International Journal on Emerging Technologies **6**(1): 69-72(2015)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

Identity-Based Key Distribution for Wireless Sensor Networks using Cryptographic Techniques

Amit Kumar Singh
Department of Electronics & Communication,
Assistant Professor, BKIT, Bhalki, Karnataka, INDIA

(Corresponding author: Amit Kumar Singh)
(Received 01 March, 2015 Accepted 08 April, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT*:* **Wireless sensor networks are being deployed for a wide variety of applications. It is an important challenge to find out practical security protocols for wireless sensor networks due to limitation of power, computation and storage resources. Symmetric key techniques are attractive due to their energy efficiency. But the drawbacks of symmetric key techniques are evident in terms of key management and security. Public key infrastructure is considered to be not suitable to provide security for wireless sensor networks because of complexity. But some studies on elliptic curves cryptography indicate that algorithm based on this kind of cryptography could be a potential choice. Fortunately, a practical identity-based cryptography is proposed recently, which gives a possibility to employ elliptic curves cryptography in wireless sensor networks. Compared with the traditional asymmetric and symmetric key techniques, the distinguishing characteristic of identity-based encryption is the ability to use any string as a public key, for example, an email address, a name, etc. Based on the Boneh-Franklin IBE algorithms, we proposed an identity-based key distribution and encryption scheme for wireless sensor networks. Analysis shows that our scheme has some advantages in terms of key management, storage requirement and security. The large number of new applications for wireless sensor networks has lead to unprecedented growth of wireless sensor networks.**

I. INTRODUCTION

Sensor networks refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of self-organizing, low-power, low-cost wireless nodes deployed to monitor and affect the environment. Sensor networks are typically characterized by limited power supplies, low bandwidth, small memory sizes and limited energy. This leads to a very demanding environment to provide security. The goal of security services in Wireless Sensor Networks (WSN) is to protect the information and resources from attacks and misbehaviour. The security requirements in WSN include:

It is an important challenge to find out suitable cryptography for wireless sensor networks due to limitations of power, computation capability and storage resources. Many schemes based on public or symmetric key cryptography are investigated. Recently, a practical identity-based encryption technique is proposed. We present an identity-based key distribution and encryption scheme for wireless sensor networks. The scheme is an elliptic curve cryptography type algorithm. We review briefly about identity-based encryption and decryption first, particularly, the Boneh-Franklin algorithms. Then we describe a key distribution and encryption scheme based on the Boneh-Franklin algorithms for wireless sensor networks.

WSNs are emerging as both an important new tier in the Information Technology ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties.

II. PROBLEM DEFINITION

Today's world straggling with problem of identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks. Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper. To address the critical security issues in wireless sensor networks we talk about cryptography, steganography and other basics of network security and their applicability. WSNs continues to grow, they become vulnerable to attacks and hence the need for effective security mechanisms. Identification of suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy, computation capability and storage resources of the sensor nodes. Symmetric based cryptographic schemes do not scale well when the number of sensor nodes increases each device, called a node, is battery powered and equipped with integrated sensors, digital signal processors (DSPs) and radio frequency (RF) circuits. Because of special characteristics and limitations of wireless sensor networks, we face an important challenge in security issue, particularly for the applications where WSNs are developed in a hostile environment or used for some crucial purposes. For example, an adversary can easily listen to the traffic and mislead communications between nodes. In order to establish a secure network, we have to design secure protocols to deal with problems about key distribution and encryption in communications.

III. LITERATURE SURVEY

Identity-Based Key Distribution and Encryption for WSNs [1]. In this survey the scheme is an elliptic curve cryptography type algorithm. Author reviewed briefly about identity-based encryption and decryption first, particularly, the Boneh-Franklin algorithms. Then they described a key distribution and encryption scheme based on the Boneh-Franklin algorithms for wireless sensor networks. They discussed the efficiency and security of their scheme by comparing with traditional public key technique and symmetric key technique. Three types of key distribution schemes have been studied in general network environments: trusted-server schemes, public-key schemes, and key pre distribution schemes. There is a trusted server in Trusted-server schemes for key distribution between nodes. Security in Wireless Sensor Networks using Cryptographic Techniques [2]. The author focused few important points on Wireless sensor networks consisting of autonomous sensor nodes attached to one or more base stations. As Wireless sensor networks continues to grow, they become vulnerable to attacks and hence the need for effective security mechanisms. Identification of suitable cryptography for wireless sensor networks is an important challenge due to limitation of energy, computation capability and storage resources of the sensor nodes. Symmetric based cryptographic schemes don't scale well when the number of sensor nodes increases. "Research on Encryption Algorithm of Data Security for Wireless Sensor Network [3]" In this paper the main focus is on WSN security mechanisms, authentication and encryption. However, sensor nodes with limited computing resources and storage resources, making the deployment of security mechanisms in the nodes need to consider their storage space, power consumption and other factors. If using hardware cryptographic module will increase the cost of the node, limiting large-scale applications. In order to reduce sensor node energy consumption, cost, space requirements, this paper has been studied and improved Advanced Encryption Standard Algorithms, and presented a lightweight high-level encryption algorithm. The algorithm conducted a variety of improvements form AES, mainly in three areas. "Secure Data Transfer using Cryptography with Virtual Energy for Wireless Sensor Network [4]" The wireless sensor network technology is one of the largest data processing and communication networks systems which continuously developed for distributed environment in field of real time application. There are so many factor associated with it such as Data security, operating speed, cost efficiency and additional sensor network constraints. Main consideration is about increase the security over existing attacks without affect the performance and complexity of overall wireless sensor network. Normally, two approach of symmetric key and asymmetric key data encryption technique is applied for it at sensor nodes. So, the proposed work is to explore design of cost efficient secure network protocol which reduces number of key transmission required in symmetric key encryption for rekeying task. In proposed algorithm mainly three steps are performed as key generation, data cryptography and data transmission. "A Method in Security of Wireless Sensor Network based on Optimized Artificial immune system in Multi-Agent Environments[5]" In this paper, they presented the review of some existing immune systems and the way of making action when confronting enemy agents in wireless sensor networks. They also discussed about representing necessary and practical algorithms for intrusion detection and confronting the intruder by an exclusive method using the available agents in the networks and representing a software simulation.

Human lymphocytes play the main role in recognizing and destroying the unknown elements. In this article, they focused on the inspiration of these defective systems to guarantee the complications security using two algorithms; the first algorithms proposed to distinguish self-nodes from non-self ones by the related factors and the second one is to eliminate the enemy node danger. The results showed a high rate success and good rate of detecting for unknown object; it could present the best nodes with high affinity and fitness to be selected to confront the unknown agents. "Wireless Sensor Network Security model using Zero Knowledge Protocol [6]. The security mechanisms used for wired networks cannot be directly used in sensor networks as there is no user-controlling of each individual node, wireless environment, and more importantly, scarce energy resources. In this paper, author addressed some of the special security threats and attacks in WSNs. They propose a scheme for detection of distributed sensor cloning attack and use of zero knowledge protocol (ZKP) for verifying the authenticity of the sender sensor nodes. The cloning attack is addressed by attaching a unique fingerprint to each node that depends on the set of neighboring nodes and itself. The fingerprint is attached with every message a sensor node sends. The ZKP is used to ensure non transmission of crucial cryptographic information in the wireless network in order to avoid man-in-the middle (MITM) attack and replay attack. The paper presents a detailed analysis for various scenarios and also analyzes the performance and cryptographic strength.

IV. OBJECTIVE

The main objective of the proposed work is as follows:
(i) To examine the data confidentiality and privacy individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
(ii) To analyses the data Integrity and programs are changed only in a specified and authorized manner.
(iii) To reveal the structure of function in an unimpaired manner in the various Identity-Based Key Distribution .
(iv) To know the challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors.
(v) To study the problem changes of incidents/parameters and communicating with other devices.

V. METHODOLOGY

The research methodology will be exploratory, interpretative, recent research results have shown that ECC is feasible on resource constrained sensor nodes. In this work we demonstrate that the related but more complex primitives of Pairing Based Cryptography (PBC) are also well suited for sensor devices. We present the research methodology study on the application and implementation of PBC to WSN. Our implementations are all the fastest yet reported, and have been implemented across a range of WSN processors. We also present a novel variant of the key exchange protocol which can be useful in even more demanding applications, and which partially solves the problem of node compromise attacks.

A. Curve Section

Authors tend to choose non super singular curves rather than super singular curves because they feel that the formers have security advantages compared to the latters. We argue that until now there is no concrete evidence for that and thus it seems that super singular curves are more adequate to WSNs since they have been shown empirically to be faster.

B. Parameters Mersenne Prime (q) And Solinas Prime (r)

The choice of the parameters q and r is a key factor in the efficiency of pairing computation, as curve operations are performed using arithmetic of the underlying field. In prime fields, by choosing q a Mersenne prime (i.e., a number of the form 2^p-1) helps in computing modular reduction operations efficiently. At the same time, by choosing a Solinas prime (in practice, a prime of low Hamming weight) reduces considerably the computation of pairings. Note, however, that because of the idiosyncrasies of the both types of primes, often it is not possible to find a pair q and r Mersenne and Solinas primes, respectively, suitable for pairings.

1) *Embedding degree k.*

We have chosen k = 2 since it provides a number of benefits while computing pairings. For example, k = 2: 1) allows the important denominator elimination optimization; 2) helps in finding a r of low Hamming weight; 3) makes Fqk arithmetic relatively easy to implement; 4) has been shown empirically to be efficient;

2) *Parameter sizes.*

Parameter sizes often pose a tradeoff between security level and efficiency. This issue is especially important when dealing with resource-constrained nodes. For most Pairing-Based Cryptography PBC schemes (including Identity-Based Encryption), the security requirements described to be satisfied by choosing r > 2160 and qk > 21024. However, security requirements in WSNs are often relaxed. This is because of their short lifetimes and because the goal is not to protect each node individually, but the network operation as a whole.

Until now, the larger parameters sizes for which the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the Discrete Logarithm Problem (DLP) are known to be solved are 2109 and 2431, respectively. Therefore, it seems that r≥2128 and qk ≥2512 are able to meet the current security requirements of WSNs.

VI. POSSIBLE OUTCOME

In this paper, we have proposed a security architecture that provides confidentiality, integrity, and authentication for a mobile wireless sensor network. For this purpose, we have presented algorithms to easily set up pairwise secret keys between the mobile sensor nodes and to establish a indent based secret key per node, in which it can communicate its messages securely. Furthermore, our solution minimizes the effects of compromised nodes. Compromising an adjustable number of sensor nodes does not compromise the whole security architecture but restricts the security breach to the immediate neighborhood of the compromised node. Finally, we have implemented a prototype of our security architecture, which clearly shows that it is a lightweight solution and applicable for self-organizing mobile wireless sensor networks.

Several directions for future research arise from our solution. First, we intend to simulate our approach, using NS-2, in order to determine the maximum grade of node-mobility our security architecture is able to cope with. Second, we would like to integrate the ability to identify compromised nodes and methods to exclude them from the network. Another interesting question is to determine how much further we can optimize the employed algorithms with respect to key distribution and speed.

REFERENCES

[1] T. Hara, V. I. Zadorozhny, and E. Buchmann, "Wireless Sensor Network Technologies for the Information Explosion Era", *Stud. Compute. Intell. Springer-Verlag,* vol. **278**, 2010,.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," *IEEE Commun. Surveys Tuts*., vol. **8**, no. 2, pp. 2–23, 2006.

[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. **30**, no. 14-15, pp. 2826–2841, 2007.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Micro sensor Networks," IEEE Trans. Wireless Commun., vol. **1**, no. 4, pp. 660–670, 2002.

[5] A. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel Distrib. Syst., vol. **13**, pp. 1290–1302, 2002.

[6] S. Yi, J. Heo, Y. Cho et al., "PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks," Comput.Commun., vol. **30**, no. 14-15, pp. 2842–2852, 2007.

[7] K. Pradeepa, W. R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int. J. Comput.Applications, vol. **47**, no. 11, pp. 23–28, 2012.

[8] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a et al., "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. **87**, pp.2882–2895, 2007.

[9] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and performance analysis of a secure clustering protocol for sensor networks," in Proc.IEEE NCA, 2007, pp. 145–152.

[10] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems based on pairing. In Symposium on Cryptography and Information Security (SCIS2000), pages 26–28, Jan 2000.

[11] M. Scott. Computing the tate pairing. In Topics in Cryptology - CT-RSA, volume **3376** of Lecture Notes in Computer Science, pages 293–304. Springer, 2005.

[12] Cryptography and Network Security Principles and Practice, by William Stallings 5th Edition

[13] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," *Computer Networks*, vol. **38**, no. 4, pp. 393–422, 2002.

[14] A. Perrig, R. Canetti, Briscoe, J. Tygar, and D. Song, "TESLA: Multicast source authentication transform," IRTF draft, draft-irtf-smug-tesla-00.txt, November 2000.

[15] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of Seventh Annual International Conference on Mobile Computing and Networks, July 2001.