International Journal of Scientific Research and Management Studies (IJSRMS)
ISSN: 23493771 **Volume 1 Issue 10, pg: 301-306**

SECURE ONLINE-OFFLINE IDENTITY-TYPED SIGNATURE SCHEME

Sattar J. Aboud
University of Bedfordshire,
Department of Computer Science and Technology, United Kingdom

ABSTRACT

In this paper, we introduce online-offline an identity-typed signature scheme for a wireless sensor network. Because of major cut in computing time, the proposed scheme is more appropriate for a wireless sensor network setting with strictly limited resources. One of the interesting characteristics of the proposed scheme is that it gives multi-time service of an offline storage, which lets the signer to reprocess offline by recalculation the data in polynomial time, against one-time service in all preceding online-offline signature schemes. As facts of a realism and viability of a proposed scheme is used in a wireless sensor network milieu, we give the achievement result of the proposed scheme.

KEYWORDS: *wireless sensor network, identity-typed signature, online-offline signature, authentication services.*

I. INTRODUCTION

The wireless sensor network is contained locative distributed independent devices to considerately monitor conditions, for example pressure, temperature, motion at diverse locations. There are various possible uses for wireless sensor network. For instance used in commercial uses to monitor information that is hard to monitor using wired sensors. They are also moved in wilds areas; where they are stay in process without want to substitute the power supply.

Wireless sensor network is weak against different attacks because of the environment of wireless communication. For instance, in data lines where sensors gather information and send them to base station, it must be certain that the collected information are real and have not been changed in broadcast to prevent failure of the employees. For instance [1] the health care system where data regarding elderly people are sent from sensor to base station. The authenticity of information sent by sensors is vital in those systems since have grave cost for the citizens in serious circumstances. As sensors have limited resources in terms of communication, giving genuineness in wireless sensor network dissimilar than conventional network security. This needs power-saving cryptography to support wireless sensor network security. The advantage can get from using public key encryption scheme to simplify necessary services with key delivery to decreases broadcast power.

One important issue must be resolved to use public key encryption in wireless sensor network is to construct the public key infrastructure to create the trusted identity. The public key infrastructure for wireless sensor network is important to build [2]. In this paper, we give information authentication services and identity-typed signature schemes for other users to check signatures that the signer produced. The Id-typed encryption, presented by Shamir [3], removed the need for verifying the validity of certificates. The private key calculates from the master private key for the users. This characteristic prevents the condition of using certificates and connects a public key to every user within the scheme. In the case of Id-typed signature, checking takes an identity together with a message and signature as input and implements the scheme straight. This is dissimilar from the conventional public key encryption, while the extra certificate checking scheme is required which is equal to the operation of two signatures checking. Identity-typed encryption might mostly be

appropriate for wireless sensor network. The lack of certificate reduces the costly certificate checking process. Also, if there is a new node added to the network. This can really decrease communication and calculation cost, which is an important issue in the wireless sensor network.

The idea of online-offline signature scheme was presented by Goldreich and Micali [4]. It performs a signature generation in two stages. The first stage is performed offline and the second stage is performed online. In wireless sensor network, the offline stage can be carried out at the base station, while the online stage is performed in the wireless sensor network node. The online stage is very quick, and can be achieved efficiently even on the vulnerable processor, such as the node in wireless sensor network. Goldreich-Micali introduced a method to change the signature to online-offline signature scheme. But, the scheme is not practical because it adds to the length of a signature. Shamir-Tauman [5] introduced the method for online-offline signature scheme. Also, their scheme is not practical. Certain solid scheme has been presented in [6] and demonstrated secure without random oracle.

In this paper, we introduce a secure online-offline Id-typed signature scheme which is appropriate for wireless sensor network. It has the following characteristics:

1. In the random oracle should be secure.
2. Compare with two existed schemes it needs less computing time and less storage cost.
3. It does not need the pairing process in signature generation and verification. Thus, the proposed scheme can be easily executed in wireless sensor network nodes.
4. It appropriate for node-to-node communication in wireless sensor network
5. It makes offline data to be re-usable. It means that the signer is not needed to execute the offline method each time if needs to sign a new message.
6. The offline signing method is not needed any private data from a signer. It can be made by any trusted authority involving the public key generation. This is useful for the wireless sensor network node as the base station. This can save many communication bandwidths.

The remaining of this paper is organized as follow. We describe the related works in Section 2. The proposed scheme is discussed in Section 3, followed by the security and performance analysis in Section 4and the paper is concluded in Section 5.

II. RELATED WORKS

There are only two existed Id-typed online and offline signature schemes. The first was presented by Xu, et al. in 2006 [7]. In their scheme, the signer requires to carry out the offline stage each time if needs to construct the signature. This means that the offline signature can be utilized only one time and it cannot be reprocessed. When we use this scheme into wireless sensor network, it becomes not practical because, the offline stage is made at the base station; involves that sensors require to return to the base station each time to find the next offline signature. Also, the verification of Xu, et al. scheme needs the pairing process, which is costly computing process for the sensor node and makes the signature scheme is not suitable for node-to-node signature in wireless sensor network. Later, it was discovered by Li et al. [8] that the Xu, et al. scheme is forgeable. The second was introduced by Liu et.al in 2010 [9]. One of the properties of this scheme is that it gives multi-time use of the offline storage, which lets the signer to reuse the offline pre-computed data in polynomial time. It means that the signer is not needed to perform the offline stage each time if needs to sign the new message. However, there is no secure identity-typed online-offline signature scheme presented so far.

III. THE PROPOSED ID-TYPED SIGNATURE SCHEME

In this section, we describe the proposed scheme. It has the following protocols:

Setup Protocol: This protocol contains the following steps:

1. Suppose that G is the multiplicative group of prime order q
2. The private key generator chooses the arbitrary generator $g \in G$
3. It arbitrarily selects $k \in Z_q^*$.

4. Compute $f = g^k \bmod q$
5. Assume that $h : (0,1) \to Z_q^*$ is a secure hash function
6. The public parameters are $e(G, q, g, f, h)$
7. The master secret key is $d = k$

Extract Protocol: To generate a private key for identity *Id*. The protocol should do the following steps:

1. The private key generator randomly chooses $l \in Z_q^*$
2. Find $w = g^l \bmod q$
3. Find $p = l + h(w, Id)k \bmod q$
4. The user private key is (w, p)
5. The properly generated private key must satisfy $g^p = fw^{h(w,Id)} \bmod q$ (1)

Offline Sign Protocol: In offline protocol the signer should do the following steps:

1. Find $n_i^{'} = g^{2^i}$ *for* $i = 0,\ldots,|q|-1$
2. Do not need to know the message and the private key.

Online Sign Protocol: In the online protocol, the signer should do the following steps:

1. Choose arbitrarily $j \in Z_q^*$
2. Assume $j[i]$ be the $i-th$ bit of j
3. Assume that $Y \subset (1,\ldots,|q|)$ to be the set of indices where $j[i] = 1$
4. Find $n = \prod_{i \in j} n_{i-1}^{'}$
5. Find $u = h(n, w, m)$
6. Find $z = j + u \cdot p \bmod q$
7. The signature is (n, w, z)

Verify Protocol: To check the signature (n, w, z) the verifier should do the following:

1. Find $u = h(n, w, m)$
2. Verify $g^z \equiv nw^u f^{u \cdot h(w,Id)} \bmod q$ (2)
3. If yes accept it. Else reject it

Correctness

We have $nw^u f^{u \cdot h(w,Id)}$

$$= g^j g^{l \cdot u} g^{k \cdot u \cdot h(w,Id)}$$
$$= g^{j+u(l+h(w,Id)k)}$$
$$= g^{j+u \cdot p}$$
$$= g^z$$

Remarks

1. The offline signing phase can be implemented by any trusted authority as no private data is included. If we set the offline signing phase as part of the process which is performed by the private key generation, the proposed scheme can be consider as the standard identity-typed signature scheme with efficient signing method that is not need any exponentiation.
2. It is potential to revoke node private keys in different ways. For instance, one can add expiration-date to an identity, so the private key connected with an identity [10]. Also, the base station can keep the revocation list on the compromised nodes, which hold the *R* values.

IV. SECURITY AND EFFICIENCY ANALYSIS

In this section we will consider the security and the performance analysis of the proposed scheme.

4.1 Security Analysis

Suppose that there is the forger *A*. We create the algorithm B that utilize by *A* to find discrete logarithm problem. The algorithm *B* is given the primitive group G with primitive g and prime order q, and the group element $t \in G$. The algorithm *B* should compute $a \in Z_q$ where $g^a = t$.

Setup: The algorithm *B* should do the following:

1. Select a secure hash function $h:(0,1)^* \to Z_q$, which similar to the random oracle.
2. Find $f = t$
3. Send a public key $e = (G, q, g, f, h)$ to *A*

Extraction Oracle: This protocol contains two phases which are as follows:
The first phase: The hacker *A* should do the following step:

1. Permit the query taking out oracle for the identity *Id*

The second phase: The algorithm *B* should do the following steps:

1. Select randomly $a, b \in Z_q$
2. Compute $w = f^a g^b$
3. Compute $p = b$
4. Compute $h(w, Id) = -a$
5. Determine (w, p) as a private key of *Id*
6. Keep the result of $(w, p, h(w, Id)Id)$ in the table.

Signing Oracle: This protocol contains two phases which are as follows:
The first phase: The hacker *A* should do the following step:

1. Check the signing oracle for m and Id

The second phase: The algorithm *B* should do the following steps:

1. Verify if Id has been checked for a random oracle
2. If yes, recovers $(w, p, h(w, Id))$ from the table
3. Sign a message m by the signing method.
4. Determine the signature (n, w, z) for the message m
5. Keep the result $h(n, w, m)$ in the hash table.
6. Implement the taking out oracle and use the related private key to sign the message

Output Calculation: This protocol contains two phases which are as follows:
The first phase: The hacker *A* should do the following step:

1. Determine the forged signature $s(n^*, w^*, z_1^*)$ on message m^* and identity Id^*

The second phase: The algorithm *B* should do the following steps:

1. The hacker *A* return to the point $h(n^*, w^*, m^*)$
2. Provide with a dissimilar value.

The hacker *A* should do the following step:

1. Compute a new pair of signature $s_2^* = (n^*, w^*, z_2^*)$

The algorithm *B* should do the following steps:

1. Find $s_3^* = (n^*, w^*, z_3^*)$
2. Reminder that n^* and w^* must be the same each time

Remarks:

1. Assume that o_1, o_2, o_3 are the result of a random oracle $h(n^*, w^*, m^*)$.
2. By $l, k, y \in Z_q$ represent discrete logarithm of w, Z, n as $g^l = w$, $g^k = f$ and $g^j = n$

3. From formula (2), we have $z_i^* = j + lo_i + ko_i h(w^*, Id) \bmod q \quad for\ i = 1,2,3$
4. In these formulas, only l, j, k are unknown to the algorithm B
5. Hacker can find these value and result k as the answer of a discrete logarithm problem

4.2 Efficiency Analysis

The exponentiation is the same as point multiplication in elliptic curve scheme and multiplication is the same as point addition in elliptic curve scheme. As 160-bit elliptic curve scheme key uses more or less the same level of security as 1024-bit RSA, we can apply the proposed scheme using elliptic curve scheme by $|q| = 160\,|G|$ and can be as short as 160 in the best case by selecting proper curve [11]. We apply the following comparison with other systems.

We compare the efficiency of the proposed system with other Id-typed online-offline systems that are Shamir-Tauman [5] and Xu, *et al* [7]. These schemes are not given the multi-time service of the online-offline schemes. We indicate C to the computing cost of operation. Also we indicate by P the pairing operation, E an exponentiation in G, M the multiplication in G, and m' a modular multiplication in Z_q^*. Table 1 illustrates the comparison of computing cost. The h, indicates the hash operation which needs no less than one E exponentiation. The s_g, and s_v denote a signature generation and verification, which need as a minimum one E exponentiation for every operation. Also, $cert_v$ indicates the certificate verification, which also needs no less than one E exponentiation.

Also, Table 1 illustrates the comparison of offline storage cost and length of the signature. For example, $|q|$ and $|G|$ are both 160 bits. The $|s|$ indicated the size of the digital signature which is as minimum 160 bits. The $|c|$ indicated the size of the digital certificate which is no less than 320 bits.

Table 1: Comparison of Computing Cost

	Scheme [5]	Scheme [7]	Proposed Scheme
Online (one-time)	m'	m'	m'
Online (multi-time)	-	$O(\|q\|)\cdot 2M + m'$	$O(\|q\|)\cdot M + m'$
Offline (one-time)	$C(h) + C(s_g)$	$2\mathrm{E} + m'$	0
Offline (multi-time)	-	$\|q\|\cdot 2\mathrm{E}$	0
Verification	$C(h) + C(s_v) + C(c_v)$	$2P + 2\mathrm{E} + M$	$2\mathrm{E} + M$
Offline storage (one-time)	$2\|q\| + \|s\| + \|c\|$ $\geq 800 bits$	$2\|G\| + 2\|q\|$ $\approx 640 bits$	$\|G\| + \|q\|$ $\approx 320 bits$
Offline storage (multi-time)	-	$2\|q\|\cdot\|G\|$ $\approx 6.4 kbytes$	$\|q\|\cdot\|G\|$ $\approx 3.2 kbytes$
Size of signature	$\|q\| + \|s\| + \|c\|$ $\geq 640 bits$	$2\|G\| + \|q\|$ $\approx 480 bits$	$2\|G\| + \|q\|$ $\approx 480 bits$

From the table 1, we can claim that the introduced scheme is more efficient than Shamir-Tauman scheme. But, if we compare it with the Xu, *et al.* scheme, we get around 50% enhancements over space and computing efficiency in both the online-offline stage. Also, in the proposed scheme the offline stage can be made by the private key generator, the signer is not has any computing cost in the offline stage while the Xu, *et al.* scheme needs more than 320 E operations. The most important enhancement concentrates on signature verification. We do not need any pairing operation whereas the Xu, *et al.* scheme needs. It is mainly proper for the wireless sensor network milieu where the sensor node is not have sufficient computing power for the pairing operation.

V. CONCLUSION

We introduced a secure online-offline Id-typed signature scheme which is not needed any certificate to be added to a signature for verification, and is not needed the pairing operation in both signature generation and verification. Also, the proposed offline signing algorithm is not needed the private key. This is an important benefit in wireless sensor network since it can reduce any transmission between the sensor node and the base station, which is believed a costly issue in the wireless sensor network. The size of this offline data is around 160 bits. It can be signing the few messages. But, if the sensor needs signing thousand of messages, these 160 bits are small. Thus the proposed scheme is appropriate for large scale network.

REFERENCES

[1] Perrig A., Stankovic J. and Wagner D., "Security in wireless sensor networks", *Communications of the ACM*, 47(6):53–57, 2004.

[2] Li, F. , Di Zhong , Takagi, T., "Practical Identity-Based Signature for Wireless Sensor Networks", Wireless Communications Letters, IEEE, Volume:1 Issue:6, 2012.

[3] Shamir A., "Identity-based cryptosystems and signature schemes", *Proceeding CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53, Springer-Verlag, 1984.

[4] Even S., Goldreich O. and Micali S., "Online/offline digital signatures", *Proceeding CRYPTO '89*, volume 2442 of *Lecture Notes in Computer Science*, pp. 263–277, Springer-Verlag, 1989.

[5] Shamir A. and Tauman Y., "Improved online/offline signature schemes", *Proceeding of CRYPTO'01*, volume 2139 of *Lecture Notes in Computer Science*, pp. 355–367, Springer-Verlag, 2001

[6] Boneh D. and Boyen X., "Short signatures without random oracles the SDH assumption in bilinear groups", *Journal of Cryptology*, 2:149–177, 2008.

[7] Xu S., Mu Y., and Susilo W., "Online-offline signatures and multi-signatures for AVOD and DSR routing security", *Proceeding of ACISP'06*, volume 4058 of *Lecture Notes in Computer Science*, pp. 99–110, Springer-Verlag, 2006.

[8] Li F., Shirase M., and Takagi T., "On the security of online-offline signatures and multi-signatures from acisp'06", *Proceeding of CANS'08*, volume 5339 of *Lecture Notes in Computer Science*, pp. 108–119, Springer-Verlag, 2008.

[9] Joseph K. Liu, Joonsang Baek, Jianying Zhou, Yanjiang Yang, and Jun Wen Wong, "Efficient online-offline identity-based signature for wireless sensor network", International Journal of Information Security, volume 9, no. 4, pp. 287-296, 2010.

[10] Jayaprakash Kar, Provably Secure Online/Off-line Identity-Based Signature Scheme for Wireless Sensor Network, https://eprint.iacr.org/2012/162.pdf

[11] Boneh D., Lynn B. and Shacham H., "Short signatures from the Weil pairing", Proceeding *of ASIACRYPT'01*, volume 2248, *Lecture Notes in Computer Science*, pp. 514–532, Springer-Verlag, 2001

Author Profile

Sattar J. Aboud, received his Master degree in 1982 and a PhD in 1988 in the area of computing system. The two degrees were awarded from U.K. In 1990, he joined the Institute of Technical Foundation in Iraq as an assistant professor. In 1994 he joined the Philadelphia University in Jordan as associate professor and chairman of computer science department. Then, he moved as a professor at the Middle East University for Graduate Studies, Amman-Jordan. Currently, he is a visiting professor at University of Bedfordshire in UK. His research interests include areas such as public key cryptography, digital signatures, identification and authentication, networks security and cyber security. He has supervised numerous PhDs and Masters Degrees thesis. He has published more than 100 research papers in a multitude of international journals and conferences.