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

Certificate less Public/Private Key Management in Wireless Sensor Networks

S.Bhargavi
M.Tech Student,
Department of CSE,
Vardhaman Engineering College.

Dr .H.Venkateswara Reddy
Professor,
Department of CSE,
Vardhaman Engineering College.

Abstract:
Securing data and communications requires suitable encryption key protocols. In this paper, we propose a certificate less-effective key management (CL-EKM) 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. A security analysis of our scheme shows that our protocol is effective in defending against various attacks.

Index Terms:
Dynamic Wireless Sensor Networks; dynamic key management; cryptography.

INTRODUCTION:
A wireless sensor network (WSN) consists of a large number of sensor nodes, which are powered by batteries, equipped with sensing, data processing and short-range radio communication components. The applications of WSNs range from the most popular ones, like environment monitoring and home automation, to more demanding ones in military or security areas, like battle field surveillance, targeting and target tracking systems. They are also used along with wearable devices that are being used in the healthcare industry to track vital signs of patients. The sensor devices are connected a central Base Station (BS) to which they send sensed data periodically. Many sensors keep sending data periodically to one base station making it a many to one communication scenario. Sensor can directly communicate with BS when no intermediary nodes are on the way to reach BS. If there are intermediary nodes, the data transmission takes place through the intermediary nodes. Usually more number of sensors is deployed for accuracy of the sensed data as the manufacturing cost of sensors is less and they are small in size.

WSNs are of two types such as static and dynamic. Static WSN is the network without node mobility while dynamic WSN is characterized by adding nodes, removing nodes besides support for node mobility. These networks can be deployed in applications such as studying wildlife habitat, monitoring hostile environments, battlefield surveillance, traffic monitoring, cattle health monitoring, vehicle status monitoring, study of traffic flow dynamics, monitoring vital signs of patients pertaining to different disease profiles, monitoring households on critical parameters and monitoring and controlling usage of electronic appliances in smart homes and so on. The list of applications provided here is by no means exhaustive as the usage of WSN is ubiquitous in different walks of life. The common thread among all these applications is the fact that the applications face limitations imposed by WSNs. The limitations stem from the short life time, limited computation capabilities, large number of nodes deployed, lack of infrastructure, besides the possible mobility nature of sensory devices causing frequent topology changes. To address these issues security, efficient resource management and scalability are given paramount importance. 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 ongoing 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 crudity 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:

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

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 along 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.

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. and Agrawal et al. 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. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes are not secure. Alagheband et al. proposed a key management scheme by using ECC-based signcryption, but this scheme is insecure against message forgery attacks. Huang et al. proposed a ECC-based key establishment scheme for self-organizing WSNs. Although many quality survey papers have been presented in the field of key management of WSNs, the scope of the survey presented in this paper still differs from the existing surveys in many aspects.

For the last decade, researchers have started to focus their interest on key management. Numerous review papers including are available, where the authors have examined and surveyed key pre-distribution schemes for key management. Further, classified key management schemes based on attack models, discussed application dependent key management schemes in WSNs, categorized key management schemes into public key schemes, key pre-distribution schemes, dynamic key management and hierarchical key management, organized key management schemes based on different key encryption mechanisms and focused on key management in cluster-based sensor network architecture.

However, to the best of our knowledge, no review paper is available where dynamic key management schemes are classified and discussed thoroughly. Considering the importance of dynamic key management in WSNs, a comprehensive survey becomes necessary at this stage. But, it should be doable for Associate in Nursing oppose to recowl initial link keys. Associate in Nursing oppose will then recover strengthened link keys from the recorded multipath reinforcement messages once the link keys are compromised. Symmetric key schemes don't seem to be viable for mobile detector nodes and so past approaches have targeted solely on static WSNs. A couple of approaches are planned supported PKC to support dynamic WSNs. Thus, during this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages.

Chuang et al. and Agawam et al. planned a two-layered key management theme and a dynamic key update protocol in dynamic WSNs supported the Daffier Hellman (DH), severally. However, both schemes don't seem to be fitted to sensors with restricted resources and area unit unable to perform valuable computations with massive key sizes (e.g. a minimum of 1024 bit). Since computer code is computationally additional economical and features a short key length (e.g. 160 bit), many approaches with certificate are planned supported computer code. However, since every node should exchange the certificate to ascertain the pair wise key and verify every other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes don't seem to be secure.

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

EXISTING SYSTEM:

In existing, 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 pair-wise key and verify each other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes are not secure.

Disadvantages:

•Unable to access with large size of keys

•Increase the overhead

•Cannot provide more secure

•Resolve the key escrow problem

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.

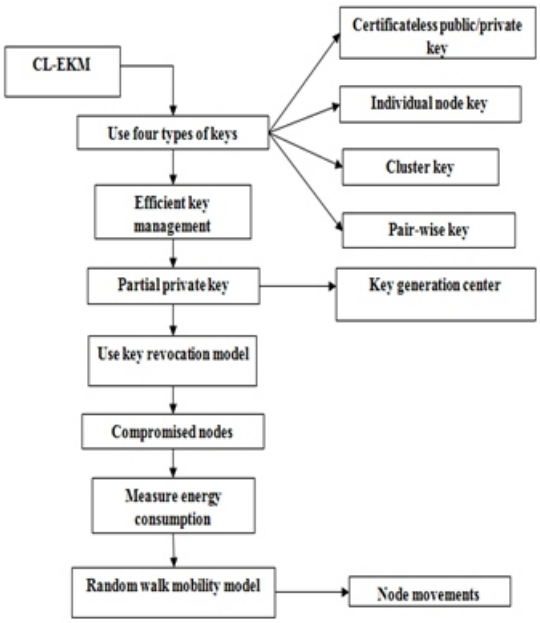
Advantages:

•Provide more security

•Decrease the overhead

•Protects the data confidentiality and integrity

FLOW DIAGRAM:



THE DETAILS OF CL-EKM:

In this paper, we propose a Certificate less Key Management scheme (CL-EKM) that supports the establishment of four types of keys, namely: a certificate less public/private key pair, an individual key, a pair wise key, and a cluster key. This scheme also utilizes the main algorithms of the CL-HSC scheme in deriving certificate less public/private keys and pair wise keys.

ATypes of Keys :

• Certificate less Public/Private Key: Before a node is deployed, the KGC at the BS generates a singular certificate less private/public key combine and installs the keys in the node. This key combine is employed to get a reciprocally authenticated pair wise key.

• Individual Node Key: every node shares a singular individual key with BS. As an example, an L-sensor will use the individual key to write Associate in Nursing alert message sent to the BS, or if it fails to speak with the H-sensor. An Hsensor will use its individual key to write the message akin to changes within the cluster. The BS also can use this key to write any sensitive information, such a compromised node info or commands. Before a node is deployed, the BS assigns the node the individual key.

• Pair wise Key: every node shares a unique pair wise key with every of its neighboring nodes for secure communications and of those nodes.

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

As an example, in order to hitch a cluster, a L-sensor ought to share a pair wise key with the H-sensor. Then, the H- sensor will firmly encrypt and distribute its cluster key to the L-sensor by victimization the pair wise key. In Associate in Nursing aggregation supportive WSN, the L- sensor will use its pair wise key to firmly transmit the detected information to the Hsensor. Each node can dynamically establish the pair wise key between itself and another node victimization their various certificate less public/private key pairs.

• **Cluster Key:** All nodes in an exceedingly cluster share a key, named as cluster key. The cluster key's chiefly used for securing broadcast messages in an exceedingly cluster, e.g., sensitive commands or the amendment of member standing in an exceedingly cluster. Only the cluster head will update the cluster key once a L-sensor leaves or joins the cluster.

IMPLEMENTATION:

Cluster Formation:

Once the nodes are deployed, each cluster head through message exchanges to sensor node. Cluster head to control a cluster with the authenticated sensor node and they share a common cluster key. The cluster head also establishes a pair wise key with each member of the cluster. To simplify the discussion, we focus on the operations within one cluster and consider ath the cluster. We also assume that the cluster head is *nCHb* with nCa $1 \leq a \leq n$ as cluster members *nC*. Establishes a cluster key for *opb* secure communication in the cluster.

Node Movement:

Once a node moves between clusters, the cluster head requirement accurately achieved cluster keys to confirm the forward/backward confidentiality. Therefore, the cluster head updates the cluster key and informs the BS of the changed node position. Over this report, the BS can directly update the node position in the M. We denote a moving node as n.

1) Forward and Backward Confidentiality:

CL-AKM provides the key update and revocation processes to confirm forward confidentiality as soon as a node leaves or compromised node is identified. Forward Confidentiality is an old key to continue decrypting the new messages and Backward Secrecy is a new key from backward encrypting old messages.

Forward and Backward Confidentiality are used to secure against node capture attack.

2) Node Leave: A node may leave a cluster due to node failure, location change or irregular communication failure. Here be located both proactive and reactive ways for the cluster head to detect when a node leaves the cluster. The proactive case happens as soon as the node nCm actively chooses to leave the cluster and informs the cluster head $nCHb$ or the cluster head chooses to revoke the node. Then in this case $nCHb$ can confirm that the node has left, it transmits a report $EKCH\ b\ 0$ (Node Leave,) to update the BS and nCm has left the cluster. When getting the report, the BS is updates the status of nCm in M and sends a credit to nC . The reactive case happens when the cluster head $nCHb$ fails to communicate with n . It may possibly occur a node expires out of battery power, fails to connect $nCHb$ due to interference or obstacles, is captured by the attacker or is moved unintentionally.

3) Node Join: Once the moving node nCm leaves a cluster, it may join other clusters or return to the previous cluster after some period. We assume that nLm wants to join the $a\ th$ cluster or return to the $b\ th$ cluster.

Key Update :

Compromised keys and frequent encryption key updates are commonly required in directive to protect against cryptanalysis and mitigate damage. Now in this section we deliver the pair wise key update and cluster key update processes.

1) Pair wise Key Update:

Only sensor nodes can update their pair wise key. Toward update a pair wise encryption key, two nodes are to shared the pair wise key perform for in a Pair wise Encryption Key Establishment process.

2) Cluster Key Update:

Only cluster head can update their cluster key. If a sensor node attempts to change the cluster key, the node is considered a malicious node.

E. Key Revocation :

We take responsibility that the BS can identify compromised sensors node and cluster head. The key revocation is nothing but the renewal of keys. The key revocation is calculated by the Certificate revocation list.

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

The Certificate Revocation list split in to two categories given by old CA and New CA. The BS can require an interference detection system or malicious nodes or adversary's device to detect. While we do not cover how the BS is can discover to a compromised sensor node or cluster head. In this paper, the BS can exploit the updated node position data of each cluster to explore an irregular node. Now our protocol, cluster head information is to change of its node position to the BS, when a node joins or leaves a cluster. Thus, the BS dismiss prompt achieve the node position in the member list μ. Designed for example, the BS can consider a node compromised if the node withdraws aimed at an assured period of time. Now in this case, the BS requirement explore the apprehensive node and it can be using the node error detection device introduced [6] and [10]. Once the BS discovers a compromised sensor node or a compromised cluster head is to be used in a key revocation process. A compromised node is denoted bynCc in the $b\ th$ cluster for a compromise sensor node situation and a compromised head by $nCHb$ for a compromise cluster head situation.

Addition of a New Node :

In the past addition of a new node into present networks, adding similar data transformation to another cluster head to senor node. The BS must ensure that the sensor node is not compromised. The new node nCn+1creates a full private/public key over the sensor node process stage. Before, the public structure parameters, a full private/public key and individual key $KnCn$+10 are stored into nCn+1

CONCLUSION:

In this paper, we propose the first certificate less effective key management protocol (CL-EKM) for secure communication in dynamic WSNs. CL-EKM supports efficient communication for key updates and management when a node leaves or joins a cluster and hence ensures forward and backward key secrecy. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. The experimental results demonstrate the efficiency of CL-EKM in resource constrained WSNs. As future work, we plan to formulate a mathematical model for energy consumption, based on CL-EKM with various parameters related to node movements.

Future Enhancement:

Even though here presented a method of certificate less effective key management, here the BS also suffer from mere problem poor encryption. Since it has four pairs of keys it is not a serious issue. Still the user or the beneficiary authority has to go for more securely encrypted key methods. This problem can be revised and solved and hence to improve this idea of secure data handling. Encryption improvement is the only method to get the most secured way of communication.

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 manage-ment 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 pre-distribution 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, 4145– 4150.

[8] 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.

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

[9] X.-J. Lin and L. Sun, "Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks," in Proc. IACR Cryptol. ePrint Archive, 2013, pp. 698–698.

[10]D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 2012, Sep. 2012, Art. ID 406254.

[11]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.

[12]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.

[13]M. R. Alagheband and M. R. Aref, "Dynamic and secure key manage-ment model for hierarchical heterogeneous sensor networks," IET Inf. Secur., vol. 6, no. 4, pp. 271–280, Dec. 2012.

[14]M. Eltoweissy, M. Moharrum and R. Mukkamala, "Dynamic Key Management in Sensor Networks," Communications Magazine, IEEE, vol 44, pp 122- 130, April 2006.

[15]Arvinderpal S. Wander, Nils Gura, Hans Eberle,Vipul Gupta, and Sheueling Chang Shantz.(2005) EnergyAnalysis of Public Key Cryptography for Wireless Sensor Networks. In Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications, pages 324– 328.