

Study of Key Pre-Distribution Schema in WSN Based on Unital Design Theroy

P.Priyanka

M.Tech, Student,

Computer Science Engineering Department,
GITAM School Of Technology,Hyd.

Mrs K.Nikitha

Asst Professor,

Computer Science Engineering Department,
GITAM School Of Technology, Hyd.

Abstract:

Wireless sensor networks are composed of small entities with limited memory, computation and communication capabilities. These entities role is to detect process and transmit information. Therefore, they are considered as embedded systems. Wireless sensor networks are deployed in many hostile environments and face many security issues. Sensor nodes are also resource-constrained. To achieve security in wireless sensor networks, many key management (distribution and share) schemes have been proposed. In this paper we aim to study these key distribution schemes and the construction of shared keys using a wireless sensor network simulator (WSNet).

To attain security in wireless sensor networks, many key management methods have been proposed in the past. In this research paper we aspire to study these key distribution. In this paper we proposed a scheme which is scalable and requires less number of keys for a given number of nodes than the existing well known methods. Our results show that the proposed approach enhances the network scalability while providing high secure connectivity coverage and overall improved performance. Moreover, for an equal network size, our solution reduces significantly the storage overhead compared to those of existing solutions.

Keywords:

Wireless, Keys, Cryptography, Embedded systems, communications.

Introduction:

Distributed sensor networks are deployed in many fields and applications (environment, military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environments, etc...).

Sensors are randomly spread over the terrain under security. To secure these networks from threats [7] (eavesdropping, message injection, message modification, message replay, impersonation DOS, etc...), symmetric cryptography is used. Its more adequate for WSN with low powered sensors. Key distribution is a serious problem in wireless sensor networks conception. Its done before the nodes deployment; nodes construct the network using their secret keys after they are deployed: when they reach their targets. Many key pre-distribution schemes have been proposed In this paper. Symmetric key establishment is then one of the most suitable paradigms for securing exchanges in wireless sensor networks.

Because of the lack of infrastructure in Wireless sensor networks, we have usually no trusted third party which can attribute Pair wise secret keys to neighboring nodes that is why most existing solutions are based on key pre-distribution. Nowadays, wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is then a challenging problem in WSNs.

Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pairwise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution. Over the last decade, a host of research work dealt with symmetric key pre-distribution issue for WSNs and many solutions have been proposed in the literature.

Nevertheless, in most existing solutions, the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or de-grade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks. In this work, our aim is to tackle the scalability issue without degrading the other network performance metrics. For this purpose, we target the design of a scheme which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. The key establishment mechanism employed in a given sensor network should meet many requirements to be efficient. These requirements may include supporting in network processing and facilitating self-organization of data, among others. However, the key establishment technique for a secure application must minimally incorporate authenticity, confidentiality, integrity, scalability, and flexibility.

• **Authenticity:**

The key establishment technique should guarantee that the communication nodes in the network have away for verifying the authenticity of the other nodes involved in a communication, i.e., the receiver node should recognize the assigned ID of the sender node.

• **Confidentiality:**

The key establishment technique should protect the disclosure of data from unauthorized parties. An adversary may try to attack a sensor network by acquiring the secret keys to obtain data. A better key technique controls the compromised nodes to keep data from being further revealed.

• **Integrity:**

Integrity means no data falsification during transmissions. Here in terms of key establishment techniques, the meanings are explained as follows. Only the nodes in the network should have access to the keys and only an assigned base station should privilege to change the keys. This would effectively prevent unauthorized nodes from obtaining knowledge about the keys used and preclude updates from external sources.

• **Scalability:**

Efficiency demands that sensor networks utilize a scalable key establishment technique to allow for the variations in size typical of such a network. Key establishment techniques employed should provide high-security features for small networks, but also maintain these characteristics when applied to larger ones.

• **Flexibility:**

Key establishment techniques should be able to function well in any kind of environments and support dynamic deployment of nodes, i.e., a key establishment technique should be useful in multiple applications and allow for adding nodes at any time. Key establishment process in Wireless sensor networks mainly consists of three phases.

1. Key pre-distribution : Pre-loading keys in sensor nodes prior to deployment. The keys present in a sensor node constitute the key ring of the sensor.

2. Shared key discovery : To find a common shared key between two communicating nodes.

3. Path key establishment : If a common key does not exist, then a path has to be found between the communicating nodes. A path key is then established between the communicating nodes.

Existing System:

Wireless sensor networks (WSNs) are increasingly used in critical applications within several fields including military, medical and industrial sectors. Given the sensitivity of these applications, sophisticated security services are required. Key management is a corner stone for many security services such as confidentiality and authentication which are required to secure communications in WSNs. The establishment of secure links between nodes is then a challenging problem in WSNs. Because of resource limitations, symmetric key establishment is one of the most suitable paradigms for securing exchanges in WSNs. On the other hand, because of the lack of infrastructure in WSNs, we have usually no trusted third party which can attribute pair wise secret keys to neighboring nodes, that is why most existing solutions are based on key pre-distribution.

Disadvantages of Existing System:

A host of research work dealt with symmetric key pre-distribution issue for WSNs and many solutions have been proposed. In the existing system many disadvantages occur: the design of key rings (blocks of keys) is strongly related to the network size, these solutions either suffer from low scalability (number of supported nodes), or degrade other performance metrics including secure connectivity, storage overhead and resiliency in the case of large networks.

Proposed System:

In this proposed system, our aim is to tackle the scalability issue without degrading the other network performance metrics. For this purpose, we target the design of a scheme which ensures a good secure coverage of large scale networks with a low key storage overhead and a good network resiliency. To this end, we make use of the unital design theory for efficient WSN key pre-distribution. The proposed algorithm a random block distribution allowing to pre-load t disjoint blocks in each sensor node.

Advantages of Proposed System:

The advantages of the proposed system as follows:

1. We propose a naive mapping from unital design to key pre-distribution and we show through analytical analysis that it allows to achieve high scalability.
2. We propose an enhanced unital-based key pre-distribution scheme that maintains a good key sharing probability while enhancing the network scalability.
3. We analyze and compare our new approach against main existing schemes, with respect to different criteria: storage overhead, energy consumption, network scalability, secure connectivity coverage, average secure path length and network resiliency.

1. Unital design for key pre-distribution in WSNS:

WSNs are highly resource constrained. In particular, they suffer from reduced storage capacity. Therefore, it is essential to design smart techniques to build blocks of keys that will be embedded on the nodes to secure the network links.

2. A new scalable unital-based key pre-distribution scheme for WSNS:

In this section, we present a new unital-based key pre-distribution scheme for WSNs. In order to enhance the key sharing probability while maintaining high network scalability, we propose to build the unital design blocks and pre-load each node with a number of blocks picked in a selective way.

Key Pre-distribution:

Before the deployment step, we generate blocks of m order unital design, where each block corresponds to a key set. We pre-load then each node with t completely disjoint blocks where t is a protocol parameter that we will discuss later in this section. In lemma 1, we demonstrate the condition of existence of such t completely disjoint blocks among the unital blocks. In the basic approach each node is pre-loaded with only one unital block and we proved that each two nodes share at most one key.

Contrary to this, pre-loading each two nodes with t disjoint unital blocks means that each two nodes share between zero and t_2 keys since each two unital blocks share at most one element. After the deployment step, each two neighbors exchange the identifiers of their keys in order to determine the common keys. If two neighboring nodes share one or more keys, we propose to compute the pairwise secret key as the hash of all their common keys concatenated to each other. The used hash function may be SHA-1 for instance.

This approach enhances the network resiliency since the attacker have to compromise more overlap keys to break a secure link. Otherwise, when neighbors do not share any key, they should find a secure path composed of successive secure links. The major advantage of this approach is the improvement of the key sharing probability.

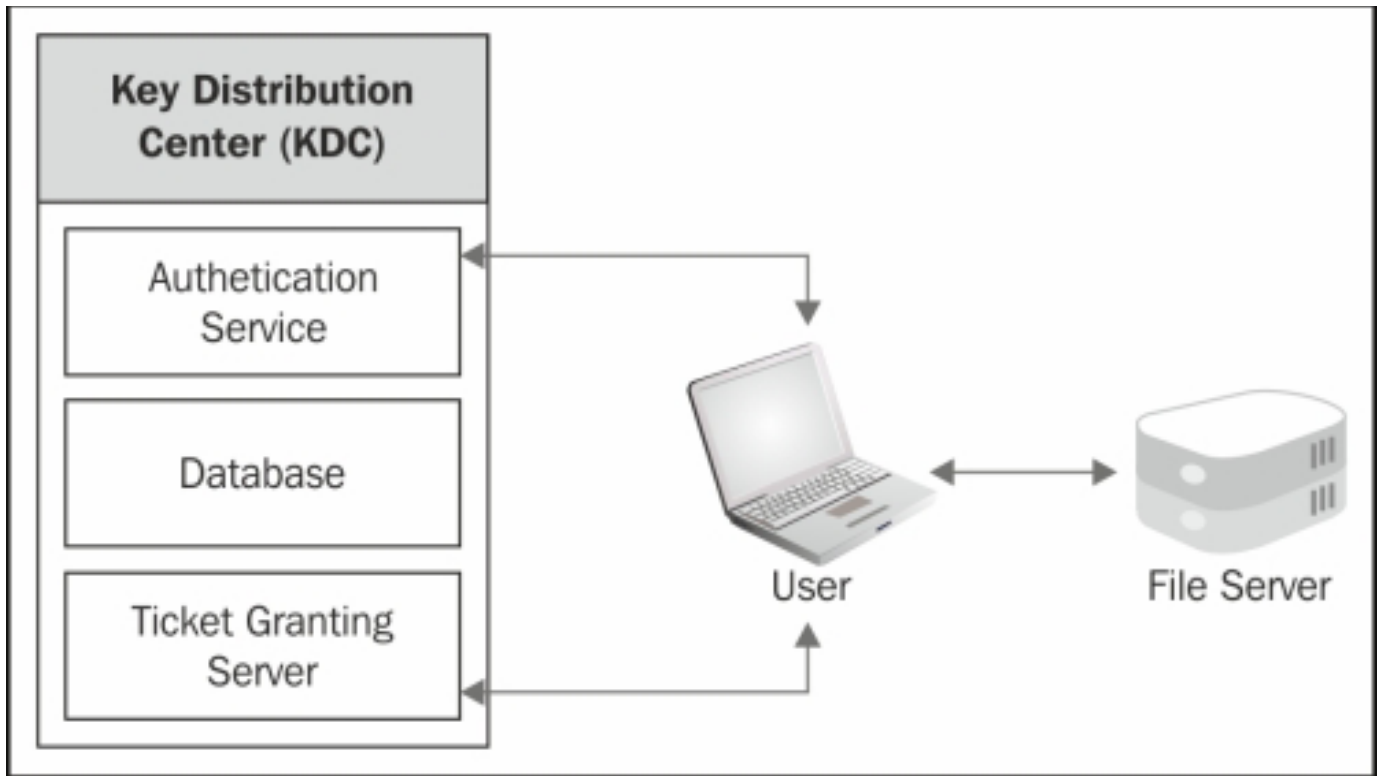
As we will prove in next subsection, this approach allows to achieve a high secure connectivity coverage since each node is pre-loaded with t disjoint blocks. Moreover, this approach gives good network resiliency through the composite pairwise secret keys which reinforces secure links.

In addition, we show that our solution maintains a high network scalability compared to existing solutions although it remains lower than that of the naïve version. To analyze the Key distribution the following parameters as a metrics.

Proof: Let us consider two nodes u and v randomly selected. Each node is pre-loaded with a key ring containing t disjoint unital blocks: $K_{Ru} = \{B_{u,1} B_{u,2} \dots B_{u,t}\}$ and $K_{Rv} = \{B_{v,1} B_{v,2} \dots B_{v,t}\}$. Let us consider $X_{p,q}$ the variable giving the number of shared keys between two unital blocks $B_{u,p}$ and $B_{v,q}$. Following equation (1) (Cf. Section 3.C), we find that $X_{p,q}$ takes only 1 and 0 values such that: $P(X_{p,q} = 1) = \frac{1}{(m+1)^2}$ and $P(X_{p,q} = 0) = 1 - \frac{1}{(m+1)^2}$. $X_{p,q}$ follows then a Bernoulli distribution of parameter $\frac{1}{(m+1)^2}$. Assuming that $t \gg m^2(m-1)$, $X_{p,q}$ intuitively become closer to independent. The number

of shared keys between K_{Ru} and K_{Rv} which represents

$$\begin{aligned}
 & \binom{t}{i} \left(\frac{1}{(m+1)^2}\right)^i \left(1 - \frac{1}{(m+1)^2}\right)^{t-i} \\
 & \text{follows then a binomial distribution } \binom{t}{i} \left(\frac{1}{(m+1)^2}\right)^i \left(1 - \frac{1}{(m+1)^2}\right)^{t-i}
 \end{aligned}$$



Connectivity:

We calculate the local connectivity as the probability of two neighboring nodes being able to find a common key.

Global Connectivity:

It is possible that the key-sharing in our scheme has a high local connectivity, but we have isolated components. Since those components are disconnected, no secure links can be established among them. Therefore, it is important to understand whether will have too many isolated components.

Conclusion and future work:

In this work We have proposed a key pre-distribution mechanism with the help of BCH coding. We have got some better resiliency than some of the existing schemes. In future research can be done in order to find a suitable coding scheme which can increase the resiliency of the network. A coding technique can be found out with large number of code words and large minimum distance so that it can be fitted to key pre-distribution. have concentrated on random node capture attack. We conducted analytical analysis and simulations to compare our new solution to existing ones, the results showed that our approach ensures a high secure coverage of large scale networks while providing good overall performances. In future research can be done so that selective node capture attack also can be taken care. Except combinatorial designs, other designs like packing designs, cover free families and many more unexploited designs can be exploited. In our work we

Reference:

[1] Walid Bechkit, Yacine Challal, Abdelmajid Bouabdallah, and Vahid Tarokh- "A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks"- IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 12, NO. 2, FEBRUARY 2013.

[2] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Communications Magazine, v.40 n.8, p.102-114, August 2002 [doi>10.1109/MCOM.2002.1

[3] Ross Anderson, Markus Kuhn, Tamper resistance: a cautionary note, Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce, p.1-1, November 18-21, 1996, Oakland, California

[4] R Blom, An optimal class of symmetric key generation systems, Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques, p.335-338, December 1985, Paris, France

[5] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, Moti Yung, Perfectly-Secure Key Distribution for Dynamic Conferences, Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, p.471-486, August 16-20, 1992

[6] D. W. Carman, P. S. Kruus, and B. J. Matt. Constraints and approaches for distributed sensor network security. NAI Labs Technical Report #00-010, available at <http://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip>, 2000.

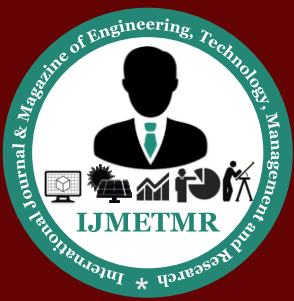
[7] Haowen Chan, Adrian Perrig, Dawn Song, Random Key Predistribution Schemes for Sensor Networks, Proceedings of the 2003 IEEE Symposium on Security and Privacy, p.197, May 11-14, 2003.

[8] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22:644-654, November 1976.

[9] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. Technical Report, Syracuse University, July 2003. Available from <http://www.cis.syr.edu/~wedu/Research/paper/ddh-cv03.pdf>.

[10] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: Mobile networking for smart dust," in Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 1999, pp. 483-492.

[11] Wireless Integrated Network Sensors, University of California, Available: <http://www.janet.ucla.edu/WINS>.



- [12]D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), Washington, DC, USA, October 27-31 2003, pp. 52-61.
- [13]H. Chan and A. Perrig, "PIKE: Peer intermediaries for key establishment in sensor networks," in Proceedings of IEEE Infocom, Miami, FL, USA, March 13-17 2005.
- [14]R. Anderson, H. Chan, and A. Perrig, "Key infection: Smart trust for smart dust," in Proceedings of IEEE International Conference on Network Protocols (ICNP 2004), 2004.
- [15]C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," Lecture Notes in Computer Science, vol. 740, pp. 471-486, 1993.
- [16]M. Tatebayashi, N. Matsuzaki, and D. B. Newman, "Key distribution protocol for digital mobile communication systems," Advances in Cryptology - CRYPTO'89, pp. 324-334, 1989, INCS Volume 435, Springer-verlag.
- "key distribution and authentication in mobile radio networks," Advances in Cryptology - EuroCrypt'93, pp. 461-465, 1993, INCS Volume 765, Springer-verlag.
- [17]M. Beller and Y. Yacobi, "Fully-fledged two-way public key authentication and key agreement for low-cost terminals," Electronics Letters, vol. 29, no. 11, pp. 999-1001, 1993.
- [18]C. Boyd and A. Mathuria, "Key establishment protocols for secure mobile communications: A selective survey," Lecture Notes in Computer Science, vol. 1438, pp. 344-355, 1998.
- [19]L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13, no. 6, pp. 24-30, 1999.
- [20]E. De Cristofaro, C. Soriente, G. Tsudik, and A. Williams. Hummingbird: Privacy at the time of twitter. In IEEE Symposium on Security and Privacy, pages 285-299. IEEE Computer Society, 2012.
- [21]A. Cuttillo, R. Molva, and T. Strufe. Safebook: A privacy-preserving online social network leveraging on real-life trust. Communications Magazine, 47(12):94-101, 2009.
- [22]R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second generation onion router. In USENIX Security Symposium, pages 303-320, 2004.
- [23]FTC. Ftc charges deceptive privacy practices in google's rollout of its buzz social network. Online, 03 2011.