Survey on Secure Data Transmission using Crypto System in Wireless Sensor Network

P. B. Arun Prasad[1] J. Naskath Begam[2] P. Oviya[3] B. Renuga Devi[4] K. Thirunavukkarasi[5]
[1]Assistant Professor [2,3,4,5]Student
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]Saranathan College of Engineering Tiruchirappalli, Tamil Nadu, India

Abstract— The nature of Wireless Sensor networks, secure data transmission from one node to another node is becomes a big issue in wireless communication. The wireless network technologies are progressively gaining consideration. In real settings, the wireless sensor networks have been broadly applied, such as target tracking and environment remote monitoring. However, data can be easily compromised by several attacks, such as data interception and data tampering, etc. It mainly focuses on transferring data securely and presents the implementation for the cryptosystem (3-des and hash function). The secure application proposes a system to securely transmit provenance for sensor data and will introduce effective technique for secure data verification. Design the system technique and prove it efficient for secure transmission. The data can be secured and the admin can give password of network allocated. The cluster network's admin and the base station can authenticate each other and it generates three level authentication propose systems.

Key words: 3-DES, Hash Function, WSN, Secure and Data

I. INTRODUCTION

Various type of information over network several different algorithms cryptographic and other techniques are used. In this paper we discuss the network security fundamentals and how Cryptography technique is meant for wireless sensor networks. To implement a network cryptographically secure, security must be combined into every node of the network. So we need to implement security in every point of network. In WSN, cryptography algorithm should be active in nature but does not consume more memory, more power and more energy so it helps to increase the lifetime of network. But in some cases the security will be depends on the types of different application and algorithm might be particular to the application.

A. Security Requirement in WSN

1) Privacy

Privacy ensure the suppression of the information from an attacker so that any information communicated via the web should be reliable. In wireless sensor technology, the issue of privacy should have…

The technology of wireless sensor node is well known technology because of its popularity. Thousands of self-organize sensor nodes are spatially distributed autonomous sensor to monitor physical or environmental conditions, Such as temperature, sound, pressure, etc. the wireless sensor network is built of "node" – from a few to several hundred or more, where each node is connected to another sensor. There is a several portion for each sensor network node. The complex algorithm cannot be played over it, because nodes have not so wealthy in terms of resources. Hence security becomes a big issue in wireless sensor network. To securely transmit the the following constraints:

- Unless a nearest node of sensor node certified they should not allow its analyses to be recovered.
- The encryption and decryption key delivery apparatus should be really strong,
- In certain situation to defend against traffic examination attacks the open evidence such as sensor features, and public keys of the node should be encrypting for security reason.

2) Validation

Validation or authentication guarantees the reliability of the information or packets by finding its genuine source. Before allowing a limited resources or information it should verifying base station cluster nodes head and other nodes. In wireless sensor network, the problem of certification should report necessity such as:

- The node which co-operating that node will privileges to be,
- At receiver side it should be verify that the received packet should be come from authorized sender node

3) Reliability

Reliability guarantees that message has not been lost; it gives reliable communication. In a WSN, the truthfulness should have constraint:

- It must be restricted that the only base station have authority that it can change the keys and web should have authority to access to the keys. Due to this, successfully check illegitimate nodes from locating information used nearby the keys and impede informs from outdoor places.
- It should defend against an energetic, smart unauthorized node that had try and capacity to successful to costume his attack as noise .The accessibility or they must be free if a particular sensor node required that resources. In WSN, the problems of accessibility should have some constraints such as:
- The security of devices or networks should be available for any time; if there is any failure or system crashes, it should be avoided.
- To transport every packet successfully to its node the central access control system mechanism is used.

II. LITERATURE SURVEY

The security of wireless sensor network, in today's world wireless technology very fast developed and mostly used in many sectors. Hence, the necessity for security becomes very cruci0l factor. Though, the wireless network technology has some restriction such as limited battery power, processing ability, and capacity of memory storage, etc. For this constrains, many new security mechanism and technologies

have been develop to overcome this challenges. There are many technologies are available to provide security against the attackers, one of the best technology is cryptography. In paper they focus on different problem in wireless sensor network. Also study on different possible attacks on WSN. In paper "Environment Based Secure Transfer of Data in Wireless Sensor Networks", converse on the security in transformation. In past few years lack of information are spread from one place to another hence it is very important that the data should transfer securely without data loss. In paper the relative study between DES, 3DES shows that the Threefold DES simply extends the key size of DES by applying the algorithm three times in progression with three different keys, hence 3DES more leading and has high performance than DES. The paper TDES is used in various cryptographic applications and wireless protocol and security layer. The encryption algorithm DES, 3DES work better against the brute-force attack here we need solution to avoid the brute force attack and smart card loss attack.

A. Triple Data Encryption Standards

Triple DES is an upgrading of DES. It has 64 bit block size and 192 bits of key size. The encryption method is analogous to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. However, DES is only a 64 bit (eight characters) block cipher, an in-depth search of 255 steps on average, can retrieve the key used in the encryption; there is no reasonable way to break DES. For this reason, it is a mutual preparation to defend serious data using something more powerful than DES. Triple DES much more secure form of DES, Triple DES is just DES done 3 times with two keys used in a particular order; hence it is much safer than the plain DES.

A different of modes of TDES:

- DES-EEE3: Three DES encryptions with three different keys.
- DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
- DES-EEE2 and DES-EDE2: Same as the previous layouts excluding the first and third operations use the same.

Let EK (I) and DK (I) denote the DES encryption and decryption of I using DES key K correspondingly.

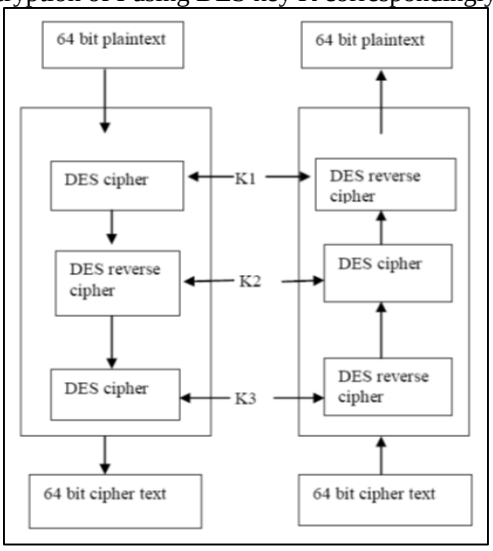

Fig. 1: Triple DES

Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations.

The following operations are:

- TDEA encryption operation: the conversion of a 64-bit block I into a 64-bit block O that is defined as follows: O = EK3 (DK2 (EK1 (I))).
- TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: O = DK1 (EK2 (DK3 (I))).

B. Architecture Diagram

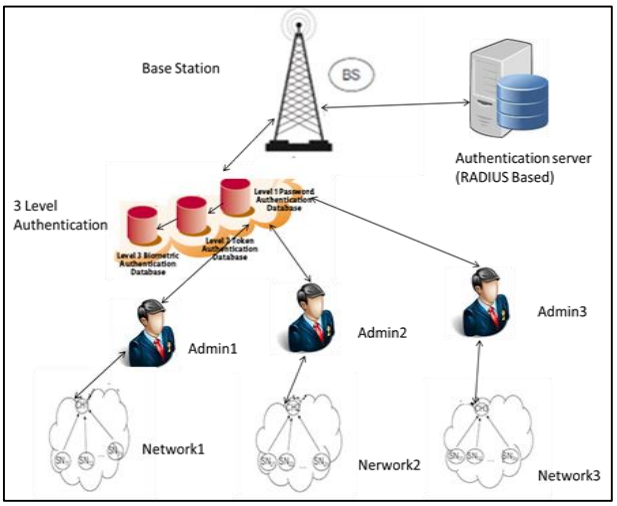

Fig. 2: Architectural Diagram

C. Description of Algorithm

Blowfish symmetric block cipher algorithm encrypts block data of 64-bits at a time.it will follows the feistel network and this algorithm is divided into two parts.

- Key-expansion
- Data Encryption

D. Key-Expansion

It will converts a key of at most 448 bits into several subkey arrays totaling 4168 bytes. Blowfish uses large number of subkeys. These keys are generate earlier to any data encryption or decryption. The p-array consists of 18, 32-bit subkeys:

P1,P2,……,P18

Four 32-bit S-Boxes consists of 256 entries each:
S1,0, S1,1,……. S1,255
S2,0, S2,1,…….. S2,255
S3,0, S3,1,…….. S3,255
S4,0, S4,1,.....S4,255

1) Generating the Subkeys

The subkeys are calculated using the Blowfish algorithm:

- Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.
- XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

- Encrypt the all-zero string with the Blowfish algorithm, using the subkeys described in steps (1) and (2).
- Replace P1 and P2 with the output of step (3).
- Encrypt the output of step (3) using the Blowfish algorithm with the modified subkeys.
- Replace P3 and P4 with the output of step (5).
- Continue the process, replacing all entries of the P array, and then all four S-boxes in order, with the output of the continuously changing Blowfish algorithm.

In total, 521 iterations are required to generate all required subkeys. Applications can store the subkeys rather than execute this derivation process multiple times.

E. Data Encryption

It is having a function to iterate 16 times of network. Each round consists of key-dependent permutation and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words.

The only additional operations are four indexed array data lookup tables for each round.

1) Algorithm: Blowfish Encryption

Divide x into two 32-bit halves: xL, xR

For i = 1to 16: xL = XL XOR Pi xR = F(XL) XOR xR Swap XL and xR Swap XL and xR (Undo the last swap.) xR = xR XOR P17 xL = xL XOR P18 Recombine xL and xR

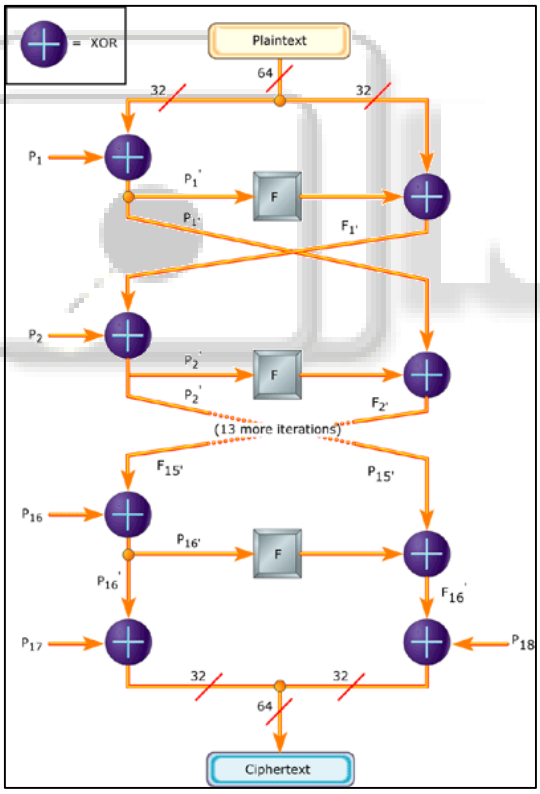

Fig. 2: Blowfish Encryption

F. Working Principle

In the WSN network each node should register their id with the master node, during the registration process using blowfish algorithm it will generate the unique number, with this id number node is register with their cluster head likewise there are number of cluster head are available which is to be connected with the master admin node. The cluster head is appointed based on their maximum value of battery power that is efficiency to send the data from node to master node. During the transmission there is a possible for hacking of information, security attacks like DOS attack, data stealing, compromising node and clone node attack. To overcome such attacks, cryptosystem is used to provide the three way authentication protocols method in WSN.

Blowfish is one of the simplest and powerful protocols for id key generations. This unique id key is stored in database of cluster node during registration. Here after that node id is taken as reference for transmitting the data from one node to another. The original data is encrypted with their key using DES algorithm. The encrypted data is transmitted in that networks, if any hackers hack the information they cannot understand what kind of data it was. It is an another way of providing security

The cluster head will get this information as encrypted format, by checking the authentication of node and the node id is store in database of cluster node and then it will be transmitted to master node. The master node receives encrypted data and the using the key value of node is used for decryption with DES algorithm, only master node can see the original data after the decryption process in between any node or attacker can steal information means they cannot view the original data.

The data transmission between nodes and calculation will take certain amount of energy in each node it is also applicable to cluster head too, Incase case the node range is reduced or any node is failure means it will be isolated from the networks. In cluster head if the node is isolated another node should act as header node it will be chosen based on the maximum value of node.

This principle of three way authentication is applied for data transmission leads to secure data transmission but the energy efficiency need for node is more and it leads the throughput of node at certain period of time. The one of the drawback is to change the cluster node from lower efficiency network and update the status of node to master node as well as each node in network. It is achieved by multicast and unicast address methods. The cluster head node will send the broadcast address method to each and every node in the network. The unicast address method is node to node ie cluster node to master node, so other network node is unaware about the network.

III. Conclusion

Trust in WSNs is still challenging field due to its dynamic nature. However it is a very rewarding area as most of the WSN applications are deployed in hostile environments such as military fields. Thse TDES, hash function algorithm can provide high security for transformation of data. TDES has better performance than DES. The electronic industry uses Triple DES to protect user content and system data. As well secrets key such as passwords is needed to be secured in computer systems for many years. Their use in encryption leaves resources vulnerable to Smart card loss attack and brute force attack.

References

[1] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no.8, pp. 2053-2064, 2014.

[2] X. Liu, H. Zhu, J. Ma, Q. Li and J. Xiong, "Efficient attribute based sequential aggregate signature for wireless sensor networks," International Journal of Sensor Networks, vol. 16, no. 3, pp. 172-184, 2014.
[3] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Parallel Computing," IEICE Transactions on Communications, vol. E98-B, no. 1, pp.190-200, 2015.
[4] A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks Limin Shen, Jianfeng Ma, Member, IEEE, Ximeng Liu, Member, IEEE, Fushan Wei and Meixia Miao
[5] R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairing," in Proc. Symposium on Cryptography and Information Security,Okinawa, Japan, pp. 26-28, 2000.
[6] M. Rezvani, A. Ignjatovic, E. Bertino et al., "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," Dependable & Secure Computing IEEE Transactions on, vol. 12, no. 1, pp. 98-110, 2015.
[7] S.S.D. Selvi, S.S. Vivek, J. Shriram et al., "Identity based partial aggregate signature scheme without pairing," in Proc. 35th IEEE. Sarnoff Symposium (SARNOFF), pp. 1-6, 2012.
[8] Nagamalleswara rao. Dasari vuda sreenivasara "Performance of multi server authentication and key agreement with user protection in network security" Nagamalleswara Rao Dasari et. al. / (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1705-1712
[9] D. Seo and P. Sweeney, "Simple authenticated key agreement algorithm, Electronics Letters, vol. 35, pp. 1073-1074, 1999.
[10] Y. Yang, S. Wang, F. Bao, J. Wang, and R. Deng, "New efficient user identification and key distribution scheme providing enhanced security," Computers and Security, vol. 23, no. 8, pp. 697-704, 2004.

