ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

A Protected Multi Authorizing Reprogramming Protocol for Wireless Sensor Networks

K.P.Thooyamani[1], R. Udayakumar[*2]

[1]Professor, School of Computing, Bharath University, Chennai, India

[2*]Associate Professor, Department of Information Technology, Bharath University, Chennai, India

ABSTRACT: Wireless reprogramming for a wireless sensor network is the process of uploading new code or changing the functionality of existing code. For security reasons, every code update must be authenticated to prevent an adversary from installing malicious code in the network. All existing reprogramming protocols are based on the centralized approach in which only the base station has the authority to initiate reprogramming. However, it is desirable and sometimes necessary for multiple authorized network users to simultaneously and directly reprogram sensor nodes without involving the base station, which is referred to as distributed reprogramming. In this case, the network owner can also assign different reprogramming privileges to different users. Motivated by this consideration, develop a secure and distributed reprogramming protocol named SDRP, which is the first work of its kind. The protocol uses identity-based cryptography to secure the reprogramming and to reduce the communication and storage requirements of each node. Moreover, our theoretical analysis demonstrates the security properties of our protocol. It also implement SDRP in a network of resource-limited sensor nodes to show its high efficiency in practice.

KEYWORDS*:* Reprogramming, security, Sensor networks, User Privilege

1. INTRODUCTION

Wireless reprogramming is the process of propagating a new code image or relevant commands to sensor nodes through wireless links after a wireless sensor network (WSN) is deployed. Due to the need of removing bugs and adding new functionalities, reprogramming is an important operation function of WSNs [1]. As a WSN is usually deployed in hostile environments such as the battlefield, an adversary may exploit the reprogramming mechanism to launch various attacks. Thus, secure programming is and will continue to be a major concern. There has been a lot of research focusing on secure reprogramming, and many interesting protocols have been proposed in recent years [6]. However, all of them are based on the centralized approach which assumes the existence of a base station, and only the base station has the authority to reprogram sensor nodes, as shown in the upper subfigure in Fig. 1. Unfortunately, the centralized approach is not reliable because, when the base station fails or when some sensor nodes lose connections to the base station, it is impossible to carry out reprogramming[3]. Moreover, there are WSNs having no base station at all, and hence, the centralized approach is not applicable. Also, the centralized approach is inefficient, weakly scalable, and vulnerable to some potential attacks along the long communication path. Alternatively, as shown in the lower subfigure in Fig. 1, a distributed approach can be employed for reprogramming in WSNs. It allows multiple authorized network users to simultaneously and directly update code images on different nodes without involving the base station. Another advantage of distributed reprogramming is that different authorized users may be assigned different privileges of reprogramming sensor nodes. This is particularly important in large-scale WSNs owned by an owner and used by different users from both public and private sectors . Quite recently, He *et al.* have proposed a secure and distributed reprogramming protocol named SDRP , which is The first work of its kind. Since a novel identity-based signature scheme is employed in generating public/private key pair of each authorized user, SDRP is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements. Furthermore, SDRP can achieve all requirements of distributed reprogramming listed in [2], while

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

keeping the merits of the well-known mechanisms such as Deluge and Seluge [5]. Also, SDRP has been implemented in a network of resource-limited sensor nodes to show its high efficiency in practice. (Cases) that define the hyper plane are the support vectors. However, preprocessing phase of SDRP, and an adversary can easily impersonate any authorized user to carry out reprogramming. To eliminate the identified security vulnerability, it propose a simple modification on SDRP without losing any features (such as distributed reprogramming, supporting different user
Privileges, dynamic participation, scalability, high efficiency, and robust security) of the original protocol. Moreover, it show that, for security and efficiency consideration, any efficient identity-based signature algorithm which has survived many years of public scrutiny can be directly employed in SDRP. This paper also reports the experimental results of the improved SDRP in laptop PCs and resource limited sensor nodes, which show its efficiency in practice. The remainder of this paper is organized as follows briefly review SDRP in Section II and reprogramming protocol Section III[4]. Section IV Experiment design Section V concludes this paper and points out future research directions.

II.RELATED WORK

In this propose the Secure and Distributed Reprogramming Protocol (SDRP), which extends Deluge to be a secure protocol. The main idea 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, and user traceability and different levels of user authorities can be supported. Since a novel identity-based signature scheme is employed in generating the public-/ private-key pair of each authorized user, the proposed protocol is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements[7]. Furthermore, the proposed protocol can achieve all the requirements of distributed reprogramming listed earlier, while keeping the merits of Deluge and Seluge. To the best of our knowledge, this is the first proposed protocol for distributed reprogramming in WSNs. As our proposed reprogramming is a distributed reprogramming protocol, each user has the different privilege of reprogramming[8]. It is not vulnerable to potential attack for long communication path It is efficient for resource limited sensor nodes

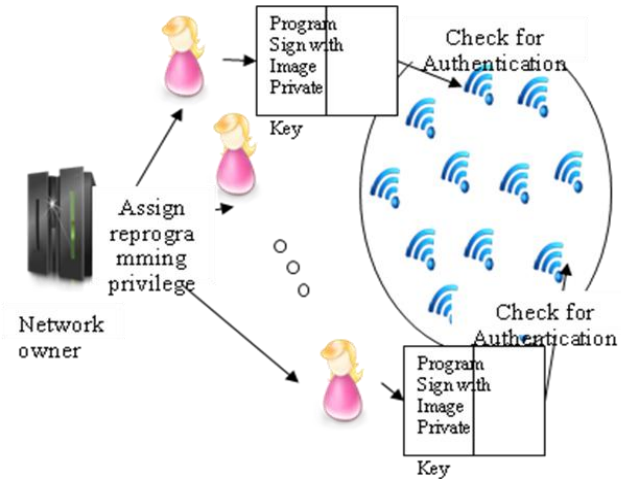

Figure 1: System Architecture

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

III.A PROTECTED MULTI AUTHORIZING RE-PROGRAMMING PROTOCOL

SELUGE REPROGRAMMING PROTOCOL

The key contribution of Seluge is a novel way to organize the packets used to distribute new code images. By carefully arranging code dissemination data items and their hash images in packets, Seluge provides *immediate authentication* of each packet upon receipt, without disrupting the efficient propagation mechanisms used by Deluge[9]. Thus, it can defeat the DoS attacks exploiting authentication delays. Seluge properly authenticates advertisement and SNACK packets. As a result, it can prevent DoS attacks exploiting the Deluge epidemic propagation and suppression mechanisms. Seluge uses a signature to bootstrap the authentication of a new code image. However, unlike the previous attempts, Seluge uses a weak authentication along with the signature. This weak authentication mechanism has nice properties: It can be efficiently verified by a regular sensor node, but it takes a computationally powerful attacker a substantial amount of time to forge a weak authenticator. Moreover, it cannot be pre-computed. Thus, this weak authentication mechanism provides an effective filter of forged signatures. As a result, Seluge is not subject to the same DoS attacks against signature verifications as the previous approaches.

DELUGE REPROGRAMMING PROTOCOL

Among these protocols, Deluge is generally regarded as the state of the art and included in TinyOS distributions[10]. It uses an epidemic protocol for efficient advertisement of metadata and spatial multiplexing for efficient propagation of code images. However, since the design of Deluge did not take security into consideration, there have been several extensions to Deluge to provide security protection for reprogramming. Among them, Seluge enjoys both strong security and high efficiency. However, all existing reprogramming protocols are based on the centralized approach in which only the base station has the authority to reprogram the sensor nodes. When the base station wants to disseminate a new code image to certain sensor nodes, it transmits the signed code image to those nodes via multihop routing, and those nodes only accept the code image signed by it.

NEED FOR DECENTRALIZED APPROACH

Unfortunately, the centralized approach is vulnerable to the single point of failure and not reliable because reprogramming becomes impossible when the base station fails or when some nodes lose connections to the base station. Also, it is inefficient, weakly scalable, and vulnerable to potential attacks along the long communication path. The base station has to be online and accessible to any user at any time during the network operation[11]. Even worse, there are some WSNs that do not have any base station. Examples of such networks include a WSN deployed along an international border to monitor weapon smuggling and human trafficking. Having a base station in these WSNs introduces a very attractive attack target. Obviously, for such networks, it is necessary to have authorized network users to be able to carry out reprogramming in a distributed manner.

IV.EXPERIMENT DESIGN

4.1 NETWORK ADMIN

The network owner allows register 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 admin involved. The network owner generates public and private key has to be generated for secure purpose of the sensor nodes.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

4.2 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. The message should contain the reprogramming privileges then targeted node identity set field indicates the identities of the sensor nodes which the network user wishes to reprogram. Partition the code image and add the signature with the code image.

4.3 NODE CATEGORIZATION

The user verify that whether the sensor node have the malicious behavior or not and infected node known as adversaries by using the following procedure.

- Nodes infected at time t might infect other nodes in the Future
- The final fraction of the infected nodes depends on the classification criterion, (e.g.,) threshold H.
- For large H only few will be infected.
- For small enough H all nodes will be infected.

4.4 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. If it is present in the sense the system public parameters assigned by the network owner is verified after the verification the sensor node believes that, the code image is from the authenticated user and the sensor node verifies the data packets in the code image.

4.5 DATA PACKETS VERIFICATION

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 such packets, based on the security of the Merkle hash tree. Once the data packets in page *I* have been verified, a sensor node can easily authenticate the data packets in the page. Only if all verification procedures described previously pass, the sensor node accepts the code image.

ITERATIVE ALGORITHM FOR NODE CLASSIFICATION

Input matrix M
Set *Si=1* for known adversaries and to *Si=0* for the rest
Set a threshold H
For each unclassified node i, iterate from t=1: TMAX

$$S_i(t+1) = \Theta[\sum_j M_{ij} S_j(t) - H]$$

Nodes with S (TMAX) =1 are classified as adversaries

Advantages

Initially infected individuals (known adversaries).Nodes infected at time **t** might infect other nodes in the future. So, Iterative method detects the malicious nodes effectively and accurately.

Procedure

- Initially infected individuals (known adversaries)
- Nodes infected at time t might infect other nodes in the Future
- The final fraction of the infected nodes depend on the classification criterion, e.g., threshold H
- For large H only few will be infected
- For small enough H all nodes will be infected

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

- Algorithm is very sensitive to H

V.CONCLUSION AND FUTURE ENHANCEMENT

CONCLUSION

Already a number of secure reprogramming protocols have been proposed, but none of these approaches support distributed operation. Therefore, in my project, a secure distributed reprogramming protocol named SDRP with node classification algorithm has been proposed. In addition to analyzing the security of SDRP, I reported the evaluation results of SDRP by using the Network simulator Ns2 with network of resource-limited sensor nodes, which shows that SDRP is feasible in practice. To the best of our knowledge, until now, our protocol is the only one that allows authorized users to reprogram sensor nodes in a distributed manner and also classify the sensor nodes before sending the code image to the sensor node. Thus our proposed protocol provides more security while reprogramming the sensor nodes.

FUTURE ENHANCEMENT

In some applications, data are also required to be kept confidential due to the possibility of message interception. The wireless sensor network is widely used in the critical application like Military application. So need to transmit some confidential information over the network. The confidentiality can provide by using cryptographic techniques. As the WSN is the resource constrained network, need to consider the energy efficiency while providing the confidentiality. In future work study how to support confidentiality in the energy efficient manner in distributed reprogramming.

LIMITATION

SDRP with node classification is only applicable for the resource constrained small WSN. The authentication only has been considered, the confidentiality of the code image is not considered. Reprogramming with security consideration decreases the lifetime of the wireless sensor networks.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their constructive comments on this paper.

REFERENCES

[1] V. C. Gungor and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258 4265, Oct. 2009.
[2] Saravanan, T., Srinivasan, V., Sandiya, V.P., "A two stage DC-DC converter with isolation for renewable energy applications", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S6) (2013) pp. 4824-4830.
[3]V. C. Gungor, B. Lu, and G. P. Hancke, “Opportunities and challenges of wireless sensor networks in smart grid,” IEEE Trans. Ind. Electron., vol. 57, no. 10, pp. 3557–3564, Oct. 2010.
[4]Saravanan, T., Srinivasan, V., Udayakumar, R., "A approach for visualization of atherosclerosis in coronary artery", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 18(12) (2013) pp. 1713-1717.
[5] J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, “Distributed collaborative control for industrial automation with wireless sensor and actuator networks,” IEEE Trans. Ind. Electron., vol. 57, no. 12, pp. 4219–4230, Dec. 2010.
[6]Srinivasan V., Saravanan T., "Analysis of harmonic at educational division using C.A. 8332", Middle - East Journal of Scientific Research, ISSN : 16(12) (2013) pp.1768-1773
[7]X. Cao, J. Chen, Y. Xiao, and Y. Sun, “Building-environment control with wireless sensor and actuator networks: Centralized versus distributed,” IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3596–3604, Nov. 2010.
[8]Srinivasan V., Saravanan T., "Reformation and market design of power sector", Middle - East Journal of Scientific Research, ISSN : 16(12) (2013) pp. 1763-1767.

ISSN(Online) :2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2015

[9]J. Carmo, P. Mendes, C. Couto, and J. Correia, "A 2.4-GHz CMOS shortrange wireless sensor-network interface for automotive applications," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1764–1771, May 2010.
[10]Srinivasan V., Saravanan T., Udayakumar R., "Specific absorption rate in the cell phone user's head", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp.1748-1750.
[11]V. Naik, A. Arora, P. Sinha, and H. Zhang, "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. 762–776, Jul. 2007.
[12] Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., "A DFIG based wind generation system with unbalanced stator and grid condition", Middle - East Journal of Scientific Research, v-20, i-8, pp:913-917, 2014.
[13] Thooyamani, K.P., Khanaa, V., Udayakumar, R., "Wireless cellular communication using 100 nanometers spintronics device based VLSI", Middle - East Journal of Scientific Research, v-20, i-12, pp:2037-2041, 2014.
[14] Vanangamudi, S., Prabhakar, S., Thamotharan, C., Anbazhagan, R., "Dual fuel hybrid bike", Middle - East Journal of Scientific Research, v-20, i-12, pp:1819-1822, 2014.
[15] Udayakumar, R., Kaliyamurthie, K.P., Khanaa, Thooyamani, K.P., "Data mining a boon: Predictive system for university topper women in academia", World Applied Sciences Journal, v-29, i-14, pp:86-90, 2014.
[16] Satheesh, S., Lingeswaran, K., "High efficiencytransformer less inverter for single-phase photovoltaic systems using switching converter", Middle - East Journal of Scientific Research, v-20, i-8, pp:956-965, 2014.