IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 18-22
www.iosrjournals.org

A Lightweight Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks – A Review

Pooja Motwani[1], Priyanka Fulare[2]
[1]*(Computer Science & Engineering Department, GHRIETW, Nagpur, India)*
[2]*(Computer Science & Engineering Department, GHRIETW, Nagpur, India)*

ABSTRACT : *Wireless reprogramming in a wireless sensor network (WSNs) is the process of propagating new code image or relevant commands to sensor nodes. While all existing insecure/secure reprogramming protocols are based on the centralized approach, it is important to support distributed reprogramming in which multiple authorized network users can simultaneously and directly reprogram sensor nodes without involving the base station. Very recently, a novel secure and distributed reprogramming protocol named SDRP has been proposed, which is the first work of its kind. The identity-based signature scheme has been chosen, which requires less computation cost and is significantly more efficient than all known IBS schemes, and the size of signatures is approximate 160 bits which is the shortest ID-based signatures so far. Compared to Deluge, Rateless Deluge has many advantages such as reducing latency at moderate levels of packet loss, being more scalable to dense networks, and generally consuming far less energy, a premium resource in WSNs.Thus, in order to further improve the reprogramming efficiency of SDRP, integrate SDRP with a more efficient reprogramming protocol like Rateless Deluge, leading to more secure and efficient distributed reprogramming.*

Keywords *-ID-based short signature,Reprogramming, Rateless Deluge, security, wireless sensor networks*

I. INTRODUCTION

Wireless reprogramming is the process of propagating a new code image or relevant commands to sensor nodes 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]–[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 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]–[10]. 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 lower 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. 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 [11], [12].

Quite recently, He *et al.* have proposed a secure and distributed reprogramming protocol named SDRP [13], 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 [13], while keeping the merits of the well-known mechanisms such as Deluge [14] and Seluge [9]. Also, SDRP has been implemented in a network of resource-limited sensor nodes to show its high efficiency in practice. However, a design weakness exists in the user preprocessing phase of SDRP [15], and an adversary can easily impersonate any authorized user to carry out reprogramming. To eliminate the identified security vulnerability, a simple modification has been proposed on SDRP without losing

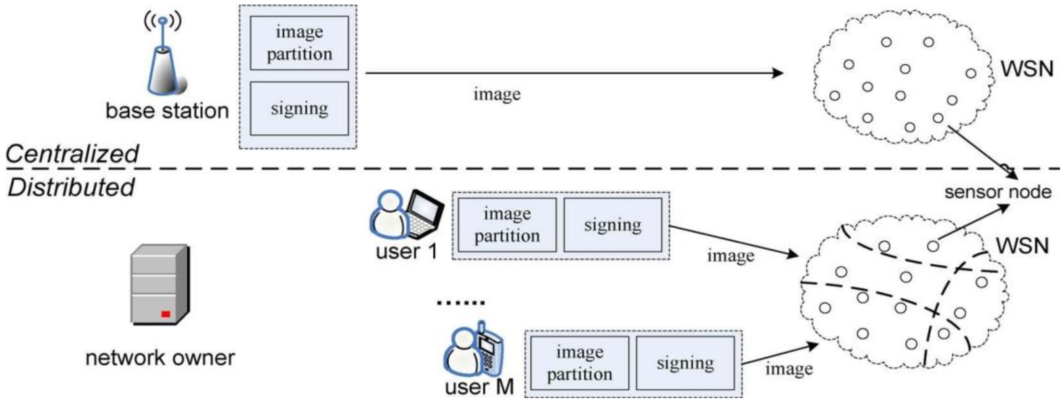

Fig.1. System overview of centralized and distributed reprogramming approaches.

any features (such as distributed reprogramming, supporting different user privileges, dynamic participation, scalability, high efficiency, and robust security) of the original protocol. Moreover, 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 [15].

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

Rateless Deluge modifies the original Deluge protocol in that it uses rateless codes to transmit data. Compared to Deluge, Rateless Deluge has many advantages such as reducing latency at moderate levels of packet loss, being more scalable to dense networks, and generally consuming far less energy, a premium resource in WSNs [17]. Thus, in order to further improve the reprogramming efficiency of SDRP in terms of energy, communication and delay, integrate SDRP with a more efficient reprogramming protocol like Rateless Deluge, leading to more secure and efficient distributed reprogramming.

The remainder of this paper is organized as follows. Section 2 briefly reviews SDRP and improved SDRP. Section 3 provides an approach to further improve the security and efficiency of SDRP. Rateless Deluge is presented in Section 4. Section 5 concludes this paper.

II. RELATED WORK

Secure and Distributed Reprogramming Protocol named SDRP [13], 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. A novel identity-based signature scheme is proposed for distributed reprogramming in WSNs. Through the proposed scheme, efforts on certificate management and the transmission overhead can be significantly reduced. Meanwhile, only the system public parameters are loaded on each sensor node. Since a novel identity-based signature scheme is employed 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.

An inherent design weakness has identified in the user preprocessing phase of SDRP [15] and demonstrates that it is vulnerable to an impersonation attack by which an adversary can easily impersonate any authorized user to carry out reprogramming. SDRP is based on a novel and newly designed identity-based signature algorithm. The simple modification can fix the identified security problem of this signature algorithm without losing any features of SDRP, but it is still uncertain whether there is any other security weakness in this modified identity-based signature algorithm. To address this issue, it is suggested 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. [18] can be chosen. Aside from providing better security, the method by Barreto et al. 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.

An identity-based signature (IBS) scheme has been chosen which requires less computation cost and is significantly more efficient than all known IBS schemes, and the size of signatures generated by scheme is approximate 160 bits, which is the shortest identity-based signatures so far. This scheme requires only a pairing computation. Although scheme [18] requires one pairing operation too, it needs two exponentiation operations on G_T, which is time consuming when the embedding degree is large, since the research [19] shows the exponentiation operation on multiplicative group is very time consuming when the embedding degree is large.

III. EFFICIENT IDENTITY-BASED SHORT SIGNATURE SCHEME

The basic signature scheme [16] consists of the following algorithms.

3.1 Setup

Given a security parameter k, the PKG choosestwo 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 PKG selects cryptographic hash functions $H_1 :\{0,1\}^* \rightarrow Z_q^*$, $H_1 :\{0,1\}^* \mathrm{x} G_1 \rightarrow Z_q^*$ andpicks a random number $s \in Z_q^*$ as its master key and computes its public key $P_{pub} = s\mathrm{P} \in G_{1.}$

Afterwards, PKG publishes the system parameters $\{k, G_1 , G_2 , e, q, P, g, P_{pub} , H_1 , H_2\}$, but keeps s secret.

3.2 Extract

Given an identity $ID \in (0,1)^*$, PKG 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 we define $Q = P_{pub} + Q_{ID}P$.

3.3 Sign

Before signing, the signer firstly picks a randomnumber $r \in Z_q^*$, 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 $m \in (0,1)^*$, the signer works as follows:

1). Sets $h = H_2 (m, U)$;

2). 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.

3.4 Verify

Given a signature*S*of an identity ID on amessage m.

1). Computes $h = H_2\,(m,U\,)$

2). Accepts the signature S and returns 1 iff the following equation holds:

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

The correctness of the verification algorithm is proved as follows:

$$e(S,U + hQ)= e(S, rQ +hQ) = e(S, (r(P_{pub} +Q_{ID}P) + h(P_{pub} +Q_{ID}P))$$
$$= e((1/(r + h) (s + Q_{ID})) P, (r + h)(P_{pub} +Q_{ID}P)) = e((1/(r + h) (s + Q_{ID})) P, (r + h)(s +Q_{ID}P))$$
$$= e(P, P) = g$$

I. RATLESS DELUGE

Rateless codes [17] provide an efficient means of addressing channel contention in sensor networks, while at the same time minimizing control messages. Fundamental to this strategy is the fact that receivers do not need to indicate which specific packets require retransmission; instead, they just have to receive a sufficient number of independent packets, which can then be used to decode the original message. Rateless coding, thus, yields several key benefits, namely: communication and energy savings, and lower control overhead. For the coding, Random Linear Codes were selected as they are rateless and allow for lightweight implementations. Random linear coding provides a simple method for file dissemination. It supports two features: (1) it has no decoding inefficiency; and (2) it is a rateless code.

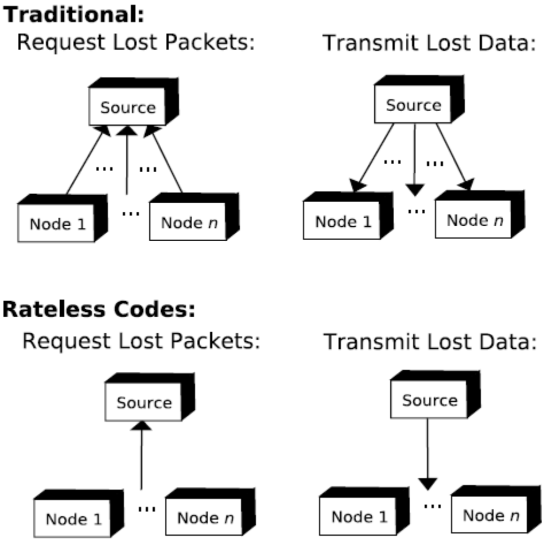

Fig. 2. A motivating example of the best-case gain achievable with rateless codes. If each receiver misses a different packet, the traditional mode requires the tranmission of *n* requests and *n* retransmissions. However, with rateless codes only 1 request and 1 retransmission is required.

As a simple example of the best-case gain achievable with rateless codes, consider a one-hop clique consisting of a basestation and *n* sensor nodes. Suppose that the base station broadcasts *n* data packets and each node in the network fails to receive a different packet. A traditional data dissemination protocol, such as Deluge, would require that each sensor transmits (on one shared broadcast channel) a NACK control packet with the ID of its missing packet. Upon reception of these *n* NACKs, the base station would have to retransmit all *n* data packets. On the other hand, with rateless coding only one sensor needs to request the transmission of an additional encoded packet (assuming the other nodes can overhear that request). Once the base station transmits one new packet, each node can use this packet to recover the data. Rateless coding thus yields an *n*-fold reduction in communication cost on boththe control and data planes in this case.

Rateless Deluge [17] modifies the original Deluge protocol in that it uses rateless codes to transmit data. This change causes significant structural changes to the mechanism for requesting and transferring data so that communications in the control and data planes are reduced. The change to the request mechanism is fairly simple. Rateless Deluge does not require knowledge of the specific packets missed and therefore the transfer of a bit vector of missed packets is unnecessary. Only the numberof missed packets must be transferred which can be represented as a single byte. In Deluge, if a node overhears a request packet, it suppresses its own requests if the overheard bit vector is a superset of its own bit vector. Otherwise, the node transmits its own request to the source. In rateless Deluge, a node requests more packets only if it does not overhear another request containing a larger number of requested packets.

II. CONCLUSION

An identity-based signature scheme has been chosen, which requires less computation cost and is significantly more efficient than all known IBS schemes, and the size of signatures is approximate 160 bits which is the shortest ID-based signatures so far. Thus, identity-based short signature scheme can be directly employed in SDRP to further improve the security and efficiency of SDRP. Compared to Deluge, Rateless Deluge has many advantages such as reducing latency at moderate levels of packet loss, being more scalable to dense networks, and generally consuming far less energy, a premium resource in WSNs.Thus, in order to further improve the reprogramming efficiency of SDRP in terms of energy, communication and delay, SDRP can be integrate with a more efficient reprogramming protocol like Rateless Deluge, leading to more secure and efficient distributed reprogramming.

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] D. 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] A. Hagedorn, D. Starobinski, and A. Trachtenberg, Rateless Deluge: Over-the-air programming of wireless sensor networks using random linear codes, *Proc. ACM/IEEE IPSN*, 2008, 457-466.

[18] 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.

[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.