Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Effect of Hash Function on Key Pre-distribution Scheme Using Keyed - Hash Chain for Wireless Sensor Network

Priyanka Manhas[1] (Student), Parminder Kaur[2](Asstt. Prof.)

Department of Computer Science & Engineering.

Chandigarh University (Gharuan, Mohali) India

Abstract- We present an effective and secure mechanism for key distribution in wireless sensor network (WSN). Wireless sensor network finds unique and special applications as compare to the Wi Fi, Wi Max and etc networks because sensors are deployed in a very secret, hostile environment like battlefield, environmental monitoring, and health care industry. Various wireless sensor nodes are interconnected and form a wireless sensor network. Wireless sensor network are infrastructure less and can operating any environment as compare to the traditional network. WSN mainly consist of large number of tiny and simple nodes that are randomly deployed in operating areas unattended. Major issue of WSN is to have a more secure network which is a function of Hash keys. More uses of Hash keys means enhance security but at the cost of power and area. In this paper, we introduce concept of Hash function to use a different key in each session between a pair of sensor, without allocating a large amount of memory space to store the keys. This scheme is based on multipath key reinforcement, this scheme is used to update the number of iteration to achieve a higher level of security. Increase usage of Hash keys means enhance security but at the cost of power and area. Paper also shown effect of number of Hash function of performance of wireless sensor node. This scheme is minimized the overhead introduce in the network.

Keywords- Hash Chain, Homogeneous Wireless Sensor Networks, Key Distribution, Multipath key reinforcement, Wireless Sensors Network (WSN),.

I Introduction

Wireless sensor network (WSN) have recently attracted much attention because of their wide range of application such as military, environmental monitoring, Tele-Health, pervasive and ubiquitous applications, and industry automation. WSN mainly consist of large number of tiny and simple nodes that are randomly deployed in operating areas in unattended [1]. Security in WSN has been receiving much attention in the literature. The symmetric key based key schemes has been presented [5,6,13,14] the design of WSN depends significantly on the application design, objectives, cost, hardware and system constraints. Another major issue of WSN is to have a secured network which is the function of Hash keys. More usage of Hash keys means enhance security in terms of recognizing sensor nodes. In our proposed scheme, we used different encryption keys for different session between the same pair of node to get maximum security. We use one way Hash function to update the key for each session after the communication has been established as storing different keys for different session prior to the deployment is not a good idea because both the sender and receiver to know it, which results in much larger size of key ring with in each node. We can change the symmetric key for each session by the changing the numbers of time the Hash function execute. For reducing communication overhead we use symmetric key approach rather then generating the key instead of the number of iterations and send it to the receiver using the multiple path.

Section 2 summarizes related work. In section 3 describe session management details. Finally, in section 4 gives conclusion and future directions.

II Related Work

The research in security aspects of WSN has been active for a long time since sensor node suffer from serious limitation of battery power processing speed, data aggregation, synchronization network lifetime, limited abilities, repair mechanism and limited energy[1] [6]. There are two types of cryptography techniques that are *public key cryptography and symmetric key cryptography*. Classical solution for key management is public key cryptography, the best examples of public key cryptography is RSA and ECC schemes. Because of resource limitation, public key cryptography is not very practical solution for WSN[9]. Liu and Ning presented time ECC, which provide a package to implement ECC in sensor node using Tiny operating system; however it still takes much more time and resources which is not always affordable. Symmetric key cryptography is active research in WSN all though it offers the simplicity that is much required in WSN. Eschenauer and Gligor proposed key distribution scheme [4], which is known as random key predistribution keys this scheme depends on probabilistic key sharing among the nodes of the random graph and uses comparatively simple protocols. The drawback of this scheme is if a single node is capture, a part of a network may be exposed as their may be keys which are shared between some other nodes. To overcome this limitations three different key predistribution schemes are established[5] these are *Q composite random key distribution scheme, multipath key reinforcement, random pair-wise scheme*.

In Q composite each pair of node needs to have a Q number of commons keys instead of one, this decreases the probability of exposing links when a single node is captured. In multipath key reinforcement links are established using basic random key predistribution scheme and than the common keys are updated using multiple paths using sender and receiver nodes. Drawback of this scheme it adds more overhead but remove the probability of network exposing when a node is captured. In random pair-wise scheme randomly select pair of keys and predistribute for those links only. The above key distribution schemes that are used for security purposes have an assumptions that they do not have previous knowledge about deployment sensor. Proposed scheme is for heterogeneous sensor networks in which key management schemes which uses the concept of generation keys and Hash function in conjunction with basic random key predistribution scheme. The concept of Hash function tried to minimize the storage space used for storing predistribution scheme. Our scheme makes use of Hash chain for authentication of the one time verification.

III Session Key Management

When two nodes M and N, start communication for first time, they must agree on a common generation key and each session, they have to decide the number of iteration the Hash function will go through to get the actual symmetric key. The symmetric key that are generated can be use to secure the session, but we do not want an adversary to have any chance to know. As the key ring of both M and N is generated by randomly picking P keys form key pool, chances are that arre the common keys between M and N will also reside is some other nodes and compromising one of them can back to security threats between M and N. the three commonly use terms in session key management is *key ring assignment, key pool generation, common key discovery, Generation key updation for each session.*

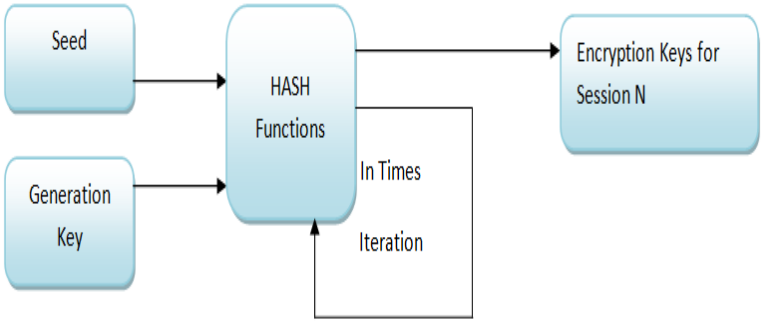

Figure: 1 Session Key Generation

In key pool generation we use large keys pool like the basic random key predistribution scheme[4]. In basic key predistribution scheme all the symmetric communication keys were stored in key pool, we store all the generation keys in stead of symmetric communication keys in our key pool. Firstly we decide the size of key pool for our network, size should be big enough so that not a huge numbers of nodes get the same key; on the other hand it should be small enough so that probability of sharing atleast one generation key between a pair of nodes remain at a satisfactory level. The optimum size of key pool depends fully on size of key ring on each node, the expected probability of key sharing between a pair of nodes and the expected size of the network. In key ring assignment when key pool is generated, we load each node with the selected numbers of generation keys. The set of generations keys stored in each node will be mentioned as key ring of that node.

In common discovery phase the steps are proceed when all nodes are deployed. The nodes start looking for neighboring nodes with which they shares common generation key. This phase performed in following four steps:

- Each node broadcast the list of its generation key Ids along with its own Id, number used ones and message authentication codes.
- Each neighbor node receive message, compares the list of generation key Ids with its own list.
- If neighboring node finds a common generation key with the broadcaster node its sends an acknowledgement message which contain list of common generation key Ids, along with the nodes Ids That is number used ones and message authentication codes.
- Nodes will perform a challenge response operation to verify common generation keys if it gives positive result than direct link between the nodes is considered to be *secured*.

In generation key update for each session it is assumed that common key discovery has been done and each node has sufficient routing information to find out the paths to its neighbors.

IV Conclusion

In this paper we propose an efficient and effective and secure key generation technique for homogeneous WSN. We use multipath key reinforcement to update initial generation key and numbers of times the Hash function is iterate. We use one way Hash function to generate different keys for different sessions. Schemes also shows effect of number of Hash function on performance of wireless sensor node. Future research includes an implementation in our scheme that adds some more computational and communication overhead, the WSN is more secure and resilient to several attacks.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, vol. 38, pp. 393-422, March 2002.

[2] P. Gupta and P. R. Kumar, "The Capacity of Wireless Networks," IEEE Trans. on Information Theory, vol. IT-46, no. 2, pp. 388-404, Mar. 2000.

[3] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks", Proceedings of the IEEE/ACM International Conference on Information Processing in Sensor Networks (IPSN), pp. 245-256, 2008.

[4] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks" , Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41 – 47, 2002.

[5] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks", Proceedings of the IEEE Symposium on Security and Privacy, 2003.

[6] F. Kausar, S. Hussain, L. T. Yang, and A. Masood, "Scalable and Efficient Key Management for Heterogeneous Sensor Networks", Special Issue in Journal of Supercomputing, (Springer, SCI), 22 pages, 2008.

[7] X. Du, Y. Xiao, S. Ci, M. Guizani, and H. Chen, "A Routing-Driven Key Management Scheme for Heterogeneous Sensor Networks", Proceedings of the IEEE International Conference on Communications (ICC), pp. 3407-3412, 2007.

[8] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge", Proceedings of IEEE Conference on Computer and Communications (INFOCOM), 2004.

[9] S. Cheung, B. Dutertre, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust", Technical Report SRI-SDL-04-02, System Design Laboratory, SRI International, April 2004.

[10] G. Gaubatz, J. Kaps, and B. Sunar, "Public Key Cryptography in Sensor Networks", Security in Ad-hoc and Sensor Networks, pp. 2-18, 2005.

[11] Lejla Batina, Nele Mentens, Kazuo Sakiyama, Bart Preneel, and Ingrid Verbauwhede. Low-cost elliptic curve cryptography for wireless sensor networks. In *Third European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks (ESAS)*, 2006.

[12] Erik-Oliver Blaß, Holger Junker, and Martina Zitterbart. Effiziente implementierung von public-key algorithmen f¨ur sensornetze. In *GI Jahrestagung (2)*, pages 140–144, 2005.

[13] Erik-Oliver Blaß and Martina Zitterbart. Towards acceptable public-key encryption in sensor networks. In *IWUC*, 2005.

