World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 299-303, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2259

Multi Resigncryption Protocol Scheme for an Identification of Malicious Mobile Agent Host

V. Khanaa, K.P. Thooyamani and R. Udayakumar

School of Computing Science, Bharath University, Chennai-73, India

Abstract: As a promising distributed computing technology, Mobile Agent (MA) can be used in many fields. But the security problem of MA is a barrier for application of MA technology. Attack on mobile agent by malicious agent and abstract all the relevant information from agent like route information, services and data is the major problem on mobile agent in distributed environment. To overcome the mobile agent attack a multi signcryption protocol scheme is being adapted to protect data integrity, data confidentiality and user authentications. Also the Multi Signcryption protocol schemes hides the route used by the mobile agent is being encrypted which is known by only the mobile agent owner alone. Mobile agent authentication, data integrity and confidentiality are being checked in electronic commerce application using signcryption protocol scheme. Multi signcryption protocol scheme can detect tampering situation and can possibly identify the responsible malicious host. With Mobile Agent is becoming common in a variety of applications on Electronic Commerce, how to protect the transaction security is the key technology of based Agent Electronic Commerce System. Also the current signcryption techniques has broadcasting problem to multiple users in the network so protected subscriber agent(PSA) is used with universal key approach along with ReSigncryption techniques for secure broadcasting over the networks.

Key words: Mobile agent · Multi signcryption · ReSigncryption · Malicious host · Protected Subscriber Agent (PSA)

INTRODUCTION

Based on message coverable signature and encryption algorithm, Nyberg and Rueppel [4] put forward an authenticated encryption scheme in the year 1994. Later on, in order to generate the authenticated scheme, both signature and encryption were merged. In the year 1997, [5] YuLiang Zheng presented an authenticated encryption scheme named signcryption; signcryption is the abbreviated form of signature and encryption. In a signcryption scheme, signature and encryption are organically combined; signcryption can achieve signature authentication and encryption transmission simultaneously in a single protocol and thus effectively prevents mutual cheating by message sender and the receiver. Signcryption provides both confidentiality and authenticity in a single protocol simultaneously. Previously, these two goals had been considered separately, with encryption scheme provide confidentiality and digital signature provides authenticity. In many cases both of these two techniques were required, so encryption operations and digital signature operations were simply sequentially composed. And it is possible to achieve significant savings both in computational and communication overhead. Since a wide variety of signcryption schemes have been proposed. [1] Compared with other schemes, such as encryption plus signature or signature plus encryption, the computation and communication in signcryption have been greatly reduced and expansion of information rate has also been successfully reduced. The study on signcryption mainly focuses on designing applicable schemes with high efficiency and feasibility and the security proof of various signcryption schemes. At present, many signcryption schemes with different properties have been presented, such as signcryption with forward security, DSA verifiable signcryption and authenticated public key signcryption, etc. In some signcryption schemes, for

Corresponding Author: V. Khanaa, School of Computing Science, Bharath University, Chennai-73, India.

example, publicly verifiable signcryption scheme of Ma-Chen, the verification by the third party will not be valid and the third party will judge valid signcryption message to be invalid with a high probability.

In this paper a major problem in signcryption is broadcasting the same signcrypted message to multiple user in network is not secured. So here we adopt a ReSigncryption techniques for broadcasting message using a protected subscriber agent along with centralized key server for all users on the network and also to overcome the mobile agent attack this scheme is being adapted to protect data integrity, confidentiality and user authentication.

Related Work: In 2009, [1] Chuanrong and Yuqing A new secure mobile agent protocol using a novel cryptographic technique signcryption was proposed. In this paper, the protocol offers confidentiality and integrity to the messages carried by a mobile agent and also provides user authentication and nonrepudiation. Moreover, its efficiency is high with respect to the computational cost and communication overhead. Typically, the route message of a mobile agent is protected by a domain-verifiable signcryption scheme and tampering situations can be detected a certain extent.

In domain verifiable signcryption scheme each participants will decrypt their own messages and all the other participants were verify it. This scheme is mainly applied in Electronic funds Transfer (EFT) protocol in [8] which was first proposed by Seo and Kim in 2004. This signcryption scheme was also applied in any other protocols in which partial information of each participant has to be kept secretly, simultaneously there total messages were authenticated by all participants. For multi users, SL multi signcryption protocol scheme was proposed by Seo and Lee in 2004 [9]. In this both the encryption and digital signature functions were satisfied for multi users. It provides user authentication, message integrity non repudiation and confidentiality.

In the signcryption scheme of [5] the (de-signcryption and signature verification) needs the recipients private key; therefore, only the recipient can verify the signature. As pointed out in [10], the constraint of using the recipient's private key in Unsigncryption is acceptable for certain applications where the recipient need not pass the signature to others for verification.

In the year 2004, universal Re-encryption concept was introduced by Golle *et al*. [11] based on ElGamal encryption scheme was implemented over any suitable algebraic group. In this scheme, a cipher text is supposed to be re-encrypted without public information corresponding to it. Moreover, only a subject that re-encrypts a cipher text can know the correspondence of original cipher text and it and the computational complexity to break the unlinkability property is equal to the semantic secrecy Based on the ElGamal cryptosystem the Re-encryption process takes place.

Bao and Deng [7] modify Zheng's signcryption scheme. This modified scheme functions in exactly the same manner as that of the signature-then-encryption approach. Klonowski *et al* proposed the scheme which adds the signature property on the cipher text given by the Universal Re-encryption (RSA-URE signature scheme) [12]. In their scheme, while the message is relayed out and re-encrypted repeatedly, the signature property is universally preserved.

Tatara and Sakurai [2] introduced universal re signcryption scheme based on the discrete logarithm.

Proposed Scheme

Signcryption: In the Signcryption scheme we present here, the sender to send a digitally signed message to the protected subscriber agnet and this agent can verify the authenticity of this message. This scheme uses the private key of the sender to sign the message and the protected subscriber agent(PSA) uses the sender's public key to verify the signature.

Re Signcryption: In the ReSigncryption scheme, the protected subscriber agent is a hide able agent sends a signcrypted message to the receivers and this agent can verify the authenticity of this message. This process uses the same procedure of the general signcryption, private key of the protected subscriber agent to sign the message and the receiver uses the subscriber agent universal public key to verify the signature. In this scheme, the protected subscriber agent maintains a registry of the authenticated subscriber details. Based on the detail, the PSA send the required message only to the authenticated subscribers.

System Architecture: The Figure 1 represents the architecture where the signcryption protocol is being built to protect the mobile agents from the malicious host of the agent's. Initially the signcryption is being done using the Key approach where a Public key is known by the entire user in the network. But since the network is large with many user is its big problem to transmit the same signcrypted message to all the user (broadcasting). To overcome the problem a protected subscriber agent is

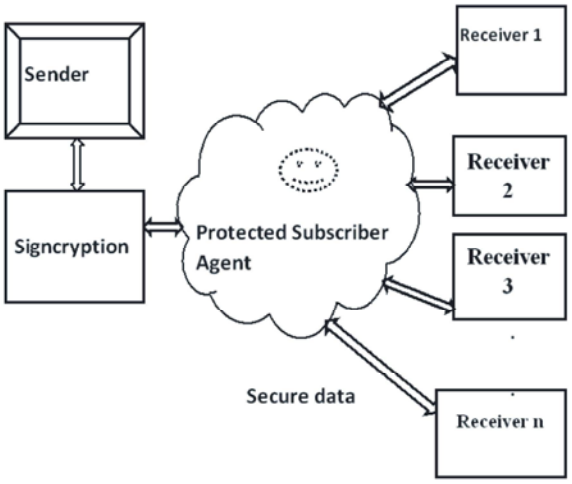

Fig. 1: Architecture for Resigncryption Scheme.

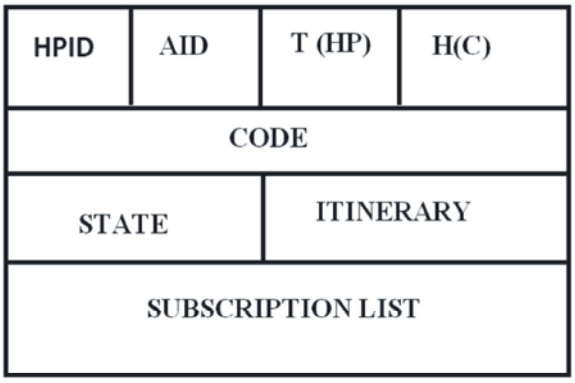

Fig. 2: Data Sheet of Subscriber Agent

adopted with ReSigncryption techniques is being done. A distributed key server is available with a manager for server contains all the information about the entire host on the networks.

Suppose a user want to send information to the all users on the network then initially the information is being encrypted and signed using signcryption techniques by public key to all hosts. Since the information in need to be transmitted to the multiuser, so the phase information sent is adopted by the protected subscriber agent on the network.

The Figure 2 represents the data sheet of subscriber agent. In this datasheet, HPID is the Home Platform Identity which is generated by the Host Agent Platform, AID represents the Identity of the Mobile Agent and is unique for a Mobile Agent in the entire system, which is generated by the Manager Agent, T (HP) represents the timestamp at which the Mobile Agent left the Home Platform and H(C) is the hash value of the Agent code obtained by means of a Hash function. The Code part of the Mobile Agent contains information about the negotiation, decisions and the next platform choice. The state contains information about the data structures and execution state containing the control information. The Subscription List has details of service subscribed and subscription validity details.

When the information is obtained from the subscriber agent, the PSA will check the authentication details. Once it is verified, the PSA will provide service to the subscriber agent by requesting the public key of the host in order to signcrypt the particular message. If all the receivers got the message, then they will resigncrypt the information using public key of the Sender. Otherwise the service provided to the subscriber agent will discard. Similarly the described signcryption process is carried for all the messages to be transmitted in a secure form.

Mobile Agent Initial Signcryption Procedure

Initialization Procedure: The public parameters:

P: a large prime.
q: a large prime factor of p - 1 and $q \in z^*_p$
g: an element of z^*_p of order q.
hash: a one-way hash function.
KH: a keyed one-way hash function.
(E, D): the encryption and decryption algorithms.
$(X_{hi}, y_{hi}) = (g^{xhi} \bmod p)$: denotes the private and public key of $host_i$ (0= i = n).
Agent owner $Host_0$: picks out n hosts (n = 1, 2, 3…n).

Signcryption Procedure: $Host_0$ randomly chooses $x_0 \in z^*_q$ then sets

$K_1 = \text{hash}(y_{hi}^{xh0} \bmod p)$, K_2, $K_3 \ldots K_n$.
$K = \text{hash}(g^{x0} \bmod p)$
$C_1 = E_{K1}(m_1)$, $C_2 = E_{K2}(m_2) \ldots C_n = E_{Kn}(m_n)$.
$r_1 = KH_K(m_1 \| C_2 \| \ldots \| C_n)$, $r_2 = KH_K(C_1 \| m_2 \| \ldots \| C_n)$,
$\ldots r_n = KH_K(C_1 \| C_2 \| \ldots \| m_n)$.
$S = x/(r_1 r_2 \ldots r_n + x_a) \bmod q$.

$Host_i$ sends $(C1, C_2 \ldots C_n, r_1, r_2 \ldots r_n, S)$ to mobile agent m_i and then mobile agent migrates to $Host_1$.

Unsigncryption Procedure: $Host_1$ calculates

$t = (y_{h0} \cdot g^{r1r2 \ldots rn})^s$ and mod p
$t_i = t^{xhi} \bmod p$.
$K = \text{hash}(t)$.
$K_i = \text{hash}(t_i)$

$m_i = D_{Ki}(c_i)$ to obtain $host_i$'s own plain text message then check whether

$KH_K(C_1 || \ldots || m_i || \ldots || C_n) = r_i$

for sign verification.

Later, if necessary the mobile agent has migrated to $Host_i$. Firstly $Host_0$'s forward $(C_1, C_2 \ldots C_n, r_1, r_2 \ldots r_n, S)$ to any other participants who want to decrypt his own message to mobile agent (m_i).

Finally, the message is transfer for resigncryption process.

Protected Subscriber Agent Resigncryption Procedure: In this section, we directly show the implementation of a protected subscriber agent a hide able agent signature using resigncryption.By using this scheme; a sender sends a single message to multiple recipients.

Setup Procedure: The original signer creates the secret (x_{ap}, K) and securely transmits it to the protected subscriber agent. Choose a secret random number x from [1…q-1] and calculate $K = g^x \bmod p$ and $x_{ap} = x_a + xK \bmod p-1$.The values (p, q, g) are public parameter of the signature scheme, K is a public value and x_{ap} is a share secret between the principle and the protected subscriber agent.

The protected subscriber agent accept x_{ap} as a valid proxy right from sender, if and only $g^{xap} = (y_a . K^K) \bmod p$.The protected subscriber agent public key $y_{ap} = y_a . K^k \bmod p$

Signcryption by Protected Subscriber Agent: X': a secret random number from [1…q-1] chosen independently for each signing operation by the protected subscriber agent.

$K = y_b^{x'} \bmod p$

$K_1 || K_2 = K$,

$r' = KH_{k2}(m)$ or equivalently hash (k_2, m),

$s' = x'/(r'+x_{ap}) \bmod q$, $C = E_{K1}(m)$ and $cryptogram_{ap}(m) = (c,r',s',K)$.

Protected signed, signcrypted message m from sender to receiver.

Unsigncryption by Receivers: Recover k from signature (r', s', K), public parameters (g, p), public key of sender ya and secret key of receiver xb as $k = (y_{ap} . g^{r'})^{s'. Xb} \bmod p$.

Split k into k_1 and k_2.Recover the message $m = D_{k1}(c)$.

Accept m as a valid message from sender if and only if $KH_{K2}(m) = r'$.

Finally, the broadcasting problem of signcryption scheme is overcome by using protected subscriber agent gives both computational and storage cost is less when compare with other scheme.

Analyzing and Security of the Signcryption Scheme: In addition to its eminence of other signcryption schemes, the scheme in this paper has the following properties:

Confidentiality: It provides privacy for messages and stored data by hiding information using this multi resigncryption technique.

Message Integrity: In our proposed scheme, the recipient can verify whether the received message is the original one that was sent by the sender or not.It is difficult for the attacker to disguise as the signer and to generate the signature in the computational complexity.

Non Repudiation: The trusted third party can solve the controversy between initiator which denies sending the cipher text and the responder. Generally, it can provide a way of providing that the message came from someone even if they try to deny it.

User Authentication: This method of signcryption is secure if even with this complete access, the eavesdropper is still unable to recover the original plaintext from the ciphertext.

Unforgeability: It is computationally infeasible for an adaptive forger, who may be a dishonest recipient and allowed to query sender's signcryption algorithm, to masquerade sender in creating an authentic signcrypted text.

In efficient authenticated encryption scheme the message can be recovered [3]. These schemes are more efficient than the scheme for encrypting the signature with a public key encryption scheme.

CONCLUSION

Signcryption techniques have been adopted along with ReSigncryption approach using the protected subscriber agent to overcome the broadcasting problem. Also secured data transmission is being carried out among the end users by our multi-resigncryption

protocol. Also instead of sending the single signcrypted message to multiple users has many problem so it's being overcome by our multi-resigncryption approach. We have presented an implementation of a new sign-and-encrypt scheme for secure message transmission by combining the signature and signcryption public key cryptography paradigms. The proposed scheme is shown to be efficient in terms of computation and communication cost. This scheme is specially suited for secure application development. As compare with the previous works, the proposed scheme is more secure and efficient. In this paper, we paid an attention to resigncryption process using protected subscriber agent to attain the objectives.

REFERENCES

1. Zhang Chuanrong and Zhang Yuqing, 2009. Secure Mobile agent protocol by using Signcryption scheme, Gradute University.
2. Kohei Tatara and Kouichi Sakurai, 2009. A Signature Scheme Associated with Universal Re-signcryption 2009 International Conference on Availability, Reliability and Security.
3. Horster, P., M. Michels and H. Petersen, 1994. Authenticated Encryption Schemes with Low Communication Costs. Electronics Letters, 30(15): 1212-1213.
4. Nyberg, K. and R. Rueppel, 1994. Message Recovery for signature Schemes based on Discrete Logarithm Problem. In Proceedings of Eurocrypt '94, LNCS 950, pp: 182-193.
5. Zheng, Y., 1997. Digital Signcryption or How to Achieve Cost (signature & encryption) << cost (signature) + cost (encryption), advances in Cryptology - Crypto'97, LNCS 1294, Springer-Verlag, pp: 165-179.
6. Yeun, C., 1999. Digital Signature with Message Recovery and Authenticated Encryption (Signcryption) - A Comparison. In Proceedings of Cryptography and Coding 99, LNCS 1746. pp: 307-312.
7. Bao, F. and R. Deng, 1998. A Signcryption Scheme with Signature Directly Verifiable by Public Key. In Proceedings of Public Key Cryptography (PKC'98), LNCS 1431, pp: 55-59.
8. Seo, M. and K. Kim, 2000. Electronic funds Transfer protocol using domain-verifiable signcryption scheme, information Security and Cryptology-ICISC'9, LNCS 1787, Springer-Verlag, pp: 269-277.
9. Seo, S.H. and S.H. Lee, 2004. A secure and flexible multisigncryption scheme, ICCSA 2004, LNCS 3046, Springer- Verlag, pp: 689-697.
10. Zheng, Y., 1997. Signcryption and its applications in efficient public key solutions, information Security. LNCS1396, Japan, pp: 291-312.
11. Golle, P., M. Jakobsson, A. Juels and P. Syverson, 2004. In Proceedings of RSA Conference 2004, Cryptographers' Track (CT-RSA 04), LNCS 2964, pp: 163-178, Springer-Verlag.
12. Klonowski, M., M. Kutylowski, A. Lauks and F. Zagorski, 2004. Universal re-encryption of signatures and controlling anonymous information flow In Proceedings of WARTACRYPT '04.