ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

A Protected Multi Authorizing Reprogramming Protocol for Wireless Sensor Network

S.Suganya, M.Thenmozhi

Department of Network Engineering, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India.

Department of Network Engineering, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India.

ABSTRACT: Reprogramming is an important operation to wireless sensor networks. Reprogramming is based on update commands, adding new functionalities or removing bugs in WSN's. Reprogram has two approaches. Namely, centralized and distributed approach. Distributed approach has more benefits compare to centralized approach .In existing ,SDRP protocol was introduced in distributed approach for secure reprogram. This protocol has some drawbacks. To overcome, In this paper, we propose an effective one way hash chain algorithm is introduce to provide more confidentiality and also increase the energy in an efficient manner.

***KEYWORDS*:** One way hash chain algorithm, SDRP, Reprogramming, WSN's.

I.INTRODUCTION

A wireless sensor network (WSN**)** of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created.

The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy,memory, computational speed and communications bandwidth. Reprogramming is a crucial and challenging problem in wireless sensor network. The need reprogram may be traceable to changing system requirements, fixing bugs, or reassigning task. Whereas, it is impractical to collect all the sensor nodes once they are deployed. Many network reprogramming approaches have been proposed in the recent years. Due to the need of removing bugs and adding new functionalities, reprogramming is an important operation function of WSNs. 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 major concern. There has been a lot of research focusing on secure reprogramming, and many interesting protocols have been proposed in recent years. 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, 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. Alternatively, 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. The protocols such as seluge , deluge are used in centralized approach. We propose the Secure and Distributed Reprogramming Protocol (SDRP), 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. Since a novel identity-based signature scheme is employed in generating the public/private-key pair of each authorized user, the proposed protocol is efficient for resource-limited sensor nodes and mobile devices in terms of communication and storage requirements. Furthermore, the proposed protocol can achieve all the requirements of distributed reprogramming listed earlier, while keeping the merits of Deluge and Seluge.

In SDRP protocol, design weakness is exist ,by this way an adversary can easily enter and drop the packets. This is major drawback in SDRP protocol. To overcome this, we propose cryptographic technique. By using One way hash chain algorithm, we create public key based on polynomial invariant key generation scheme.

II PREVIOUS WORK

A.SDRP

The SDRP consists of three phases: system initialization, user preprocessing, and sensor node verification. In the system initialization phase, the network owner creates its public and private keys and then assigns the reprogramming privilege and the corresponding private key to the authorized user(s). Only the 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 code image, it will need to construct the reprogramming packets and then send them to the sensor nodes. In the sensor node verification phase, if the packet verification passes, then the nodes accept the code image.

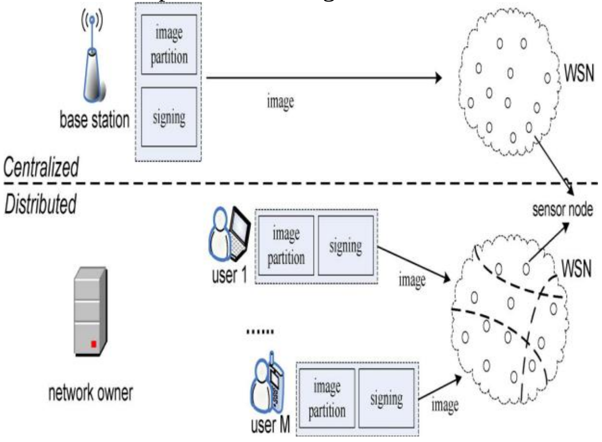

Fig. 1. system overview of centralized and distributed reprogramming approaches

B. NC Algorithm

A simple yet effective scheme to catch packet droppers. In this scheme, a Tree on DAG (ToD) structure rooted at the sink is first established. When sensor data is transmitted along the tree structure towards the sink node, each packet sender or forwarder adds a small number of extra bits, which is called packet marks to the packet. Based on the packet marks, the sink node can figure out the dropping ratio associated with every sensor node, and then runs our proposed *node categorization algorithm* to identify nodes that are packet droppers for sure, suspicious packet droppers, or no packet droppers. Our proposed scheme has the following features: (i) being effective in detecting the dropping packets, (ii) low communication and energy overheads, (iii) being compatible with existing false packet filtering schemes. Extensive simulation on ns2 simulator is conducted to verify the effectiveness. In every round, for each sensor node *u*, the sink node *s* keeps track of the number of packets sent from *u* and the number of packets received to *s*. In the end of each round, the sink node *s* calculates the dropping ratio for each node *u*. suppose *Nf is* the number of transmitted packets and *Nr* is the number of received packets. Based on the dropping ratio of every sensor node and the tree topology, the sink categories the nodes based upon the node categorization algorithm. This algorithm identifies the nodes that are droppers for sure, possibly droppers and suspicious droppers.

III.PROPOSED WORK

A.One Way Hash Chain Algorithm

One-way chains are an important cryptographic primitive in many security applications. As one-way chains are very efficient to verify, they recently became increasingly popular for designing security protocols for resource-constrained mobile devices and sensor networks, as their low-powered processors can compute a one-way function within milliseconds, but would require tens of seconds or up to minutes to generate or verify a traditional digital signature. Recent sensor network security protocols thus extensively use one-way chains to design protocols that scale down to resource-constrained sensors. A one-way function is a function that is easy to compute on every input, but hard to invert given the image of a random input. Here "easy" and "hard" are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. Not being one-to-one is not considered sufficient of a function for it to be called one-way hash chain is the successive application of a cryptography hic hash function to a piece of data. In computer security, a hash chain is a method to produce many one-time keys from a single key or password. For non-repudiation a hash function can be applied successively to additional pieces of data in order to record the chronology of data's existence. A hash chain is a successive application of a cryptographic hash function to a string. By using this algorithm we generate public key in Polynomial bivariate key generation scheme.

B.Polynomial bivariate key generation

One of the important fundamental problems in cryptography is a Polynomial Reconstruction Problem (PRP). There are several public key cryptographic systems constructed based on this problem. This paper provides an analytical study on a public key cryptosystem (*PKC*) that is based on bivariate polynomial Reconstruction Problem (*BPRP*) and takes into considerations the developments performed on the (*PKC*). A modification is proposed using bivariate polynomial instead of univariate polynomial which is used in the original Augot's system to enhance its security. The analysis concerned mainly the mathematical backgrounds related to bivariate polynomials and the operation, valid generally for these polynomials, especially in the finite fields *GF*(*q*). The coding problem is included in the public key cryptosystem that considers the (*BPRP*). The Reed-Solomon Code is used .

A polynomial in two variables (that is a bivariate polynomial) with constant coefficients is given by

$$a_{nm}x^ny^m + \cdots + a_{22x^2y^2} + a_{21x^2y} + a_{12}xy^2 + xy + a_{10}x + a_{01}y + a_{00.}$$

The sum of two polynomials is obtained by adding together the coefficients sharing the same powers of variables.

$$(a_2x^2 + a_1x + a_0) + (b_1 + b_0) = a_{2x^2} + (a_1 + b_1) + (a_0 + b_0).$$

the first public key encryption scheme based on the (PRP). This section will present discussion of the performances and state the parameters that are required to reach the desired security level from such scheme. Let us consider the following parameters: *Fq* is a finite field, *q* is the size of *Fq*, *n* is the length of the Reed –Solomon code used by this scheme. *k* its dimension. *W* is the weight of a large error *E*, so that the PRP for *n*, *k*, *W* is believed to be hard, or it must have *W* >(*n* - *k*) / 2 which need to be verified. *w* is the weight of a small error *e*, such that *w* ≤(*n* - *k*) / 2.

Key Generation Process

Let us consider that we have two parties ***A*** and ***B***. Then want to have their communication using modified cryptosystem based on the bivariate polynomial. ***A*** secretly does the followings:

- Choose the sets *x* and *y*.

-Generates a monic (unitary) bivariate polynomial *p*(*x*, *y*) of degree equal to *k* -1**,** with respect *x* and of degree equal to *k*-1 with respect *y*.

-Generates an error vector *E* of dimension *n* with the weight *W*, where *W* is exactly non zero coordinates.

-Computes the codeword *C* = *ev*(*p*(*X*, *Y*)) = *p*(*xi* , *yj*) of *RSk* , ∃ *xi* = *I* and *j y* = *j* for *i* = 1,2,…….,*n* and *j* = 1,2,…….,*n*.

Computes *Pk* = *C* + *E*,s where *Pk* is the public-key, while *C* and *E* are kept secret or the secret-key is (*C*, *E*).

IV.PERFORMANCE ANALYSIS

The simulation results bring out some important characteristic function based on the cost and overhead Comparisons.

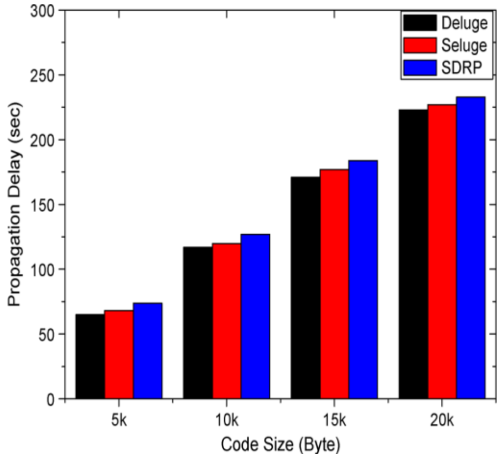

Fig .2.Propagation delay of deluge,seluge and SDRP.

The above figure shows the linearly increases the propagation delay of all schemes.

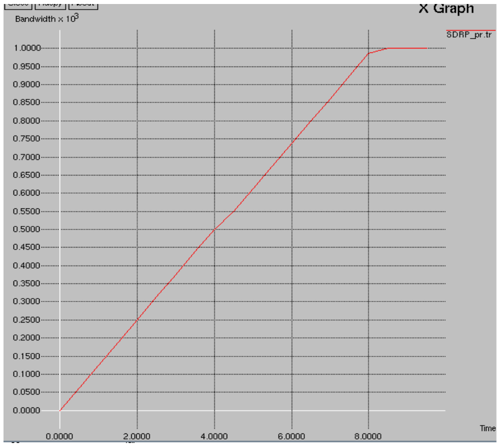

Fig. 3.Throughput.

The above figure shows number packets transmitted successively during time period.

V.CONCLUSION

In some applications, data are also required to be kept confidential due to the possibility of message interception. The wireless sensor network is widely used in the critical application like Military application. So we need to transmit some confidential information over the network. The confidentiality can provide by using cryptographic techniques. As the WSN is the resource constrained network, we need to consider the energy efficiency while providing the confidentiality. we will study how to support confidentiality in the energy efficient manner in distributed reprogramming.

REFERENCES

[1] D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and efficient reprogramming protocol for wireless sensor networks," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.

[2]" Security Analysis and Improvement of a Secure andDistributed Reprogramming Protocol for Wireless Sensor Networks", IEEE Transactions On Industrial Electronics, Vol. 60, No. 11, November 2013.

[3] V. C. 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.

[4] V. C. 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.

[5] J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," IEEE Trans. Ind. Electron., vol. 57, no. 12, pp. 4219–4230,Dec. 2010.

[6] 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. 3596–3604, Nov. 2010.

[7] J. Carmo, P. Mendes, C. Couto, and J. Correia, "A 2.4-GHz CMOS shortrange wireless-sensor-network interface for automotive applications," IEEE Trans. Ind. Electron., vol. 57, no. 5, pp. 1764–1771, May 2010.

[8] 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., vol. 6 no. 7, pp. 762–776, Jul. 2007.

[9] L.Mottola and G. Picco, "Programming wireless sensor networks: Fundamental concepts and state of the art," ACM Comput. Surv., vol. 43, no. 3, pp. 1–51, Apr. 2011.

[10] H. Song, V. Shin, and M. Jeon, "Mobile node localization using fusion prediction-based interacting multiple model in cricket sensor network, "IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4349–4359, Nov. 2010.

[11] R. C. Luo and O. Chen, "Mobile sensor node deployment and asynchronous power management for wireless sensor networks," IEEE Trans.Ind. Electron., vol. 59, no. 5, pp. 2377–2385, May 2012.

[12]" Bivariate Polynomials Public Key Encryption Schemes", Ruma Kareem Ajeena,HailizKamarulhaili and Sattar B. Almaliky, International Journal of Cryptology Research 4(1): 73 - 83 (2013).