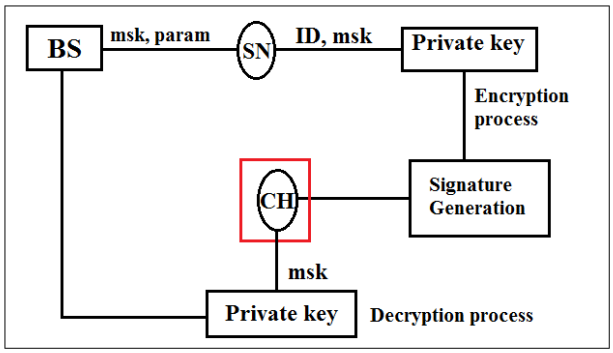

Figure 2. SET-IBS

SET-IBOOS stands for secure and efficient data transmission - Identity-based online and offline digital signature. This protocol is used to reduce the computational overhead and storage cost of digital signature. This method uses the Online and Offline signature. Generation work of Offline signature (Figure 3) is faster which performs easily and effectively.

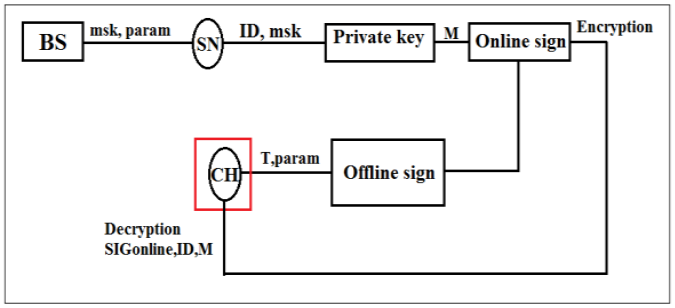

Figure 3.SET-IBOOS

The advantages of SET-IBS and SET-IBOOS are providing authentication to the data. SET-IBOOS minimize the computation overhead and storage cost.

IV. CONCLUSION

In WSN security is one of the main issues for both data transmission and network. In this paper, we considered necessity of requirements and algorithmic approach to resolve security issue in WSN. We had made a brief

discussion on various algorithms and protocols to ensure that security during data transmission and network. Among the different methods asymmetric cryptography provides the better security and enhanced approach when compared to symmetric cryptography along with signature schemes are one of the best security providence.

REFERENCES

[1] Ashmita Debnath, Pradheepkumar Singaravelu and Shekhar Verma, "Privacy in wireless sensor networks using ring Signature", Journal of King Saud University – Computer and Information Sciences, Page No (228-236), **2014**.

[2] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar, "Issues in Wireless Sensor Networks", Proceedings of the World Congress on Engineering, London, U.K, **2008**.

[3] Triana Mugia Rahayu, Sang-Gon Lee and Hoon-Jae Lee, "A Secure Routing Protocol for Wireless Sensor Networks Considering Secure Data Aggregation", Sensors, **2015**.

[4] Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", American Journal of Engineering Research (AJER), Volume 03, Issue 01, Page No (50-56), **2014**.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing, Department of Computer Science, Wayne State University, **2006**.

[6] Cam H, Ozdemir S, Muthuavinashiappan D, Nair P, "Energy efficient security protocol for wireless sensor networks", In IEEE VTC Fall Conference, October **2003**.

[7] Rudranath Mitra, Tauseef Khan, "Secure and Reliable Data Transmission in Wireless Sensor Network: A Survey", International Journal Of Computational Engineering Research(IJCER), Volume 02, Issue 03, Page No (748-754), June **2012**.

[8] Asha Rani Mishra, Mahesh Singh, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network", International Journal of Engineering Research & Technology (IJERT), Volume 01, Issue 03, May **2012**.

[9] Sandhyarani.B.H, Nagnath Biradar, T.S.Vishwanath, "An Authenticative Way to Data Transmission for Cluster Based Wireless Sensor Network", International Journal of Research in Engineering and Technology (IJRET), Volume 04, Special Issue 05, Page No (26-29), May **2015**.

[10] M.C.Swathi, A.Dhasaradhi and P.Nirupama, "Providing Efficient and Secure Data Transmission in CWSNs", International Journal of Advance Research in Computer Science and Management Studies (IJARCSMS), Volume 02, Issue 11, Page N0 (75-83), November **2014**.

