Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 7, July-2017, pp. 308-312 www.ijcert.org

Effective Key Management In Dynamic Wireless Sensor Networks

Uma Vasala [1], **Dr. G. R. Sakthidharan** [2]

[1] M.Tech [CSE],Gokaraju Rangaraju Institute of Engineering and Technology
[2] Professor/CSE,Gokaraju Rangaraju Institute of Engineering and Technology
Email ID: umareddyvasala@gmail.com[1], grsdharan@griet.ac.in[2]

Abstract: -Recently, wireless detector networks (WSNs) have been deployed for a good form of applications, including military sensing, and pursuit, patient standing watching, traffic flow watching, wherever sensory devices typically move between different locations. Securing knowledge and communications need suitable encoding key protocols. In this paper, we tend to propose a certificate less efficient key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports economic key updates once a node leaves or joins a cluster and ensures forward and backward key secrecy.

The protocol conjointly supports economic key revocation for compromised nodes and minimizes the impact of a node compromise on the protection of alternative communication links. A security analysis of our theme shows that our protocol is effective in defensive against separate attacks. We implement CL-EKMin Contiki OS and simulate it mistreatment Cooja machine to assess its time, energy, communication, and memory performance.

Keywords:- Wireless sensor networks, certificate less public key cryptography, key management scheme.

1. Introduction

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 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 Thus, security is one of the most important issues in many critical dynamic WSN applications.

To address security, encryption key management protocols for dynamic WSNs have been proposed in the past based on symmetric key encryption. Such type of encryption is well-suited for sensor nodes because of their limited energy and processing capability.

The problems of knowledge-based DYNAMIC wireless detector networks (WSNs), that change quality of detector nodes, facilitate wider network coverage and correct additional service than static WSNs. Therefore, dynamic WSNs area unit being apace adopted in observance applications, like target following in a piece of land police work, tending systems, traffic flow and vehicle standing observance, cattle health observance. However, detector de-vices area unit susceptible to malicious attacks like impersonation, interception, capture or physical destruction, as a result of their unattended operative environments and lapses of property in wireless communication. Thus, security is one among the foremost vital problems in several vital dynamic WSN applications. Dynamic WSNs, therefore, ought to address key security necessities, like node authentication, information confidentiality, and integrity, whenever and where the nodes move.

A certificate-less effective key management (CL-EKM) scheme for dynamic WSNs. In certificate-less 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 secret value

2. Existing Methodology

The following describes the existing method.

1. Symmetric Key Scheme: Not appropriate For Mobile sensing element Node.
2. Two- superimposed Key Management scheme: Not suitable for sensors with restricted resources and unable to perform advanced computation with massive key size.
3. Elliptic Curve Cryptography(ECC): Due Exchange of certificate, the communication, and computation over-head will increase.
4. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes are not secure

2.1 Disadvantages in Existing System

1. Symmetric Key Scheme: Not appropriate For Mobile sensing element Node.
2. Two-Layered Key Management scheme: Not suitable for sensors with restricted resources and unable to perform advanced computation with massive key size. Elliptic Curve Cryptography (ECC): Due Exchange of certificate, the communication, and computation over-head will increase.
3. Unable to access with large size of keys
4. Increase the overhead
5. Cannot provide more secure

3. Proposed System

1. The Users full private key's combination of a partial non-public key generating by a Key Generation Center (KGC) and therefore the user's secret price.
2. Special Organization of the complete private/public key combine removes the requirement for the certificate.
3. Effective sharing between 2 nodes while not requiring onerous pairing operations and therefore the exchange of certificate.
4. We present a certificate-less effective key management (CL-EKM) scheme for dynamic WSNs.

2.2 Advantages

1. Provide more security
2. Decrease the overhead
3. Protects the data confidentiality and integrity

3. Related Work

In the area unit several styles of the major management strategies projected within the field of distributed key management methodology, terrier, and leg of lamb initial given a random key distribution methodology. In this method, every node haphazardly selects keys from the key pools be-fore preparation. If the adjacent nodes a minimum of have one same key, they will directly establish a session key. Chan et additionally projected {a methodology|away|a technique} supported the E-G methodology that is termed -composite key management method. The adjacent nodes will establish communication if they a minimum of have same keys. The association rate of those 2 strategies is lower, and also the price of keys storage is higher within the field of cluster-based key management strategies, Zhu et al. devised a technique known as LEAP. This methodology not solely will support the process within the network, however, is also a sort of key management methodology with the fine ability of resistance to capture. In or-der to fulfill the various security needs, LEAP supports the institution of 4 styles of keys. They are individual key, group key, clustered key, and combine key, severally. It additionally provides the network node authentication supported unidirectional key chain. However its mechanisms of the key update, revocation, nodes canceling, and nodes adding aren't good, and clusters can dynamically be modified in practical applications. Jolly projected a low-energy key management protocol that supports revocation for the attkcked nodes.

4. System Architecture

The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w, we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task management. These layers of the WSN are used to accomplish the n/w and make the sensors work together to raise the complete efficiency of the network.Please follow the below link for Types of wireless sensor networks and WSN topologies

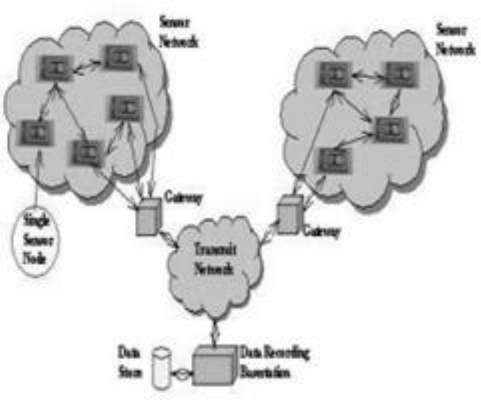

Figure 1. WSN System Architecture

5. Applications

1. Military Applications
2. Health Applications
3. Environmental Applications
4. Home Applications
5. Commercial Applications
6. Area monitoring
7. Health care monitoring
8. Environmental/Earth sensings
9. Air pollution monitoring
10. Forest fire detection
11. Landslide detection
12. Water quality monitoring
13. Industrial monitoring.

6. Algorithm

The Shoulder aquatics bar - identification generation Graphical identification systems are a sort of knowledge-based authentication that decide to leverage the human memory for visual information In Pass Points, passwords encompass a sequence of 5 click-points on a given image.Suppose three level image identification is chosen Then download 3+(3) pictures from the drop box and set coordinates as identification.

The CL-EKM is comprised of 7 Phases :

1. System Setup
2. pairwise key generation
3. cluster formation
4. key update
5. node movement
6. key revocation
7. the addition of a new node

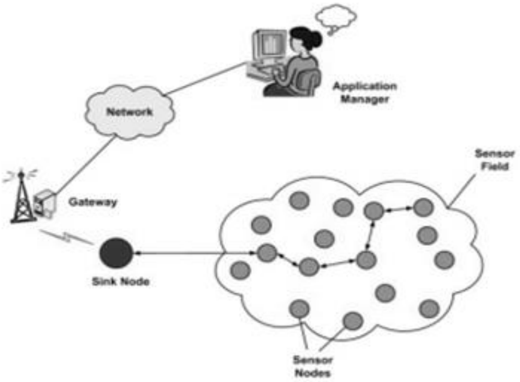

Figure 2. CL-EKM Architecture

7.Conclusion

In this, we tend to give an outline of state of the art dynamic key management schemes in WSNs. With the wide application of WSNs, in a concert of the core security problems, dynamic key management is attracting additional attention from the researchers and industrial engineers and lots of schemes were already planned. We tend to mentioned the fundamental necessities of dynamic key management in WSNs, surveyed the planned themes for these environments and highlighted the safety and Performance benefits and downsides of every scheme. Finally, we have got summarized and analyzed these techniques in line with the mentioned analysis metrics.

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, "Two-layered dynamic key management in mobile and long-lived cluster-based 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] J.David Sukeerthi Kumar," Investigation on Secondary Memory Management in Wireless Sensor

Network,” International Journal of Computer Engineering In Research Trends.,vol .2,no.6,pp.387-391,June 2015.

[17] Kuruva Laxmanna, N.Poorna Chandra Rao, Dr.S.Prem Kumar,” Moderating vampire attacks in Wireless Sensor Network,” International Journal of Computer Engineering In Research Trends.,vol.1,no.3,pp.143-151,September 2014.

[18].P.G.V.SureshKumar,Seelam Sowjanya,”Developing an Enterpriseenvironment By Using Wireless Sensor Network System Architecture,” International Journal of Computer Engineering In Research Trends.,vol .2,no.10,pp.902-908,October 2015.

[19] Dr. C. Gulzar,AmeenaYasmeen," Maximum network lifetime with load balance and connectivity by clustering process for wireless sensor networks,”International Journal of Computer Engineering In Research Trends.,vol.3,no.7,pp.375-383,July 2016.

[20] A.Yogananda ,Chepuri Sai Teja ," A Multi-level Self-Controllable Authentication in Distributed m-Healthcare Cloud Environments, ” International Journal of Computer Engineering In Research Trends.,vol.3,no.8,pp.436-440,August 2016.