Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 2, February 2017, pg.36 – 40

Enhancing Key Management Process in Wireless Sensor Network

Prof. A.B.Raut, Miss. Snehal Mankar
Computer Science & Engineering & Sant Gadagebaba, Amravati University
Computer Science & Information Technology & Sant Gadagebaba, Amravati University
anjali_dahake@gmail.com, snehalmankar24@gmail.com

Abstract—This paper shows the certificateless key management protocol for secure communication in wireless sensor network. This paper proposes 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, elliptic curve cryptography (ECC), cluster.

I. INTRODUCTION

Dynamic wireless sensor networks (WSNs), which enable mobility of sensor nodes, facilitate wider network coverage and more accurate service than static WSNs. Therefore, dynamic WSNs are being rapidly adopted in monitoring applications, such as target tracking in battlefield surveillance, healthcare systems, traffic flow and vehicle status monitoring, dairy cattle health monitoring [9]. However, sensor devices are vulnerable to malicious attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of connectivity in wireless communication. Thus, security is one of the most important issues in many critical dynamic WSN applications. Dynamic WSNs thus need to address key security requirements, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move.

This paper 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. 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 also 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.

II. LITRATURE SERVEY

We propose the first certificateless effective key management protocol for secure communication in dynamic WSNs. Certificateless effective key management 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.CERTIFICATELESS EFFECTIVE KEY MANAGEMENT SCHEME

Types of Keys

• Certificateless Public/Private Key: Before a node is deployed, the KGC at the BS generates a unique certificateless private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pairwise key.

• Individual Node Key: Each node shares a unique individual key with BS. For example, a L-sensor can use the individual key to encrypt an alert message sent to the BS, or if it fails to communicate with the H-sensor. An H-sensor can use its individual key to encrypt the message corresponding to changes in the cluster. The BS can also use this key to encrypt any sensitive data, such as compromised node information or commands. Before a node is deployed, the BS assigns the node the individual key.

• Pairwise Key: Each node shares a different pairwise key with each of its neighboring nodes for secure communications and authentication of these nodes. For example, in order to join a cluster, a L-sensor should share a pairwise n key with the H-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by using the pairwise key. In an aggregation supportive WSN, the L-sensor can use its pairwise key to securely transmit the sensed data to the H-sensor. Each node can dynamically establish the pairwise key between itself and another node using their respective certificateless public/private key pairs.

• Cluster Key: All nodes in a cluster share a key, named as cluster key. The cluster key is mainly used for securing broadcast messages in a cluster, e.g., sensitive commands or the change of member status in a cluster. Only the cluster head can update the cluster key when a L-sensor leaves or joins the cluster.

IV. WORKING OF PROPOSE KEY MANAGEMENT SYSTEM

A. system setup:

1) Generation of System Parameters : The KGC at the BS runs the following steps by taking a security parameter k ∈ Z+ as the input, and returns a list of system parameter _ = {Fq , E/Fq , Gq , P, Ppub = x P, h0, h1, h2, h3} and x.

2) Node Registration : The BS assigns a unique identifier, denoted by Li , to each L-sensor nLi and a unique identifier, denoted by Hj , to each H-sensor nHj, where $1 \leq i \leq N1$, $1 \leq j \leq N2$, $N = N1 + N2$. Here we describe the certificateless public/private key and individual node key operations for Li , the same mechanisms apply for H-sensors. During initialization, each node nLi chooses a secret value $xLi \in_R Z * q$ and computes PLi = xLi P. Then, the BS requests the KGC for partial private/public keys of nLi with the input parameters Li and PLi. The KGC chooses $rLi \in_R Z * q$ and then computes a pair of partial public/private key (RLi , dLi) as below:

RLi = rLi P

dLi = rLi + x · h0(Li , RLi , PLi) mod q.

B. Pairwise Key Generation:

1) Pairwise Master Key Establishment: In this paragraph, we describe the protocol for establishing a pairwise master key between any two nodes nA and nB with unique IDs A and B, respectively. We utilize the CL-HSC scheme [13] as a building block. When nA receives an advertisement message from nB, it executes the following encapsulation process to generate a long-term pairwise master key KAB and the encapsulated key information, ϕA = (UA,WA).

2) Pairwise Encryption Key Establishment : Once nA and nB set the pairwise master key KAB, they generate an HMAC of KAB and a nonce $r \in_R Z * q$. The HMAC is then validated by both nA and nB. If the validation is successful, the HMAC value is established as the short-term pairwise encryption key kAB.

C. Cluster Formation:

1) Node Discovery and Authentication: For node discovery, nHj broadcasts an advertisement message containing Hj and pkHj. Once nLi within Hj 's radio range receives the advertisement, it checks Hj and pkHj , and initiates the Pairwise Key Generation procedure. Note that nLi may receive multiple advertisement messages if it is within the range of more than one H-sensor. However, nLi must choose one H-sensor, may be by prioritizing over the proximity and signal strength. Additionally, nLi can record other H-sensor advertisements as backup cluster heads in the event that the primary cluster head is disabled. If nLi selects multiple cluster heads and sends a response to all of them, it is considered as a compromised node. nLi and nHj perform the Pairwise Key Generation procedure to obtain a pairwise master key, KLi Hj and a pairwise encryption key, kLi Hj .

2) Cluster Key Generation: nHj chooses $x\ j \in_R Z * q$ to generate a cluster key GKj as follows GKj = HMAC(x j ,Hj) Then, nHj computes C2 = EkLi Hj (GKj , Hj , Li) to distribute the GKj. Then nHj sends Hj and C2 to nLi . nLi decrypts C2 to recover Hj , Li and GKj by using kLi Hj . If nLi fails to check Hj , Li , it discards the message and reports nHj to the BS as an illegitimate cluster head.

3) Membership Validation: After discovering all the neighboring nodes nLi ($1 \leq i \leq n$) in the j th cluster, nHj computes C4 = EK0H j(Hj ,Mj) and transmits C4 and Hj to the BS.

D. Key Update:

1) Pairwise Key Update: To update a pairwise encryption key, two nodes which shared the pairwise key perform a Pairwise Encryption Key Establishment process. On the other hand,

the pairwise master key does not require periodical updates, because it is not directly used to encrypt each session message.
2) Cluster Key Update: Only cluster head H-sensors can update their cluster key. If a L-sensor attempts to change the cluster key, the node is considered a malicious node.

E. Node Movement:
1) Node Leave: A node may leave a cluster due to node failure, location change or intermittent communication failure. There are both proactive and reactive ways for the cluster head to detect when a node leaves the cluster.
2) Node Join: Once the moving node nLm leaves a cluster, it may join other clusters or return to the previous cluster after some period. For the sake of simplicity, we assume that nLm wants to join the l th cluster or return to the j th cluster.

F. Key Revocation:
1) Compromised Node: The BS generates a CompNode message and a EK0H (CompNode, Lc). Then it sends EK0j (CompNode, Lc) to all nHj , ($1 \leq j \leq N2$). After all cH-sensors decrypt the message, they update the revocation clist of their clusters. Then, if related keys with nLc exist, the c related keys are discarded. Other than nLc , nHj performs the cNode leave operations to change the current cluster key with c the remaining member nodes.
2) Compromised Cluster Head: After the BS generates a CompHeader message and a EK0L i(CompHeader, Hj), it sends the message to all nLi ($1 \leq i \leq n$) in the j th cluster. The BS also computes EK0Hi(CompHeader, Hj), ($1 \leq i \leq N2$, i _= j) and transmits it to all H-sensors except nHj.

G. Addition of a New Node:
Before adding a new node into an existing networks, the BS must ensure that the node is not compromised. Then new node nLn+1 establishes a full private/public key through the node registration phase. Then, the public system parameters, a full private/public key and individual key K0L n+1 are stored into nLn+1 . The BS generates EK0H j (NewNode, Ln+1, pkLn+1) and sends it to all nHj , ($1 \leq j \leq N2$).

V. Conclusions

This paper 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. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity.

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 Dynamic Wireless Sensor Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015
[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 2010.
[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.

