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: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.449 – 452

SURVEY ON EFFECTIVE KEY MANAGEMENT IN DYNAMIC WIRELESS SENSOR NETWORKS

Ms. Chethana M[1], Mrs. S Rajeswari[2]

[1]M.Tech Student Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India

[2]Senior Assistant Professor, Department of Information Science and Engineering, New Horizon College of Engineering, Bangalore, India

[1] chethanam9214@gmail.com, [2] raji_sura@yahoo.com

ABSTRACT: Nowdays, 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) 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.

KEYWORDS: Wireless sensor networks, certificateless public key cryptography, key management schema.

I. INTRODUCTION

Dynamic Wireless Sensor Networks (WSNs) enables to have more number of sensor node, hence facilitate wider network coverage and provide more accurate service than static WSNs .Dynamic WSNs are widely used in monitoring applications, such as target tracking in battlefield surveillance, traffic flow and vehicle status monitoring, dairy cattle health monitoring and healthcare systems. But sensor device are vulnerable to various

attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of connectivity in wireless communication .Hence security is the major issue in critical dynamic WSN applications. To overcome these issues dynamic WSNs need to address the key security requirements, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move.

To address key security encryption key management protocols for dynamic WSNs was proposed, based on symmetric key encryption. Because the energy and processing capability was limited the encryption key management protocol was well-suited for sensor nodes. But they suffered from high communication overhead and to store the shared pair wise keys requires large memory space. It is also not scalable and not resilient against compromises, and unable to support node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs.

Later, asymmetric key approaches was proposed for dynamic WSNs, it took the advantage of public key cryptography (PKC) such as elliptic curve cryptography (ECC) or identity-based public key cryptography (ID-PKC)in order to simplify key establishment and data authentication between nodes. It is also more scalable, flexible and resilient to node compromise attacks.PKC is relatively more expensive than symmetric key encryption with respect to computational costs. However, recent improvements in the implementation of ECC has demonstrated the feasibility of applying PKC to WSNs.

The major drawback of ECC is security weakness and are vulnerable to message forgery, key compromise and known-key attacks .Hence to overcome all this drawback a Certificateless effective key management (CL-EKM) scheme for dynamic WSNs is proposed. In this schema users private key is the combination of partial private key which is generated by key generation center (KGC) and users own secret key.To support node mobility CL-EKM also supports lightweight processes for cluster key updates executed when a node moves, and key revocation is executed when a node is detected as malicious or leaves the cluster permanently. CL-EKM is scalable in case of additions of new nodes after network deployment. CL-EKM is secure against node compromise, cloning and impersonation, and ensures forward and backward secrecy.

II. RELATED WORK

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.

N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz[7] proposed a light weighted implementation of public key called as cluster based public infrastructure (CBPKI), it is based on security and the authenticity of base station for executing a set of handshakes that establish session keys between the base station and sensors over the networks that are used for ensuring the data confidentiality and integrity.

III. PROPOSED TECHNIQUE

The most effective key for dynamic WSNs is Certificateless effective key management protocol(CL-EKM), it supports four types of keys each of them are used for different purposes, especially for including secure pair-wise node communication and group-oriented key communication within the clusters. This schema uses the main algorithms of the CL-HSC 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.

- Certificateless public/private key: this key generates a mutually authenticated pair-wise key.
- Individual node key: each node will have individual key.
- Pairwise key: to have a secure communication and authentication of nodes each node shares a different pairwise key with the neighbouring nodes.
- 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 and movement of nodes.

Compared to other approach the proposed schema provides more security, decrease overhead and protect data confidentiality and integrity.

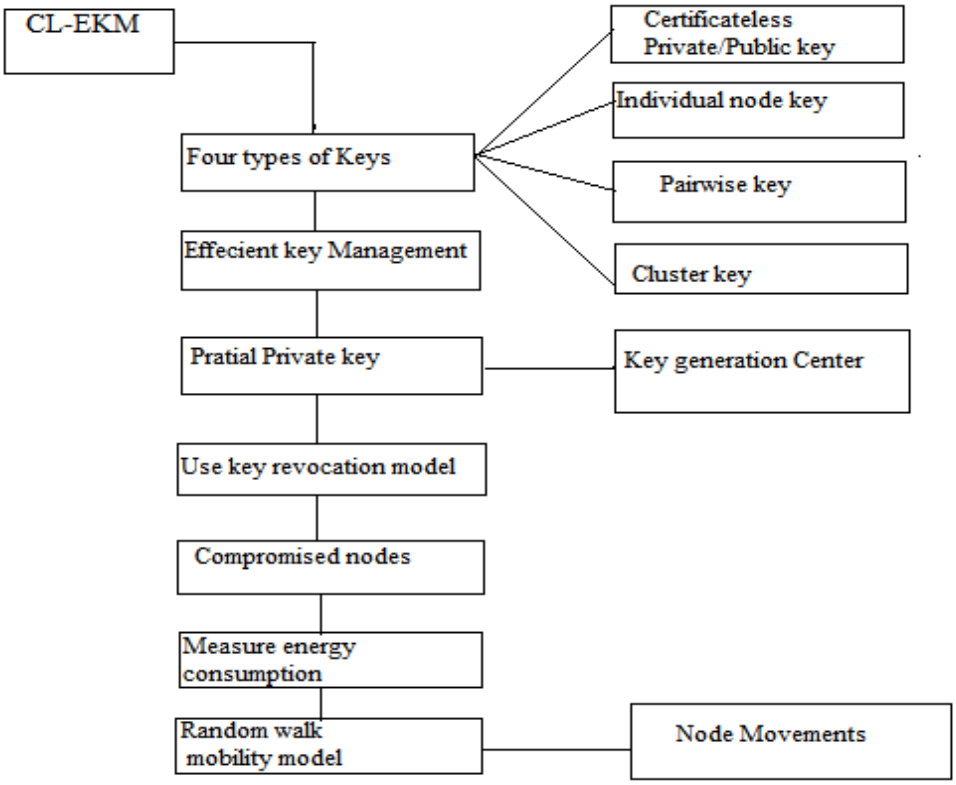

Figure 1: System Flow of Proposed System

Security analysis of CL-EKM, security of CL-HSC uses a building block of CL-EKM, hence CL-EKM achieves our security goals. The CL-HSC provides both confidentiality and unforgetability for signcrypted messages based on the intractability of the EC-CDH. Moreover, it is not possible to forget or expose the full private key of an entity based on the difficulty of EC-CDH, without the knowledge of both KGC's master private key and an entity's secret value. Therefore, the confidentiality is defined as indistinguishability against adaptive chosen cipher-text and identity attacks (IND-CCA2) while unforgetability is defined as existential unforgetability against adaptive chosen messages and identity attacks (EUF-CMA).

IV. CONCLUSION

A survey on effective key management in Dynamic WSNs is done. Certificateless effective key management (CL-EKM) protocol is proposed to provide a secure communication for Dynamic WSNs, it also support an efficient communication for providing key updates and managements of nodes when it leaves and joins a cluster and ensures forward and backward key secrecy. The scheme is also resilient against node compromise, cloning and impersonation attacks and protects the data and integrity.

REFERENCES

[1] 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 clusterbased wireless sensor networks," in Proc. IEEE WCNC, Mar. 2007, pp. 4145–4150.

[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] 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.

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

[9] 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.

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

[11] 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.

[12] 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.

