RESEARCH ARTICLE OPEN ACCESS

Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks using Identity-Based Short Signature Scheme

Pooja Motwani*, Priyanka Fulare**
*(Computer Science and Engineering Department, GHRIETW, Nagpur
Email: poojamot@gmail.com)
** (Computer Science and Engineering Department, GHRIETW, Nagpur
Email: priyanka.fulare@raisoni.net)

ABSTRACT
Wireless reprogramming in a wireless sensor network (WSN) is the process of uploading a new code image or relevant commands to sensor nodes or changing the functionality of existing code. As a WSN is usually deployed in hostile environments, so for security reasons every code update must be authenticate to prevent an opponent from installing malicious code in the network. A secure and distributed reprogramming protocol named SDRP is the first distributed reprogramming protocol for WSNs. SDRP is based on distributed reprogramming approach that allows multiple authorized network users to simultaneously and directly reprogram sensor nodes without involving the base station. However, in this paper, the identity-based signature scheme has been chosen, which is significantly more efficient than all known IBS schemes and requires less computation cost, and the size of signatures is approximate 160 bits which is the shortest identity-based signatures generated so far. Thus in order to further improve the security and efficiency of SDRP, identity-based short signature scheme can be directly employed in SDRP.

Keywords – Efficiency, Identity-based short signature, Reprogramming, Security, Wireless sensor networkshas the authority to reprogram sensor nodes, as

I. Introduction

Wireless sensor networks may be deployed for extended periods of time during which the requirements from the network owner and users or the environment in which the sensor nodes are deployed may change. The change may necessitate propagating a new code image or relevant commands to sensor nodes or retasking the existing code with different sets of parameters. These activities are referred as reprogramming. Reprogramming is a significant operation function of WSNs due to the need of removing bugs and adding new functionalities [1]-[5]. 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 reprogramming is and will continue to be a major issue.

There has been a lot of research focusing on secure reprogramming, and several reprogramming protocols have been proposed in recent years [6]–[10]. However, all of them are based on the centralized approach in which only the base station shown in the lower subfigure in Fig. 1. Unfortunately, the centralized approach is not reliable because, when the base station cease to function or when some sensor nodes lose connections to the base station, it is impossible to carry out reprogramming. Also it is weakly scalable, inefficient, and vulnerable to potential attacks along the long communication path. Moreover, there are WSNs having no base station at all, and hence, the centralized approach is not suitable.

Alternatively, a distributed approach can be employed for reprogramming in WSNs as shown in the lower subfigure in Fig. 1. It allows multiple authorized network users to simultaneously and directly updates code images on different sensor nodes without involving the base station. Another benefit 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 [11], [12].

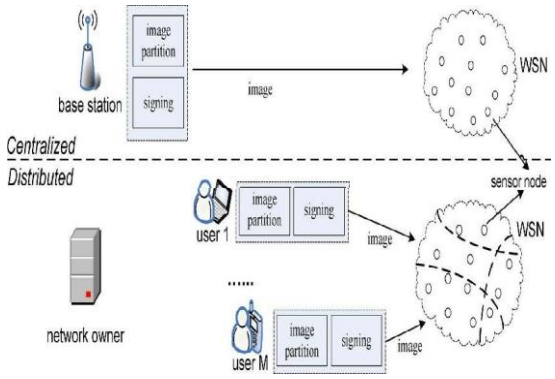

Fig. 1. System overview of centralized and distributed reprogramming approaches.

Quite recently, a novel secure and distributed reprogramming protocol named SDRP has been proposed, which is the first work of its kind. Since a novel identity-based signature scheme is utilized 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. Also, SDRP can accomplish all requirements of distributed reprogramming listed in [13], while keeping the merits of well-known mechanisms such as Deluge [14] and Seluge [9]. However, a design weakness exists in the user preprocessing phase of SDRP [15], and an antagonist can easily impersonate any authorized user to carry out reprogramming. To remove the identified security vulnerability, a simple modification has been proposed on SDRP without losing any features (such as distributed reprogramming, supporting different user privileges, user traceability, scalability, high efficiency, and robust security) of the original SDRP. Furthermore, for security and efficiency consideration, any efficient identity-based signature scheme which has survived many years of public scrutiny can be directly employed in SDRP [15].

The identity-based signature (IBS) scheme has been chosen which support all desirable characteristics of previous IBS schemes, and requires general cryptographic hash functions instead of MapToPoint hash function that is inefficient and probabilistic. Furthermore, this IBS scheme is significantly more efficient than all known IBS schemes and requires less computation cost, and the size of signatures is approximate 160 bits which is shortest identity-based signature generated so far [16]. Thus, in order to further improve the security and efficiency of SDRP, identity-based short signature scheme can be directly employed in SDRP.

The remainder of this paper is organized as follows. Section II briefly review SDRP and improved SDRP. Section III provides an approach to further improve the security and efficiency of SDRP. Section IV concludes this paper.

II. Brief Overview of SDRP and Improved SDRP

Secure and Distributed Reprogramming Protocol named SDRP [13], which expands Deluge to be a secure protocol. The main notion 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. A novel identity-based signature scheme is proposed for distributed reprogramming in WSNs. The proposed scheme can be significantly reduced efforts on certificate management and the transmission overhead. Since a novel identity-based signature scheme is utilized in generating the 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.

The SDRP consists of three phases: system initialization, user preprocessing, and sensor node verification. In the system initialization phase, the network owner creates its public and private keys and then assigns the reprogramming privilege and the corresponding private key to the authorized user(s). Only the public parameters are loaded on each sensor node before deployment. In the user preprocessing phase, if a network user enters the WSN and has a new code/program image, it will need to build the reprogramming packets and then send them to the sensor nodes. In the sensor node verification phase, if the packet verification passes, then the nodes accept the

code/program image.

An inherent design weakness has recognized in the user preprocessing phase of SDRP [15] and demonstrates that it is vulnerable to an impersonation attack by which an opponent can easily impersonate any authorized user to carry out reprogramming. SDRP is based on a novel and newly designed identity-based signature scheme. The simple alteration can fix the identified security problem ofthis signature algorithm without losing any traits of SDRP, but it is still uncertain whether there is any other security weakness in this modified identity-based signature algorithm. To address this problem, it is proposed that, instead of this novel identity-based signature algorithm, some efficient identity-based signature algorithms which have survived many years of public scrutiny can be directly employed in SDRP. For example, the provably secure identity-based signature proposed by Barreto et al. [17] can be chosen. The method proposed by Barreto et al. provides better security but it also improves the efficiency of SDRP due to the following two reasons. First, its signature verification operation only needs one pairing computation and, hence, is among the most efficient ones. Second, the length of its signature is reduced due to bilinear pairing.

Compared to the signature verification algorithm of the original SDRP which mainly requires two pairing, one hash-to-point, and one point scalar multiplication operations on a sensor node, the signature verification algorithm of the improved SDRP mainly requires one pairing, one point scalar multiplication, and one exponentiation operations on a sensor node and, thus, is more efficient. Different from that in [13], here, the implementation of sensor node side programs is completely based on TinyPairing (a pairing-based cryptographic library) [18], and there is no need to do any optimization.

III. Further Improvement of SDRP

An identity-based signature (IBS) scheme has been chosen which upholds all desirable features of previous IBS schemes, and requires general cryptographic hash functions instead of MapToPoint hash function that is inefficient and probabilistic. Moreover, this IBS scheme is significantly more efficient than all known IBS schemes and requires less computation cost, and the size of signatures is approximate 160 bits, which is the shortest identity-based signatures generated so far [16].

A comparison between short IBS scheme and BLM scheme [17] is listed in table I. Concretely, denote by sm a scalar multiplication in G_1 and by pr computation of one pairing and by exp an exponentiation computation in a multiplication group. Due to the cost of pairing computation, which is higher than that of other operations, short IBS scheme requires only a pairing computation. The scheme [17] requires one pairing operation too but it needs two exponentiation operations on G_T, which is time consuming when the embedding degree is large, since the research shows the exponentiation operation on multiplicative group is very time consuming when the embedding degree is large [19].

TABLE I
Efficiency Comparisons

Scheme	BLM[17]	Short IBS
Pre-Computation	1pr	1pr+2sm
Setup	1sm	1sm
Extract	1sm	1sm
Sign	1sm+1exp	1sm
Verify	1sm+1exp+1pr	1sm+1pr
Signature-Size	320bits	160bits

3.1. Improved SDRP using Identity-Based Short Signature

3.1.1. System Initialization Phase: The network owner executes the following steps.

3.1.1.1. Key Setup: Given a security parameter k, the network owner chooses two groups G_1 and G_2 of same prime order $q > 2^k$ and a modified Weil pairing map e: $G_1 \times G_1 \rightarrow G_2$. P is a generator of groups G_1. Let $g = e(P, P)$, then the network owner selects cryptographic hash functions $H_1 :\{0,1\}^* \rightarrow Z_q^*$, $H_1 :\{0,1\}^* \text{xG}_1 \rightarrow Z_q^*$ and picks a random number $s \in Z_q^*$ as its master key and computes its public key $P_{pub} = s\text{P} \in G_1$. Afterwards, the network owner publishes the system parameters $\{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$, but keeps s secret.

3.1.1.2. User public/private key generation: Given an identity $ID \in (0,1)^*$, the network owner computes $Q_{ID} = H_1(ID)$, $d_{ID} = (1/(s + Q_{ID}))\ P$, *and* sends d_{ID} to the user of identity ID as his private key by a secure channel. Here $Q = P_{pub} + Q_{ID}\ P$.

3.1.2. User Preprocessing Phase: User takes the following actions.

3.1.2.1. This step is the same as step 1) of the user preprocessing phase of the original SDRP.

3.1.2.2. Before signing, user firstly picks a random number $r \in Z_q^*$, computes $U = rQ = r(P_{pub} + Q_{ID} P)$ and broadcasts U as a public parameter, and then keeps r secret. In order to generate a signature for an identity ID on a message $m \in (0,1)^*$, user's work as described in the following. Sets $h = H_2 (m, U)$ and Computes $S = 1/(r + h), d_{ID} = (1/(r + h) (s + Q_{ID})) P$. Then S is the signature of an identity ID on a message m.

3.1.2.3. This step is the same as step 3) of the user preprocessing phase of the original SDRP.

3.1.3. Sensor Node Verification Phase: Upon receiving a signature message, each sensor node verifies it as follows.

3.1.3.1. This step is the same as step 1) of the sensor node verification phase of the original SDRP.

3.1.3.2. Given a signature S of an identity ID on a message m. Computes $h = H_2 (m,U)$ and Accepts the signature S and returns 1 iff the following equation holds:

$$Ver(m, ID, S) = 1 \Leftrightarrow e(S, U + hQ) = g;$$

otherwise, the node simply drops the signature.

3.1.3.3. This step is the same as step 3) of the sensor node verification phase of the original SDRP.

3.2. Performance Evaluation

Our Simulation based project has been designed in VB.Net. Table II Shows parameters used in the design.

TABLE II
Parameters Used in the Design

Routing Protocol	Deluge, SDRP
Nodes	35
Transmission Range	250m
Energy	100J
Mac Layer	802.11

The performance of improved SDRP using identity-based short signature scheme has been evaluated by considering metrics such as execution time, delay and network lifetime. The execution time measures the time duration of each operation of improved SDRP. The network lifetime chiefly depends on the energy consumption of the node.

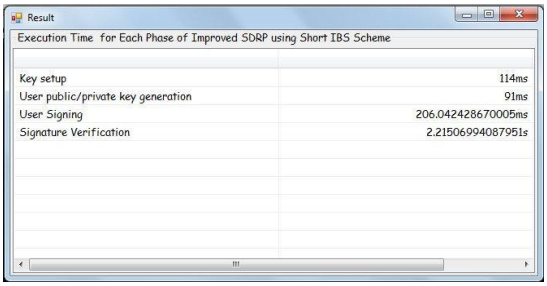

Fig.2. Execution time for each phase of Improved SDRP using short IBS scheme

Fig.2 shows execution time for each phase of improved SDRP using identity-based short signature scheme. Our evaluation shows that proportion of signature verification time in total reprogramming time is very small, so identity-based short signature scheme improve the efficiency of SDRP.

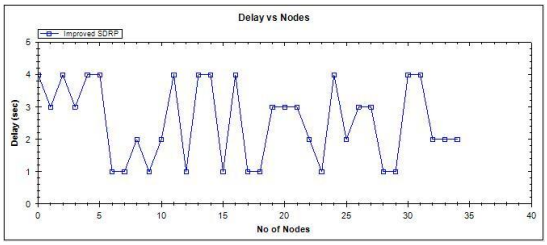

Fig.3. Delay Graph (Delay Vs Nodes)

Fig.3 shows improvement in packet delay performance.

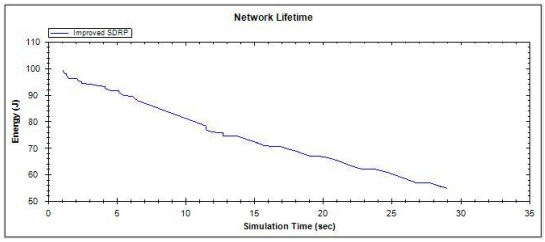

Fig.4. Network Lifetime (Energy Vs Simulation

Time)

Fig.4 shows energy consumption decreases with respect to simulation time.

IV. CONCLUSION

An identity-based signature scheme has been chosen, which upholds all desirable traits of previous IBS schemes, and is significantly more efficient than all known IBS schemes. Furthermore, this IBS scheme schemes requires less computation cost and the size of signatures is approximate 160 bits, which is the shortest ID-based signatures generated so far. So it can be used widely, especially in low-bandwidth communication environments. Thus, identity-based short signature scheme is directly employed in SDRP to improve the security and efficiency of SDRP.

REFERENCES

[1] V. C. Gungor and G. P. Hancke, Industrial wireless sensor networks: Challenges, design principles, and technical approaches, *IEEE Trans. Ind. Electron., 56(10)*, 2009, 4258–4265.

[2] V. C. Gungor, B. Lu, and G. P. Hancke, Opportunities and challenges of wireless sensor networks in smart grid, *IEEE Trans. Ind. Electron., 57(10)*, 2010, 3557–3564.

[3] 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., 57(11)*, 2010, 3596–3604.

[4] 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., 6(7)*, 2007, 762–776.

[5] R. C. Luo and O. Chen, Mobile sensor node deployment and asynchronous power management for wireless sensor networks, *IEEE Trans. Ind. Electron., 59(5)*, 2012, 2377–2385.

[6] P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, Securing the deluge network programming system, *Proc. IPSN*, 2006, 326–333.

[7] 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., 2011(1)*, 2011, 1–21.

[8] C. Parra and J. Garcia-Macias, A protocol for secure and energy- aware reprogramming in WSN, *Proc. IWCMC*, 2009, 292–297.

[9] S. Hyun, P. Ning, A. Liu, and W. Du, Seluge: Secure and DoS-resistant code dissemination in wireless sensor networks, *Proc. IPSN*, 2008, 445–456.

[10] D. He, S. Chan, C. Chen, and J. Bu, Secure and efficient dynamic program update in wireless sensor networks, *Secur. Commun. Netw., 5(7)*, 2012, 823–830.

[11] (2011) Geoss. [Online]. Available: http://www.epa.gov/geoss/

[12] (2012) NOPP. [Online]. Available: http://www.nopp.org/

[13] D. He, C. Chen, S. Chan, and J. Bu, SDRP: A secure and distributed reprogramming protocol for wireless sensor networks, *IEEE Trans. Ind. Electron., 59(11)*, 2012, 4155–4163.

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

[15] . He, C. Chen, S. Chan, and J. Bu, L. T. Yang, Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks, *IEEE Trans. Ind. Electron., 60(11)*, 2013, 5348– 5354.

[16] H. Du, Q. Wen, An Efficient Identity-based Short Signature Scheme from Bilinear Pairings, Proc. *IEEE CIS*, 2007, 725-729.

[17] P. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, Efficient and provably-secure identity-based signatures and signcryption from bilinear maps, *Proc. ASIACRYPT*, 2005, 515–532.

[18] X . Xiong, D. S. Wong, and X. Deng, TinyPairing: A fast and light- weight pairing-based cryptographic library for wireless sensor networks, *Proc. IEEE WCNC*, 2010, 1–6.

[19] N. Koblitz, A. Meneze, Pairing-based cryptography at high security levels, *Cryptography and Coding: 10th IMA International Conference*, LNCS 3796, Springer-Verlag, 2005, 13-36.