International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 2 (March-April, 2016), PP. 250-254

EFFECTIVE KEY MANAGEMENT USING CL-EKM PROTOCOL

R.Kishen[1], Kesari Nikhil[2], P.Nathiya Devi[3]
[1,2] Department of CSE, [3] Asst. Professor, M.E
Dhanalakshmi College of Engineering, Tambaram, Chennai
kishen10@gmail.com

***Abstract*—** Key management has remained a difficult issue in wireless device networks (WSNs) as a result of the constraints of device node resources. Various key management schemes that trade off security and operational necessities are proposed in recent years. Wireless device Networks (WSNs) comprises tiny sensor nodes with strained energy, memory and computation capabilities. Sensors can also be embedded into wearable devices to track vital signs of patients in healthcare domain. Mobility of sensor devices as per the demands of the application makes WSNs dynamic. Addressing key security requirements such as node authentication, data integrity and confidentiality is crucial for the success of critical WSN applications.In this paper, we propose a certificate less-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.

Index terms- **Dynamic Wireless Sensor Networks; dynamic key management; cryptography.**

I. INTRODUCTION

A wireless sensor network (WSN) consists of a large number of sensor nodes, which are powered by batteries, equipped with sensing, data processing and short-range radio communication components. The applications of WSNs range from the most popular ones, like environment monitoring and home automation, to more demanding ones in military or security areas, like battle field surveillance, targeting and target tracking systems. They are also used along with wearable devices that are being used in the healthcare industry to track vital signs of patients. The sensor devices are connected a central Base Station (BS) to which they send sensed data periodically. Many sensors keep sending data periodically to one base station making it a many to one communication scenario. Sensor can directly communicate with BS when no intermediary nodes are on the way to reach BS. If there are intermediary nodes, the data transmission takes place through the intermediary nodes. Usually more number of sensors is deployed for accuracy of the sensed data as the manufacturing cost of sensors is less and they are small in size.

WSNs are of two types such as static and dynamic. Static WSN is the network without node mobility while dynamic WSN is characterized by adding nodes, removing nodes besides support for node mobility. These networks can be deployed in applications such as studying wildlife habitat, monitoring hostile environments, battlefield surveillance, traffic monitoring, cattle health monitoring, vehicle status monitoring, study of traffic flow dynamics, monitoring vital signs of patients pertaining to different disease profiles, monitoring households on critical parameters and monitoring and controlling usage of electronic appliances in smart homes and so on. The list of applications provided here is by no means exhaustive as the usage of WSN is ubiquitous in different walks of life. The common thread among all these applications is the fact that the applications face limitations imposed by WSNs. The limitations stem from the short life time, limited computation capabilities, large number of nodes deployed, lack of infrastructure, besides the possible mobility nature of sensory devices causing frequent topology changes. To address these issues security, efficient resource management and scalability are given paramount importance.

Key management is a core mechanism to ensure security in network services and applications of WSNs. Key management can be defined as a set of processes and mechanisms that support key establishment and the maintenance of on going keying relationships between valid parties according to a security policy. Since sensor nodes in WSNs have constraints in their computational power and memory capability, security solutions designed for wired and adhoc networks are not suitable for WSNs. Hence, techniques for reliable distribution and management of these keys are of vital importance for these curity in WSNs.Due to their importance, the key management systems for WSNs have received increasing attention in scientific literature, and numerous key management schemes have been proposed for WSNs . Depending on the ability to update the cryptographic keys of sensor nodes during their run time (rekeying), these schemes can be classified into two different categories: static and dynamic. In static key management, the principle of key pre-distribution is adopted, and keys are fixed for the whole life time of the network. However, as a cryptographic key is used for along time, its probability of being attacked increases significantly. Instead, in dynamic key management, the cryptographic keys are refreshed throughout the lifetime of the network. Dynamic key management is regarded as a promising key management in sensor networks. In this paper our focus is more on the security issues of dynamic WSN and our study throws light on latest developments in dynamic key management in dynamic WSN. Our contributions in this paper include investigating the present state-of-the- art of key management in WSN and provide insights into possible directions for future work. This paper reveals that dynamic key management in dynamic WSN is still the potential research area.

II. RELATED WORK

Symmetric key schemes are not viable for mobile sensor nodes and thus past approaches have focused only on static WSNs. A few approaches have been proposed based on PKC to support dynamic WSNs. Thus, in this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al. and Agrawal et al. proposed a two-layered key management scheme and a dynamic key update protocol in dynamic WSNs based on the Diffie-Hellman (DH), respectively. However, both schemes are not suited for sensors with limited resources and are unable to perform expensive computations with large key sizes (e.g. at least 1024 bit). Since ECC is computationally more efficient and has a short key length (e.g. 160 bit), several approaches with certificate have been proposed based on ECC. However, since each node must exchange the certificate to establish the pairwise key and verify each other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes are not secure. Alagheband et al. proposed a key management scheme by using ECC-based signcryption, but this scheme is insecure against message forgery attacks. Huang et al. proposed a ECC-based key establishment scheme for self-organizing WSNs.

Although many quality survey papers have been presented in the field of key management of WSNs, the scope of the survey presented in this paper still differs from the existing surveys in many aspects. For the last decade, researchers have started to focus their interest on key management. Numerous review papers including are available, where the authors have examined and surveyed key pre-distribution schemes for key management. Further, classified key management schemes based on attack models, discussed application dependent key management schemes in WSNs, categorized key management schemes into public key schemes, key pre-distribution schemes, dynamic key management and hierarchical key management, organized key management schemes based on different key encryption mechanisms and focused on key management in cluster-based sensor network architecture. However, to the best of our knowledge, no review paper is available where dynamic key management schemes are classified and discussed thoroughly. Considering the importance of dynamic key management in WSNs, a comprehensive survey becomes necessary at this stage.

But, it should be doable for Associate in Nursing oppose to re- cowl initial link keys. Associate in Nursing oppose will then recover strengthened link keys from the recorded multi-path reinforcement messages once the link keys are compromised. Symmetric key schemes don't seem to be viable for mobile detector nodes and so past approaches have targeted solely on static WSNs. A couple of approaches are planned supported PKC to support dynamic WSNs. Thus, during this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al. and Agawam et al. planned a two-layered key management theme and a dynamic key update protocol in dynamic WSNs supported the Daffier-Hellman (DH), severally. However, both schemes don't seem to be fitted to sensors with restricted resources and area unit unable to perform valuable computations with massive key sizes (e.g. a minimum of 1024 bit). Since computer code is computationally additional economical and features a short key length (e.g. 160 bit), many approaches with certificate are planned supported computer code. However, since every node should exchange the certificate to ascertain the pair wise key and verify every other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management.

Moreover, existing schemes don't seem to be secure. Alagheband et al. planned a key management theme by victimization ECC-based signcryption, but this theme is insecure against message forgery attacks. Huang et al. planned a ECC-based key institution scheme for self-organizing WSNs. However, we tend to found the security weaknesses of their theme. In a step, a sensor node U sends $z = q_U \cdot H\,(MacK\,ey) + d_U\,(modn)$ to the other node V for authentication, where qU is a static private key of U. But, once V receives the z, it can disclose qU, because V already got macKey and $q_U = (z - d_U) \cdot H\,(MacK\,ey)^{-1}$. Thus, the sensor node's private key is exposed to the other node during the key establishment between two nodes. Zhang et al. proposed a distributed deterministic key management scheme based on ECC for dynamic WSNs. Its uses the symmetric key approach for sharing the pairwise key for existing nodes and uses an asymmetric key approach to share the pairwise keys for a new node after deployment. However, since the initial key K_I is used to compute the individual keys and the pairwise keys after deployment for all nodes, if an adversary obtains K_I, the adversary has the ability to compute all individual keys and the pairwise keys for all nodes. Thus, such scheme suffers from weak resilience to node compromises. Also, since such scheme uses a simple ECC-based DH key agreement by using each node's long-term public key and private key, the shared pairwise key is static and as a result, is not secure against known-key attacks and cannot provide re-key operation. Du et al. use a ECDSA scheme to verify the identify of a cluster head and a static EC-Diffie-Hellman key agreement scheme to share the pairwise key between the cluster heads. Therefore, the scheme by Du et al. is not secure against known-key attacks, because the pairwise key between the cluster heads is static.

On the opposite hand, Du et al. use a standard arithmetic-based isosceles key approach to share the pair wise key between a detector node and a cluster head. In their theme, in order to ascertain a pair wise key between two nodes within the same cluster, the cluster head arbitrarily generates a pair wise key and encrypts it victimization the shared keys with these two nodes. Then the cluster head transmits the encrypted pairwise key to every node. Thus, if the cluster head is compromised, the pair wise keys between non-compromised detector nodes in the same cluster will be compromised.

III. SYSTEM MODEL& ANALYSIS METRICS

A. System Model

The basic system model of this paper is pictured in Figure.1.It consists of 1 BS and lots of uniform sensing element nodes with distinctive ID. It uses cluster and two-layer design for scalability. Every cluster has some key generation nodes (KGNs) that distribute point keys among that cluster. These KGNs is also the final sensing element nodes elect by cluster heads (CHs).We assume that the fundamental system model is deployed for the purpose of watching the hostile atmosphere. End-to-end node communication is unusual as a result of sensing element nodes in each cluster monitor the finite space. For the info aggregation, there square measure several communications between the nodes among the same cluster. Thus, the most task of this model could be a information transfer from sensing element nodes to BS and an information aggregation in every cluster.

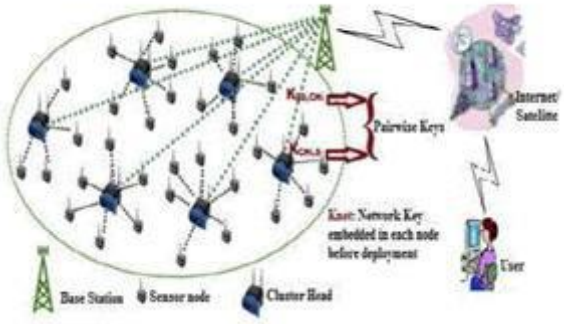


Fig. 1. Hierarchical wireless sensor network architecture

B. ANALYSIS METRICS

WSNs have some criteria that represent fascinating characteristics in key management scheme. To boot, energy consumption is that the most vital criterion thanks to the power constraint of detector nodes. Energy consumption might affect primarily the network lifespan. The key criteria square measure shown below.

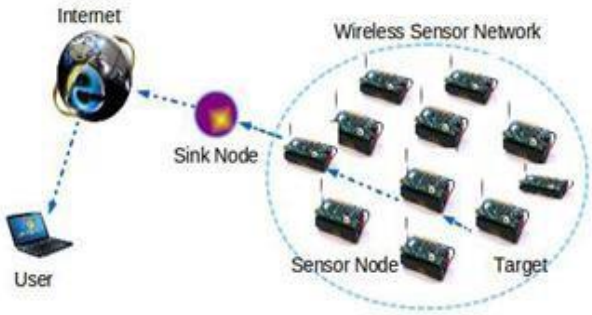
IV. PROPOSED SCHEME

In this paper, we 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 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. 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)

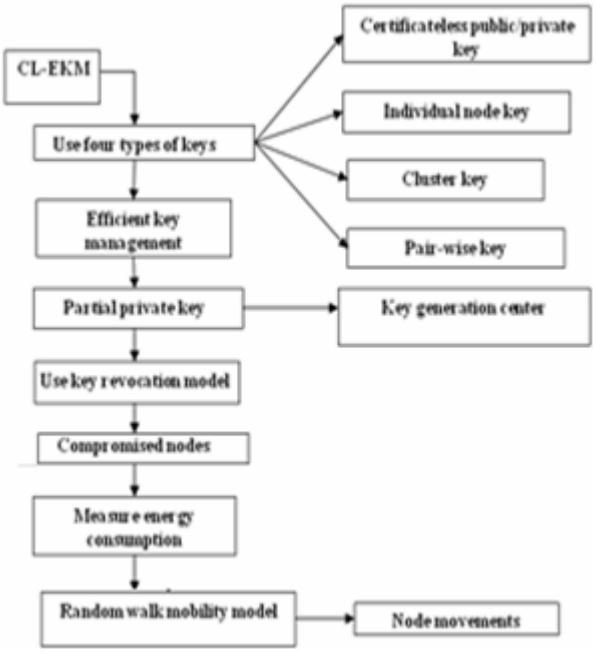
A. Overview

A certificate less effective key management (CL-EKM) scheme for dynamic WSNs is proposed.

In certificate less public key cryptography (CL-PKC), the user's full private key is the combination of a partial



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. 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)



V. OVERVIEW OF THECERTIFICATELESS EFFECTIVE KEY MANAGEMENTAND SECURITY MODEL SCHEME

KEY MANAGEMENT Before WSN will exchange information firmly, encryption keys should be established among sensing element nodes. Key distribution refers to the

distribution of multiple keys among the sensing element nodes, which is typical in an exceedingly non-trivial security theme. Key management could be a broader terms for key distribution, which conjointly includes the processes of key setup, the initial distribution of keys, and key revocation — the removal of a compromised key.

A. Network Model

We contemplate a heterogeneous dynamic wireless device network. The network consists of variety of stationary or mobile device nodes and a bachelor's degree that manages the network and collects knowledge from the sensors. Device nodes will be of 2 types: (i) nodes with high process capabilities, referred to as H-sensors, and (ii) nodes with low process capabilities, said as L-sensors. We have a tendency to assume to own N nodes within the network with variety N1 of H-sensors and variety N2 of L-sensors, wherever N = N1 + N2, and N1 N2. Nodes could be part of and leave the network, and thus the network size could dynamically amendment. The H-sensors act as cluster heads whereas L-sensors act as cluster members. They are connected to the bachelor's degree directly or by a multi-hop path through other H-sensors. H-sensors and L- sensors will be stationary or mobile. Once the network preparation, every H-sensor forms a cluster by discovering the neighboring L- sensors through beacon message exchanges. The L-sensors will be part of a cluster, move to different clusters and conjointly re-join the previous clusters. To maintain the updated list of neighbors and property, the nodes in an exceedingly cluster sporadically exchange very light-weight beacon messages. The H-sensors report any changes in their clusters to the bachelor's degree, as an example, once an L- sensor leaves or joins the cluster. The bachelor's degree creates a listing of legitimate nodes; Associate in Nursing updates the standing of the nodes once an anomaly node or node failure is detected.

The bachelor's degree assigns every node a unique symbol. A L-sensor nil is unambiguously known by node ID Li whereas a H-sensor nHj is assigned a node ID Hj. A Key Generation Center (KGC), hosted at the bachelor's degree, generates public system parameters used for key management by the BS and problems certificateless public/private key pairs for every node within the network. In our key management system, a unique individual key, shared solely between the node and also the bachelor's degree is assigned to every node. The certificateless public/private key of a node is employed to ascertain pair wise keys between any 2 nodes. A cluster secret's shared among the nodes in a very cluster.

B. Adversary Model and Security Requirements

We assume that the adversary can mount a physical attack on a sensor node after the node is deployed and retrieve secret information and data stored in the node. The adversary can also populate the network with the clones of the captured node. Even without capturing a node, an adversary can conduct an *impersonation* attack by injecting an illegitimate node, which attempts to impersonate a legitimate node. Adversaries can conduct passive attacks, such as, eavesdropping, replay attack, etc to compromise data *confidentiality* and *integrity*. Specific to our proposed key management scheme, the adversary can perform a *known-key* attack to learn pairwise master keys if it somehow learns the short-term keys, e.g., pairwise encryption keys.

VI. THE DETAILS OFCL-EKM

In this paper, we propose 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.

A. ATypes of Keys

• *Certificate less Public/Private Key:* Before a node is deployed, the KGC at the BS generates a singular certificate less private/public key **combine** and installs the keys in the node. This key combine is employed to get a reciprocally authenticated pair wise key.

• *Individual Node Key:* every node shares a singular individual key with BS. As an example, an L-sensor will use the individual key to write Associate in Nursing alert message sent to the BS, or if it fails to speak with the H- sensor. An H-sensor will use its individual key to write the message akin to changes within the cluster. The BS also can use this key to write any sensitive information, such a compromised node info or commands. Before a node is deployed, the BS assigns the node the individual key.

• *Pair wise Key:* every node shares a unique pair wise key with every of its neighboring nodes for secure communications and of those nodes. As an example, in order to hitch a cluster, a L-sensor ought to share a pair wise key with the H-sensor. Then, the H- sensor will firmly encrypt and distribute its cluster key to the L-sensor by victimization the pair wise key. In Associate in Nursing aggregation supportive WSN, the L- sensor will use its pair wise key to firmly transmit the detected information to the H-sensor. Each node can dynamically establish the pair wise key between itself and another node victimization their various certificate less public/private key pairs.

• *Cluster Key:* All nodes in an exceedingly cluster share a key, named as cluster key. The cluster key's chiefly used for securing broadcast messages in an exceedingly cluster, e.g., sensitive commands or the amendment of member standing in an exceedingly cluster. Only the cluster head will update the cluster key once a L-sensor leaves or joins the cluster.

VII. CONCLUSIONS AND FUTUREWORKS

In this paper, 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. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. The experimental results

demonstrate the effi-ciency of CL-EKM in resource constrained WSNs. As future work, we plan to formulate a mathematical model for energy consumption, based on CL-EKM with various parameters related to node movements. This mathematical model will be utilized to estimate the proper value for the T_{hold} and $T_{backoff}$ parameters based on the velocity and the desired tradeoff between the energy consumption and the security level.

REFERENCES

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

[2] 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.

[3] W. Du, J. Deng, Y. S. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, 2005.

[4] 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.

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

[6] D. S. Sanchez and H. Baldus, "A deterministic pairwise key pre-distribution scheme for mobile sensor networks," in *Proc. 1st Int. Conf. SecureComm*, Sep. 2005, pp. 277–288.

[7] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Two-layered dynamic key management in mobile and long-lived cluster-based wireless sensor networks," in *Proc. IEEE WCNC*, Mar. 2007, 4145–4150.

[8] Q. Huang, J. Cukier, H. Kobayashi, B. Liu, and J. Zhang, "Fast authenticated key establishment protocols for self-organizing sensor networks," in *Proc. 2nd ACM Int. Conf. WSNA*, 2003, pp. 141–150.

[9] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in *Proc. IACR Cryptol. ePrint Archive*, 2013, pp. 698–698.

[10] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2012, Sep. 2012, Art. ID 406254.

[11] 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.

[12] 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.

[13] M. R. Alagheband and M. R. Aref, "Dynamic and secure key manage-ment model for hierarchical heterogeneous sensor networks," *IET Inf. Secur.*, vol. 6, no. 4, pp. 271–280, Dec. 2012

[14] M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic Key Management in Sensor Networks," Communications Magazine, IEEE, vol 44, pp 122-130, April 2006.

[15] Arvinderpal S. Wander, Nils Gura, Hans Eberle,Vipul Gupta, and Sheueling Chang Shantz.(2005) EnergyAnalysis of Public Key Cryptography for Wireless Sensor Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324– 328.