IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 52-55
www.iosrjournals.org

Precious Solution Regulation in Active Wireless Sensor Networks

Ms.P.Subha[1], Mrs.S.Jayabharathi[2]
[1]*M.sc, M.Phil., Full Time Scholar, Department of Computer Science, Vivekanandha College for Women.*
E-Mail id:subhaaathi16@gmail.com.
[2]*M.sc,MCA,M.Phil.Assistant Professor , Department of Computer Science, Vivekananda College of Arts and Science for Women.*
E-Mailid:jayabharathi8383@.com

Abstract*: Now days, Wireless sensor networks (WSNs) are widely used in wide variety of application 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 certificate less – effective key management (CL-EKM) protocol is proposed to have 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, Certificate less public key cryptography, Key management schema.*

I. Introduction

Wireless detector Networks are consisting of distributed autonomous sensors to watch physical or environmental conditions, just like the temperature, sound, pressure, etc. and additionally to hand in glove pass the info through the network to a main location. the trendy networks are bi-directional, additionally we are able to management the detector activity. The event of wireless detector networks was impelled by the military applications like field of battle surveillance; these days, such networks are employed in several industrial and client applications, like process observance and management, machine health observance. The WSN consists of "nodes" from some to many a whole lot or perhaps thousands, wherever every node connected to at least one (or generally several) sensors. Every such detector network node can have generally many parts: a radio transceiver that has an enclosed ANtenna or affiliation to an external antenna, a microcontroller, AN electronic circuit for the interface with the sensors ANd an energy supply, sometimes battery or AN embedded style of energy storage.A detector node could vary in size from that of a shoebox right down to the dimensions of a grain of mud, though functioning "motes" of real microscopic sized image is nevertheless to be created. The prices of detector nodes are equally variable, starting from some to many USD; that depends on the quality of the individual detector nodes. Size and value constraints on detector nodes lead to corresponding constraints on the offered resources like energy, memory, and machine speed and communications information measure. The topology of the WSNs is varied from a straightforward star network to advanced multi-hop wireless mesh network. The propagation technique between the hops of the network is by routing or flooding.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. Thus, security is one of the most important issues in many critical dynamic WSN applications.

II. Litrature Survey

2.1 Tao Shu and Marwan Krunz, Fellow,IEEE,[1]

Describe the 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 performance

Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen,[2] describe the 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.

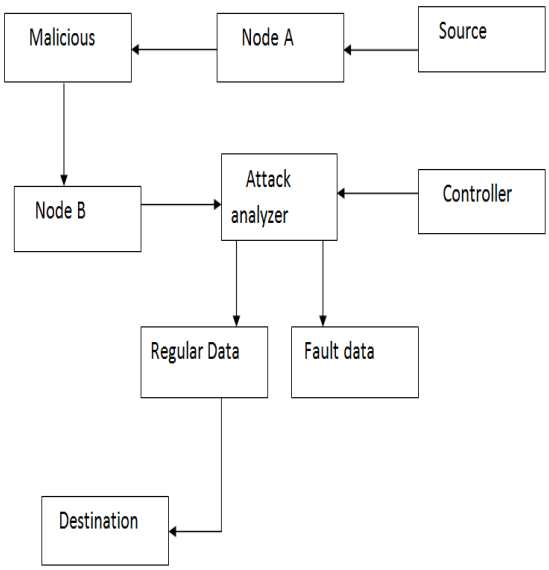
X. Zhang, J. He, and Q. Wei[3] describe the energy-efficientdistributed deterministic key management scheme (EDDK).With the help of this scheme pairwise keys and cluster keys of sensor nodes are well established as well as maintained securely and communication overhead is also less. They also made use 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

N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz[4] describe the 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. System Model

3.1 Network Model

The scheme is meant for protecting WSN from malicious attacks. The network is secured using the proposed scheme which takes care of initialization, secure key distribution, key update and key revocation.

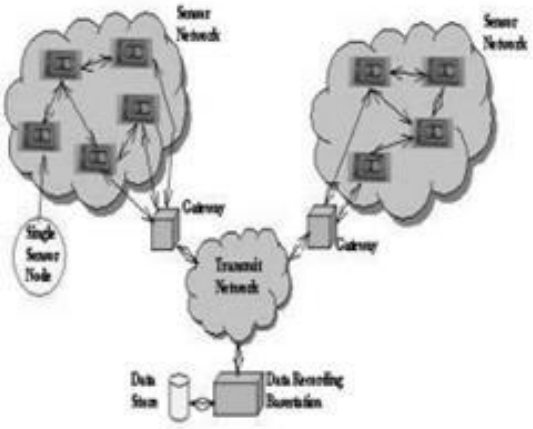


3.2 Overview of the proposed scheme

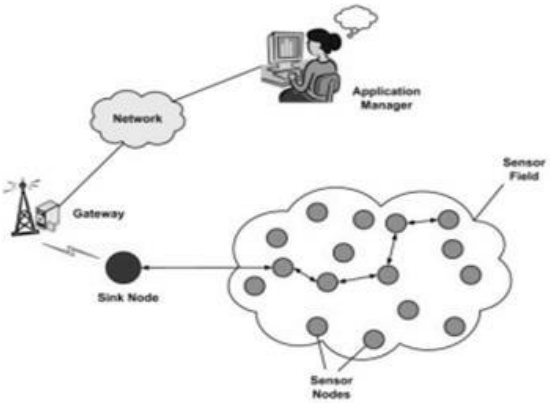
We implemented attack analyzer which takes care of security issues besides ensuring that the communications in the network are protected from malicious attacks. The controller sensor nodes and the attack analyzer work in tandem with each other in order to prevent attacks and promote secure communications.The 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. Special Organization of the complete private/public key combine removes the requirement for the certificate. Effective sharing between 2 nodes while not requiring onerous pairing operations and therefore the exchange of certificate. We present a certificate-less effective key management (CL-EKM) scheme for dynamic WSNs.With the development of science and technology, cryptography has also been considerable development both in theory and in practice. For different applications, there are many different cryptography systems, such as the symmetric cryptography, public key cryptography and so on. All of these algorithms have the strengths and weaknesses in different applications, but we have not found that a theory which would be able to meet all application requirements in the WSNsThe 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.

IV. System Architecture



WSN System Architecture



Cl-Ekm Architecture

V. Conclusion And Future Enhancement

We have a tendency to given an outline of state of the art dynamic key management schemes in WSNs. With the wide application of WSNs, in concert of the basic security problems, dynamic key management is attracting additional attention from the researchers and industrial engineers and lots of schemes were already planned. we have a tendency 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've got summarized and analyzed these techniques in line with the mentioned analysis metrics.

Acknowledgment

My heartfelt gratitude goes to my beloved guide Mrs.S.Jayabharathi Assistant Professor, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India for dedication and patience in assigning me her valuable advice and efforts during the course of my studies.

References

[1]. Tao Shu and Marwan Krunz, Fellow,IEEE "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING. VOL. 14, Issue NO. 4, pp 813-828- APRIL 2015.

[2]. Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen, "Side Channel Monitoring: Packet Drop Attack Detection in Wireless Ad Hoc Networks", IEEE ICC international conference on communication,11year 2011.

[3]. Yu Zhang, Loukas Lazos, Member, IEEE, and William Jr. Kozma. "AMD: Audit-Based Misbehavior Detection in Wireless Ad Hoc Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 15, NO. 8, pp1893-1907-AUGUST 2016.
[4]. Vijayakumar.Aa*, Selvamani Kb*, Pradeep kumar Aryac," Reputed Packet Delivery using Efficient Audit Misbehaviour Detection and Monitoring Method in Mobile Ad Hoc Networks,". ELSEVIER procedia computer science. VOL. 48, pp485-495- 2015
[5]. Mohammad Taqi Soleimani, Mahboubeh Kahvand, "Defending Packet Dropping Attacks Based on Dynamic Trust Model in Wireless Ad Hoc Networks" ,Mediterranean electrotechnical conference. Vol. 13, pp362-366- 16 April 2014.
[6]. 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.
[7]. S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in Proc. 9th Int. Conf. ASIACRYPT, vol. 2894. 2013, pp. 452–473.
[8]. 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
[9]. 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.
[10]. 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.