ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

A Review on Certificateless Key Management Policy in Wireless Sensor Network

Snehal R Mankar, Prof.A.B.Raut

M.E.Student (CSIT), H.V.P.M. College of Engineering & Technology, Amravati, Maharastra, India

H.O.D. (CSE) H.V.P.M College of Engineering & Technology, Amaravati, Maharashtra, India

ABSTRACT: This paper propose a certificateless-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. Many cluster-based wireless sensor network routing protocols have been proposed. However, most of them take little consideration on communication protection, which is important to ensure the network security. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. wireless sensor systems (WSNs) have been conveyed for a wide assortment of utilizations, including military detecting and following, tolerant status observing, activity stream checking, where tactile gadgets regularly move between distinctive areas. Securing information and interchanges requires suitable encryption key conventions.

KEYWORDS: Wireless sensor networks, certificateless public key cryptography, security, clustering.

I. INTRODUCTION

Wireless sensor network (WSN) is a network of collection of tiny sensor nodes called as motes which are densely deployed over target area. The sensor are able to sense the data through events occurring in their coverage area and are able to either forward the data or process the data in some cases as shown in Fig 1. A sensor network node typically consists of Radio transceiver, a microcontroller and battery or typical form of an embedded type of energy source[6]

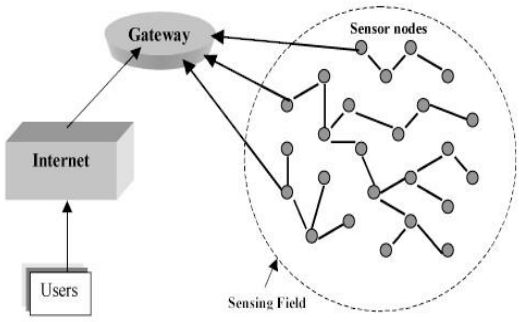

Fig. 1.Typical wireless sensor network

There are many advantages of using wireless sensor networks. One of these advantages is reducing the cost of the applications by having many sensors with little cost communicate with each other and with the base station providing full network function. At the same time sensor networks have some special characteristics compared to traditional networks which make it hard to deal with such kind of networks. The most important property that affects these types of network is the limitation of the available resources, especially the energy. security is one of the most important issues in many critical dynamicWSNapplications. DynamicWSNs thus need to address key security requirements, such as node authentication, data confidentiality and integrity.[1]

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

In This paper We present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs. In certificateless public key cryptography (CL-PKC) [12], the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value.

II. LITRATURE SERVEY

we propose the first certificateless effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM supports efficient communication for key updates and management when a node leaves or joins a cluster and hence ensures forward and backward key secrecy[1]. Wireless sensor networks come with huge application domain but on the other hand require the same level of security. The paper discusses various authentication techniques available in wireless sensor network and analyzes them. Some techniques are very helpful but come with some disadvantages. The effort is also done to point out these difficulties. Authentication is one of the best security solutions which protects whole sensor network.[2]]. We have identified wireless sensor network applications, classified sensor networks into different classes and identified security attacks that can take place in each class of sensor networks.[7]

III. RELATED WORK

1] Key Management Through Symmetric key Encryption :

Symmetric key encryption suffers from high communication overhead and requires large memory space to store shared pairwise keys. It is also not scalable and not resilient against compromises, and unable to support node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs[2]

2] Key Management Through Asymmetric key Encryption :

Asymmetric key based approaches suffer from the certificate management overhead of the entire sensor nodes and so are not a practical application for large scale WSNs.[5]

3] Need of Certificateless key management:

This paper present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs. In certificateless public key cryptography (CL-PKC), the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key.we take the benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length. In order to dynamically provide both node authentication and establish a *pairwise key* between nodes, we build CL-EKM by utilizing a pairing-free certificateless hybrid signcryption scheme (CL-HSC).[12]

IV. CONCLUSION

[1]In this paper, we propose the first certificateless effective key management protocal (CL-EKM) for secure correspondence in element WSNs. CL-EKMbolsters effective correspondence for key upgrades and administration when a hub leaves or joins a bunch and consequently guarantees forward and in reverse key mystery. Our plan is flexible against hub trade off, cloning and mimic assaults and secures the information secrecy and trustworthiness. Wireless sensor networks come with huge application domain but on the other hand require the same level of security [6]

REFERENCES

1. Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, Fellow, IEEE," Effective Key Management in DynamicWireless Sensor Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

2. G. de Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in Proc. IEEE Int. Conf. Wireless Mobile Comput., Oct. 2008, pp. 580–585.
3. W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A key predistribution scheme for sensor networks using deployment knowledge," IEEE Trans. Dependable Secure Comput., vol. 3, no. 1, pp. 62–77, Jan./Mar. 2006.
4. I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.
5. Seyed Hossein Erfani1, Hamid H. S. Javadi2, and Amir Masoud Rahmani," Analysis of Key Management Schemes in Dynamic Wireless Sensor Networks", ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 1, No.13 , January 2015
6. Sagar D. Dhawale Dr. B. G. Hogade Dr. S. B .Patil ," Design and Implementation of a Dynamic Key Management Scheme for Node Authentication Security in Wireless Sensor Networks", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 4, April 2015
7. Syed Muhammad Khaliq-ur-Rahman Raazi and Sungyoung Lee†,"A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks," Journal of Computing Science and Engineering, Vol. 4, No. 1, March 2010
8. Mohammed A. Abuhelaleh and Khaled M. Elleithy," SECURITY IN WIRELESS SENSOR NETWORKS: KEYMANAGEMENT MODULE IN SOOAWSN", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010DOI :
9. Ali Bagherinia, Akbar Bemana, Sohrab Hojjatkhah, Ali Jouharpour," A KEY MANAGEMENT APPROACH FOR WIRELESS SENSOR NETWORKS", International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3, August 2014.
10. (2013). Contiki: The Open Source OS for the Internet of Things, http://www.contiki os.org/download.html, accessed Dec. 2014.
11. M. A. Rassam, M. A. Maarof, and A. Zainal, "A survey of intrusion detection schemes in wireless sensor networks," Amer. J. Appl. Sci., vol. 9, no. 10, pp. 1636–1652, 2012.
12. Shweta Rajendra Joshi1, Prof. Archana Lomte2," Digital Certificateless Key Management in Dynamic Wireless Sensor Networks", International Journal of Advance Engineering and Research Development Volume 2,Issue 12,December -2015 @