www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume2 Issue 8 August, 2013 Page No. 2628-2634

Review On Secure and Distributed Reprogramming Protocol

Ruchika Markan[1] ,Gurvinder Kaur[2]

[1] Assistant Professor in Computer Science & Engineering Department
RIMT-Institute of Engineering &Technology
Mandi Gobindgarh, Punjab
ruchikajerath@yahoo.co.in

[2] Assistant professor in Computer Science & Engineering Department
RIMT-Institute of Engineering &Technology
Mandi Gobindgarh, Punjab

ABSTRACT
Wireless reprogramming is very important in sensor networks. Reprogramming is defined as the process of loading a new code image or relevant commands to sensor nodes. For security reasons every code update must be authenticated to prevent an attacker from installing malicious scripts in the network. A number of protocols have been defined for reprogramming the wireless sensor networks. SDRP is the first distributed reprogramming protocol in which multiple authorized network users can simultaneously and directly reprogram sensor nodes without involving the base station. The protocol uses identity-based cryptography to secure the reprogramming and to reduce the communication and storage requirements of each node. Preserving data privacy is a challenging problem in wireless sensor networks. On comparison, Elliptic Curve Integrated Encryption Scheme (ECIES) provides great solution for security and authorization in the sensor network.

Keywords- ECC, Reprogramming, Security, WSN, Data Dissemination.

1. INTRODUCTION

Wireless sensor networks show great promise in their ability to provide extensive, monitoring for extended periods of time. These networks are composed of large numbers of small, inexpensive nodes that integrate sensing, computation, and wireless communication. One of the advantages of sensor networks is their ability to operate for extended periods of time. Sometimes it may be necessary to upload a new code image or retasking the existing code with different sets of parameters. We refer to both of these activities as reprogramming. To support network reprogramming, protocols for the reliable distribution of a program image to nodes are required. In this research different reprogramming protocols are discussed based on the centralized and distributed approach. SDRP is the only protocol which supports distributed environment while number of protocols is defined for the centralized environment.

2. PROPERTIES OF THE REPROGRAMMING PROTOCOL

- **Distributed**: Multiple authorized network users can simultaneously and directly make changes on the nodes.
- **User traceability**: In most applications, traceability is highly desirable, particularly for reprogramming.
- **Data Optimization:** Data Optimization is important for reprogramming. It has a direct impact on the transmission power used and thus on sensor network lifetime.
- **Partial reprogram capability**: There are special modules on each sensor node which can only be modified by the network.
- **Energy Efficient:** As energy is a limited resource in sensor networks, so a protocol does not effect the network lifetime.
- **Scalability**: The protocol needs to be efficient even in a large-scale WSN with thousands of sensor nodes.

3. NETWORK REPROGRAMMING PROTOCOL

Several different reprogramming protocols have been developed. In this section we described only three reprogramming protocols.

3.1 Dissemination Protocol

Deluge, a reliable data dissemination protocol for propagating large amounts of data from one or more source

nodes to all other nodes over a multihop, wireless sensor network. A data object can be represented as a set of fixed-sized pages provides a manageable unit of transfer.

Deluge is a NACK-based protocol that provides periodic information to keep nodes informed of their neighbours states. Deluge uses three phase handshaking mechanism to distribute the code.[2][7]

3.2 Seluge Protocol

Secure and DoS-Resistant Code Dissemination in wireless sensor networks is a secure extension to Deluge, an open source, state of-the-art code changing system for wireless sensor networks. It provides security protections for code updating, including the integrity protection of code images and prevent from the attacks. Seluge properly authenticates advertisement and SNACK packets. Seluge uses a signature to self-sustaining process the authentication of a new code image. It can be efficiently verified by a regular sensor node, but it takes a computationally powerful attacker a substantial amount of time to forge a weak authenticator. Moreover, it cannot be pre-computed. Thus, this weak authentication mechanism provides an effective filter of forged signatures. As a result, Seluge is not subject to the same DoS attacks against signature verifications.[11]

3.3 Secure and Distributed Reprogramming Protocol

SDRP is the first protocol which supports distributed reprogramming. While all existing insecure/secure reprogramming protocols are based on the centralized approach, it is important to support distributed reprogramming in which number of authorized network users can simultaneously and directly update sensor nodes. SDRP, is the first work of its kind. SDRP consists of three phases: system initialization, user preprocessing, and sensor node verification. In the system initialization phase, the network owner defines its public and private keys and then provides the reprogramming authorities and the corresponding private key to the authorized users. Only the system 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 program code, then the reprogramming packets will be constructed to send them to the sensor nodes. In the sensor node verification phase, if the packet verification passes, then the nodes accept the new program code.[1]

4. METHODOLOGY

Communication security is one of the areas where research is highly required. The data used in communication is very sensitive and needs to be protected. The recent branch of Network security is Cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public-key based mechanisms that provide encryption, digital signatures and key exchange algorithms. The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES)[16][17] which is included in IEEE and also in SECG SEC 1 standards.

4.1 Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. 'Domain parameters' in ECC is an example of such constants. A 160-bit key in ECC is considered to be as secured as 1024-bit key in RSA.

4.2 ECIES is the best known encryption scheme ECIES provides some valuable advantages over other cryptosystems as RSA.

ECIES is an integrated encryption scheme which uses the following functions[18]:

•Key Agreement (KA): This function is used to generate the secret key which will be shared by two parties.

•Key Derivation Function (KDF): This function produces a set of keys from keying material and some optional parameters.

•Encryption (ENC): Symmetric encryption algorithm is used.

•Message Authentication Code (MAC): The Data used to authenticate messages.

•Hash (HASH): The function, used within the KDF and the MAC functions.

In order to describe the steps that must be taken in order to encrypt a clear message, we will follow the tradition and will assume that Anny wants to send a message to Joy. In that scenario, Anny's ephemeral private and public keys will be represented as u and U, respectively. Similarly, we will refer to Joy's private and public keys as v and V, respectively.

The steps (shown in Fig. 2) that Anny must complete are the following:

1) Anny must create an ephemeral key pair consisting in the finite field element u and the elliptic curve point $U=u\cdot G$.

2) After the ephemeral keys u and U are generated, Anny will use the Key Agreement function, KA, in order to create a secret value, which is the result of the scalar multiplication $u\cdot V$, considering as input values Anny's ephemeral private key u and Joy's public key V.

3) Then, Anny must take the secret value $u\cdot V$ and optionally other parameters as input data for the Key Derivation Function, KDF. The output of this function is the concatenation of the symmetric encryption key, kENC, and the MAC key, kMAC.

4) With the element kENC and the message, m, Anny will use the symmetric encryption algorithm, ENC, in order to produce the encrypted message, c.

5) Taking the encrypted message c, kMAC and optionally other parameters, such as a text string previously agreed by both parties, Anny must use the selected MAC function in order to produce a tag.

6) Finally, Anny will take the temporary public key U, the tag, and the encrypted message c, and will send the cryptogram (U||tag||c) consisting of those three concatenated elements to Joy.

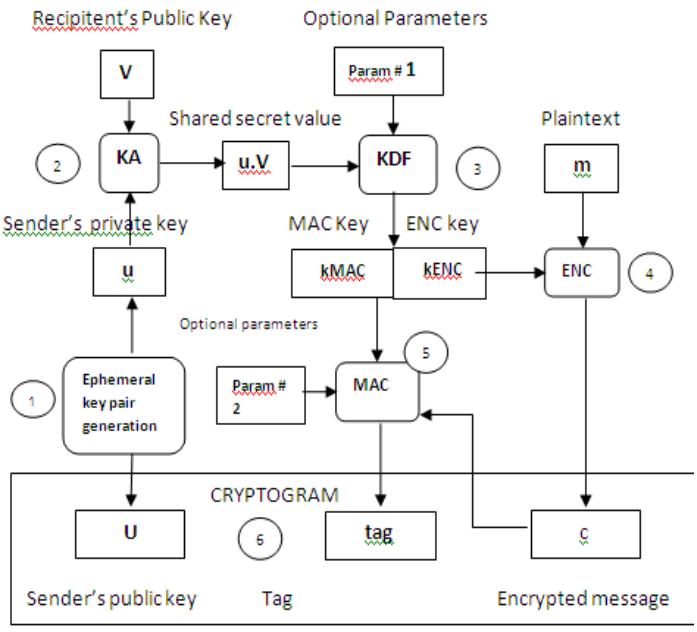

Fig 2. ECIES encryption functional diagram

Regarding the decryption process, the steps that Joy must perform (shown in Fig. 3) are the following:

1) After receiving the cryptogram (U||tag||c) from Anny, Joy must retrieve the ephemeral public key U, the tag, and the encrypted message c, so he can deal with those elements separately.
2) Using the retrieved ephemeral public key, U, and his own private key, v, Joy will multiply both elements in order to produce the shared secret value v·U, as the result of this computation is the same that the product u·V, which is the core of the Diffie-Hellman procedure ([1] and [7]).
3) Taking as input the shared secret value v·U and the same optional parameters that Anny used, Joy must produce the same encryption and MAC keys by means of the KDF procedure.
4) With the MAC key kMAC, the encrypted message c, and the same optional parameters used by Anny, Joy will first compute the element tag*, and then he will compare its value with the tag that he received as part of the cryptogram. If the values are different, Joy must reject the cryptogram due to a failure in MAC verification procedure.
5) If the tag value generated by Joy is the correct one, then he will continue the process by deciphering the encrypted message c using the symmetric ENC algorithm and kENC. At the end of the decryption process, Joy will be able to access the plaintext that Anny intended to send him.

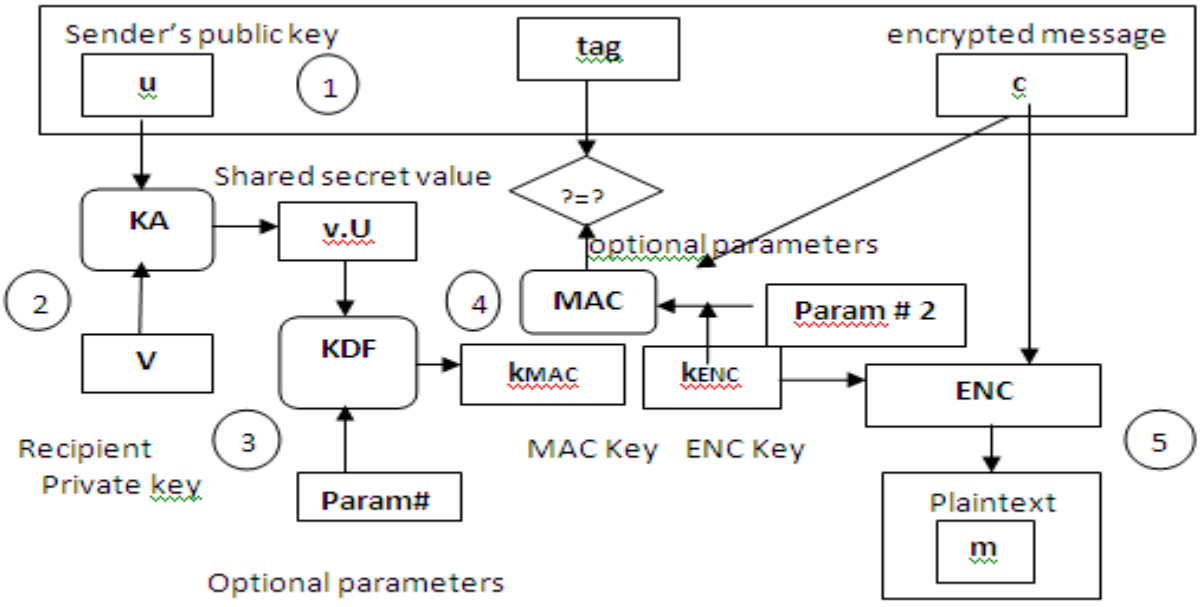

Fig 3.ECIES decryption functional diagram

5. CONCLUSION

In this paper the reprogramming protocols are discussed and also classify the different reprogramming protocols. SDRP is the distributed protocol which supports multiple users simultaneously and also it is important in large-scale sensor networks used by different users from both public and private sectors. The security to this protocol is provided by Elliptic curve encryption Scheme but the Elliptic Curve Integrated Encryption Scheme (ECIES) is the best Encryption scheme. The research focuses on achieving secrecy using ECIES algorithm for encryption, and authentication using Hashing technique.

6. REFERENCES

[1] Daojing He, Chun Chen, Shammy Chan, Jiajun Bu,"SDRP: A Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks", IEEE, Vol.59, No.11, November 2012.

[2] Adam Chlipala, Jonathan Hui, Gilman Tolle"Deluge: Data Dissemination for Network Reprogramming", University of California at Berkeley Computer Science Division Berkeley, CA 94720.

[3] H. Guo, K.-S. Low, and H.-A. Nguyen, "Optimizing the localization of a wireless sensor network in real time based on a low-cost microcontroller,"*IEEE Trans. Ind. Electron.*, vol. 58, no. 3, pp. 741–749, Mar. 2011.

[4] He, L. Cui, H. Huang, and M. Ma, "Design and verification of enhanced secure localization scheme in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 7, pp. 1050–1058, Jul. 2009.

[5] Gungor and G. P. Hancke, "Industrial wireless sensor networks Challenges, design principles, and technical approaches," *IEEE Trans.Ind. Electron.*, vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[6] Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Electron.*,vol. 57, no. 10, pp. 3557–3564, Oct. 2010.

[7] Tae Ho kim, Chang Hoon Kim,"Comparison of network reprogramming protocol for wireless Sensor Nodes"

[8] S. Hyun, P. Ning, A. Liu, and W. Du, "Seluge: Secure and dos-resistant code dissemination in wireless sensor networks," in *Proc. ACM/IEEE IPSN*, 2008, pp. 445–456.

[9] 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.*, vol. 57, no. 11, pp. 3596–3605, Nov. 2010.

[10] P. K. Dutta, J. W. Hui, D. C. Chu, and D. E. Culler, "Securing the deluge network programming system," in *Proc. ACM/IEEE IPSN*, 2006,pp. 326–333.

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

[12] Sangwon Hyun, Peng Ning, An Liu, Wenliang Du,"Secure and DoS-Resistant Cod Dissemination in Wireless Sensor Networks", Proc. Of the 7th international conference on information processing in sensor networks, page 445-456,IEEE Computer Society, Washington,USA.

[13] Wassim Drira," A Hybrid Authentication and Key Establishment Scheme for WBAN", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Vol. 2, No.3, 2012.

[14] Shanta Mandal and Rituparna Chaki," A Secure Encryption Logic for Communication in Wireless Sensor Networks", International Journal on Cryptography and Information Security (IJCIS), Vol.2, No.3, pp. 78-82, September 2012.

[15] Amar Rasheed, " The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 5, May 2012. Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", International conference on Information, Networking and Automation(ICINA),Kunming, IEEE, pp. 215-218, 2010.

[16] Xixiang LV, Hui LI, Baocang WANG,"Identity-based key distribution for mobile Ad Hoc networks", Springer-Verlag Berlin Heidelberg 2011

[17] V. Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, "A Survey of the Elliptic Curve Integrated Encryption Scheme", Journal Of Computer Science And Engineering, Volume 2, Issue 2, August 2010.

[18] D.Hankerson, A.J.Menezes, and S.Vanstone, Guide to Elliptic Curve Cryptography",New York;Springer-Verlag,2003.