International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

Productive Key Administration in WSN

Devendra Terse (1st *Author*)
Department of Information Technology
PHCET, Panvel
Navi Mumbai, India

Archana Augustine (2nd *Author*)
Asst. Prof. (Department of IT)
PHCET, Panvel,
Navi Mumbai, India

Abstract—Wireless Device Networks or Wireless Sensor Network (WSNs) comprises tiny sensor nodes with strained energy, memory and computation capabilities. They are typically deployed within the unattended and hostile environment. So device no des area unit susceptible to attacks such as no de capture and collusion attack by adversaries. Its associate degree energy efficient dynamic key management scheme that performs localized re-keying to reduce overhead. Key management has remained a difficult issue in Wireless Device Networks (WSNs) as a result of the constraints of device no de resources. Various key management schemes that trade off security and operational necessities are proposed in recent years. A certificate oriented-effective key management (CO-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CO-EKM underpins key upgrades once a node leaves or joins a cluster and guarantees forward and in reverse key secrecy. The protocol furthermore supports key revocation for traded off or compromised nodes and limits the effect of a node compromise on the protection of alternative links for communication. A security analysis of theme shows that protocol is effective in defensive against varied attacks and simulates it using Network Simulator2 to assess its time, energy, communication, and memory performance.

Keywords—WSN; Cetrificate Oriented Effective Key Management; Key Management;

I. INTRODUCTION

Wireless sensor networks are a promising enabling technology for future information retrieval and secure communication purposes. Typical wireless sensor nodes are relatively cheap and are expected to become even cheaper in near future, making it feasible to rapidly deploy wireless networks formed by hundreds or thousands of nodes for secure transmission of data between the nodes.

A wireless sensor network is a collection of nodes organized into a co-operative network. Each node consists of processing capability (one or more micro controllers, CPUs or DSP chips), it may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single Omni-directional antenna), a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an Ad-HOC fashion. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is sensible to expect that in 10-15 years that the world will be secured with wireless sensor networks with access to them through the Internet. This can be considered as the Internet turning into a physical network. Wireless Sensor Network is broadly utilized as a part of electronics devices.

Wireless sensor networks can have both static and dynamic types. Dynamic Wireless sensor networks is more efficient than static wireless sensor network. Dynamic wireless sensor networks (WSNs), which enable mobility of sensor nodes, facilitate wider network coverage and more accurate service than static WSNs.

II. RELATED WORK

Dynamic wireless sensor networks(WSNs), which empower versatility of sensor hubs, en-courage more extensive system scope and more exact administration than static WSNs. Along these lines, dynamic WSNs are all around immediately grasped in observing applications, for example, target following in combat zone reconnaissance, social insurance frameworks, movement stream and vehicle status checking, dairy steers wellbeing observing [2]. On the other hand, sensor gadgets are helpless against malignant assaults, for example,

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

mimic, block attempt, catch or physical devastation, due to their unattended agent circumstances and breaks of network in remote correspondence [4]. Along these lines, security is a standout amongst the most imperative issues in numerous basic element WSN applications. Dynamic WSNs subsequently need to address key security prerequisites, for example, hub confirmation, information classification and honesty, at whatever point and wherever the hubs move. In this approach, we introduce a certificate-less viable key administration (CL-EKM) plan for element WSNs. In certificate-less open key cryptography (CL-PKC) [3], the client's full private key is a mix of a fragmentary private key delivered by a key period focus (KGC) and the client's own specific mystery esteem. The remarkable association of the full private/open key pair uproots the prerequisite for authentications besides determines the key escrow issue by emptying the commitment in regards to the client's full private key. Likewise take the benefit of ECC keys characterized on an additional substance pack with a 160 piece length as secure as the RSA keys with 1024-piece length.

III. Problem Defination

Symmetric key schemes are not suitable for mobile sensor nodes and thus past approaches have focused just on static WSNs. A couple approaches have been proposed based on PKC to support dynamic WSNs. Thus, in this section, we survey previous PKC-based key administration schemes for dynamic WSNs and break down their security weaknesses or disadvantages. Huang et al. [6] and Agrawal et al. [7] proposed a two-layered key management scheme and a dynamic key update protocol in dynamic WSNs based on the Di e-Hellman (DH), respectively. However, both schemes [6], [7] are not suited for sensors with constrained resources and can't perform expensive computations with huge 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 [5], [8] have been proposed based on ECC. However, since every node must trade/exchange the certificate to establish the pair-wise key and check every others certificate before use, the correspondence and calculation overhead increase significantly. Also, the Base Station users from the overhead of certificate administration. In addition, existing schemes [5], [8] are not secure. Alagheband et al. [5] proposed a key management scheme by using ECC-based sign-encryption, in any case, this plan is unreliable against message imitation attacks. Huang et al. proposed an ECC-based key establishment scheme for self-arranging WSNs.

Sensor devices are defenseless against malicious attacks, for example, impersonation, block attempt, physical destruction, because of their unattended agent situations or operative environment and slips of network in wireless communication.

Security is a standout amongst the most vital issues in many of the critical dynamic WSN applications.

Symmetric key encryption experiences high communication overhead and requires vast memory space to store shared pair-wise keys. It is additionally not versatile and not flexible against compromises, and not able to support node portability or mobility. Along these lines symmetric key encryption is not appropriate for dynamic WSNs.

Symmetric key based approaches suffer from the certificate management overhead of the entire sensor nodes and so are not a practical application for large scale WSNs.

IV. Proposed System

A certificate-oriented effective key Management (CO-EKM) approach for dynamic WSNs. In certificate-oriented public key cryptography (CO-PKC), the clients full private key is a mix of an partial private key produced by a Key Generation Center (KGC) and the clients own secret value.

DSA keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length to have more control over the key structure. We are not only passing the key pair but also self-sign certificate to enhance the security. Finding the attacker node (if certificate expire) and removing the node from communication as resolution. Certificate gives the better security w.r.t finding as well as removing the node if there is any attack.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

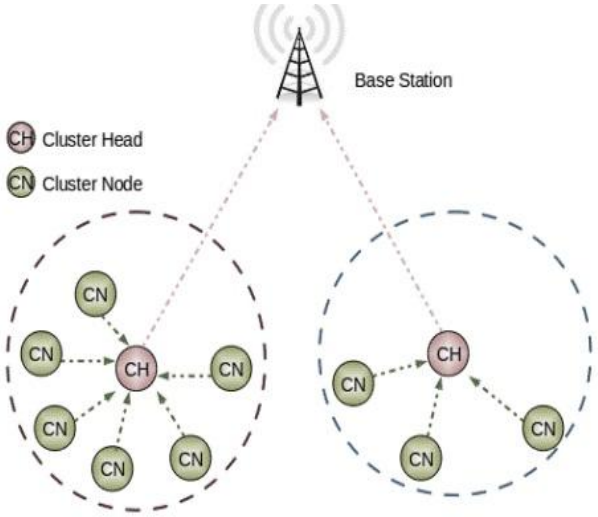

Fig. 1 : Proposed Scheme Structure

V. OVERVIEW OF THE CO-EKM AND SECURITY MODEL SCHEME KEY MANAGEMENT

Before WSN will trade data immovably, encryption keys ought to be set up among detecting component nodes. Key distribution alludes to the distribution of different keys among the detecting component nodes, which is regular in an exceedingly non-minor security subject. Key administration could be a more extensive terms for key distribution, which conjointly incorporates the procedures of key setup, the underlying distribution of keys, and key renouncement the expulsion of a traded off key.

A. Network Model

We examine a heterogeneous dynamic wireless device network. The network comprises of assortment of stationary or cell phone nodes and a bachelor's degree that deals with the network and gathers learning from the sensors. Device nodes will be of 2 sorts: (i) nodes with high process capacities, alluded to as H-sensors, and (ii) nodes with low process abilities, said as L-sensors. We tend to accept to possess N nodes inside the network with assortment N1 of H-sensors and assortment N2 of L-sensors, wherever N = N1 + N2, and N1 N2. Nodes could be a piece of and leave the network, and therefore the network size could dynamically change. The H-sensors go about as cluster heads though L-sensors go about as cluster individuals. They are associated with the bachelor's degree specifically or by a multi-jump way through other H-sensors. H-sensors and L-sensors will be stationary or portable. Once the network arrangement, each H-sensor frames a cluster by finding the neighboring L-sensors through guide message trades. The L-sensors will be a piece of a cluster, move to various clusters and conjointly re-join the past clusters. To keep up the refreshed rundown of neighbors and property, the nodes in an exceedingly cluster sporadically trade light-weight reference point messages.

The H-sensors report any changes in their clusters to the bachelor's degree, for example, once a L-sensor leaves or joins the cluster. The bachelor's degree makes a posting of bona fide nodes; Associate in Nursing revives the staying of the nodes once an inconsistency center point or center point dissatisfaction is recognized. The bachelor's degree allocates every center point a stand-out picture. A L-sensor nil is unambiguously known by center point ID Li while a H-sensor nHj is doled out a center point ID Hj. A Key Generation Center (KGC), encouraged at the bachelor's degree, makes open structure parameters used for key organization by the BS and issues presentation less open/private key sets for every center point inside the network. In our key organization structure, a remarkable individual key, shared only between the center and moreover the bachelor's degree is assigned to every center point. The underwriting less open/private key of a center point is used to find join wise keys between any 2 nodes. A cluster secret's shared among the nodes in an incredibly cluster.

B. Adversary Model and Security Requirements

We expect that the enemy can mount a physical attack on a sensor node after the node is sent and recover mystery data and information put away in the node. The foe can likewise populate the network with the clones of the caught node. Indeed, even without catching a node, an enemy can direct a pantomime attack by infusing an ill-conceived node, which endeavors to mimic a real node. Enemies can direct passive attacks, for example, listening in, replay attack, and so forth to trade off information confidentiality and integrity. Particular to our proposed key administration plot, the enemy can play out a known-key attack to learn pairwise ace keys on the off chance that it by one means or another takes in the here and now keys, e.g., pairwise encryption keys.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 4
April 2017

VI. IMPLEMENTATION

A. *Certificate oriented Public/Private Key:*

Before a node is deployed, the KGC (Key Generation Center) at the BS (Base Station) generates a unique certificate oriented private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pair wise key.

B. *Individual Node Keys:*

Each node shares a unique individual key with BS. For example, a L-sensor can use the individual key to encrypt an alert message sent to the BS, or if it fails to communicate with the H-sensor. An H-sensor can use its individual key to encrypt the message corresponding to changes in the cluster. The BS can also use this key to encrypt any sensitive data, such as compromised node information or commands. Before a node is deployed, the BS assigns the node the individual key.

C. *Cluster Key*

All nodes in a cluster share a key, named as cluster key. The cluster key is mainly used for securing broadcast messages in a cluster, e.g., sensitive commands or the change of member status in a cluster. Only the cluster head can update the cluster key.

D. *Certificate Check*

Certificate assign to individual node is having the details of energy level and other parameters like different Keys.

Every Cluster Head(CH) is responsible to check Energy level by looking into certificate of a node before node do any communication. For every communication CH always check the energy level of Node who is trying to communicate. If the energy level of node goes down, then CH will take that node out of the communication/network. It will also help to find the affected node and/or attacker node.

VII. SIMULATION RESULTS

Network simulator is an object-oriented discrete event simulator. It is also a package of tools that simulates behavior of networks. It is primarily UNIX based. It creates network topologies. It is written in C++ (TCL scripting with object oriented extensions). NS is primarily useful for simulating local and wide area networks. It can be used to simulate a variety of IP networks. It implements network CO-EKM protocol. NS also implements multicasting. The objective of the paper to reduce a data loss between the node, to give more security using the Certificate authentication, and secure transmission of data between the node.

Data loss occur during the transmission data between the nodes. For secure transmission of data between the nodes CO-EKM protocol is used. It is observed that data loss increases as the number of nodes is attacked from outside.

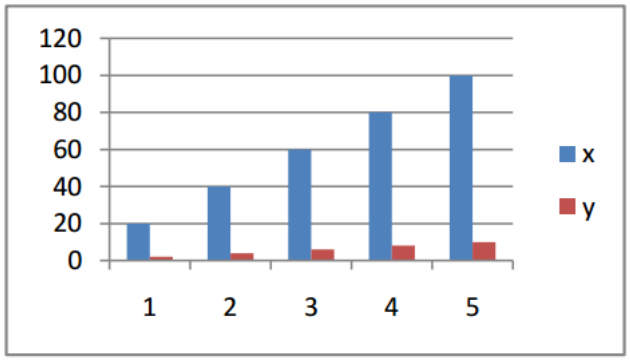

Fig. 2: To show data loss between the nodes in give time interval.

VIII. CONCLUSION

In this project, I propose the certificate oriented effective key management protocol (CO-EKM) for more secure and authentic communication in dynamic WSNs. CO-EKM maintained by Cluster-head(CH) and all the clusters are connected to Base-station. Efficient communication by updating key as and when cluster-node(CN) leaves or join the cluster. This scheme is effective against node compromise, impersonation attacks also protects the security principles such as confidentiality and integrity. The result demonstrates the efficiency of CO-EKM over CL-EKM in WSNs. As future work I plan to formulate the CO-EKMs certificate parameters based on node movement. This model will be utilized to calculate the threshold value of node energy level based on energy consumption and security level.

References

[1] Seung-Hyun Seo and Salmin Sultana, E ective Key Management in Dynamic Wireless Sensor Networks in Proc. IEEE Transaction, Feb 2015.

[2] H. Chan, A. Perrig, and D. Song, Random key predistribution schemes for sensor net-works, in Proc. IEEE Symp. SP, May 2003, pp. 197213.

[3] 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. 6277,Jan./Mar. 2006.

[4] 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. 228258, 2005.

[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] 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.

[7] 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. 194207.