IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 04, Issue 03 (March. 2014), ||V3|| PP 01-04

A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security

Swapna B Sasi[1], Dila Dixon[2], Jesmy Wilson[2],
[1]*Asst. Professor, Department of Computer Science and Engineering,Jyothi Engineering College,Thrissur, India*
[2]*Department of Computer Science and Engineering,Jyothi Engineering College, Cheruthuruthy, Thrissur, India*

Abstract: - a lot of advancements are being carried out in the field of wireless sensor networks in recent years. The wireless sensor networks are employed in a variety of fields such as military, health care, industry etc. Due to the increasing acceptance of this technology leads us to consider more about the security aspects of the WSNs. To ensure the integrity and to protect data from unauthorised accesses some method of cryptographic technologies must be employed. The symmetric and asymmetric encryption techniques can be employed in the WSN architecture to provide security. The asymmetric key encryption techniques may provide a higher level of security but compared to the symmetric key encryption it causes more overheads to the sensor nodes. Another method of location based encryption which can be used along with these technologies provides an extra layer of security by restricting the cipher text to be decrypted only at a specified location. A review of all these systems is described in this paper.

Keywords: - *symmetric encryption, asymmetric encryption, location based encryption, security, data transfer*

I. INTRODUCTION

A wireless sensor network consists of a large collection of self-organised sensor nodes that detects the changes in its environments and intelligently responds to those changes. In CPSs (Cyber-Physical Systems) we exploit these WSN technologies to a great extent. The sensor node takes inputs from its environments and co-operatively passes this for further analysis. In various industries, where a network of sensors are being used for detecting the changes in temperature, pressure, etc. In the field of medicine and healthcare we make use of WSN for monitoring various metabolic activities of body. As a result, it may cause major problems if the data exchanged between any two entities underwent forging and hence it is important to consider about the security concerns of the wireless sensor networks. The messages transmitted between the sensor nodes can be made secure by using cryptographic algorithms. Cryptography is the study and practice of secure communication in presence of a third party. It constructs and analyses protocols that are helpful in overcoming the impact of adversaries.

II. SECURITY REQUIREMENTS

The security requirements of a system deals with the fields where the adversaries can influence and they are related to various aspects in information security. It includes data confidentiality, data integrity, authentication, and non-repudiation.

1.1.1 **Confidentiality:** it provides a set of rules and regulations or a promise that limits access or places restrictions on certain types of information. It conceals the messages transmitted between two communicating nodes from a third party access. The confidentiality must be ensured in WSNs to address the following issues, (i) a sensor node should not allow its readings to be accessed by any other nodes unless they are authorised to do so, (ii) the mechanism of key distribution must be extremely robust, and (iii) to protect against the traffic analysis technique, public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases.

1.1.2 **Authentication:** authentication is the action that confirms the truth of an attribute of an entity. It ensures the reliability of the message by checking the origin of a message what it claims to be. Before granting access to a limited resources or revealing information, nodes, cluster heads, and base stations must provide authentication. Authentication must face the following issues,(i) communicating node must be ensured what it claims to be, (ii) the receiver node must verify that the received packet is unambiguously came from that node itself.

1.1.3 **Integrity:** It refers to the maintenance and assurance of the accuracy and the consistency of data over its life-cycle. It is the ability to confirm that a message has not been tampered with, changed or altered while on the network. It must address the following the requirements, (i) only the nodes in that particular network must be allowed to give access to the keys, (ii) only the assigned base station should have the privilege to change the keys, (iii) provides protection against attacks those are in the form of noise.

1.1.4 **Non-repudiation:** it simply refers to the issue where the authenticity is being repudiated. It comes as an issue when the maker of a message is not able to successfully challenge the validity of the message. A good integrity service can ensure the case with non-repudiation.

Security concerns of wireless sensor networks: Due to the wide variety of application of WSNs in a various fields such as climatic change monitoring and analysis, traffic monitoring, home automation etc. the security of the messages transmitted between the sensor nodes must be ensured. Symmetric and asymmetric key encryption techniques can be used for this. But the resource constraints of the sensor node must be considered as well. The sensor nodes lacks in terms of computing, communication and battery power. Hence the cryptographic technique that is to be adopted for the WSN must be light weight, it does not incur lot of overhead to the sensor nodes. The cryptographic techniques in WSNs that are reviewed here are, symmetric key cryptography, asymmetric key cryptography and a location based encryption technology that provides an extra layer of security.

2. **Types of cryptographic techniques**: the cryptographic techniques that must be implemented in the WSN must ensure all the cryptographic requirements. The sensor nodes lacks in the resource constraints such as computational and memory capabilities.

1.1 Symmetric cryptographic techniques:

Symmetric-key cryptographic algorithm includes a class of algorithms for cryptography that uses same cryptographic key for the purpose of encryption of plain text and the decryption of cipher text. It is the oldest known encryption method. The secret key can be as simple as a number or a string of letters etc. The keys, in practice, represent a shared secret between the participating parties to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption. Symmetric-key encryption can use either of the stream cipher or block cipher, where a stream cipher encrypts the digits/bytes of a message one at a time and the block cipher take a number of bits as input and encrypt them as a single unit. The popular symmetric cryptographic algorithms include, AES, Blowfish, RC5, DES, 3DES and IDEA.

When using symmetric algorithms, same key is used for encryption and decryption by both the parties. To encrypt the data, the sender uses this key and an encryption algorithm and likewise, to decrypt the data, receiver uses the same key and decryption algorithm correspondingly [1].This key required to be kept secret to provide privacy. It is not secure any more once someone else gets to know the key. Also it is not preferred to use symmetric key cryptography where it uses a public network for sharing the key. The chance for malicious insertion and modification is higher in symmetric key cryptographic techniques. By analysing the traffic flow an intelligent attacker may decode the plain text and allows a counterfeit or new message that may look genuine to be placed in place of the original. The Symmetric algorithms are always seemed to have the advantage of not consuming too much computing power. Since only a single key is being used for symmetric encryption, symmetric encryption algorithms are always less complex as compared to asymmetric algorithms.it has an advantage of low error propagation, i.e., an error in the encryption process affects only that character as each symbol is separately encoded. Asymmetric cryptographic algorithm are dissimilar from symmetric cryptographic algorithm in the manner that they use pairs of keys; one is used for encryption and the other one for decryption in contrast to the symmetric algorithm's single key encryption and decryption.

1.2 Asymmetric cryptographic techniques:

In Asymmetric key cryptography, also known as public key cryptography, two mathematically linked keys are employed .Typically, the decryption key is kept secretly, therefore called as "private key" or "secret key", while the encryption key is called as "public key" since it is spread to everyone those who might need to send the encrypted messages [2]. It is possible for anyone having the public key to send the encrypted messages to the owner of the private key. The private key cannot be reconstructed from the public key. The idea of asymmetric algorithms was first published by Diffie and Hellmann in 1978. Some of examples for asymmetric key cryptosystem are RSA, ELGAMAL, and ECC etc.

Transport Layer Security (TLS) and Pretty Good Privacy (PGP) protocols are comprehensively utilized and brings out by the asymmetric cryptography. Ideally, they seem to be well suited for the real-world use: The risk of getting known is much less as the private key does not have to be shared. Every user only required to keep one private key in secrecy and a group of public keys that only required to be protected against being altered. Every pair of users would require having its own secret key that is shared, with symmetric ones. However, asymmetric algorithms are much slower than symmetric algorithms as it requires much more computation and therefore, in many applications, a combination of both is being used [3]. The asymmetric keys are used for authentication purposes and after this have been successfully completed; symmetric keys are produced and exchanged using the asymmetric encryption. The advantages of both algorithms can be used in

this way. Some typical examples are the DSA/BLOWFISH used by GnuPG or the RSA/IDEA combination of PGP2.

The asymmetric key cryptographic algorithms involve large mathematical calculations and therefore the time complexities are quite high. For the same key size, the average brute force search time of both the algorithms was extremely same. For symmetric key algorithms it needs a key distribution centre for the secure transmission of the key and for an asymmetric key algorithms, the service of a certification authority is required for ensuring the ownership of the public key.

Here in case of WSNs, a lot of factors need to be considered before employing an encryption method. As a sensor node has strong resource constraints the system implemented for security must not incur much stress to the sensor nodes. A symmetric cryptographic system holds this condition but the level of security that it provides is much lesser. We can see that, the asymmetric algorithms mechanism makes the procedure too slow while giving higher security to the WSN. In most of the technologies, employs a hybrid method by efficiently incorporating both of these techniques. For the purpose of sending messages, symmetric encryption technique, which causes lesser overhead, is used and for key sharing, to establish a secure communication, the asymmetric key algorithms can be employed.

A location based encryption technique can be employed for providing an extra layer of security to the WSN system. Location based encryption is a technology that can be incorporated with any existing encryption standards in order to achieve a higher level of security. For ordinary encryption technologies, they provide security by simply encrypting the data using a key. They do not place any restriction in terms of time, position or any such constraints. The term geoencryption implies including location parameters to the encryption process so that it provides an extra level of security [5]. The term location based encryption or geoencryption refers to any method of encryption that restricts the decryption to be done in a specified place. If somebody attempts to decrypt it at some other location, the decryption fails and reveals nothing about the plain text.

The node which needs to send data first obtains the location details of the receiver. Using these details the data to be transmitted is encrypted and send. For a device to decrypt the incoming encrypted message, gets its own location details via location sensors such as a GPS receiver. This method can be efficiently implemented so as to limit the right for decryption to a particular facility, i.e., the company headquarters or any particular office. Some other parameter values can also be incorporated along with it like time, velocity etc [4]. Placing a time constraint restricts the time within which the message is to be decrypted. Trying to decrypt the cipher text before or after the specified time constraint may cause the production of some invalid text patterns [6]. The velocity constraint can be added if the encrypting and decrypting nodes are mobile. The sending node considers the velocity at which the receiver node is moving and it calculates the location of the receiving node using this velocity value. The more the parameters you take the more security that you provide. There are a number of methods for improving location based encryption [4]. A few are as given below,

1) Use MAC at the end of each messages
2) Use suitable distance tolerance
3) Enhancing quality of location dependent features
4) Enhancing quantity of location dependent features

Using MAC for each message may help to preserve the integrity of the message, i.e. we can check whether any unauthorised modification has been done. The concept of tolerance distance is introduced for overcoming the inaccuracy and inconsistency of GPS receiver. The quality of parameters implies the fineness or accuracy of the parameters and the quantity of parameters refers to as the number of parameters taken for consideration.

The location based encryption technique restricts the decryption of data to a particular geographical area. It can be incorporated along with any encryption technique. The location details are used for the key generation phase of the cryptographic algorithm.

III. CONCLUSION

With the rapid growth of wireless sensor networks, strict security constraints have to be considered. As the sensor nodes follow tight resource constraints, expensive cryptographic algorithms are not always a practical solution. Choosing the appropriate cryptographic algorithm for sensor nodes is the primary need to provide security services in WSNs. This paper provides a general comparison between symmetric key cryptosystem and asymmetric key cryptosystem. A location based encryption technique, which restricts the decryption process. It can be used to improve the security features of the existing system. The information provided in this paper may be used for further researches and enhancements in the field of Wireless Sensor Networks.

REFERENCES

[1] Yogesh Kumar, Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat), Rajiv Munjal, lecturer in CSE Deptt., CBS Group of institution (Jhajjar), Harsh Sharma, Lecturer in CSE Deptt, BPR College of Engg Gohana (Sonipat), 2011, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures", IJCSMS International Journal of Computer Science and Management Studies

[2] Manish Singh, Shailender Gupta and Bharat Bhushan, YMCA University of Science and Technology, Faridabad, 2012, "Comparison of symmetric and asymmetric key cryptography: A study", Proceeding of the National Conference "Science in Media 2012" Organized by YMCA University of Science and Technology, Faridabad, Haryana (India)

[3] Lalit Singh, Dr. R.K. Bharti (C.S.E) BTKIT Dwarahat, 2013, "Comparative Performance Analysis of Cryptographic Algorithms", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper

[4] Logan Scott, GeoCodex LLC, LS Consulting, Dorothy E. Denning, GeoCodex LLC, Naval Postgraduate School, 2003, "A Location Based Encryption Technique and Some of Its Applications", proceedings of the 2003 National Technical Meeting of The Institute of Navigation

[5] Karimi, R. , Dept. of Comput., Islamic Azad Univ., Qazvin, Iran , Kalantari, M.,2011, "Enhancing Security and Confidentiality in Location-Based Data Encryption Algorithms", Roedunet International Conference(RoEduNet)

[6] Shraddha D.Ghogare, Swati P. Jadhav, Ankita R. Chadha, Hima C. Patil, 2012 "Location Based Authentication: A New Approach towards Providing Security" International Journal of Scientific and Research Publications.