ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

SDRP and SSO Mechanism for Impersonation Attack in Wireless Sensor Networks

[I]Subhaponmani S, [II]Balakrishnan C
[I,II]S.A Engineering College, Chennai, India

Abstract
Wireless sensors in network work with each other to sense some physical phenomenon and then the information gathered is processed to get relevant results. Reprogramming protocols are based on centralized approach. If base station is affected at any causes the whole process will be failed. To overcome this problem, secure and distributed reprogramming protocol (SDRP) is used. In distributed reprogramming mechanism multiple authorized network users can simultaneously and directly reprogram sensors nodes without the involvement of base station. Secure and Distributed Reprogramming Protocol (SDRP) consists of three phases: System initialization phase, user preprocessing phase, and sensor node verification phase. An inherent design weakness in the user preprocessing phase of SDRP is identified such that the node is vulnerable to an impersonation attack. Impersonation attack means the adversary successfully attempts to identify one of the legitimate parties to launch various attacks. To solve this problem the single sign on mechanism (SSO) have been proposed.

Keywords
Network Security, Wireless sensor networks (WSNs), Secure and Distributed Reprogramming Protocol (SDRP), Single Sign On Mechanism (SSO)

I. Introduction

A wireless sensor network (WSN) [7] [14] [15] is a computer networks composed of many, spatially distributed small devices that use sensors to monitor environment in different locations.WSN applications are: military applications, commercial applications, health application, environmental application. For example in military applications they use the sensor nodes to identify the attackers in battlefield surveillance. Wireless sensor networks can be used in broadcast communications. The use of wireless sensor networks needs limited energy, power and computational capability. WSNs contain self-organizing and self-healing networks. Self-organizing networks allow a new node to automatically join the network without the need for manual intervention.

In SDRP [13] contains three phases: System initialization phase, user Pre-processing phase, and Sensor Node verification [1]. Impersonation attack will occur in user Preprocessing phase. To overcome the impersonation attack single sign on mechanism can be used. The user contains multiple username and password for accessing the different service providers [9]. But in single sign on mechanism only need single username and password for accessing the different service providers.

The single sign on mechanism [12] contains three security requirements: i.e., , , Unforgeability, soundness and Credential Privacy[12]., Unforgeability means, except the authorized person, even a non-trusted authority and service providers are not able to forge valid records for a new user. Soundness means that the unauthorized party cannot be able to access the any service providers. Credential privacy guarantees that untrusted authority should not be able to impersonate the trusted party and also does not recover the user details.

Chang–Lee scheme [12] is insecure by two attacks, i.e., impersonation attack and credential recovery attack without credentials. Without any valid credential the impersonation attack may enable an outside attacker to impersonate a legal user or even a nonexistent user to have free access to the services. The impersonation attack means the adversary successfully assumes and identity one of the legitimate parties in a computer protocol or in a system. In the credential recovery attack, a malicious service provider who has communicated with a legal user twice can successfully recover the user's credential. The malicious service provider can impersonate the user to access the resources and then the services can provide by other service providers.

These two attacks can imply that the Chang–Lee SSO scheme fails to meet soundness and credential privacy, which are essential requirements for SSO schemes and authentication protocols. We also can identify the flaws in their security [6] [10] arguments to explain why it is possible to mount our attacks against their scheme. Similar attacks can also be applied to the Hsu–Chuang scheme is based on chang–Lee scheme.

Finally, to avoid these two attacks, propose an improved SSO scheme to enhance the user authentication phase of the Chang-Lee scheme. To this end, we employ the efficient RSA-based verifiable encryption of signatures (VES) to securely and verifiably encrypt a user's credential. VES was originally introduced to realize the fair exchange. There are no similar attacks in the SSO, and this is also the first time of using VES to design an SSO scheme, to the best of our knowledge.

II. Preliminaries

A. Existing System

Secure and Distributed Reprogramming Protocol (SDRP) is used. In distributed reprogramming mechanism multiple authorized network users can simultaneously and directly reprogram sensors nodes without the involvement of base station. Secure and Distributed Reprogramming Protocol (SDRP) consists of three phases: System initialization phase, user pre-processing phase, and sensor node verification phase.

- System Initialization Phase: The network owner creates a private and public key and assigns the reprogramming privileges.
- User Pre-processing phase: If network owner enters a WSN and has a new code image and construct the reprogramming packets.
- Sensor node verification phase: If packet Verification passes. The node accepts the code image.

An inherent design weakness in the user preprocessing phase of SDRP is identified such that the node is vulnerable to an impersonation attack. Impersonation attack means the adversary successfully attempts to identify one of the legitimate parties to

launch various attacks. To solve this problem the single sign on mechanism have been proposed.

B. Proposed System

Chang and Lee's single sign-on scheme is a remote user authentication scheme, supporting user anonymity and session key establishment. In their scheme, RSA algorithms are used to initialize an authorized user, called as a service providers and (SSO) Single Sign On Mechanism. The session keys are established using the technique called Diffie–Hellman key exchange. In the Chang–Lee scheme, individual person can apply a valid record from the authorized user SSO; RSA signature is used for the identification of the user to check the user details. The service providers can maintains its own RSA key pair for doing the server authentication. The Chang–Lee's SSO (Single Sign On) scheme consists of a three phases: system initialization, registration p, and user identification.

• System Initialization phase: The trusted person SSO selects a two prime numbers p and q. After that, SSO determines its RSA key pair. SSO chooses a generator, where is also a large prime number. Finally, SSO publishes, keeps as a secret, and erases immediately once this phase has been completed.

A. Single Sign On Mechanisms

SSO (Single Sign-On) is a authentication process for an user that permits a user to enter single username and password to access the multiple service providers. The process is authenticates the user for all the providers when they switch applications during a particular session.

SSO is an ability for a user to enter the same username and password to log on to the multiple service providers. As passwords is an mechanism for the secure authentication, a single sign on has now become also known as an (Reduced Sign On) RSO. Single Sign On mechanism is a property of access control of multiple related but independent software systems.

Benefits of Single Sign On mechanism are reducing password fatigue from different username and password combinations, and also reducing the time spent for re-entering passwords for the same user identity.

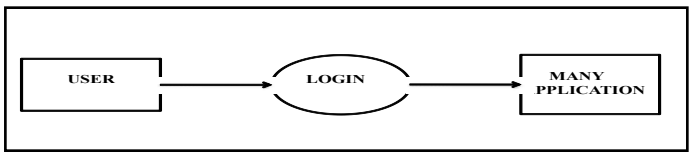

Fig: 1.2: Single Sign On

B. User Identification Phase

In the user identification phase check RSA signature use Diffie–Hellman (DH) key .To access the resources of an service provider, user can needs to go through the authentication protocol . A symmetric key encryption scheme which is used to protect the confidentiality of user's identity. Suppose service request messages from user, service providers generates and return user message which is made up by RSA on Signature Once this signature is validated, it means that user has authenticated service provider successfully. If users receive any message service provider can conform validity by checking. After that the user generates the key temporarily. Once u close the process the same key does not work automatically your session are stopped.

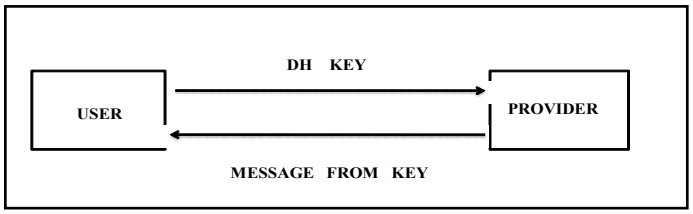

Fig: 1.3: User Identification Phase

C. Attacks against the Chang Lee Scheme

The Chang–Lee scheme is actually not a secure SSO scheme because there are two potential effective and concrete impersonation attacks. The first attack, an "impersonation attack without credentials, "to identify like as an behavior of trusted party and copy the details in a system or in a communications protocol and make use of services and resources offered by service providers, since the attacker can violate the requirement of soundness for an SSO scheme and thus successfully impersonate a legal user without holding a valid credential.

The other attack, the "credential recovering attack" compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. In real life, these attacks may be both users and service providers at high risk.

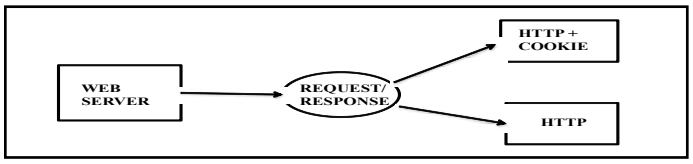

Fig. 1.4: Attacks against the Chang-Lee Scheme

D. Recovering Attack

On the one hand, the Chang–Lee SSO scheme specifies that is a trusted party. So, that this implies the service providers could be malicious and are not trusted parties. By agreeing with them, "the Wu–Hsu's modified version could not be protect the user's token against a malicious service provider, the work also agrees implicitly that there is the potential for attacks from the malicious service providers against an Single Sign On (SSO) schemes.

In fact, for all service providers are assumed to be an trusted, to identify him/her user can simply encrypt the message for his/her credential under the RSA public key of service provider. Then, can easily decrypt an cipher text to get 's credential and verify its validity by checking if it is a correct signature issued by them . In fact, such a straightforward scheme with strong assumption is more efficient, much simpler and has better security.

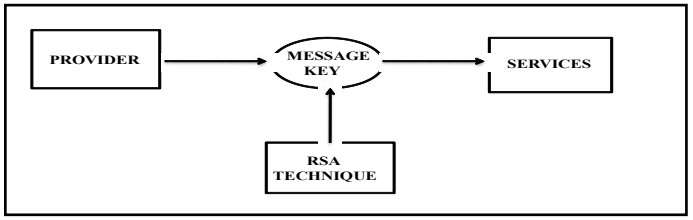

Fig. 1.5: Recovering Attack

E. Security Analysis

The security of the improved SSO scheme by focusing on the security of the user authentication part, especially credential privacy and soundness due to two reasons. On the one hand, the security of service provider authentication is ensured by the enforceability of

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

the secure signature scheme and the enforceability of the credential is guaranteed by the enforceability of RSA signatures, chosen by each service provider.

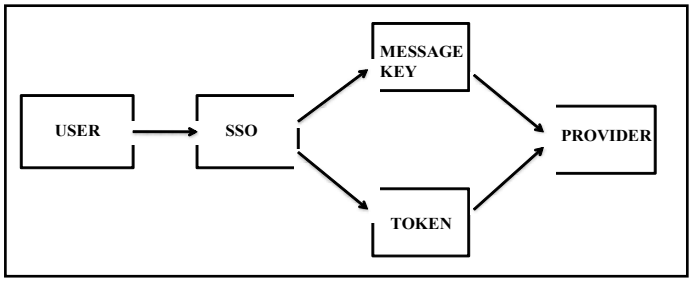

Fig: 1.6: Security Analysis

III. System Architecture

The distributed network users or multiple user can register the username and password in single sign on mechanism(SSO).that SSO mechanism can provide the secret token to the users .Any cloud provider or social network i.e. gmail,yahoo,facebook,twitter likewise they also register with an SSO mechanisms. If user can access the Gmail means using WSNs they securely access the network with single username and password. For example: in Gmail user have one username and password, likewise yahoo, twitter, fb user have same username but using different password. In SSO mechanism provide only one username and password to access the different networks.

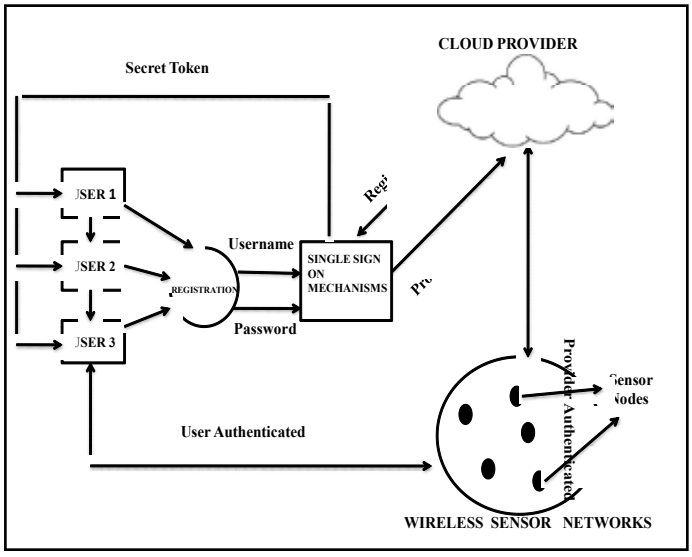

Fig: 1.1: System Architecture

A. Advantages of Single Sign On Mechanisms

1. Users need only single password for access to all the service providers/applications and systems. Users have immediately have access to all necessary password-protected applications.
2. Users don't need to remember multiple passwords.
3. Users don't have to guess the passwords.

The implementation of SSO Mechanism (Single Sign On) Architecture as shown in Fig 1.1 is following below. Here implement the RSA algorithm for secure authentication purpose. The RSA algorithm can encrypt and decrypt the message.

First, single user or multiple users can register with an SSO mechanism. The SSO mechanism can check the user details and provide secret token to the user. As likely same as the cloud provider can register with an SSO mechanism then the SSO mechanism provide token to the cloud provider. Once the user and cloud provider can register with an SSO mechanism they can directly communicate with an multiple service providers with the help of wireless sensor networks

IV. Conclusion

The existing system demonstrate the two attacks The first attack, is an "impersonation attack, "to identify like as an behavior of trusted party and copy the details in a system or in a communications protocol and make use of services and resources offered by service providers, since the attacker can violate the requirement of soundness for an SSO scheme and thus successfully impersonate a legal user without holding a valid credential.

The other attack, the "credential recovering attack" compromises the credential privacy in the Chang–Lee scheme as a malicious service provider is able to recover the credential of a legal user. In real life, these attacks may be both users and service providers at high risk. In proposed system using Single Sign On mechanisms can be used. By using Single user name and password to access the different networks without any attacks.

Using RSA technique to encrypt and decrypt the message and to securely access the authenticated and communicated with a user .With the help of secure socket layer to protect the message from attacker. The result is to provide high security without any attacks.

V. Results

In Existing System identify a two attacks.i.e Impersonation attack and credential recovering attacks. In proposed system using RSA algorithm to provide high security and overcome those two attacks. In RSA algorithm, we have to encrypt and decrypt the message so no attacks will be occurring. Therefore the message is high secure.

References

[1] *T.-S.Wu and C.-L. Hsu, "Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks,"Comput. Security, vol. 23, no. 2, pp. 120–125, 2004.*

[2] *K. Sun, P. Ning, and C. Wang, "Tinysersync: Secure and Resilient Time Synchronization in Wireless Sensor Networks," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 264-277, 2006.*

[3] *W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," IEEE Trans. Ind. Electron.,vol. 15, no. 6, pp. 2551–2556, Jun. 2008.*

[4] *L. Barolli and F. Xhafa, "JXTA-OVERLAY: A P2P platform for distributed,collaborative and ubiquitous computing," IEEE Trans. Ind. Electron., vol. 58, no. 6, pp. 2163–2172, Oct. 2010.*

[5] *X. Li,W. Qiu, D. Zheng, K. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793–800,Feb. 2010.*

[6] *J. Jin et al., "Handling inelastic traffic in wireless sensor networks,"IEEE Trans. Sel. Areas Commun., vol. 28, no. 7, pp. 1105–1115, Jul.2010.*

[7] *M. Cheminod, A. Pironti, and R. Sisto, "Formal vulnerability analysis of a security system for remote fieldbus access," IEEE Trans. Ind. Inf.,vol. 7, no. 1, pp. 30–40, Feb. 2011.*

[8] Y.-C. Wu, Q. Chaudhari, and E. Serpedin, "Clock Synchronization of Wireless Sensor Networks," IEEE Signal Processing Magazine, vol. 28, no. 1, pp. 124-138, Jan. 2011.
[9] D. G. Zhang and X. J. Kang, "A novel image de-noising method basedon spherical coordinates system," EURASIP J. Adv. Signal Process, vol. 1, p. 110, 2012.
[10] B. Fabian, T. Ermakova, and C. Muller, "SHARDIS: A privacy-enhanced discovery service for RFID-based product information," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 707–718, Aug. 2012.
[11] A. Valenzano, L. Durante, and M. Cheminod, "Review of security issues in industrial networks," IEEE Trans. Ind. Inf., vol. PP, no. 99,2012, DOI 10.1109/TII/2012.2198666.
[12] H.-M. Sun, Y.-H. Chen and Y.-H. Lin, "oPass: A user authentication protocol resistant to password stealing and password reuse attacks,"IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 651–663, Apr.2012.
[13] Guilin Wang, Jiangshan Yu, and Qi Xie, "Security Analysis of a Single Sign On mechanism for Distributed Computer Networks," IEEE transactions on information informatics, vol. 9, no. 1, February 2013.
[14] Daojing He and Laurence T. Yang, "Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks," IEEE transactions on parallel and distributed systems, vol. 60, no. 11, November 2013.
[15] Kasim Sinan Yildirim and Aylin Kantarci, "Time Synchronization Based on Slow-Flooding in Wireless Sensor Networks," IEEE transactions on parallel and distributed systems, vol. 25, no. 1, January 2014.
[16] Degan Zhang, Guang Li, Ke Zheng, Xuechao Ming and Zhao-Hua Pan, " An Energy-Balanced Routing Method Based on Forward-Aware Factor for Wireless Sensor Networks ," ieee transactions on industrial informatics, vol. 10, no. 1, February 2014.

Ms S. Subhaponmani is in final year P.G degree in Computer Science and Engineering in S.A. Engineering College, Chennai. She has completed UG degree from Kalasalingam University, Krishnankovil.Her areas of Interest are Network Security, Data Structure, Database Technology and Mobile Computing.

C.Balakrishnan working as Assistant Professor (Sr.Gr) at S.A.Engineering College ,Chennai, Tamilnadu in the Department of PG Studies in Engineering. He is currently working towards a Ph.D. degree with the Department of Information and Technology, Anna University, MIT Campus, Chennai, Tamilnadu. His main fields of interest are Computer Networks, Network Security, Advanced operating System and AdHoc Networks.