IMPLEMENTATION AND ANALYSIS OF BOOTSTRAPPING PROTOCOL USING PUBLIC KEY CRYPTOGRAPHY IN WSN

Ashok Raj K[1]

[1]*Student of M.Tech, Software Technology, VIT University, Tamilnadu, India*

Abstract

In Wireless Sensor Network security, the open challenge is forming a secure network infrastructure using a bootstrapping protocol. The bootstrapping protocol which is a key pre-distribution technique has to be efficient and not complex as well, since sensor nodes have numerous limitations and constraints such as storage, energy, computational power in it. Also sensor nodes are vulnerable to attacks an authenticated broadcast scheme must be used. Many Key pre distribution schemes have been proposed and each scheme has its own advantages and drawbacks. Based on recent researches it has been proved that public key cryptography can be used in key agreement protocol of wireless sensor networks to establish a secure link among nodes for communication. In our paper, we implement a pre-key distribution scheme using public key cryptography where the public key and private key of each node is distributed as a priori. The public key and private key are generated using RSA algorithm. The Scheme is evaluated with various performance evaluation metrics and graphs are generated using Omnet++ simulator.

Keywords: *Key Pre-Distribution, Wireless Sensor Networks, Omnet++, Public Key Cryptography, RSA*

----------***----------

1. INTRODUCTION

Wireless Sensor Networks has significant growth over wired networks in simplified design with low cost, low power and multifunctional processing. WSN are used in various fields such as Military fields, environment pollution monitoring, person location, traffic analysis on road. But the sensor nodes are very prone to failures in harsh environment also due to energy constraints. Hence secure data transfer scheme must be established improve the security in wireless sensor networks [9].

There are various security requirements for wireless sensor networks such as data availability, data integrity, authentication etc [4]. Also sensor nodes are vulnerable to various types of attacks. Hence various types of defensive measures such as secure Key establishment phase to provide secure broadcasting and authentication must be included. There have been many traditional mechanisms which are used to provide secured broadcast [1] [7].

It is widely accepted that the public key cryptography schemes cannot be implemented due to energy constraints in wireless sensor nodes. But recent researches have proved that public key cryptography can be used in advanced sensor nodes which would give acceptable performance also. Public key cryptography has many advantages than symmetric cryptography in terms of node capture, node scalability [2].

Since public key cryptography can be used in wireless sensor nodes, the advantages of traditional algorithm can be fully utilized to provide secure broadcasting network. This traditional cryptography method is used to create a bootstrapping protocol along with Key pre-distribution scheme, which forms a novel framework with advantages of both public key cryptography and key pre-distribution scheme. The key pre distribution is one of the widely used Key Distribution schemes where key related information is stored as priori.

The rest of the paper is organized as follows: Section 2 defines the problem statement Chapter 3 explains the existing methods and drawbacks. Chapter 4 focuses on the implementation methodologies of the proposed system. Chapter 5 outlines the performance evaluation metrics. Chapter 6 discusses Simulation environment and its results. Chapter 7 concludes the research work pointing out recommended direction towards future work.

2. PROBLEM STATEMENT

The bootstrapping protocol will establish a secure communication infrastructure with a set of sensor nodes, after initializing some secret key information in each node. Because of constraints in the senor nodes the protocol need to be designed efficiently. Since future generation sensor nodes will be produced with ultra power and multifunctional capacity, a strong and traditional public key cryptography scheme can be easily employed in the nodes which will be more secure.

3. RELATED WORK

Key Distribution is the first phase in wireless sensor network formation after deployment of nodes. It is a newly developing technique due to the recent development in the wireless sensor nodes. In that, key pre-distribution scheme has many advantages over all other traditional key distribution schemes. In general key pre-distribution scheme is distributing the keys to the individual nodes before deployment, which in turn used by the nodes for communication and building a secure network.

The various key pre distribution schemes is portrayed one by one. The first method is using a Master Key. The nodes will establish a link based on the pre initialized master in each node. This scheme fails to provide security to node capture. The next scheme is random pre key distribution scheme. In this method the nodes are initialized with set of keys from a shared key pool, such that neighbor nodes share a common key among them to form a link. This scheme fails to support nodes scalability. The third method is pair wise key scheme, which stores n-1 keys in a node, where n is the total number of nodes. This scheme is not suitable at all since the memory consumption will be very high [2][5][6][8].

The next generation sensor nodes are expected to combine ultra power circuitry for more power supply, which makes the possibility of using public key cryptography schemes in key distribution phase [3]. Instead of random set of keys or Pair-wise keys the nodes can be initialized with set of public key and corresponding private keys. Since sensor nodes can communicate only with neighbor nodes, the source node stores only the public keys of neighbor node to form a secure link.

The session key can be sent after RSA encryption and the destination node performs RSA decryption to get session key. The power of public key cryptography can be fully utilized here [2][3].

4. PROPOSED WORK

4.1 Representation of Proposed Work

A wireless senor node consists Key storage component, RSA component, which together performs the process of public key distribution and encryption /decryption process. The application layer of the sensor node is responsible for the actual key generation, key distribution, key storage and encryption/decryption process. The RSA component has the algorithm for encryption and decryption. The key storage component stores all the incoming public keys from neighbor nodes. After the first stage of public key distribution and key storage, the nodes start sending encrypted packet to the neighbor nodes by encrypting the session key with the target nodes public key. After receiving the public key the nodes will decrypt the session key with nodes private key and deletes the packet.

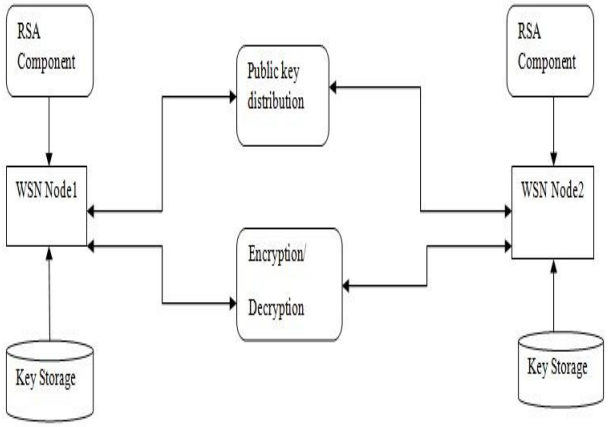

Fig -1: Diagrammatic Representation of Proposed Work

4.2 Key Pre Initialization

Key pre initialization is the key concept of this project where the public keys and private key for each wireless sensor node is initialized prior to the deployment. These keys are generated using RSA algorithm which is a public key cryptography algorithm. The public key and private key are generated based on RSA by selection of various set of prime numbers for each node[10]. These keys are initialized in the nodes.

4.3 Public Key Distribution

After the nodes are initialized with public key (puk , n) and private key (prk,n) the nodes must start publish the public keys to neighbor nodes. The assumption is, the nodes will broadcast packets only to the nodes which is in the transmission range of sending node. There is no separate module for neighbor discovery. The nodes which are in the range of sending node are called as neighbor nodes. The nodes start to publish public keys as well as it stores the source address and public keys of incoming packets.

4.4 Link Establishment

During stage 1, nodes perform public key distribution and key storage. In stage 2 , the nodes perform link establishment. The node encrypts the session key with its private key and then with public key of destination node. This is a two stage encryption according to public key cryptography. The node performs this process till it sends encrypted session key to all neighbor nodes.

$$E_{PUK}{}^{J}[E_{PRK}{}^{I}[SessionKey]] \xrightarrow[D_{PRK}{}^{I}]D_{PUK}{}^{I}]} \underset{\text{cipher text}}{[[SessionKey]}$$

5. PERFORMANCE EVALUATION METRICS

5.1 Memory Overhead

According to [13], the memory overhead is calculated based on the number of cryptographic keys a node has to be stored. In this scheme, each node stores its own public key, private key and 'n' neighbor public keys to establish symmetric communication among neighbor nodes. Memory overhead is given by

Memory Overhead = (n) * size of public key+2

5.2 Communication Complexity

According to [12], communication complexity is given as the sum of total number of packets sent by the application layer and total number of packets received by the application layer of the node.

Communication complexity = [Number of packets sent * size of packet + Number of packets received * size of packet]

5.3 Latency Period

It is the time delay or gap between the data packet creation and the data packet reception at the destination.

Latency Period (delay) = t[packet reception at destination] –t[packet creation at source]

*t - > represents time

Table – 1: Metric Model

Metric	Equation
Memory Overhead	(n) * size of public key+2
Communication Complexity	[Number of packets sent * size of packet + Number of packets received * size of packet]
Latency Period	= t[packet reception at destination] –t[packet creation at source]

6 SIMULATION ENVIRONMENT

6.1 Memory Overhead

Chart-1 illustrates the memory overhead of this implemented scheme. For simplicity, 8byte RSA public keys are initialized. For example, if node[0] has 3 neighbors(n). Then the memory overhead is (3*8)+2 = 26 bytes. The nodes with more number of neighbors have high memory overhead. The nodes which are out of range has a memory overhead of 2, as it contains only public and private key.

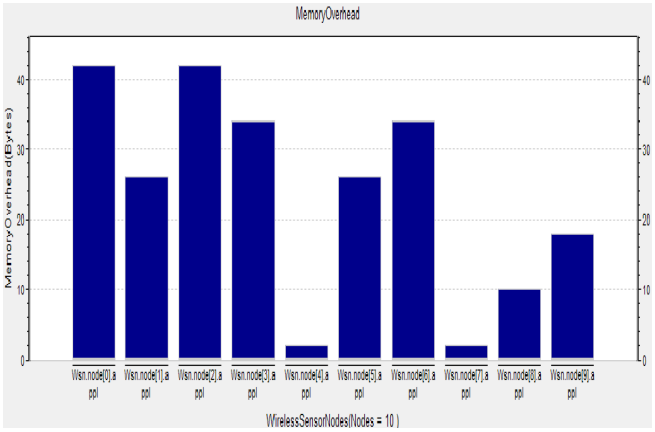

Chart-1 Memory overhead

6.2 Communication Complexity

The size of sending data is 10 bytes. Since the header length of application layer packets is 2 bytes and the public key size is 8 bytes as we already seen. The size of receiving packet depend on the size of session key also. Here the session key is considered to be of 8 bytes plus header length 2 bytes. So the equation will be of the form,

[Number of packets sent + Number of packets received]* 10 bytes

Chart-2 depicts the communication complexity achieved by each node during the simulation.

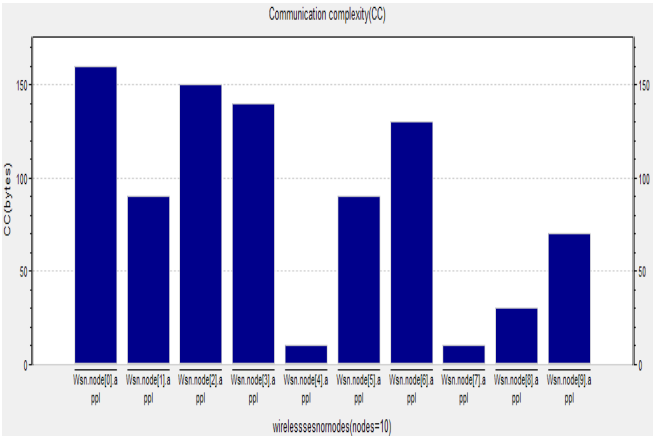

Chart-2 Communication Complexity

The communication complexity is compared with the memory overhead is shown in the Chart-3.

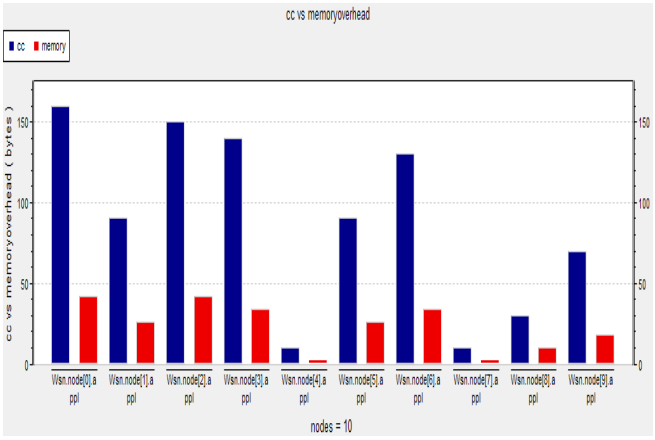

Chart-3 CC Vs Memory Overhead

6.3 Latency Period

The latencies caused by nodes during the simulation time is given in Chart-4. It is the delay created during a packet transmission over the simulation time.

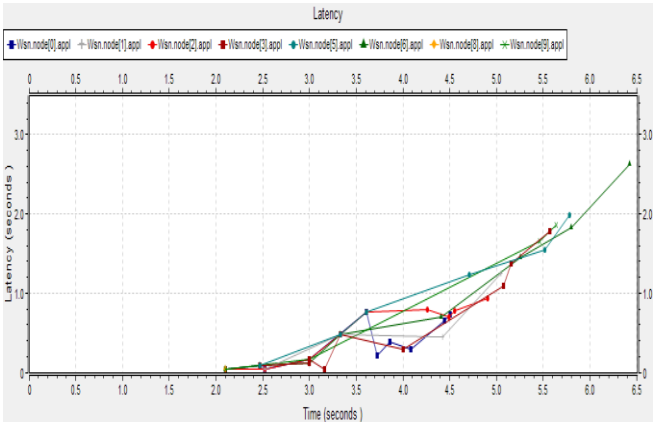

Chart-4 Latency (Delay)

7. CONCLUSIONS

In this paper, a secure framework for link establishment among wireless sensor nodes has been implemented, which is a key pre-distribution scheme using public key cryptography implemented in omnet++ simulation environment. RSA algorithm is used for public key cryptography. This scheme has three core stages which are key initialization, public key distribution to the nodes in range and link establishment as the final stage. The storage of Base Station master public key in nodes is left, assuming all the nodes are authenticated nodes and hence authentication of nodes by base station is omitted. This scheme is successfully implemented and analyzed using three metrics. They are communication complexity, memory overhead and latency. Each metric is analyzed with a set of 10 nodes and the graphs are generated. The nodes with more number of neighbors will have high communication complexity and high memory overhead. The scalability of nodes has no issues expect that, the system administrator must carefully choose the prime factors for key generation which will be tedious when nodes range are scaled up to 50 or 100. This paper can be used as a reference for key pre-distribution using public key cryptography with RSA algorithm in Omnet++ simulator.

As a future work, the ECC algorithm of public key cryptography can be implemented and compared with the current framework in terms of speed and memory consumption. This paper can also be referenced to compare with various pre key distribution schemes. The other protective measures such as revocation of compromised node can be done with the inclusion of base station in this scheme.

REFERENCES

[1]. Padmavathi, Dr G., and Mrs Shanmugapriya. "A survey of attacks, security mechanisms and challenges in wireless sensor networks." arXiv preprint arXiv: 0909. 0576 (2009)

[2]. Iftekhar Salam, M., Pardeep Kumar, and HoonJae Lee. "An efficient key pre-distribution scheme for wireless sensor network using public key cryptography." Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference on. IEEE, 2010.

[3]. Eldefrawy, Mohamed Hamdy, Muhammad Khurram Khan, and Khaled Alghathbar. "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography." In Anti-Counterfeiting Security and Identification in Communication (ASID), 2010 International Conference on, pp. 1-6. IEEE, 2010.

[4]. Walters, John Paul, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary. "Wireless sensor network security: A survey." Security in distributed, grid, mobile, and pervasive computing 1 (2007): 367, 2007.

[5]. Hwang, Joengmin, and Yongdae Kim. "Revisiting random key pre-distribution schemes for wireless sensor networks" In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 43-52 ACM, 2004

[6]. H. Chan, A Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," In Proceedings of IEEE symposium on security and prroacy,pp. 1 97-2 1 3,2003.

[7]. López, Javier, and Jianying Zhou, eds. Wireless sensor network security. Vol. 1 IOS Press, 2008

[8]. W. Du, 1. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," In Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 42-51, 2003.

[9]. Yong Wang, Garhan Attebury, And Byrav Ramamurthy,"A Survey Of Security Issues In Wireless Sensor Networks, IEEE Communications Surveys & Tutorials • 2nd Quarter 2006.

[10]. Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key

cryptosystems" Communications of the ACM 21, no. 2 (1978): 120-126, 1978.
[11].http://www.omnetpp.org/doc/omnetpp/manual/usman.html
[12]. Banimelhem, Omar, Qasem Abu Al-Haija, and Ahmad Al-Badawi. "Performance Evaluation of Probabilistic Key Management Approaches for Wireless Sensor Networks." Proceedings of the first International Conference in Information and Communication Systems-ICICS2009, Paper495 2009
[13]. Khalil, Önder, and Suat Özdemır. "Performance Evaluation of Key Management Schemes in Wireless Sensor Networks" Gazi University Journal of Science 25.2 (2012)

BIOGRAPHIE

Mr. Ashok Raj K, M.Tech (2nd Year), VIT University