

An Improved CL-EKM based Key Management System

Mr. Sanket Patil¹, Prof. Mrs. Snehal Bhosale²

Student (ME), Electronics and Telecommunication, R.M.D. Sinhgad School of Engineering, Pune, India¹

Professor, Electronics and Telecommunication, R.M.D. Sinhgad School of Engineering, Pune, India²

Abstract: In not distant future, the Wireless Sensor Networks (WSN) is widely used in many applications like military and civil domains. The wireless sensor networks are always deployed in hostile and pervasive environment. Security is major worry in wireless sensor network. The traditional network security methods are not suitable for wireless sensor networks because of limited resource. Several Key management and establishment schemes have been suggested to provide light weight ciphers. The key management schemes play an important role in wireless sensor networks to achieve security. Basically, key management includes two aspects: key distribution and key revocation. Key distribution refers to the task of distributing secret keys between communicating parties to provide secrecy and authentication. Key revocation directs to the task of securely removing compromised keys. By revoking all of the keys of a compromised sensor node, node can be removed from the network. As compared to key distribution, key revocation has received very little attention. In this paper a survey of key management schemes in wireless sensor networks has been executed.

Keywords: Secret key sharing, key management schemes, wireless sensor network, symmetric algorithms.

I. INTRODUCTION

Last decade has witnessed the widespread usage of WSNs in real time applications. Many sensory devices are employed to form a network known as Wireless Sensor Network (WSN). WSNs are of two types such as static and dynamic. Static WSN is the network which do not have node mobility while dynamic WSN is characterized by adding nodes, removing nodes besides support for node mobility. 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. 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 [1]. Therefore, security mechanisms in WSN are required to provide data confidentiality, integrity, freshness, availability and authentication. To address security, various cryptographic algorithms has been proposed in the past broadly classified into symmetric and asymmetric algorithm depending on the type of key they use for encryption and decryption. Symmetric algorithm uses same key for encryption and decryption while asymmetric algorithm uses different keys for encryption and decryption. Key management is a security foundation of wireless sensor network, and based on it, security services such as authentication, confidentiality, integrity can be realized. In general use of

sensor network, key management includes two essential aspects: One is establishing pairwise keys, which can be used to protect data delivered between sensors; another is distributing cluster key, which can be used to realize secure data fusion in a cluster. In this paper our focus is more on the security issues of dynamic WSN and our study shed lights on latest developments in dynamic key management in dynamic WSN. There are various types of key management systems proposed in the past such as Secret-sharing-based Key Management [2], Digital Signature Based Key Management Protocol [3], Certificateless Effective Key Management [4] etc. The remainder of the paper is structured as follows. Section II presents security requirement for key management system. Section III focuses on related work. Section IV presents proposed system key management schemes.

II. SECURITY REQUIREMENTS FOR KEY MANAGEMENT SCHEME

A good key distribution or establishment and management schemes for sensor networks needs to consider few security points [5].

1. The scheme must work without prior knowledge of which nodes will come into communication range of each other after deployment.
2. Deployed nodes must be able to set up secure node-to-node communication.
3. Additional legitimate nodes deployed at a later time can form secure connections with already deployed nodes.

4. Unauthorized nodes should not be able to get entry into the network or become members of the network.
5. Sensor nodes have limited resources so computational and storage requirements of the scheme must be low.
6. If a node becomes compromised, the key management scheme must be able to securely remove the compromised node from the network

III. RELATED WORK

There are different key management schemes proposed over last decades.

A. Certificateless Key Management scheme

Seung-Hyun Seo and Jongho Won proposed [4] a Certificateless Key Management scheme (CL-EKM) that supports the establishment of four types of keys, namely: a certificateless public/private key pair, an individual key, a pairwise key, and a cluster key.

This scheme also utilizes the main algorithms of the CL-HSC scheme in deriving certificateless public/private keys and pairwise keys. We briefly describe the major notations used in the paper, the purpose of these keys and how they are setup.

- **Certificateless Public/Private Key:** Before a node is deployed, the Key Generator Circuit 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 adjoining nodes for secure communications and authentication of these nodes. For example, in order to join a cluster, a L-sensor should share a pairwise 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 change in member status in a cluster. Only the cluster head can update the cluster key when a L-sensor leaves or joins the cluster.

B. Key Management For Hierarchical Heterogeneous Sensor Network

Alagheband and Aref [6] proposed a dynamic key management scheme for hierarchical heterogeneous sensor networks. This scheme is based on Elliptic Curve Cryptography (ECC) and signcryption method. Especially the ECC is used among base station and cluster leaders. Moreover within the clusters a special mechanism is employed in order to have periodical authentication and sensor node mobility. There were many improvements in their work including complete security using signcryption, ability to support mobility of sensor nodes, a novel registration model and periodic authentication to be robust for node compromise. The key management scheme has four parts. They are key assignment, inter-cluster communication, registration, sensor node mobility and periodic authentication, and intra-cluster communication among sensor nodes. Prior to this work many hierarchical heterogeneous key management schemes came into existence. The scheme proposed by Riaz et al. [7] has a network in which every sensor node has a common key known to base station for communication. On the other hand cluster leaders do have an additional key that is used to communicate with other cluster leaders and base station. The key associated with SN is used for intra-cluster communication. There is a master key with 1024 bits associated with each sensor node and cluster leader. The scheme is also equipped with a mechanism to identify compromised node and revoke it. Nevertheless an intruder can try to abuse the master key by pretending as a new comer to the network. When a single SN is compromised, the whole network becomes vulnerable. This scheme has some drawbacks such as heavy communication and computational overhead.

C. Secret sharing based key management

LAN Yunl, WU Chunying [2] considered a static WSN consisting of a base station and sensor nodes that can self-organize into cluster. Suppose the WSN can be represented as a graph $G(V, E)$, where $V = \{v_1, \dots, v_{|V|}\}$ is a finite set of sensor nodes (vertexes) and $E = \{e_1, \dots, e_{|E|}\}$ is a finite set of links (edges). $|V|$ and $|E|$ indicate cardinality of sets V and E , respectively. Here V denotes a sensor node; and an edge e_{ij} indicates a communication link between the two given sensors v_i and v_j clusters [8].

After deployment, the base station assigns each sensor an initial key K_{init} . Since the BS is credible and has sufficient capacity and energy, it keeps all IDs and keys. Meanwhile, BS chooses polynomials and the corresponding number of polynomial values for each cluster. Assume there are $m-1$ clusters C_i ($i = 1, \dots, m-1$), each cluster has a cluster head CH, and k ($k \geq t$) member nodes. Shamir's (t, n) threshold scheme based on Lagrange interpolating polynomial, there are n shareholders $U = \{U_1, \dots, U_n\}$ and mutually trusted dealer D . The scheme consists of share generation phase and secret reconstruct phase.

Wu chunying and Li shundong [12] also present a novel key management based on secret sharing (KMSS). In



KMSS, considering about the energy efficiency is a dominant consideration problem in WSN, firstly make use of the maximum energy cluster head (MECH) protocol to divide cluster. Different from other partition cluster architecture,

MECH protocol restricts the size of cluster to generate uniform cluster. In each cluster, there is a sensor, called cluster head (in short, CH), which collects information from other member nodes in one cluster and transmits the processed information to the base station.

D. Secured and Efficient key management

Majid Alshammari and Khaled Elleithy [9] came up with a very Secure and Efficient Key Management Protocol for WSN, called SEKMP. The proposed protocol (SEKMP) adapts a new key management approach by inheriting the advantages of asymmetric cryptography and utilize it in very efficient way for delivering the session key to sensor nodes. Symmetric-based key management protocols are considered more resource-efficient than Asymmetric-based key management. The drawback of these protocols are:

- 1) Maintaining a large number of keys
- 2) Dependency on intermediary nodes for the keys distribution.

For example, [10] Asymmetric-based key management protocols proved to be secure in literature, and thus, they are one of the best protocols for the key distribution. The downside is, the direct application of these protocols in WSN leads to have many keys, and as a result, affecting the protocol performance. For example, in [11] the sink node must maintain n keys with sensor nodes. Where n is the number of nodes.

E. Digital Signature Based Key Management

Shruthi G J and Hemavathi[3] proposed Digital signature based key management protocol for secure data transfer in dynamic WSNs and key size also increased upto 1024 bit. It explains identification of authorized users, original content of document and it also verifies packets. Authors done implementation using network simulator -2 (NS-2).

In proposed system Energy consumption, false data injection rate and Node failure rate is reduced as compared to existing system

A. Node Deployment In node deployment stage, network will be initialized with 82 numbers of nodes. Distance between each node is calculated by using the formula,

$$D = \sqrt{(y_2 - y_1)^2 + (x_2 - x_1)^2}$$

where x_2, x_1 - x axis position of node
 y_2, y_1 - y axis position of node

B. Neighbour Node Discovery In neighbour node discovery, each node will send beacon messages to other nodes to identify neighbour nodes and then moves further to authenticate them. To verify signature of user Public key is used which will be known by everyone. Private Key is known only for user and it is never shared with anyone and also it is used for signature generation.

C. Key distribution mechanism:

In key distribution mechanism, input parameters are nodes. Energy of each node will be calculated; digitally signed key will be distributed to each authenticated node. Public key is used to verify signature whereas private key is known only for user and it will be kept secret. In key distribution mechanism, DSA (digital signature algorithm) is used. Digital signatures (DS) are used to increase the security. DS verifies the sender of documents identity. String of binary digits represents digital signature. Unauthorized modifications to data can be detected by using digital signature. Here hash function is used to generate the key. It compresses the data and compressed data is called message digest. This message digest produces digitally signed message. At the receiver side also hash function is used for verification purposes. Message which is less than 264 bits as input, message digest will be of 160 bits. As message digest is of small size compared to message, efficiency can be improved by signing the message digest.

IV. PROPOSED SYSTEM

We consider a heterogeneous dynamic wireless sensor network (See Fig.1). The network consists of a number of stationary or mobile sensor nodes. Sensor nodes can be of two types: (i) nodes with high processing capabilities, referred to as H-sensors, and (ii) nodes with low processing capabilities, referred to as L-sensors. We assume to have N nodes in the network with a number N_1 of H-sensors and a number N_2 of L-sensors, where $N = N_1 + N_2$, and $N_1 \ll N_2$. Nodes may join and leave the network, and thus the network size may dynamically change. The H-sensors act as cluster heads while L-sensors act as cluster members. They are connected to the BS directly or by a multi-hop path through other H-sensors. H-sensors and L-sensors can be stationary or mobile. After the network deployment, each H-sensor forms a cluster by discovering the neighbouring L-sensors through beacon message exchanges.

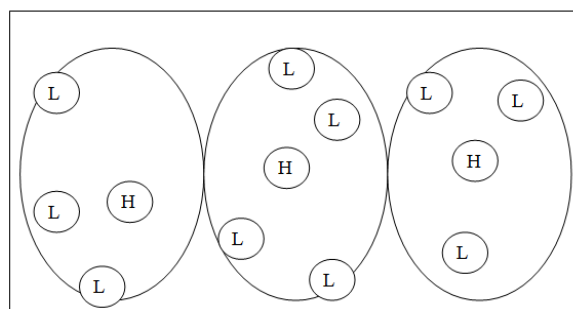


Fig. 1. Network Model

The L-sensors can join a cluster, move to other clusters and also re-join the previous clusters. Cluster head keeps the list of legitimate nodes and updates the list if nodes joins or leaves.

The proposed system consists of three modules:



- Personal Computer
- Microcontroller
- Sensor

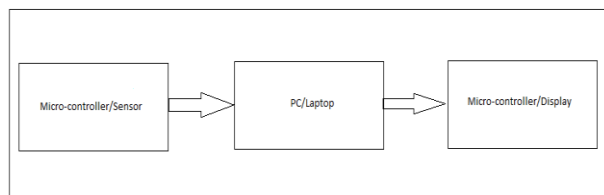


Fig. 1. Basic Architecture

Hardware includes sensor, microcontroller, display and software is implemented using Java. Sensor and microcontroller are used for providing input data to source node simulated using java to send data to the destination node. After the decryption of the encrypted data, to make sure original data is recovered controller and display are used on output. Proposed system is based on Certificateless Key Management system with public/private key pair, an individual key, a pairwise key, and a cluster key. In proposed system, multiple paths are calculated from source to destination and shortest path is selected to send data. If this shortest path is failed due to node failure or compromised node then next shortest path will be used to transmit data. ECC algorithm is used for key generation, encryption and decryption.

V. SUMMARY

In this paper we enlighten different key management scheme in WNSs and their significance in secure communication. We propose a key management scheme based on CL-EKM. It supports efficient communication for key updates and management when a node leaves or joins a cluster and hence ensures forward and backward key secrecy. This scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. The experimental results demonstrate the efficiency of CL-EKM in resource constrained WSNs. SSKM has an authentication mechanism to ensure the scalability, which can not only authenticate the new sensor but also can isolate the compromised node. The security analysis shows that proposed solution cannot reduce the energy consumption effectively but enhance the security level. Digital signature ensures efficient communication and updates node movements. This system increases data security and confidentiality, reduces Energy consumption, false data injection rate and Node failure rate with the increase in number of nodes.

REFERENCES

[1] 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..

- [2] LAN Yun, WU Chunying, ZHANG Yiying "A Secret-sharing-based Key Management in Wireless Sensor Network" *Software Engineering and Service Science (ICSESS)*, 2013 4th IEEE International Conference.
- [3] Shruthi G J, Hemavath, "Digital Signature Based Key Management Protocol for Secure Data Transfer in Dynamic Wireless Sensor Networks", *IEEE International Conference On Recent Trends In Electronics Information Communication Technology*, May 20-21, 2016, India.
- [4] Seung-Hyun Seo and Jongho Won, "Effective Key Management in Dynamic Wireless Sensor Networks", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 10, NO. 2, FEBRUARY 2015.
- [5] Ms. Nimisha Chunilal Chaudhari, "Key Management in Wireless Sensor Network A Survey", *International Journal of Application or Innovation in Engineering & Management* Volume 2, Issue 2, February 2013.
- [6] E. Khan E. Gabidulin B. Honary H. Ahmed. (2012). Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks. *The Institution of Engineering and Technology* 2012.2 (2), p.2001-2015.
- [7] Ramu Kuchipudi, Dr. Ahmed Abdul Moiz Qyser and Dr. V. V. S. S. S. Balaram, "Latest Developments on Dynamic Key Management for Dynamic Wireless Sensor Networks", *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016*.
- [8] S. Bandyopadhyay and E. I. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks", in *Proceeding of IEEE TNFOCOM'03*, San Francisco, April 2003.
- [9] Majid Alshammari and Khaled Elleithy, "Secure and Efficient Key Management Protocol (SEKMP) for Wireless Sensor Networks", *Architectures for Networking and Communications Systems (ANCS)*, 2014 ACM/IEEE Symposium.
- [10] H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2005, pp. 524-535.
- [11] Y. Zhang, "The scheme of public key infrastructure for improving wireless sensor networks security," in *Software Engineering and Service Science (ICSESS)*, 2012 IEEE 3rd International Conference on, 2012, pp. 527-530.
- [12] Wu chunying, Li shundong, Zhang yiying, "Key Management scheme based on secret sharing for Wireless Sensor Network" 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies.

BIOGRAPHIES



Mr. Sanket Patil, currently studying ME in VLSI and Embedded system at RMD Sinhgad School of Engg. Pune. The author has his personal field of interest in domain of wireless sensor networks.



Prof. Mrs. Snehal Bhosale, currently heading Department of E&TC at RMD Sinhgad School of Engg. Pune. Her main research interests are computer networks, network security and wireless sensor networks. She is currently doing her research on security in IoT in Pune University.