International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-4, April 2013

Cluster Based Key Revocation and Key Distribution in Wireless Sensor Network a Survey

Nimisha C. Chaudhari

Abstract — Key management has become a challenging issue in the design and deployment of secure wireless sensor networks. key management includes two aspects: key distribution and key revocation. Key distribution refers to the task of distributing secret keys between communicating parties to provide secrecy and authentication. Key revocation refers to the task of securely removing compromised keys. By revoking all of the keys of a compromised sensor node, the node can be removed from the network. Compared to key distribution, Wireless sensor networks consist of sensor nodes with limited computational and communication capabilities. In this paper, the whole network of sensor nodes is divided into clusters based on their physical locations. In addition, efficient ways of key distribution among the nodes within the cluster and among controllers of each cluster are discussed. Also, inter and intra cluster communications are presented in detail. The security of the entire network through efficient key management by taking into consideration the network's power capabilities is discussed. In this paper, we have discussed several existing methods for key revocation.

Index Terms— Key distribution, Key revocation, heterogeneous atmosphere, wireless sensor node, Security Requirements, Sensor Network, clusters, nodes

I. INTRODUCTION

Wireless Sensor Networks have become popular in recent past. The use of sensor networks is not limited to military applications, but also in civilian applications such as health monitoring, industry, wildlife monitoring and so on. A lot of research has been carried out in this field to improve hardware specifications, protocols for communications and information security [1]. Previous research on sensor network security mainly considers homogeneous sensor networks. Research has shown that homogeneous sensor networks have poor performance and scalability compared to heterogeneous sensor networks [2-3]. Many security schemes designed for homogeneous sensor networks have high communication overhead, computation overhead and large storage requirement. Sensor network applications mainly designed and developed for military [4] but now it has civilian applications too. Applications vary in scope from military applications to vehicular applications to medicine applications [5-6].

A sensor network consists of spatially distributed nodes with limited computational and communication capabilities. These are used in varied applications such as monitoring environmental conditions, military and other industrial purposes.

The nodes which are distributed spatially have to communicate with each other in a secured manner since the data associated with these nodes may be confidential. Efficient cryptography techniques are to be used for communication among the nodes. Use of public key cryptography is omitted here keeping in mind the computational limitations of sensor nodes . Also, using a single key for the entire network may be a compromise on the security of the system as a threat on even one node would bring the system down.

Due to the storage limitations of the sensors nodes, all unique keys cannot be stored. Consider a total of m nodes out of which two nodes share a unique key. This will result in a total of $m(m-1)2$ keys in the network with each node storing $m-1$ keys. This is very high owing to the storage constraints of a node if m is large. Also, considering the ad-hoc nature of the sensor networks, some nodes will continue to be added to the network over time. Thus efficient key management has to be performed in order to store keys in nodes such that the network security is not compromised and also the total number of keys stored in the node is reduced.

The key ring approach requires that data be routed over many nodes before it reaches its destination. This indicates that there is an underlying connection between routing and security and that implicit security technique may be used to route data via multiple channels, thus spreading the vulnerability over several nodes and communication channels making an adversary's task harder. There is also the question of node compromise which may be countered by using tamper-resistance hardware in each node. Further, overlay architecture has been used to achieve balance between number of keys per node and routing complexity.

II. SECURITY REQUIREMENTS FOR KEY MANAGEMENT SCHEME

A good key distribution or establishment and management schemes for sensor networks needs to consider few security points.

The scheme must work without prior knowledge of which nodes will come into communication range of each other after deployment.

Deployed nodes must be able to establish secure node-to-node communication.

Additional legitimate nodes deployed at a later time can form secure connections with already deployed nodes. Unauthorized nodes should not be able to take entry into the network or become members of the network.

Sensor nodes have limited resources so computational and storage requirements of the scheme must be low.

Manuscript published on 30 April 2013.
***** Correspondence Author (s)
Ms. Nimisha Chaudhari, LDRP Institute of Technology and Research, Gandhinagar (Gujrat), India

If a node becomes compromised, the key management scheme must be able to securely remove the compromised node from the network.

III. RELATED WORK

A lot of work has been done in sensor networks related to key distribution. However, key revocation has received relatively little attention. The task of securely removing the compromised keys is known as key revocation. This chapter provides brief overview and analysis of the current key revocation schemes for sensor networks.

A. *Eschenauer and Gligor's scheme*

Eschenauer and Gligor [8] proposed the probabilistic key pre-distribution scheme. In most of papers this scheme is referred as basic scheme. In this scheme, three phases are needed to set up the secret keys between sensor nodes. These phases are key predistribution, shared key discovery and path key establishment. In first phase each sensor node randomly assigned k different keys from a big key pool. This is shown in figure 1 where nodes A, B, C, D, E are randomly assigned k keys from the key pool.

Stored keys in each sensor node are called keyring of the node and each key has a corresponding id. Next two phases are done when nodes are deployed. In the shared key dis covery phase nodes find the common key between them and establish a secure connection. In this phase each node discovers its neighbors in communication range with which it shares common keys. shows sample the sample graph after shared key discovery. In this network node pairs A and B, and A and C can set up secure links through their common keys.

It might happen that nodes are in communication range but do not share any keys, these nodes may be connected by one or more hops links through path key establishment phase. nodes B and C are in communication range but do not share a common key. The path key establishment phase assigns a path key to the sensor nodes via node A and then they can set up secure link between them. Most of the pre-distribution schemes are based on this model.

In wireless sensor network base station is known as centralized authority. Base station is used to revoke the compromised nodes. Eschenauer and Gligor presented a key management scheme for wireless sensor network in [8]. It is a centralized key revocation scheme. If a node is compromised, the base station can send a message to all other sensors to revoke the compromised node's key ring. The revocation scheme in [8] can be divided into three phases: signature key distribution, key revocation and link reconfiguration.

In the signature key distribution phase, the base station generates a signature key. The base station unicast a signature key to each node. The signature key is encrypted with a pairwise key shared by the base station with the sensor node. In the key revocation phase, the base station broadcast single key revocation message signed by the signature key. This message contains a list of key identifiers for the key ring to be revoked. Each sensor verifies the signature of the key revocation message locates those identifiers in its key ring and removes the corresponding keys.

Some links may disappear if the keys are removed from the key rings and the affected nodes need to reconfigure those links by restarting the shared-key discovery and the path-key establishment phase.

The key revocation scheme in [8] requires n unicast messages and one broadcast message. In a large scale sensor network, distributing the signature key might be a problem. Pre-distributing the signature key might be possible, however once the signature key is compromised, the adversary could use the signature key to duplicate the revocation messages from the base station.

B. *Clustering*

Grouping of nodes in a network into clusters will be done by the *k*-means++ clustering algorithm [7]. In *k*-means++ clustering algorithm, the number of clusters is fixed *a priori*. We assume that the number of clusters to be chosen is *k* and this choice is based on the network size and geographical positions of each node. Consequently, we will have *k* sub controllers monitoring nodes in their respective clusters.

According to *k*-means++ clustering algorithm, initially *k* means are to be identified, one for each cluster. For this, as explained in *k*-means++ approach, following steps are to be followed,

1. Choose an initial centre *x*, from the set of all node points say μ, at random.
2. Choose next mean from the set and name it *y* with probability $D(y)2\ D(x)2x\epsilon\mu$ proportional to $D(x)2$
3. Repeat step 2 until all the *k* centers are identified.

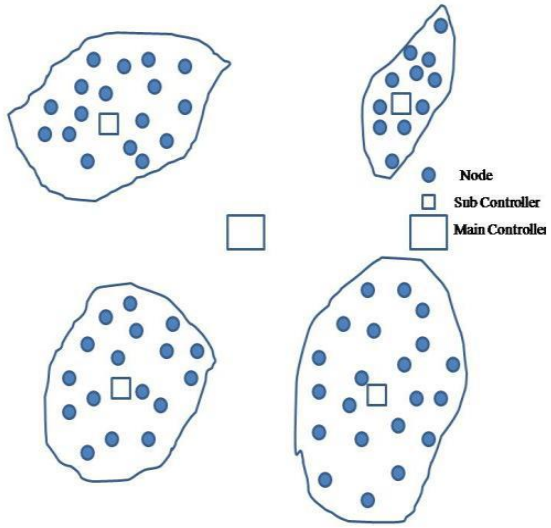

Figure 1. A network divided into various clusters

Once these centers are identified, these would be the means of the clusters and each node distance from all the means is calculated and is associated to the nearest mean, this process is called binding. This process is repeated up to a stage where all the positions of nodes in the network are visited at least once. After this, *k* new means will be calculated. Once the positions of *k* new means are identified, binding is done again. This process is repeated until there is no change in the location of means.

C. *Key Distribution*

As the communication can be both inter and intra cluster, the key distribution should also be considered for two cases, one among nodes and other among sub controllers.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

IV. CONCLUSION

The scheme presented in this paper is an effective protocol for dividing the network into clusters and for distributing keys among them. This method is efficient when the nodes in the network are divided randomly and can be clustered easily rather than the nodes when distributed in a uniform fashion. Simulations were run for the proposed design and the results are presented in graphs. These results show that the performance in terms of number of hops and number of keys stored in a node improves as the number of clusters increases. The developments in sensor networks occurring at a very fast pace, but compared to that security within sensor networks has not gained significant interest. This is partially because of the lack of understanding of the potential of these tiny devices, and partially due to the lack of commercial motivation. In this paper, we have discussed various existing key management schemes for wireless sensor networks.

REFERENCES

[1] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, 2006.

[2] X. Du, Y. Xiao, M. Guizani, H.H. Chen, An Effective Key Management Scheme for Heterogeneous Sensor Networks, Ad Hoc Networks, Elsevier, vol. 5, issue 1, January 2007, pp. 24–34.

[3] P. Traynor, R. Kumar, H. B. Saad, G. Cao, and T. L. Porta, "LIGER: Implementing efficient hybrid security mechanisms for heterogeneous sensor networks," in *Proc. MobiSys'06*, Uppsala, Sweden, 2006.

[4] Chee-Yee Chong and S. P. Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, 2003.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, August 2002.

[6] S. Kroc and V. Delic. Personal wireless sensor network for mobile health care monitoring. In *Telecommunications in Modern Satellite, Cable and Broadcasting Service, 2003. TELSIKS 2003. 6th International Conference on*, volume 2, pages 471–474 vol.2, Oct. 2003.

[7] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communication Magazine, Aug. 2002.

[8] Zhang W, Song H, Zhu S, Cao G. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *MobiHoc '05: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM Press: New York, NY, USA, 2005; 378–389.

[9] Karp B, Kung HT. GPSR: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the6th Annual International Conference on Mobile Computing and Networking*. ACM Press: New York, NY, USA, 2000; 243–254.

[10] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2003, 197–213.

[11] Chan H, Gligor V, Perrig A, Muralidharan G. On the distribution and revocation of cryptographic keys in sensor networks. *IEEETransactions on Dependable and Secure Computing* 2005; **2**(3):233–247.

[12] O. Kachirski and R. Guha, "Effective intrusion detection uses multiple sensors in wireless ad hoc networks," in System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on, p. 8 pp., 2003.

[13] X. Zou, B. Ramamurthy, and S. S. Magliveras, *Secure Group Communications Over Data Networks*, Springer, 2005.

[14] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*. New York, NY, USA: ACM Press, 2003, pp. 231–240.

[15] Parakh and S. Kak, Online data storage using implicit security. Information Sciences, vol. 179, pp. 3323-3331, 2009.

[16] A. Parakh and S. Kak, Internet voting protocol based on improved implicit security. Cryptologia, vol. 34, pp. 258-268, 2010.

[17] A. Parakh and S. Kak, Space efficient secret sharing for implicit data security. Information Sciences, 2010.

[18] S. Kak, On secret hardware, public-key cryptography. Computers and Digital Technique (Proc. IEE - Part E), vol. 133, pp. 94-96, 1986.

[19] D. Arthur and S. Vassilvitskii, *k*-means++: the advantages of careful seeding. *Proceedings of the eighteenth annual ACM-SIAM symposium on Discrete algorithms*. pp. 1027–1035, 2007.

[20] E. H. McKinney, Generalized birthday problem. American Mathematical Monthly 73, 385–387,1966.

[21] M. Klamkin and D. Newman, Extensions of the birthday surprise. Journal of Combinatorial Theory 3, 279–282, 1967.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)