EKM-CI: Effectual key administration in dynamic wireless sensor network

Shalini M S [1], Hemanth S R [2]

[1]*M.Tech 4th sem, Department of Computer Science and Engineering, Maharaja Institute of Technology, Mysore, Karnataka, India*
[2]*Associate Professor, Department of Computer Science and Engineering, Maharaja Institute of Technology, Mysore, Karnataka, India*

---***---

Abstract - *Recently, wireless sensor networks (WSNs) have been deployed for a wide variety of applications, including military sensing and tracking, patient status monitoring, traffic flow monitoring, where sensory devices often move between different locations. Securing data and communications requires suitable encryption key protocols. In this paper, we 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. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks. We implement CL-EKM in Contiki OS and simulate it using Cooja simulator to assess its time, energy, communication, and memory performance.*

Key Words: **Key Management; Wireless Sensor; Cola machine; node mobility;**

1. INTRODUCTION

Autonomous robots are mostly used in many industrial, agricultural and military applications. Research in the path planning is one of the most important aspects in mobile robot domain. Path planning for a mobile robot need to find a collision free path in dynamic environment from the specified start location to a desired (target) goal location while satisfying certain optimization conditions. Existing path planning methods like graphical methods such as visibility graph, the potential field and the cell decomposition are designed for dynamic environments, in which there are dynamic obstacles. In practical systems such as Marine Science Research [4], Mobile Robots in Industry, and military combat applications, robots usually face dynamic environments where both moving and stationary obstacles exist. The concept of Rapidly-exploring Random Tree (RRT) as a randomized data structure (graph) is designed for a broad class of path planning problems [2].

Now days, wireless sensor networks (WSNs) are widely used in wide variety of applications. So to improve security for WSNs and to protect the WSNs from various attack uses key management which is an effective way. A suitable encryption key protocol are used to secure data and communication .In this paper, a certificateless –effective key management (CL-EKM)[1] protocol is proposed to have a secure communication in dynamic WSNs characterized by node mobility. The CL-EKM protocol supports an economical communication for key updates and manages once a node joins or leaves a cluster and ensures forward and backward key secrecy. A protocol also supports key revocation for compromised nodes and to minimize the impact of a node compromise on the protection of alternative communication links. The security analysis states that CL-EKM protocol is effective in defensive against varied attacks.

2. LITERATURE SURVEY

I.-H.Chuang, W.-T.Su, C.-Y. Wu,et al,[1] proposed a two layered dynamic key management(TDKM) approach for cluster-based WSN (CWSN).To show the efficiency, TDKM is compared with other key management protocols . Key generation overhead, network security, and secured data transmission overhead in CWSN are analyzed by finding the relationship between the number of groups and system performance. M. Rahman and K. El-Khatib[2] proposed a novel key agreement protocol which is based on pairing-based cryptography over an elliptic curve. With the help this protocol, if any two nodes want to communicate independently can use the same secret key by using pairing and identity-based encryption properties. The proposed technique reduces the key space of a node and also shows that it is robust against various attacks such as masquerade attacks, reply attacks, and message manipulation attacks.

S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito[3] presented an effective mutual authentication and key establishment scheme for heterogeneous sensor networks which includes numerous mobile sensor nodes and only a few more powerful fixed sensor nodes. The outcome of this approach is less communication overhead during authentication and key establishment and as better network resilience against mobile nodes attacks compared to other approaches for authentication and key establishment. X. Zhang, J. He, and Q. Wei[4] proposed an energy-efficient distributed deterministic key management scheme (EDDK).With the help of this scheme pairwise keys and cluster keys of sensor nodes are well established as well as maintained securely and communication overhead is also less. They also made use of elliptic curve digital signature algorithm in EDDK, which provided the support for the establishment of pairwise keys and local cluster keys under the node mobility scenario.

M. R. Alagheband and M. R. Aref[5]proposed dynamic key management framework which is based on elliptical curve cryptography and signcryption method for heterogeneous WSNs. The proposed schema as network scalability and sensor node mobility in the liquid environments. The proposed schema had less communication overhead and worked better in terms of computation and key storage. X. He, M. Niedermeier, and H. de Meer[6] made the investigation on the special requirements of dynamic key management in sensor environments and introduced several basic evaluation metrics ,also explained that resource constrained nature of sensor nodes hinder the use of dynamic key management solutions.

3-PROPOSED WORK

This paper introduces an Energy-Efficient Dynamic Key Management (EEDKM)[7] proposal that uses two-layer architecture. In the lower layer, similar to LOCK, re keying is performed confined using the EBS and the t-degree vicariate polynomial. Each cluster has a clear number of KGNs which makes it hard that an attacker can exposes the network keys by obtaining some KGNs. In upper layer, re keying is performed using the secret key between BS and sensor node. The secret key is loaded before in each sensor node with unique ID and authenticates the node to the BS. The BS generates one t-degree vicariate polynomial key and distributes it by means of session key shared by all CHs. This makes the communication between CHs efficient. The rest of this section describes the bootstrapping, initial key distribution mechanism and some general operations in our key management scheme. Figure 1 shows overall system flow of proposed system. This may help you to understand our scheme.

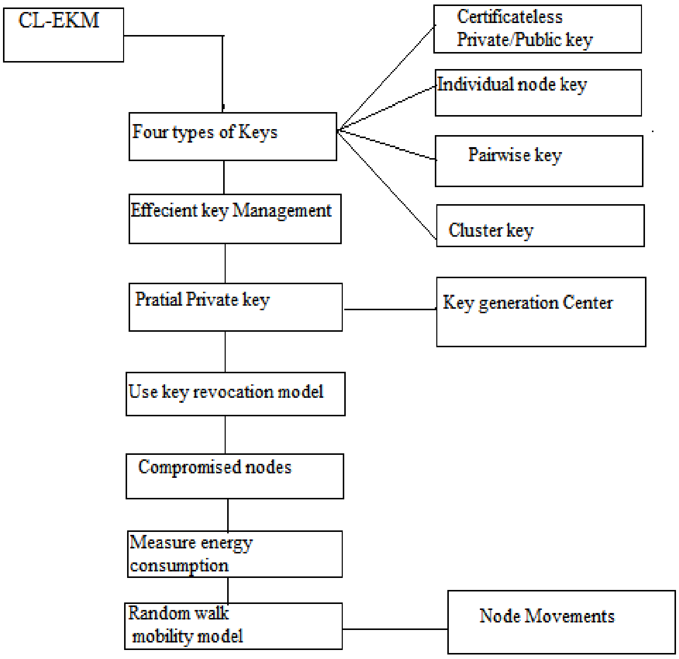


Figure 1: System Flow of Proposed System

4-OVERVIEW OF THE CERTIFICATE LESS EFFECTIVE KEY MANAGEMENT AND SECURITY MODEL SCHEME

The most effective key for dynamic WSNs is Certificateless effective key management protocol(CL-EKM)[8], it supports four types of keys each of them are used for different purposes, especially for including secure pairwise node communication and group-oriented key communication within the clusters. This schema uses the main algorithms of the CL-HSC[9] scheme to derive certificateless public/private keys and pair-wise keys. It also take the advantage of ECC keys defined on an additive group with a 160-bit length. The types of key are Certificateless public/private key, Individual nodes key, Pairwise key and Cluster key.

1. **Certificateless public/private key:** this key generates a mutually authenticated pair-wise key.

2. **Individual node key:** each node will have individual key.

3. **Pairwise key:** to have a secure communication and authentication of nodes each node shares a different pairwise key with the neighbouring nodes.

4. **Cluster key:** All the nodes in a cluster share a key and these keys are named as cluster key.

The special organization of the full private/public key pairs removes the need for certificates and also resolves the key escrows problems by eliminating the responsibility for the users full private key, figure 1 explains the generation of CL-EKM[10] and movement of nodes. Compared to other approach the proposed schema provides more security, decrease overhead and protect data confidentiality and integrity.

5. SYSTEM SETUP

Before the network deployment, the BS generates system parameters and registers the node by including it in a member list M.

I. 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. Choose a k-bit prime q Determine the tuple {Fq, E/Fq, Gq, P}. Choose the master private key x ∈R Z∗q and compute the system public key Ppub= x P. Choose cryptographic hash functions {h0, h1,h2, h3} so that h0 : {0, 1}∗ × G2 q → {0, 1}∗, h1 :G3 q × {0, 1}∗ × Gq→ {0, 1}n, h2 : Gq× {0, 1}∗ × Gq× {0, 1}∗ × Gq× {0, 1}∗ × Gq→ Z∗q, andh3 : Gq×{0, 1}∗×Gq×{0, 1}∗×Gq×{0, 1}∗×Gq→ Z∗q. Here, n is the length of a symmetric key. The BS publishes and keeps x secret.

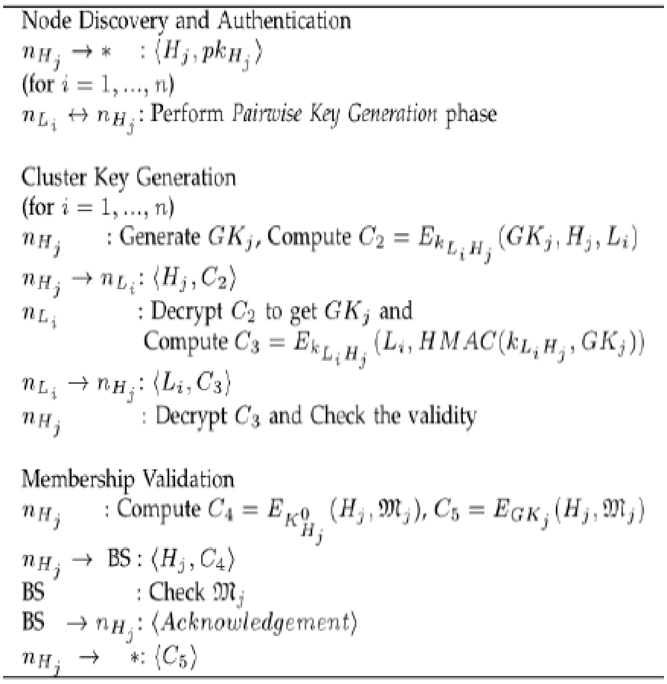
II. Node Registration:

The BS assigns a unique identifier, denoted by Li , to each L-sensor nLi and a unique identifier,denoted by H j, to each H -sensor n H j , where 1 ≤ i ≤ N1, 1 ≤ j ≤ 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 choose a secret value xLi∈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 K GC chooses rLi∈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

The Li can validate its private key by checking whether the condition dLi P = RLi+ h0(Li, RLi , PLi)Ppub holds

III. Cluster Formation



Node Discovery and Authentication

$n_{H_j} \rightarrow * \quad : \langle H_j, pk_{H_j} \rangle$

(for $i = 1, \ldots, n$)

$n_{L_i} \leftrightarrow n_{H_j}$: Perform *Pairwise Key Generation* phase

Cluster Key Generation

(for $i = 1, \ldots, n$)

n_{H_j} : Generate GK_j, Compute $C_2 = E_{k_{L_iH_j}}(GK_j, H_j, L_i)$

$n_{H_j} \rightarrow n_{L_i}$: $\langle H_j, C_2 \rangle$

n_{L_i} : Decrypt C_2 to get GK_j and Compute $C_3 = E_{k_{L_iH_j}}(L_i, HMAC(k_{L_iH_j}, GK_j))$

$n_{L_i} \rightarrow n_{H_j}$: $\langle L_i, C_3 \rangle$

n_{H_j} : Decrypt C_3 and Check the validity

Membership Validation

n_{H_j} : Compute $C_4 = E_{K^0_{H_j}}(H_j, \mathfrak{M}_j)$, $C_5 = E_{GK_j}(H_j, \mathfrak{M}_j)$

$n_{H_j} \rightarrow$ BS : $\langle H_j, C_4 \rangle$

BS : Check $\mathfrak{M}_j$

BS $\rightarrow n_{H_j}$: $\langle Acknowledgement \rangle$

$n_{H_j} \rightarrow \quad *: \langle C_5 \rangle$

6. CONCLUSION AND FUTURE WORK

This paper proposed to the primary certificate less effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM support economical communication for key updates and management once a node leaves or joins a cluster and thence ensures forward and backward key secrecy. Our theme is resilient against node compromise, cloning and impersonation attacks and protects the info confidentiality and integrity. This paper have a tendency to introduce a replacement theme which will be used for establish varied keys (pair wise keys, path keys and cluster keys) for wireless device networks. It is able to do quick credibility while not further computations and communications.

The experiment result shows the performance of TKLU is fresh. Associate in nursing energy-efficient dynamic key management theme victimization the EBSs, polynomials and secret symmetry keys. EEDKM provides localized re keying which is effectively performed not poignant the opposite elements of WSN. The BS suffer from mere problem of poor encryption. Since it has four pairs of keys it is not a serious issue. Still the user or the beneficiary authority has to go for more securely encrypted key methods. This problem can be revised and solved and hence to improve this idea of secure data handling. Encryption improvement is the only method to get the most secured way of communication

References

[1] H. Chan, A. Perrig, D. Song, "Random key predistribution schemes for sensor networks", Proc. IEEE Symp. SP, pp. 197-213, May 2003.

[2] M. Rahman and K. El-Khatib, “Private key agreement and secure communication for heterogeneous sensor networks,” J. Parallel Distrib.Comput., vol. 70, no. 8, pp. 858–870, 2010.

[3] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, “An energy and memory-efficient key management scheme for mobile heterogeneous sensor networks,” in Proc. 6th Int. Conf. CRiSIS, Sep. 2011, pp. 1–8.

[4] X. Zhang, J. He, and Q. Wei, “EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks,” EURASIPJ. Wireless Commun. Netw., vol. 2011, pp. 1–11, Jan. 2011.

[5] M. R. Alagheband and M. R. Aref, “Dynamic and secure key management model for hierarchical heterogeneous sensor networks,” IET Inf.Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012.

[6] X. He, M. Niedermeier, and H. de Meer, “Dynamic key management in wireless sensor networks: A survey,” J. Netw. Comput. Appl., vol. 36, no. 2, pp. 611–622, 2013.

[7] P. Shi and Y. Zhao, An efficient path planning algorithm for mobile robot using improved potential field, IEEE International Conference on Robotics and Biomimetics, pp. 1704-1708, (2009).

[8] A. Ghorbani, Using Genetic Algorithm for a Mobile Robot Path Planning, International Conference on Future Computer and Communication, pp. 164-166, (2009).

[9] K. Sugawara, Foraging behavior of interacting robots with virtual pheromone, Proceedings of the International Conference on Intelligent Robots and Systems, pp. 3074-3079 vol. 3, (2004).

[10] H. Qu, Real-time robot path planning based on a modified pulse-coupled neural network model, Neural Networks, IEEE Transactions on, vol. 20, pp. 1724-1739, (2009).