Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 1, January -2017

# CL-KEM:Secure And Dynamic Effective Key Management Scheme

[1]Miss.Shobha Akaram Padalkar, [2]Prof.D.O.Shamkuwar

[1,2]*Dept.Of Comp.Engg.Flora Institute Of Technology,Khopi,Pune*

**Abstract---** *Recently, wireless detector networks (WSNs) are deployed for a good type of applications, as well as military sensing and chase, patient standing watching, traffic flow watching, wherever sensory devices usually move between totally different locations. Securing knowledge and communications needs appropriate encoding key protocols. During this paper, we have a tendency to propose a certificateless-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node quality. The CL-EKM supports economical key updates once a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol conjointly supports economical key revocation for compromised nodes and minimizes the impact of a node compromise on the safety of different communication links. A security analysis of our theme shows that our protocol is effective in defensive against numerous attacks.*

**Keywords---** *Diffie-Hellman (DH), WSN, CL-EKM, ECC, SN, BS.*

## I. INTRODUCTION

Dynamic wireless detector networks (WSNs), that modify movableness of detector nodes, facilitate wider network coverage and additional correct service than static WSNs. during this manner, dynamic WSNs square measure being chop-chop adopted in observance applications, such as, target pursuit in parcel of land police work, tending systems, traffic flow and vehicle standing observance, oxen health observance. In any case, detector devices square measure prone to malicious attacks like impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of property in wireless communication. Therefore, security is one among the foremost imperative problems in various crucial dynamic WSN applications. Dynamic WSNs after got to address key security conditions, for instance, node authentication, information confidentiality and trait i.e. integrity, at no matter purpose and where the nodes move.

To address security, cryptography key management protocols for dynamic WSNs are planned within the past supported symmetric key cryptography. Such kind of cryptography is suitable for detector nodes due to their restricted energy and process capability. However, it suffers from high communication overhead and needs giant memory area to store shared pairwise keys. It's additionally not ascendible and not resilient against compromises, and unable to support node quality. So symmetric key cryptography isn't appropriate for dynamic WSNs. additional recently, uneven key based mostly approaches are planned for dynamic WSNs. These approaches cash in of public key cryptography (PKC) like elliptic curve cryptography (ECC) or identity-based public key cryptography (ID-PKC) so as to change key institution and information authentication between nodes. PKC is comparatively costlier than symmetric key cryptography with reference to machine prices. Recent enhancements within the implementation of error correction code have incontestable the feasibleness of applying PKC to WSNs.

In our work, we have a tendency to introduce a certificateless effective key management (CL-EKM) set up for dynamic WSNs. In certificateless public key cryptography (CL-PKC), the client's full non-public secret is a mixture of Associate in nursing partial non-public key created by a key generation center (KGC) and therefore the client's own secret worth. The special organization of the complete non-public/public key combine removes the requirement for certificates and conjointly resolves the key written agreement drawback by removing the responsibility for the user's full private key. We have a tendency to likewise take the advantage of computer code keys outlined on Associate in nursing additive cluster with a 160-piece length as secure because the RSA keys with 1024-piece length.

With a selected finish goal to dynamically provide each node authentication and discovered a pairwise key between nodes, we have a tendency to construct CL-EKM by utilizing a pairing-free certificateless hybrid signcryption theme (CL-HSC) planned by America in Associate in Nursing earlier work. thanks to the properties of CL-HSC, the pairwise key of CL-EKM are often expeditiously shared between 2 nodes while not requiring heavy pairing operations and therefore the exchange of certificates. To support node quality, our CL-EKM in addition supports light-weight procedures for cluster key upgrades dead once a node moves, and key revocation is dead once a node is detected as malignant or leaves the cluster for good. CL-EKM is ascendable just in case of additives of recent nodes once network readying. CL-EKM is secure against node compromise, biological research and impersonation, and ensures forward and backward secrecy. The safety examination of our set up demonstrates its effectiveness.

 

## II. LITERATURE SURVEY

**2.1 Paper Name: Dynamic and secure key management model for hierarchical heterogeneous sensor networks (2012).**
**Authors: M.R. Alagheband and M.R. Aref**
**Description:** Many applications that utilize wireless device networks (WSNs) need primarily secure communication. However, WSNs suffer from some inherent weaknesses owing to restricted communication and hardware capabilities. Key management is that the crucial necessary building block for all security goals in WSNs. Most existing researches tried to assign keys presumptuous solid specification. Recently, many key management models for heterogeneous WSNs are planned. During this study, the authors propose a dynamic key management framework supported elliptical curve cryptography and signcryption methodology for heterogeneous WSNs. The planned theme has network quantifiability and device node (SN) quality particularly in liquid environments. Moreover, each periodic authentication and a replacement registration mechanism area unit planned through bar of atomic number 50 compromises. The authors analyze a number of the additional seminal hierarchic heterogeneous WSN key management themes and compare them with the planned scheme. On examination the planned theme with the additional seminal hierarchic heterogeneous WSN key management schemes, the planned framework separately proves to be higher in terms of communication, computation and key storage.

**2.2 Paper Name: An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks (2011)**
**Authors: Sarmad Ullah Khan, Claudio Pastrone, Luciano Lavagno, Maurizio A. Spirito**
**Description:** Wireless detector Network (WSN) technology is being a lot of} adopted in a very wide selection of applications starting from home/building and industrial automation to more safety vital applications as well as e-health or infrastructure observation. Considering quality within the on top of application eventualities really introduces further technological challenges, particularly with relevance security. The resource strained devices ought to be sturdy to numerous security attacks and communicate firmly whereas they're occupation the thought-about setting. To the current aim, correct authentication and key management schemes supporting node quality ought to be used. This paper presents a good mutual authentication and key institution theme for heterogeneous detector networks consisting of diverse mobile detector nodes and solely many a lot of powerful fastened detector nodes. Moreover, OMNET++ simulations are accustomed give a comprehensive performance analysis of the projected theme. The obtained results show that the projected answer assures higher network property, consumes less memory, has low communication overhead throughout the authentication and key institution section and has higher network resilience against mobile nodes attacks compared with existing approaches for authentication and key institution.

**2.3 Paper Name: Certificate less Public Key Cryptography (2004).**
**Authors: Sattam S. Al-Riyami and Kenneth G. Patersony**
**Description:** This paper introduces the thought of certificateless public key cryptography (CL-PKC). In distinction to ancient public key cryptanalytic systems, CL-PKC doesn't need the utilization of certificates to ensure the believability of public keys. It will have faith in the utilization of a trusty third party (TTP) UN agency is in possession of a passkey. In these respects, CL-PKC is analogous to identity-based public key cryptography (ID-PKC). On the opposite hand, CL-PKC doesn't suffer from the key written agreement property that looks to be inherent in ID-PKC. So CL-PKC may be seen as a model for the utilization of public key cryptography that's intermediate between ancient credentialed PKC and ID-PKC. We tend to create concrete the thought of CL-PKC by introducing certificate less public key encoding (CL-PKE), signature and key exchange schemes. We tend to conjointly demonstrate however hierarchal CL-PKC may be supported. The schemes are all derived from pairings on elliptic curves. the dearth of certificates and therefore the want to prove the schemes secure within the presence of Associate in Nursing opponent UN agency has access to the passkey needs the careful development of recent security models. For reasons of brevity, the main focus during this paper is on the safety of CL-PKE. We tend to prove that our CL-PKE theme is secure during a totally adaptation AL adversarial model, given that Associate in Nursing underlying downside closely associated with the linear Diffee-Hellman downside is difficult.

**2.4 Paper Name: Elliptic Curve Cryptography based Certificateless Hybrid Signcryption Scheme without Pairing (2013).**
**Authors: Seung-Hyun Seo and Elisa Bertino**
**Description:** Signcryption could be a theme that has confidentiality and authentication whereas keeping prices low as compared to freelance encoding and message language. Since Zheng introduced the thought of signcryption, a range of schemes are given in. we are able to divide the themes in 2 ways that to construct the signcryption scheme like a public signcryption and a hybrid signcryption. Within the public signcryption theme, the method of encoding and language square measure performed utilizing the general public key operation. However, within the hybrid signcryption theme, solely the language method uses the general public key operation whereas the even key setting is employed for the encoding. That is, we are able to construct the hybrid signcryption theme by combining 2 methods: (1) associate degree uneven half, takes a non-public associate degreed a public key because the input and outputs an appropriately sized

 

random even key and so performs an encapsulation of the key, (2) the symmetric half takes a message associate degreed a symmetric key because the input and outputs an echt encoding of the message. Thus, a hybrid signcryption approach will with efficiency encapsulate new keys and firmly transmit information for varied applications like Advanced Metering Infrastructures (AMIs) and Wireless sensing element Networks (WSNs).

**2.5 Paper Name: Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks (2013).**
**Authors: Xi-Jun Lin and Lin Sun.**
**Description:** In 2012, Alagheband and Aref gave a dynamic and secure key management model for class-conscious heterogeneous detector networks. They projected a signcryption algorithmic rule that is that the main building block in their key management model. They tried the algorithmic rule is as robust because the elliptical curve distinct power downside. During this work, we tend to study the protection of their signcryption algorithmic rule. It's sorry that we tend to found their algorithmic rule is insecure. The opponent will impersonate the bottom station by causing solid messages to the cluster leaders once capturing the signcrypted messages. Hence, the key management model projected by them is insecure. Then, we tend to propose associate improved signcryption algorithmic rule to mend this weakness.

## III. PROPOSED SYSTEM

1. In this paper, we tend to gift a certificateless effective key management (CL-EKM) theme for dynamic WSNs.
2. In certificateless public key cryptography (CL-PKC), the user's full personal secret's a mix of a partial personal key generated by a key generation center (KGC) and therefore the user's own secret price.
3. The special organization of the total personal/public key try removes the necessity for certificates and additionally resolves the key written agreement downside by removing the responsibility for the user's full private key.
4. We additionally take the good thing about code keys outlined on Associate in Nursing additive cluster with a 160-bit length as secure because the RSA keys with 1024-bit length.

**3.1 Advantages of Projected System:**

1. Provide a lot of security.
2. Decrease the overhead.
3. Protects the information confidentiality and integrity.

## IV. SYSTEM ARCHITECTURE

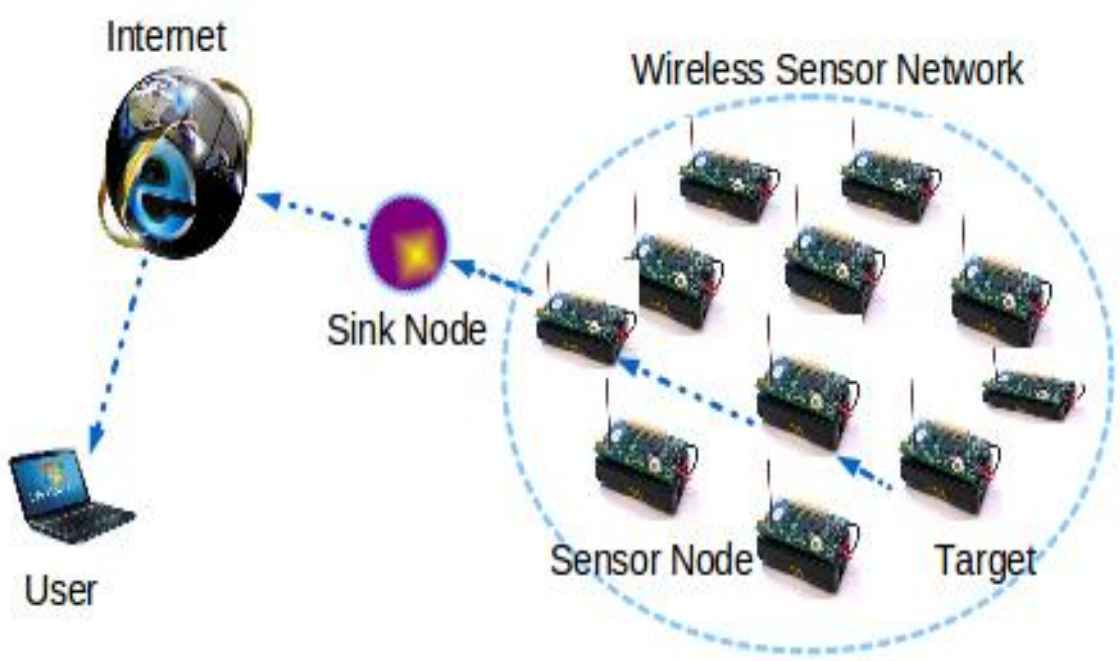


***Figure 1. System Architecture of Proposed System***

 

1. We proposed a certificateless effective key management (CL-EKM) theme for dynamic WSNs.
2. In certificateless public key cryptography (CL-PKC), the user's full non-public secret's a mix of a partial non-public key generated by a key generation center (KGC) and also the user's own secret worth.
3. The special organization of the complete non-public/public key try removes the necessity for certificates and conjointly resolves the key written agreement downside by removing the responsibility for the user's full private key.
4. We conjointly take the good thing about error correction code keys outlined on Associate in Nursing additive cluster with a 160-bit length as secure because the RSA keys with 1024-bit length.

## V. CONCLUSION

In this work, we have a tendency to propose the primary certificateless effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM supports economical communication for key updates and management once a node leaves or joins a cluster and thence ensures forward and in reverse key secret.

Our theme is resilient against node trade compromise, biological research and impersonation attacks and protects the information confidentiality moreover, integrity. The check results show the effectiveness of CL-EKM in resource forced WSNs. As future work, we have a tendency to conceive to formulate a scientific model for energy utilization, supported CL-EKM with totally different parameters known with node movements. This mathematical model is wont to appraise the simplest potential value for the Thold and Tback of fparameters taking under consideration the speed and also the unreal trade-off between the vitality utilization and also 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 management 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 predistribution 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, "Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks," in *Proc. IEEE WCNC*, Mar. 2007, pp. 4145–4150.

[8] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in *Proc. 8th Int. Conf. ICISS*, vol. 7671. 2012, pp. 194–207.

[9] 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.

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

[11] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proc. 6th Int. Workshop Cryptograph. Hardw. Embedded Syst.*, 2004, pp. 119–132.

[12] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. 9th Int. Conf. ASIACRYPT*, vol. 2894. 2013, pp. 452–473.

 

[13] S. Seo and E. Bertino, "Elliptic curve cryptography based certificateless hybrid signcryption scheme without pairing," CERIAS, West Lafayette, IN, USA, Tech. Rep. CERIAS TR 2013-10, 2013. [Online]. Available: https://www.cerias.purdue.edu/apps/reports_and_papers/.Seung-Hyun

[14] S. H. Seo, J. Won, and E. Bertino, "POSTER: A pairing-free certificateless hybrid sign-cryption scheme for advanced metering infrastructures," in *Proc. 4th ACM CODASPY*, 2014, pp. 143–146.

[15] 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.

[16] 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.

[17] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "NanoECC: Testing the limits of elliptic curve cryptography in sensor networks," in *Proc. 5th Eur. Conf. WSN*, vol. 4913. 2008, pp. 305–320.

[18] K. Chatterjee, A. De, and D. Gupta, "An improved ID-based key management scheme in wireless sensor network," in *Proc. 3rd Int. Conf. ICSI*, vol. 7332. 2012, pp. 351–359.

[19] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in mobile sensor networks: Theory and approaches," *Secur. Commun. Netw.*, vol. 5, no. 5, pp. 496–507, 2012.

[20] 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.

[21] P. Jiang, "A new method for node fault detection in wireless sensor networks," *Sensors*, vol. 9, no. 2, pp. 1282–1294, 2009.

[22] L. Paradis and Q. Han, "A survey of fault management in wireless sensor networks," *J. Netw. Syst. Manage.*, vol. 15, no. 2, pp. 171–190, 2007.

[23] (2013). *All About Battery*. [Online]. Available: http://www.allaboutbatteries.com/Energy-tables. html, accessed Dec. 2014.

[24] A. Liu and P. Ning, "TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks," in *Proc. Int. Conf. IPSN*, Apr. 2008, pp. 245–256.

[25] 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.

[26] 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.

[27] 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.

 