ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Certificate Less Key Management for Enhanced Security in Dynamic Wireless Sensor Networks

Wisam Mohammed Abed
Msc(Is),
Department Computer Science (PG),
Nizam College-Osmania Universtiy.

T. RamdasNaik
Assistant Professor,
Department Computer Science (PG),
Nizam College-Osmania Universtiy.

Abstract:

Wireless sensor network (WSN) is an emerging class of systems made possible by cheap hardware, advanced programming tools, complex algorithms, long lasting power sources and energy efficient radio interfaces.Wireless sensor network is a new paradigm in designing fault tolerant mission critical systems, to enable varied applications like threat detection, environmental monitoring, traditional sensing and actuation and much more. Key management has remained a difficult issue in wireless device networks (WSNs) as a result of the constraints of device node resources. Various key management schemes that trade off security and operational necessities are proposed in recent years.

Wireless device Networks (WSNs) comprises tiny sensor nodes with strained energy, memory and computation capabilities. Sensors can also be embedded into wearable devices to track vital signs of patients in healthcare domain. Mobility of sensor devices as per the demands of the application makes WSNs dynamic. Addressing key security requirements such as node authentication, data integrity and confidentiality is crucial for the success of critical WSN applications. In this paper, we implement a certificate less-effective key management (CLEKM)protocol for secure communication in dynamic WSNs characterized by node mobility.

The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links.

Keywords:

WSNs, Dynamic WSNs, Key management, Security, Cryptography.

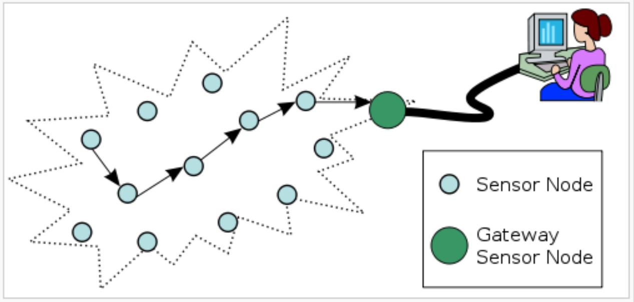
Introduction:

Wireless sensor networks (WSN), sometimes called wireless sensor and actuator networks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity.

The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created.

The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.



Typical multi-hop wireless sensor network architecture

The main characteristics of a WSN include:

- Power consumption constraints for nodes using batteries or energy harvesting
- Ability to cope with node failures (resilience)
- Some mobility of nodes (for highly mobile nodes see MWSNs)
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use
- Cross-layer design

Key management is a core mechanism to ensure security in network services and applications of WSNs. Key management can be defined as a set of processes and mechanisms that support key establishment and the maintenance of on going keying relationships between valid parties according to a security policy. Since sensor nodes in WSNs have constraints in their computational power and memory capability, security solutions designed for wired and adhoc networks are not suitable for WSNs. Hence, techniques for reliable distribution and management of these keys are of vital importance for these curity in WSNs.

Due to their importance, the key management systems for WSNs have received increasing attention in scientific literature, and numerous key management schemes have been proposed for WSNs . Depending on the ability to update the cryptographic keys of sensor nodes during their run time (rekeying), these schemes can be classified into two different categories: static and dynamic. In static key management, the principle of key pre-distribution is adopted, and keys are fixed for the whole life time of the network.

However, as a cryptographic key is used for a long time, its probability of being attacked increases significantly. Instead, in dynamic key management, the cryptographic keys are refreshed throughout the lifetime of the network. Dynamic key management is regarded as a promising key management in sensor networks. In this paper our focus is more on the security issues of dynamic WSN and our study throws light on latest developments in dynamic key management in dynamic WSN.

Our contributions in this paper include investigating the present state-of-the- art of key management in WSN and provide insights into possible directions for future work.

This paper reveals that dynamic key management in dynamic WSN is still the potential research area.

Types of Keys

• Certificate less Public/Private Key: Before a node is deployed, the KGC at the BS generates a unique certificate less private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pair wise key.

• Individual Node Key: Each node shares a unique individual key with BS. For example, aL-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.

• Pairwise Key: Each node shares a different pairwise key with each of its neighboring nodes for secure communications and authentication of these nodes. For example, in order to join a cluster, aL-sensor should share a pairwise key with the H-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by using the pairwise key. In an aggregation supportive WSN, the L-sensor can use its pairwise key to securely transmit the sensed data to the H-sensor. Each node can dynamically establish the pairwise key between itself and another node using their respective certificateless public/private key pairs.

• 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 when aL-sensor leaves or joins the cluster.

RELATED WORK:

Symmetric key schemes are not viable for mobile sensor nodes and thus past approaches have focused only on static WSNs. A few approaches have been proposed based on PKC to support dynamic WSNs. Thus, in this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages. Chuang et al.andAgrawal et al. [8] proposed a two-layered key management scheme and a dynamic key update protocol in dynamic WSNs based on the Diffie-Hellman (DH), respectively. However, both schemes are not suited for sensors with limited resources and are unable to perform expensive computations with large 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 have been proposed based on ECC. However, since each node must exchange the certificate to establish the pairwise key and verify each other’s certificate before use, the communication and computation overhead increase dramatically.

EXISTING SYSTEM:

- Existing System Techniques use: symmetric key encryption and asymmetric key based approaches have been proposed for dynamic WSNs.
- Asymmetric key based approaches found the security weaknesses of existing ECC-based schemes that these approaches are vulnerable to message forgery, key compromise and known-key attacks. Also, we analyzed the critical security flaws of that the static private key is exposed to the other when both nodes establish the session key. Moreover, these ECC-based schemes with certificates when directly applied to dynamic WSNs, suffer from the certificate management overhead of all the sensor nodes and so are not a practical application for large scale WSNs. The pairing operation based ID-PKC schemes are inefficient due to the computational overhead for pairing operations.

DISADVANTAGES OF EXISTING SYSTEM:

- 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

- Security is one of the most important issues in many critical dynamic WSN applications.
- Symmetric key encryption suffers from high communication overhead and requires large memory space to store shared pairwise keys. 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.
- Asymmetric 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.

PROPOSED SYSTEM:

❖ In this paper, we present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs. In certificateless 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 own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key. We also take the benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bit length.

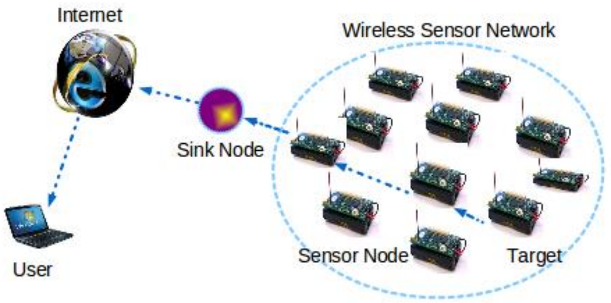
❖ In order to dynamically provide both node authentication and establish a pairwise key between nodes, we build CL-EKM by utilizing a pairing-free certificateless hybrid signcryption scheme (CL-HSC)

ADVANTAGES OF PROPOSED SYSTEM:

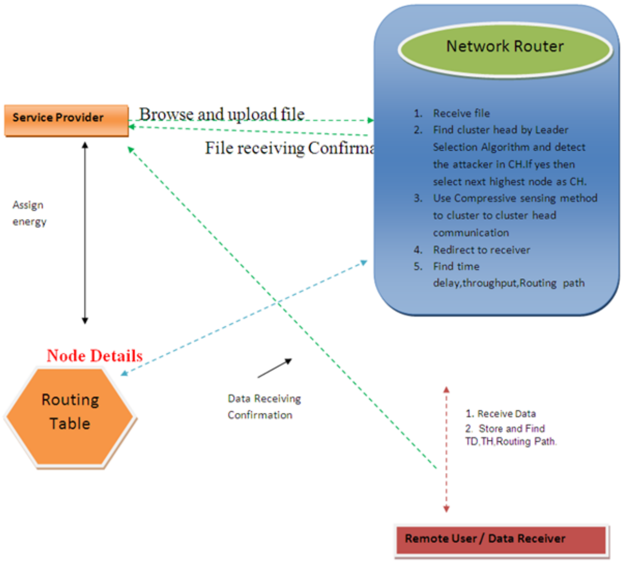
✓ To support node mobility, our CL-EKM also supports lightweight processes for cluster key updates executed when a node moves, and key revocation is executed when a node is detected as malicious or leaves the cluster permanently.

✓ 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. The security analysis of our scheme shows its effectiveness.

SYSTEM MODEL:



SYSTEM ARCHITECTURE:


Network Router
1. Receive file
2. Find cluster head by Leader Selection Algorithm and detect the attacker in CH.If yes then select next highest node as CH.
3. Use Compressive sensing method to cluster to cluster head communication
4. Redirect to receiver
5. Find time delay,throughput,Routing path
Service Provider
Browse and upload file
File receiving Confirma
Assign energy
Node Details
Routing Table
Data Receiving Confirmation
1. Receive Data
2. Store and Find TD,TH,Routing Path.
Remote User / Data Receiver

IMPLEMENTATION:

- Service provider:

In this module, the service provider will browse the data file and then send to the particular receivers. Service provider will send their data file to router and router will connect to clusters, in a cluster highest energy sensor node will be activated and send to particular receiver (A, B, C…). And if any attacker will change the energy of the particular sensor node, then service provider will reassign the energy for sensor node.

- Router

The Router manages a multiple clusters (cluster1, cluster2, cluster3, and cluster4) to provide data storage service. In cluster n-number of nodes (n1, n2, n3, n4…) are present, and in a cluster the sensor node which have more energy considered as a cluster head and it will communicate first. In a router service provider can view the node details, view routing path, view time delay and view attackers. Router will accept the file from the service provider, the cluster head will select first and it size will reduced according to the file size, then next time when we send the file, the other node will be cluster head. Similarly, the cluster head will select different node based on highest energy. The time delay will be calculated based on the routing delay. Attacker will be found if malicious data is added to corresponding node.

- Cluster

In cluster n-number nodes are present and the clusters are communicates with every clusters (cluster1, cluster2, cluster3 and cluster4).In a cluster the sensor node which have more energy considered as a cluster head. The service provider will assign the energy for each & every node. The service provider will upload the data file to the router; in a router clusters are activated and the cluster-based networks, to select the highest energy sensor nodes, and send to particular receivers.

- Receiver (End User)

In this module, the receiver can receive the data file from the service provider via router. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

- Attacker

Attacker is one who is injecting the fake energy to the corresponding sensor nodes. The attacker decries the energy to the particular sensor node. After attacking the nodes, energy will be changed in a router.

Conclusion:

In this paper, we propose the Certificate less Active Key Management Protocol (CL-AKM) to support effective key revocation for secure communication in dynamic WSNs. Key updated after a node movement of node leaves or node connections a cluster and key revocation for compromised nodes are supported by our proposed scheme and ensures go forward and backward key confidentiality. Our proposed scheme of security research is effective in a number of attacks and strong compared to compromise node. From the simulation results, our proposed scheme has better performance in terms of energy, throughput and delay. The investigational results establish the good organization of CL-AKM to support effective key revocation is in resource controlled WSNs.

REFERENCE:

[1] Seung-Hyun Seo, Member, IEEE, Jongho Won, Student Member, IEEE, Salmin Sultana, Member, IEEE, and Elisa Bertino, Fellow, IEEE, "Effective Key Management in Dynamic Wireless Sensor Networks", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 2, FEBRUARY 2015.

[2] M.Rajasekhar & N.Venkateswara Rao, An Analytical study on Key Pre-distribution in Wireless Sensor Networks, IJMETMR, Volume No: 1(2014), Issue No: 10 (October),

http://www.ijmetmr.com/oloctober2014/MRajasekhar-NVenkateswaraRao-47.pdf

[3] Carman D. W., Krus P. S, and Matt B. J, “Constraints and approaches for distributed sensor network security”. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood,MD, 2000.

[4] Hsun Chuang I., Wei-Tsung Su, Chun-Yi Wu, Jang-Pong Hsu,Yau-Hwang Kuo.,”Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks”.,Dept. of Comput. Sci. & Inf. Eng., National Cheng Kung Univ., Tainan.

[5] Huang, Q.; Cukier, J.; Kobayashi, H.; Liu, B.; Zhang, J.,” Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks” TR2003-102 February 2004.

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

[7] Lazos L., and Poovendran R.,. “Serloc: Robust localization for wireless sensor networks”. ACM Trans. Sen. Netw., 1(1):73–100,2005.

[8] Liu, D. and Ning P. 2003. Establishing pairwise keys in distributed sensor networks. In CCS '03: Proceedings of the 10th ACM conference on Computer and communications security. ACM, New York, NY, USA, 52−61.

[9] Liu D., and Ning P., “Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks”. In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 263–276, 2004.

[10] ParadisL.and Han Q., “A survey of fault management in wireless sensor networks,” J. Netw. Syst. Manage., vol. 15, no. 2, pp. 171–190, 2007.