ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhancing the Efficiency of Secure and Distributed Reprogramming Protocol for Wireless Sensor Network

Sandeepa Perumalsamy[1], Balaji Subramani[2]

M.Tech, Department of IT, V.S.B Engineering College, Karur, TamilNadu, India[1]

Assistant Professor, Department of IT, V.S.B Engineering College, Karur, TamilNadu, India[2]

ABSTRACT: Wireless reprogramming is a method of modifying the working of existing code or transferring new code image to sensor nodes in order to improve its performance in sensor network. Reprogramming the sensor network in a secure way is a challenging task. For security purpose every code update must be authenticated to prevent an attacker from installing malicious code in the network. A Secure and Distributed Reprogramming protocol named SDRP is the first protocol which has been established to reprogram the sensor nodes in a distributed way without involving the base station, where different reprogramming privileges will be given to several authorized users. The protocol uses identity based cryptography to secure the reprogramming and also to reduce the communication overhead and storage requirements of each node. After analyzing this protocol, it is found that it is tractable to impersonation attack. Hence adding 1-byte redundant data has been proposed as a solution to prevent the impersonation attack. The proposed solution will improve the performance and efficiency of the SDRP protocol.

KEYWORDS: Sensor network, Reprogramming, Security, and Authentication

I. Introduction

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, like temperature, sound, pressure, etc... The major functions of sensor nodes are sensing, computing and communicating with other nodes in the sensor network. The WSN will be deployed once and it is aimed to operate for long period of time. At that situation some of the issues like an updating the operating system, updating an application, addition of new application, modification of arguments in existing application may arise. So reprogramming is an essential task in order to overcome the above issues.

Many reprogramming protocols have been established recently and their main goal is to disseminate the code images to the sensor nodes. Reprogramming the sensor nodes manually will consume more cost and sometimes it is not possible to perform such operation when the network is huge in size. So we are opting either centralized method or distributed method. In centralized approach, only two participants will be involved (base station and sensor nodes). The network owner has the entire control to perform the reprogramming tasks like solving bugs, changing the functionality of the working software or adding new function to improve the performance of the network. The network owner will propagate the code images to sensor nodes and the nodes will accept the image only if it is signed by him. The transmission of code images takes place by means of multi-hop routing. Regrettably this method is dangerous to single point of failure and hence reprogramming is not possible at that instant. So to overcome the above problem, we can move towards distributed method.

In distributed approach, three kinds of participants will be involved (network owner, authorized users, sensor nodes). The network administrator will admit several authorized users to perform the reprogramming task. Reprogramming the sensor nodes in a secure way is also an important criteria which is to be considered to prevent the adversaries from injecting the malicious code in the sensor network, So different privileges will be given to different authorized users to perform the reprogramming task without involving the base station. The following frameworks need to be considered while implementing this: Scope selection: Choosing either all the nodes in the sensor network or particular node to perform the reprogramming job. Encoding/decoding: In order to provide security, the code images have to be encoded and decoded appropriately. Code dissemination: It is the process of propagating the code images to the specified target nodes. It works jointly with scope selection. Completion validation: It ensures that the code images received by the target nodes are complete and also error free. Code acquisition: In order to actuate the events some conditions must be specified in sensor nodes. If a condition is satisfied, then the sensor node will send code acquisition requests to find source node that have the desired program, module, or patch. After that, route will be built to send the codes from the source node to the requesting node.

II. SECURITY REQUIREMENTS

As Sensor networks are used widely in many applications, security is a major concern which will assure the secure communication among the nodes in wireless network. The security requirements of wireless sensor network are as follows.

1) Authenticity: It refers to trustfulness of origin. Before installing the program image, a sensor node must verify the source of the packet. This will ensure that the code images came from the authorized users.
2) Integrity: It helps to prevent the changes made by unauthorized users. For that purpose, a message authentication code (MAC) is generated by the sender using some MAC key and that is sent with the encrypted message. At the other end, the receiver will verify the authenticity of the received message by using that MAC key.
3) Confidentiality: It refers to concealment of information. To achieve this, messages will be encrypted before transmitting through the communication channel.
4) Freshness: Even if data integrity and confidentiality are assured, it is also required to ensure the freshness of each message. Informally, data freshness indicates that the data is recent, and it assure that no old messages have been replayed.
5) Node compromise tolerance: This prevents the compromised node from inducing the uncompromised node to violate the security requirements.
6) Distributed: This allows the authorized users to update the code images directly without involving the base station and also it should prevent the code updates made by unauthorized users.
7) Supporting different user privileges: The network owner will grant different privileges to authorized users.
8) Partial reprogram capability: This prevents the sensor nodes from being totally controlled by the authorized network user. Major changes can be made only by the network owner.
9) Scalability: The key management scheme should be scalable in the sense that if network size grows, it should not increase the chances of node compromise and communication overhead. It should allow nodes to be added in network after the deployment as well.
10) Self-Organization: A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations.
11) Time Synchronization: Most sensor network applications depend on some type of time synchronization. In order to save power, an individual sensor's radio may be turned off for periods of time.
12) Secure Localization: Often, the effectiveness of a sensor network will depend on its ability to accurately and automatically locate each sensor in the network.

III. RELATED WORKS

Recently several methods have been developed to provide secure code dissemination for wireless sensor networks. All methods are extension to deluge. Lanigan et al. proposed a set of rules called Sluice to incorporate cryptographic hash function and signature which provides efficient authentication for code propagation. This method adopts deluge to divide each code image into pages. The hash image of first page is included in the signature packet, second page is included in the first page and in similar way the following pages are included in previous page. In sluice, a node can perform authentication only when it receives an entire page and hence it cannot authenticate individual packet immediately when it is received. When adversary sends a large number of packets during code dissemination, a node cannot notify whether it is authentic or not. So finally the adversary may force the sensor node to accept the bogus packet and to drop the authenticate packet.

Similar to sluice another technique have been proposed for securing the deluge network programming method. In this technique the hash image of first packet is signed and included in the advertisement packet whereas the hash images of following packets are included in the previous packet. Here the author proposed a scheme such that the packets have to be authenticated individually when the node receives and unusable packets will be stored separately. Unfortunately this method also will lead to DoS attacks, as the adversary will exhaust the buffers of receivers by sending more packets. The DoS attacks can be avoided by not storing the unusable packets but the code dissemination process will not be efficient. During transmission if one packet is dropped from a page then the node have to follow retransmission process of all packets in the particular page.

Deng et al. proposed a method to improve the code dissemination process by the use of Merkle hash tree which prevents the DoS attacks. In addition to the hash image of each page it also uses Merkle hash tree for immediate authentication of packets as soon as the node receives. But Merkle hash tree will be transmitted for every page and due to this the overhead will be increased. The hash tree will be distributed in the level-by-level fashion. The packets in one level will receive the hash tree and after verifying all the packets the next level will sends a request. But this approach will leads to higher propagation delays. However all the existing approaches are based on deluge none of the method provides the acceptable solution for the authentication of the packets. In order to exhaust the battery power, the adversary may send the packet request repeatedly. If adversary catches the hash value during the genuine code dissemination, the value can be reused to send the fake signature to the other regions of the network. Because of low bandwidth and multi hop transmission in wireless sensor network, the adversary has adequate time to launch the DoS attacks against the sensor nodes

I V. Code Dissemination Process in WSN

Fig 4.1 describes about the code dissemination process which has following steps:

1. The node which acts as a base station reads the code images and split into packets for dissemination.
2. The node disseminates packets to all other sensor nodes which are within their communication range.
3. After receiving the packets sensor nodes stores it in external flash memory. Also the node will request if any packets missed during transmission.
4. The node will keep on forwarding the packets to its neighbors until all nodes get the new code image.
5. After receiving all the packets the node will start to verify the program image in external flash memory. If verification passes it will transfer the code image to program memory and restart it to begin the new code.

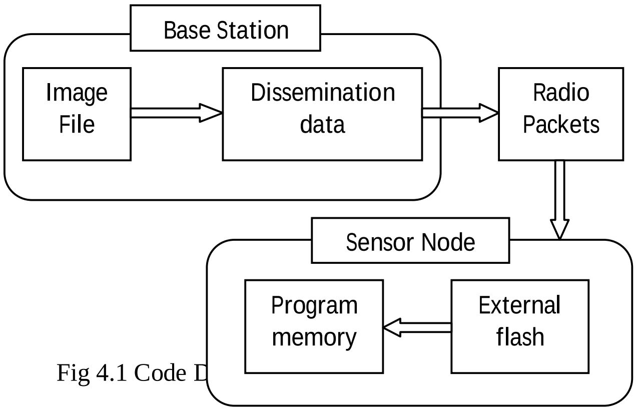

Fig 4.1 Code D

V. The SDRP Protocol

SDRP is the first protocol which is used to perform reprogramming process in a distributed manner. This protocol extends Deluge to be a secure protocol. The design of SDRP is to map the identity and reprogramming privilege of an authorized user into a public/private-key pair. Based on the public key, user identity and his reprogramming privilege can be verified, user traceability and different levels of user authorities can be supported. A novel identity-based

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

signature scheme is employed in generating the public/private-key pair of each authorized user, and then this protocol is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements. Moreover, the proposed protocol can achieve all the requirements of distributed reprogramming

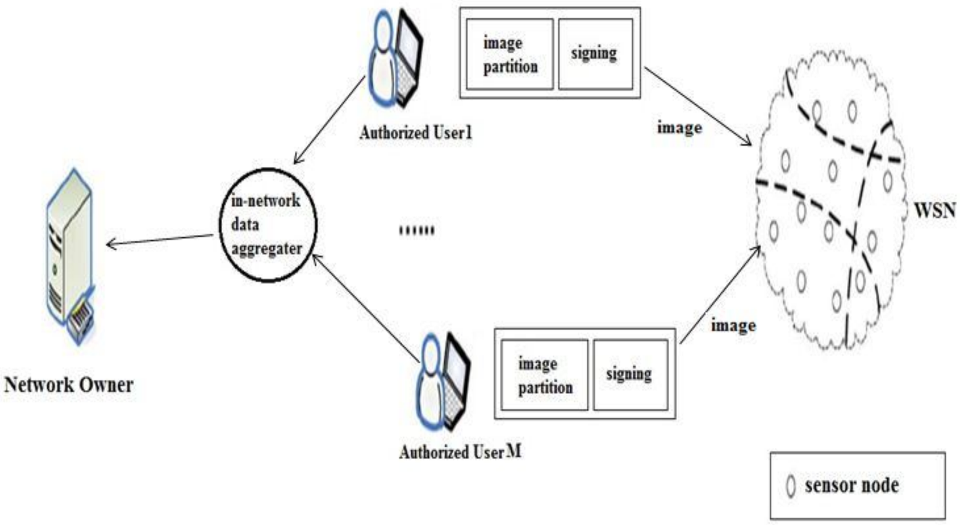

Fig 5.1 Overview of distributed reprogramming approach

Fig 5.1 shows overview of distributed reprogramming approach. This approach consists of three kinds of participants namely network owner, authorized network users and all sensor nodes. Here the network owner is not needed to be in online always, he can also be in offline. After registering to the owner the user can enter into the WSN. The owner will assign certain privileges to the user in order to perform the reprogramming process in the sensor network. In-network data aggregator is used to summarize the resultant data which enhance the robustness and accuracy of information obtained by entire network and also it reduces the traffic load and conserves energy of the sensors. The SDRP Protocol consists of following phases.

A. System Initialization

The network owner performs the following steps:

1. Generate the public parameters and load them in all the sensor node before deployment. Public parameter=$\{G_1,G_2,G_3,g_{1,}g_2,g,\hat{e}\psi,Qpub,H3,H4\}$ where (G_1,G_2,G_3) are bilinear group of large prime order P with generators ($g_2 Є G_2$), $g_{1=}\ \psi(g2)ЄG_1$ and $g=\hat{e}\ (g_{1,}g_2)$. Randomly choose a random number $sЄZp^*$ as the master key. Compute public key as Q_{pub}=s. $g_2\ ЄG_2$.The cryptographic hash functions $H_3:\{0,1\}^* \rightarrow Z_p$ *and $H_4:\{0,1\}^* \times G3 \rightarrow Zp^*$

2. User Public/Private key generation: Let us consider a user U_j with identity $UID_j\ Є\{0,1\}^*$.The network owner sets U_j's public key as $P_j=H_3(UID_j||\ P_{rij})EZ^*{}_p$.The private key is computed as $S_j=(1/P_j+s).g_1=(1/(H_3(UID_j||P_{rij})+S)).g_1$.Then the public key, private key and privilege of the user $\{P_{j,}S_j,P_{rij}\}$ will be sent through the secure channel. Then the user will be allowed to reprogram the nodes in the specific region for the subscription period.

B. User Preprocessing

After entering the WSN user has to perform the following actions if he has a new program image.

1. The user U_j partitions the program image to Y fixed-size pages and denoted from page 1 through page Y. Then the user splits the page i into N fixed size packets where $1 \leq i \leq Y$. The packet is denoted as $Pkt_{i,1}$ through $Pkt_{i,N}$. The hash value of each packet in page Y is appended to the corresponding previous packet i.e the value of packet Y is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

included to the packet Y-1, similarly the value of packet Y-1 is included in packet Y-2 and process goes on until the U_j finishes hashing all the packets in page 2 and including their hash values in co9rresponding packet in page 1. Merkle hash tree is used to smooth the progress of authentication of hash values of the packets in page 1. The packets related to this Merkle hash tree are referred collectively as page 0. The signature message m consists of information about the root of the Merkle hash tree, metadata about the code image and signature. Metadata means version number, targeted node identity set and program image size. The format of the message m is represented as shown in fig 5.2.

Version num (1)	Targeted node identities set (6)	Code image size (2)	Root of the Merkle hash tree (20)

Fig 5.2 Format of the message m

The targeted node identity set indicates the identities of sensor node, the network user wishes to reprogram. Let us assume that the length of identity of each sensor node is 2B, in this case protocol supports up to 65535 nodes. The identity field is set according to the reprogramming privilege of the user. In order to ensure authenticity and integrity of new code, U_j has to take following actions to construct the signature message.

2. The user U_j can compute the signature σ_j of message m with the private key S_j as follows.Choose a random number $x \in \mathbb{Z}^*_p$, compute $r=g^x$. set $h=H_4(m,r) \in \mathbb{Z}^*_p$ and calculate $W=(x+h). S_j$. The Signature σ_j is the pair $(h,W) \in \mathbb{Z}^*_p \times G_1$.
3. U_j transmits the signature message $\{UID_j,Pri_j,m, \sigma_j\}$ to the targeted nodes.

C. Sensor node verification

After receiving the signature message sensor node verifies as follows.

1. The sensor node first checks the programming privilege Pri_j and message m.If it is valid then the verification process goes to next step.
2. With the help of public parameter the sensor node checks whether h^* is equal to h or not. The signature is valid only if the result is positive otherwise node drops the signature.
$$h^*=H_4(m,e(W,H_3(UID_j||Pri_j).g_2+Q_{pub})g^{-h})$$
3. If the verification passes the sensor node believes that message came from authorized user and it accepts the root of the Merkle hash tree. Based on the security of hash tree node authenticates the hash packets. After verifying the hash packets node can easily verify data packets based on one way hash function property. Similarly after verifying the packets in page i the packets in page i+1 (i=1,2,..,Y-1) will also be verified and node accepts the image only if the verification passes.

VI. CONCLUSION AND FUTURE WORK

A number of secure reprogramming protocols have been proposed, but none of these approaches support distributed operation. A Secure and Distributed Reprogramming Protocol is the only method which supports reprogramming in a distributed manner. It allows authorized users to reprogram the sensor nodes in a distributed way. This protocol uses identity based signature scheme for key generation and Elliptic curve cryptography for encrypting the code images. By using 1-byte redundant data the security protection will be enhanced for reprogramming which prevents the impersonation attacks that make use of distributed reprogramming protocol.

The future work may focus on various cryptographic techniques and also how to improve the efficiency of SDRP by integrating with existing centralized reprogramming protocol like Rateless Deluge and DIP.

REFERENCES

[1] Ahmad Abed Alhameed Alkhatib, Gurvinder Singh Baicher," Wireless Sensor Network Architecture," 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012) IPCSIT vol.35(2012).

[2] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu," SDRP: A Secure and Distributed Reprogramming Protocol for wireless sensor networks", IEEE Trans. Industrial Electronics, vol 59, No.11, Nov 2012.

[3] Deng. J, Han. R and Mishra. S, "Secure code distribution in dynamically programmable wireless sensor networks," in Proc. ACM/IEEE IPSN, 2006, pp. 292–300.

[4] Gowrishankar. S, Basavaraju. T. G, Manjaiah. D. H, Subir Kumar Sarkar, "Issues in Wireless Sensor Networks," Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.

[5] Hemanta Kumar Kalita1 and Avijit Kar, "wireless sensor network security analysis," International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.

[6] Hui. J. W and Culler. D, "The dynamic behavior of a data dissemination protocol for network programming at scale," in Proc. ACM SenSys, 2004, pp. 81–94.

[7] Hyun. S, Ning. P, Liu. A, and Du. W, "Seluge: Secure and dos-resistant code dissemination in wireless sensor networks," in Proc. ACM/IEEE IPSN, 2008, pp. 445–456.

[8] Lanigan. P. E, Gandhi. R, and Narasimhan. P, "Sluice: Secure dissemination of code updates in sensor networks," in Proc. ICDCS, 2006, p. 53.

[9] Mohamed Watfa , William Daher and Hisham Al Azar,"A Sensor Network Data Aggregation Technique", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009 1793-8201.

[10] Naik. V, Arora. A, Sinha. P, and Zhang. H, "Sprinkler: A reliable and energy efficient data dissemination service for extreme scale wireless networks of embedded devices," IEEE Trans. Mobile Comput., vol. 6, no. 7, pp. 777–789, Jul. 2007.

[11] Thangaraj. M and Punitha Ponmalar. P," A Survey on data aggregation techniques in wireless sensor networks," International Journal of Research and Reviews in Wireless Sensor Networks (IJRRWSN) Vol. 1, No. 3, September 2011, ISSN: 2047-0037.

[12] Vaibhav Pandey, Amarjeet Kaur and Narottam Chand, "A review on data aggregation techniques in wireless sensor network," Journal of Electronic and Electrical Engineering ISSN: 0976–8106 & E-ISSN: 0976–8114, Vol. 1, Issue 2, 2010, pp-01-08.

[13] X. Xiong, D. S. Wong, and X. Deng, "TinyPairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks," in Proc. IEEE WCNC, 2010, pp. 1–6.

[14] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004.

[15] Y. Law, Y. Zhang, J. Jin, M. Palaniswami, and P. Havinga, "Secure rateless deluge: Pollution-resistant reprogramming and data dissemination for wireless sensor networks," EURASIP J. Wireless Commun. Netw.,vol. 2011, pp. 1–21, 2010.