International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 02, February-2016

WSN Security: An Asymmetric Encryption and Hash Function based Approach

Anita Daniel. D
Research Scholar
Faculty of Electrical & Electronics,
Sathyabama University,
Chennai-600119, India.

Emalda Roslin. S
Faculty of Electrical & Electronics,
Sathyabama University,
Chennai-600119, India.

***Abstract*— Wireless Sensor Network (WSN) security is important for various futuristic applications like military, nuclear power plant, health care etc., In these applications the security is considered along with the additional challenging tasks such as low energy consumption, low computation capability and limited memory. In this paper a detailed investigation on the security related issues and challenges in WSN based on an asymmetric approach are made. Also an overview on various security frameworks based on asymmetric encryption and hash function is given.**

Keywords*— *Wireless Sensor Networks, Asymmetric Encryption, Security, Survey, Frameworks.

I. INTRODUCTION

A wireless sensor network (WSN) is a novel technology to monitor physical or environmental conditions such as radiation level, temperature, sound, pressure etc. and to cooperatively pass their data to main location. WSN is especially attractive for installing additional sensors in existing plants and remote locations. Building a WSN is usually less expensive than a wired system due to savings in cabling and deployment time [13].

Deploying a wireless sensor network in a nuclear facility or in battle field surveillance is challenging because of the high data reliability requirement and a potentially harsh environment. Securing the communications in these applications is a very important issue just because of the consideration of active and passive attacks. Passive attacks attempt to retrieve vulnerable information and active attacks attempt to disrupt operation [14].

It is necessary to provide security at every point of the network and cryptography can be used for security but the cryptographic algorithms should be designed to use less memory, less power and less energy so the network lifetime can be increased [3][4].

Cryptographic techniques can be classified into three types: 1.Symmetric cryptographic techniques 2.Asymmetric cryptographic techniques 3.Hybrid cryptographic techniques.

In Symmetric cryptographic techniques, same cryptographic key is used between the two communicating nodes both for encryption and decryption. This cryptographic key has to be kept secret in the network and this technique is preferred due to its ease of implementation on hardware and small energy requirements. Since there is no cryptographic key transmitted with the message, the chances of message being decrypted are null. A system only which possesses the shared secret key can decrypt a message. Symmetric cryptosystems have a problem of key distribution. The key should be transmitted to the receiving end before the actual message is transmitted. It is insecure when communication channels are used to transmit the key and also this technique cannot provide digital signatures that cannot be repudiated [3],[4] and [5].

In asymmetric cryptographic technique, a private key can be used to decrypt and sign message while a public key can be used to encrypt and verify the message. The private key needs to be kept secret while the public key can be published freely. This technique increases the security because the private keys do not ever need to be transmitted or revealed to anyone. It is also known as Public key cryptography. In this technique, there is no need for exchanging keys, thus eliminating the key distribution problem [6].

Hybrid cryptographic techniques are based on the combination of two approaches; symmetric cryptography and asymmetric cryptography [3].

This paper describes an asymmetric cryptographic technique which is used where more security is needed. Since key management consumes more battery power, energy preservation is a primary concern for achieving WSN security. Though considerable research is carried out in this area, an efficient encryption technique for managing keys is yet to be evolved [9].

In this paper a detailed investigation on the security related issues and challenges in WSN based on asymmetric approach are made.

This paper is organized as follows. Section 2 describes some of the security related issues and challenges in WSN. Section 3 discusses on various existing asymmetric encryption and hash based approaches in WSN. Section 4 concludes the paper by highlighting future scope of our work.

II. SECURITY ISSUES AND CHALLENGES IN WSN

WSN finds a wide range of different applications require different security requirements. For example, in temperature monitoring application, the safety requirements are not very important. But in radiation analysis near a nuclear power plant requires all the security requirements which are given below.

As the security techniques are getting evolved, the types of intrusion and spoofing attack mechanisms also are getting increased. The goal of security schemes in WSNs is to provide protection for the data even when the intervention of various attackers are present, with less energy usage and increased network lifetime. An asymmetric encryption method is used to achieve more security as well as it should avoid all types of attacks given below [10].

A. Types of Attacks in WSN

- Denial of Service: is an attack meant to shut down a network, making it inaccessible to its intended users.
- Jamming attack: is an attack to jam a node or set of nodes.
- Sybil attack: A malicious node forges the identities of more than one node in the network is the Sybil attack.
- Black hole/Sinkhole Attack: Malicious node acts as a black hole and that node inserts itself between the communicating nodes and it is able to do anything with the data passing between them.
- Hello Flood Attack: Uses HELLO packets as a weapon to convince the nodes in WSN.
- Wormhole Attack: Attacker records the data at one location in the network and tunnels those to another location.
- Replay Attack: To degrade the network performance, an attacker copies a forwarded packet and later sends out the copies repeatedly and continuously to the victim node.
- Impersonate attack: An attacker node impersonates another node's identity to establish a connection with a victim node [8][15].

B. Security requirements

Security requirements in WSNs include availability, authentication assurance, freshness, confidentiality and integrity [3].

- *Confidentiality:* omission of data leaks to neighboring networks.
- *Integrity:* non altered transmission of data.
- *Authenticity:* verification of sender/receiver.
- *Availability:* ensures the survivability of the network despite denial of service attacks.
- *Freshness:* ensuring data is recent while allowing for delay estimation [12], [13] and [15].

III. Existing Asymmetric Encryption and Hash Function Based Approaches

A. Elliptic Curve Cryptography(ECC)

ECC method is used for an application where more security is needed but lacks the power, storage and computational power. ECC is a public-key crypto technique just like RSA, Rabin, and ElGamal. In this technique every user in the network has both a public and a private key. For encryption/signature verification public key is used. Like that for decryption/signature generation private key is used. These methods are used as an extension to other current crypto techniques such as

- Elliptic Curve Diffie-Hellman Key Exchange
- Elliptic Curve Digital Signature Algorithm

Both sender and receiver must agree to some publicly-known data items

- The elliptic curve equation $y^2 = x^3 + ax + b$
  - values of *a* and *b*
  - prime, *p*
- The elliptic group is computed from the elliptic curve equation
- A base point, B, taken from the elliptic group

Each user generates their public/private key pair

- Private Key = an integer, x, selected from the interval [1, p-1]
- Public Key = product, Q, of private key and base point
  - (Q = x*B)

The main advantage of using ECC cryptosystem is to protect a 128 bit AES key it would only take an ECC key size of 256 bits whereas RSA Key Size would be 3072 bits [7], [8].

B. Hash Function

Unlike private key and public key algorithms, hash functions also called message digests or one way encryption, have no key. The major application of Hash function in cryptography is message integrity. The Hash value ensures that the message has not been altered by an intruder or by other means. Hash can be used any time to prove message integrity [5], [6].

C. MAC

A Message Authentication Code (MAC) also called a Keyed (Cryptographic) hash function protects both a message's data integrity as well as authenticity. MAC values are generated and verified using the same secret key [1], [2] and [3].

D. HMAC

HMAC (Hash based Message Authentication Code) is a MAC based on cryptographic Hash function with a secret key and the size of the secret key defines the cryptographic strength of HMAC [4].

Many studies have evaluated performance of cryptographic techniques in WSNs, but there is no standardization in the performance analysis. Existing cryptographic techniques using asymmetric encryption and hash function based approaches are tabled below.

TABLE 1: DETAILED INFORMATION ABOUT AVAILABLE ASYMMETRIC ENCRYPTION AND HASH BASED APPROACHES FOR WSN

Author/ Year	Techniques used	Keys used	Security provided
Joyce Jose et al.,2013	MAC	Varying encryption key for each session	It reduces the replay attack and the frequency of node compromising attack.
Liehuang Zhu et al.,2014	MAC, Result Checking Mechanism	Light weight homomorphic encryption.	It provides end to end confidentiality.
Gopi Saminathan et al.,2013	MAC and ECC	Secret Key and Public Key	It is resistant to replay attacks, node compromising attacks, impersonation attacks
Yonglei Yao et al.,2014	HMAC	Master key and pseudo random function	Sensor nodes data is protected from other nodes, aggregator, sink and an eavesdropper.
Reza Soosahabi et al.,2014	Probabilistic encryption method	Stochastic cipher matrix key	Data confidentiality is provided in the presence of passive eavesdropping
Madhumita Panda 2014	RSA and ECC	Public and Private key	It provides a good trade- off between key size and security
Shih-I Huang et al.,2009	Irreversible hash function	Random keys	It is resilient to Known- plaintext attacks, chosen-plaintext attacks, cipher text-only attacks and man-in-the-middle attacks

IV. CONCLUSION

In this paper, the importance of encrypting data in WSN is discussed, as the number of attackers, and spying attempts on private data have recently been increased. Thus, it is mandatory to think of new ways to overcome this problem as designing a framework with more security. In this field, research and development is needed for e.g., to track the performance of nuclear plant sensors where it needs more security with less energy consumption. Existing techniques are ECC, MAC and HMAC etc. to provide more security. But with this technique it is necessary to overcome the limitations of the sensors. Performance analysis of all these schemes with energy calculation will be considered as a future work.

REFERENCES

[1] Joyce Jose, M Princy and Josna Jose, “EPSDA: Energy Efficient Privacy preserving Secure Data Aggregation for Wireless Sensor Networks” , International Journal of Security and Its Applications Vol. 7, No. 4, July, 2013.

[2] Liehuang Zhu,Zhen Yang, Jingfeng Xue and Cong Guo, “An Efficient Confidentiality and Integrity Preserving Aggregation Protocol in Wireless Sensor Networks”, Hindawi, International Journal of Distributed Sensor Networks, Volume 2014, Article ID 565480.

[3] Gopi Saminathan and S. Karthik, “Development of an energy efficient, secure and reliable Wireless Sensor Networks Routing Protocol based on Data Aggregation and user Authentication” , American Journal of Applied Sciences 10 (8): 832-843, 2013.

[4] Yonglei Yao, Jingfa Liu and Neal N. Xiong, “ Privacy-Preserving Data Aggregation in Two-Tiered Wireless Sensor Networks with Mobile Nodes”, Sensors 2014, 14, 21174-21194.

[5] Reza Soosahabi and Dmitri Perkins, “Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Networks”, IEEE Transactions On Information Forensics And Security, Vol. 9, No. 3, March 2014.

[6] Madhumita Panda, “Security in Wireless Sensor Networks using Cryptographic Techniques”,American Journal of Engineering Research (AJER) 2014 Volume-03, Issue-01, pp-50-56.

[7] Shih-I Huang, Shiuhpyng Shieh and J.D.Tygar, “Secure encrypted-data aggregation for Wireless Sensor Networks”, Springer May 2009.

[8] Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, Feb. 20- 22, 2006 ICACT2006.

[9] Khawla Naji Shnaikat and Ayman Ahmed AlQudah, “Key Management Techniques in Wireless Sensor Networks”, International Journal of Network Security & Its Applications (IJNSA) Vol.6, No.6, November 2014.

[10] Madhav Bokare and Anagha Ralegaonkar, “Wireless Sensor Network: A Promising Approach for Distributed Sensing Tasks”, Excel Journal of Engineering Technology and Management Science, Vol1, No:1, 2012.

[11] Gaurav Sharmaa, Suman Balaa and Anil K. Vermaa, “Security Frameworks for Wireless Sensor Networks-Review”, 2nd International Conference on Communication, Computing & Security- Procedia Technology 6 (2012) 978 – 987.

[12] Reshma Patil and Prof.Sharmila.M.Shinde, “Secure Energy Efficient Routing in Wireless Sensor Network-A Survey on Existing Techniques”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.

[13] K.Venkatraman, J.Vijay Daniel and G.Murugaboopathi, “Various Attacks in Wireless Sensor Network: Survey”, International Journal of Soft Computing and Engineering (IJSCE), Volume-3, Issue-1, March 2013.

[14] Muhammad Waseem Khan, “SMS Security in Mobile Devices: A Survey” , Int. J. Advanced Networking and Applications Volume: 05, Issue:02,Pages:1873-1882(2013).

[15] Anita, D.D and Emalda, R.S, “A review on existing security frameworks with efficient energy preservation techniques in Wireless Sensor Networks”, Apr 2015, ICCSP, IEEE, pg.no 0652-0662.