IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 19-23
www.iosrjournals.org

Performance Analysis of Sdrp for Wsn Using Diffie – Hellman Algorithm

Geetha. J[1], Jayalakshmi. J[2]
[1](PG scholar, Electronics and Communication Engineering, Saveetha Engineering College, India)
[2](Assoc prof, Electronics and Communication Engineering, Saveetha Engineering College, India)

Abstract: *Wireless Sensor Network is a group of wireless nodes exclusively designed for the continuous sensing of information at human inaccessible locates. Reprogramming is a definite need at such situations when the monitoring conditions vary according to the environmental changes or other user requirements. Insecure transmission of reprogramming code to such areas can ruin the entire operation of the network. To avoid this, Secure and Distributive Reprogramming Protocol (SDRP) was proposed for user privilege maintenance. In this paper, Diffie-Hellman key(DH) exchange mechanism is implemented as an enhancement to the existing method to further improve security between the forwarding nodes. A network simulator simulation analysis and discussion is provided for the proposed SDRP-DH.*

Keywords: *Diffie-Hellman, key exchange, reprogramming, security, sensor networks, user privilege*

I. Introduction

In recent years, wireless sensor networks (WSNs) have gained worldwide attention for use in different applications. Each Sensor node is placed across a large area of interest to sense, measure, and gather information and transmit the data to the user. The nodes are typically equipped with radio transceivers, micro-controllers, and batteries. All nodes are spatially distributed from each other. Wireless reprogramming is the process of propagating a new code image or significant commands to sensor nodes through wireless links after a wireless sensor network (WSN) is deployed. In order to remove bugs and for the purpose of adding new functionalities the most important operation in the Wireless Sensor Networks is the reprogramming process [1]–[5].

Secure and Distributed Reprogramming Protocol (SDRP) provides security for data packets.However it cannot provide the efficient security and privacy. In this paper, we propose the Secure and Distributed Reprogramming Protocol – Diffie Hellman (SDRP – DH). It provides more efficient security for data packets. We use Diffie Hellman Algorithm, it can provide security for each and every packets.

II. Related Work

Secure and distributed reprogramming protocol named SDRP[3], which is the first work. Since an identity-based signature technique is employed in generating public/private key pair of each authorized user, SDRP is efficient mechanism used for resource-limited nodes and mobile devices in terms of communication and storage. An improvement in SDRP was proposed in [5]. Centralized approach connects the nodes to the base station, whenever a node needs to reprogram base station is needed for privilege list maintenance. In distributed approach nodes are formed as clusters. Cluster heads are connected to the base station.

A. DIFFIE HELLMAN KEY EXCHANGE

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. The key value is used to encrypt subsequent data using a symmetric key cipher.

Suppose *A* and *B* follow this key exchange procedure with *C* acting as a man in middle interceptor. The steps followed in this algorithm that make sure that *C* never gets to know the final keys through which actual encryption of data takes place.

- First, both *A* and *B* agree upon a prime number and another number that has no factor in common. p is the prime number and the another number is g. *g* is also known as the generator and p is known as prime modulus.
- Now, since *C* is in between and listening to this communication so *C* also gets to know p and g.
- Now, the modulus arithmetic says that *r = (g to the power x) mod p*. *r* produces an integer between 0 and *p*.
- The first trick here is that given *x* (with *g* and *p* known), it is very easy to find *r*. But given *r* (with *g* and *p* known) it is difficult to deduce *x*.
- This problem is estimated as the discrete logarithmic problem.

- Coming back to the communication, all the three *B*, *A* and *C* now know *g* and *p*.
- Now, *A* selects a random private number *xa* and calculates (*g* to the power *xa*)mod *p* =*ra*. This resultant *ra* is sent on the communication channel to *B*. Intercepting in between; *C* also comes to know *ra*.
- Similarly *B* selects his own random private number *xb*, calculates (*g* to the power *xb*) mod *p* = *rb* and sends this *rb* to *A* through the same communication channel. Obviously *C* also comes to know about *rb*.
- So *C* now has information about *g*, *p*, *ra* and *rb*.
- Now comes the heart of this algorithm. *A* calculates (*rb* to the power *xa*) mod *p* = Final key which is equivalent to (*g* to the power (*xa***xb*))mod *p*) .
- Similarly B calculates (*ra* to the power xb) mod *p* = Final key which is again equivalent to (g to the power(*xb* * *xa*)) mod *p*.
- So both *A* and *B* were able to calculate a common Final key without sharing each other's private random number and *C* sitting in between will not be able to determine the Final key as the private numbers were never transferred.

The Diffie-Hellman algorithm works perfectly to generate cryptographic keys which are used to encrypt the data being communicated over a public channel.

III. Proposed Work

In this paper, we propose the Secure and Distributed Reprogramming Protocol – Diffie Hellman (SDRP-DH). The proposed work can be split into the following modules that are described in sections that follow. The flow of this system is illustrated in Fig. 1.

MODULES:

- Initialization
- User Preprocessing
- Check User Privileges
- Diffie Hellman Key Exchange
- Performance Comparison

1. Initialization:

The network owner allows registration of the users and assigning the privilege to set of sensor nodes. The user has the privilege to access its neighbour sensor nodes. The owner allows to user can reprogram without base station involved. The network owner generates public and private key has to be generated for secure purpose of the sensor nodes.

2. User Preprocessing:

The network owner set the privilege for the user and calculates the hash value of each packet in the page is added to the packet. The user has to provide signature for overall pages to ensure authentication.

3. Check User Privileges:

The sensor node checks the user privilege to analyses the particular user has the privilege to reprogram that sensor node and first pays attention to the legality of the programming privilege and the message. The sensor node checks that, the identity of that particular sensor node is present in the privilege list of the user or not.

4. Diffie Hellman Key Exchange:

The interpretation of the data packets for verification is performed only when the nodes pass the Diffie Hellman key exchange mechanism.A Merkle tree is a tree in which every non-leaf node is labeled with the hash of the labels of its children nodes. The sensor nodes can authenticate the hash packets in page 0 once the nodes receive packets, the packets are checked based on security of the Merkle hash tree.

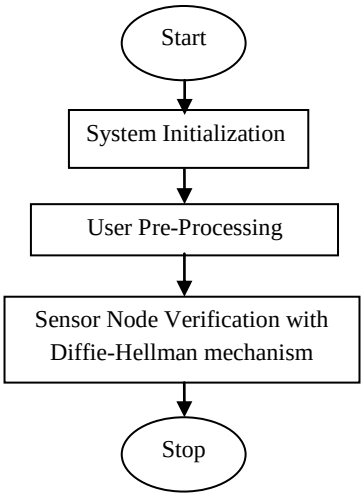

Fig. 1 Working Flow of the SDRP-DH

5. Performance Comparison:

The existing SDRP and the proposed SDRP-DH with an augmentation on the Diffie Hellman key exchange mechanism are evaluated for the quality of service. The intermediate nodes cannot misuse the forwarding information or interpret the data. Simulation of the SDRP and SDRP-DH in network simulator has provided a comparison of throughput, delay and loss in the system.

IV. Simulation And Analysis

The simulation is done by using the simulator NS2. Network simulator is a discrete event time driven simulator. NS2 is open source software which uses C++ and Tool Command Language (TCL) for simulation. C++ is used for packet processing and fast to run. TCL is used for simulation description and used to manipulate existing C++ objects. It is faster to run and change. NS2 is widely used to simulate the networking concepts. The simulation parameter used in the simulation is shown below.

5.1 Throughput

Fig. 2 explains the throughput. The number of packets successfully delivered over the wireless channel in spite of the interference and other environmental attenuation.

x axis denotes time in milliseconds(ms) and y axis denotes bandwidth in megabyte(MB).

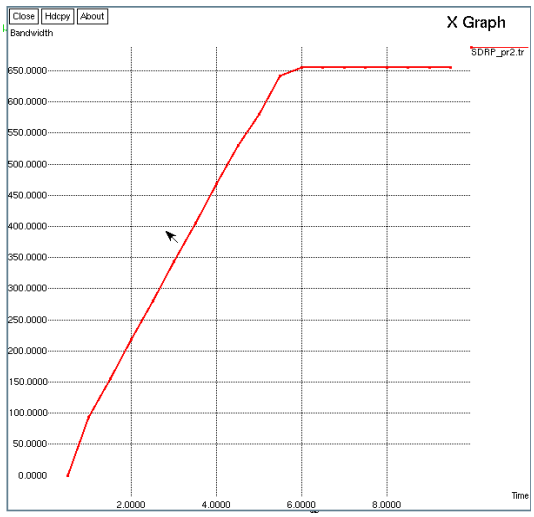

Fig. 2 Throughput

5.2 Packet Loss Ratio

Fig. 3 explains packet loss comparison. Packet loss occurs when one or more packets of data travelling across a network fails to reach their destination.

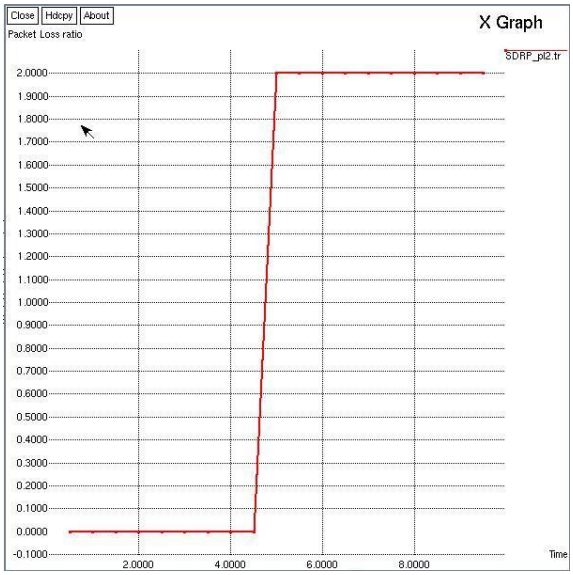

Fig. 3 Packet Loss Ratio

x axis denotes time in milliseconds(ms) and y axis denotes packet loss in megabyte (MB). The packet loss ratio remains 0 for about 4ms. Above 4ms the packet loss ratio increases linearly and remains constant and linearly increases again.

5.3 Packet Delay

Fig. 4 explains packet delay. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node to another.

x axis denotes time in milliseconds(ms) and y axis denotes delay time in milliseconds (ms).

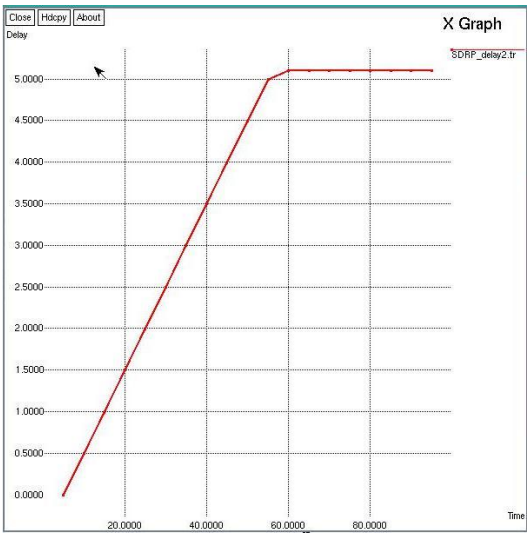

Fig. 4 Packet Delay

V. Conclusion

In this paper, an inherent design weakness in the user preprocessing phase of SDRP is estimated. So Diffie Hellman algorithm is proposed, to provide the more efficient transmission. This algorithm keeps secrecy of sender and receiver's reprogramming packets. Both sender and receiver share their public key and if both get identical values then they will send the private key. Hence it provides secured transmission. Delay increases

since separate key exchange mechanism is performed during transmission between each nodes. A future work for minimizing the delay in Diffie- hellman will be designed.

References

[1]. V. C. Gungor and G. P. Hancke, Oct. 2009 "Industrial wireless sensor networks: Challenges, design principles, and technical approaches," IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265.

[2]. V. C. Gungor, B. Lu, and G. P. Hancke, Oct. 2010 "Opportunities and challenges of wireless sensor networks in smart grid," IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564.

[3]. J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, Dec. 2010 "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," IEEE Trans. Ind. Electron., vol. 57, no. 12, pp. 4219–4230.

[4]. X. Cao, J. Chen, Y. Xiao, and Y. Sun, Nov. 2010 "Building-environment control with wireless sensor and actuator networks: Centralized versus distributed," IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3596–3604.

[5]. H. Song, V. Shin, and M. Jeon, Nov. 2010 "Mobile node localization using fusion prediction-based interacting multiple model in cricket sensor network," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4349–4359.

[6]. Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, Laurence T. Yang, Nov. 2013 "Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks," IEEE Trans. Ind. Electron,. vol. 60, no. 11.

[7]. D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and efficient reprogramming protocol for wireless sensor networks," IEEE Trans. Ind.Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.

[8]. D. He, S. Chan, C. Chen, and J. Bu, Jul. 2012 "Secure and efficient dynamic program update in wireless sensor networks," *Secur. Commun. Netw.*, vol. 5, no. 7, pp. 823–830.

[9]. C. Lim, Apr. 2011 "Secure code dissemination and remote image management using short-lived signatures in WSNs," *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 362–364.