IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Distributed Schemes in Wireless Sensor Networks

Mohamed Asharaf K.

Lecturer in Electronics Engineering,

Institute Of Printing Technology and Government Polytechnic College, Shoranur, Palakkad, Kerala.

Abstract:

A wireless sensor network (WSN) is made up of numerous sensor nodes that are distributed throughout a planned area and have limited power, computation, and communication capabilities. Applications involving high security wireless sensor networks, such as military target tracking, border security, and scientific research, are in a dangerous environment. In our proposed scheme, sensor nodes in WSNs are grouped according to a hierarchical structure. An end-to-end secure communication protocol is used in the top wired layer to distribute group keys for subgroups to trusted head nodes.

Keywords: Wireless sensor networks, pre-distribution, Security, Sensor nodes, Hierarchical WSN, Distributed WSN, Security Issues, Vulnerabilities.

Introduction:

The development of transistors and semiconductor devices has resulted in the deployment of wireless sensor networks (WSNs). A wireless sensor network (WSN) is a self-organized network made up of many low-cost and low-powered sensor devices that can be deployed in the field, the air, vehicles, on bodies, underwater, and inside buildings. These small sensing devices can work together to monitor physical or environmental conditions in the real world, such as temperature, pollution, pressure, light, voltage, humidity, and motion. They are also regarded as specific networks that are widely used in commercial and industrial areas, such as transportation tracking, environmental and habitat monitoring, healthcare, and so on. WSNs can also be used for target tracking and battlefield surveillance in military applications. The data sensed by nodes in many of these applications is frequently unreliable. Multiple noises and errors, missing values, duplicated data, or inconsistent data all have an impact on data quality.[1-2]

There are six challenges to WSN security. (i) To communicate wirelessly, (ii) To operate without fixed infrastructure, and (iii) Sensor nodes have limited resources. (iv) WSNs can be large and dense; (v) network topology is unknown prior to deployment; and (vi) physical attacks on unattended sensors are common. As a result, security is a top priority, especially in hostile environments like military bases. An adversary, for example, could capture sensor nodes, intercept transmitted messages, and propagate bogus messages to networks. Researchers have looked into the security of WSNs from a variety of angles. In wireless sensor networks, key distribution is critical for security. Sensor nodes must adapt to their surroundings and create a secure network by employing techniques such as key pre-distribution and exchanging data with their immediate neighbours or computationally strong nodes. [3-8]

A sensor node is a small device that includes the following components: a processing unit, a sensing unit, a transceiver, and a power unit.

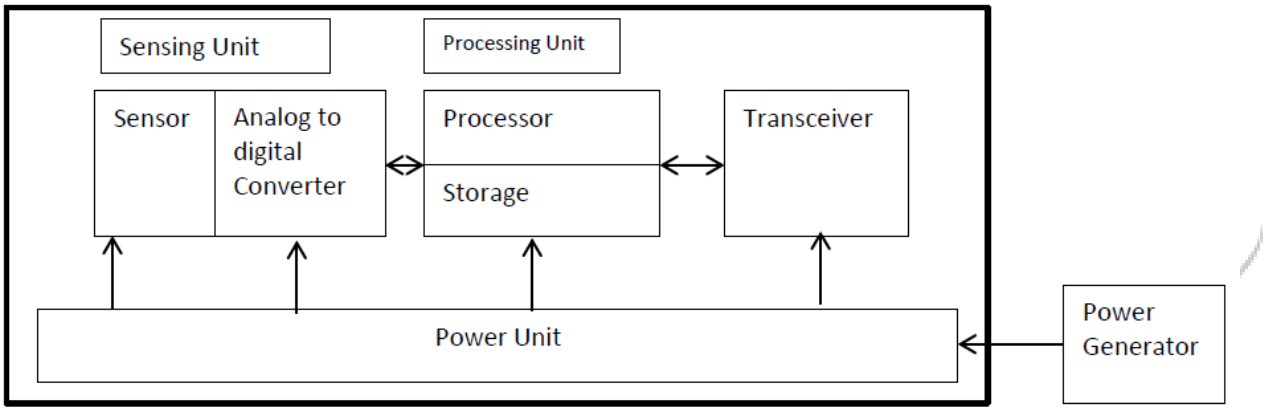

Figure 1: Components of a sensor node [9]

The Berkeley Mica Motes sensor node hardware configuration includes an 8-bit 4 Mhz Atmel ATmega 128L processor with 128Kbytes programme store and 4Kbytes SRAM [8].

Network Models:

WSN communication is typically ad hoc, and it is similar to wireless ad hoc networks. Similarly, WSNs are dynamic in the sense that radio range and network connectivity change over time; sensor nodes die and new nodes join the network. WSNs, on the other hand, are more constrained, denser, and may suffer from (or benefit from) redundant information.

1. Hierarchical WSN (HWSN) [10]:

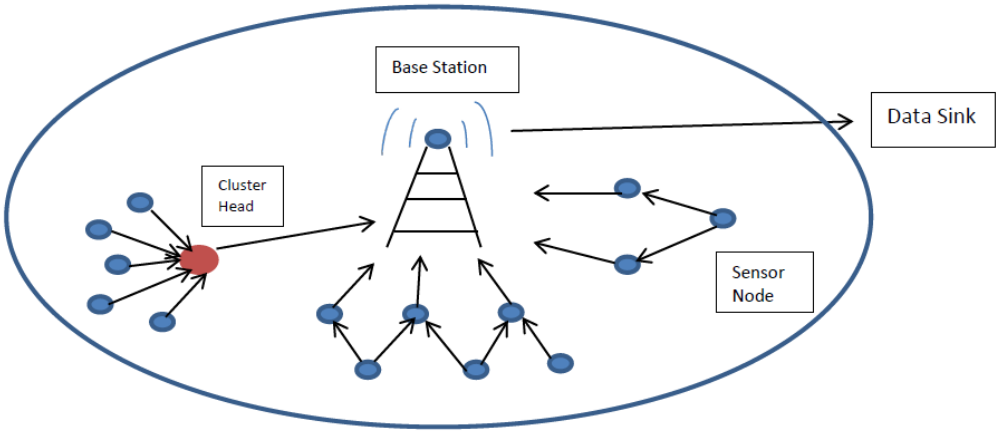

Figure 2: Hierarchical WSN [10]

The Hierarchical WSN is depicted in the figure above, with nodes arranged in a hierarchy based on their capabilities. As shown in the diagram above, there are three types of nodes: The base station, cluster head, and sensor nodes are all more powerful than the other two. A base station is the beating heart of a WSN; it is a powerful data processing/storage centre or an access point to human interface, and it is typically a gateway to another network. Aside from that, it collects sensor readings, performs costly operations on behalf of sensor nodes, and manages the network. It is assumed to be the most trusted and tamper-resistant key distribution centre in some applications.

2. Distributed WSN (DWSN) [10]:

The sensor nodes in DWSN are randomly distributed throughout the target area, as shown in the figure below. As a result, the DWSN lacks fixed infrastructure and the network topology is unknown prior to deployment. When deployed, sensor nodes identify their neighbours by scanning their radio coverage area. The data flow is similar to that of HWSN, with the exception that every sensor node can send data network-wide (broadcast). Sensor nodes in this case either use keying materials to generate pairwise and group-wise keys dynamically or directly use pre-distributed keys.

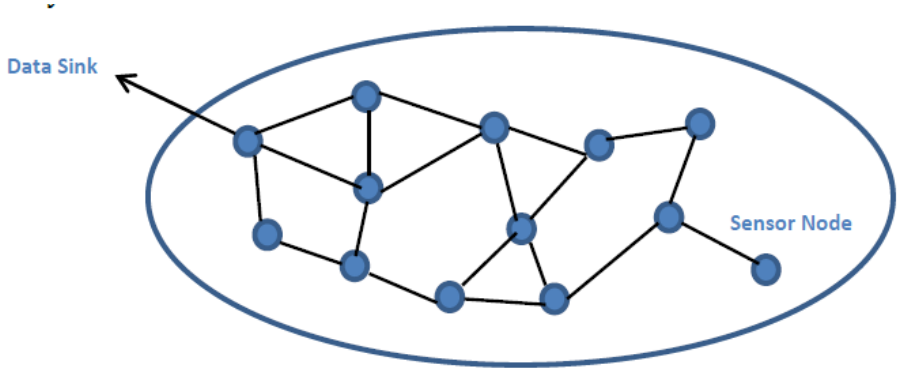

Figure 3: Distributed WSN [10]

To overcome the difficulty of distributing keys and keying materials to sensor nodes prior to deployment, one of three approaches (i) probabilistic (ii) deterministic (iii) hybrid is used.

Security Issues

Vulnerabilities

Adversaries want to manipulate application data (eavesdrop, modify, insert, delete, and jam). Adversaries' capabilities in a WSN are enhanced by the wireless nature of communication, a lack of infrastructure, and uncontrolled environments. Stationary adversaries equipped with powerful computers and communication devices may gain remote access to the entire WSN. They can move around or within the WSN by using powerful laptops, batteries, and antennas. They have the ability to set up their own sensor nodes, base stations, or cluster heads, as well as replace, compromise, or physically damage existing ones. Wireless communication enables adversaries to carry out a variety of passive, active, and stealth attacks [10]. In passive mode, adversaries silently listen to radio channels for data and security credentials (i.e., keys or cryptographic tools to derive them). In active attacks, adversaries may actively intercept key management traffic, capture, read, or modify the contents of sensor nodes. They can use wireless devices with varying capabilities to play man-in-the-middle or hijack a session. They can insert, modify, replay, delete, or jam traffic [11-12]. In stealth attacks, an adversary manipulates a set of nodes and the routing information that flows through them to carry out various attacks such as network disconnections and traffic hijacking.

The solution to pair-wise and group-wise key distribution is shown in the table below.

Table 1: Solutions on key distribution problem in Distributed WSN

Problem	Approach	Mechanism	Keying style
Pair-wise	Probabilistic	Pre-distribution	Random Key-chain
			Pairwise key
	Deterministic	Pre-distribution	Pairwise key
			Combinatorial
		Dynamic Key Generation	Master Key
			Key Matrix
			Polynomial
	Hybrid	Pre-distribution	Combinatorial
		Dynamic Key Generation	Key Matrix
			Polynomial
Group-wise	Deterministic	Dynamic Key Generation	Polynomial

BLOM'S KEY PRE-DISTRIBUTION SCHEME

Blom proposed a method of key pre-distribution that allows any pair of nodes in a network to find a pairwise secret key. The network is perfectly secure as long as no more than nodes are compromised (this is known as the -secure property). We describe Blom's λ-secure key pre-distribution system in detail. Blom's scheme was not designed for sensor networks, so we have made some minor changes to the original scheme in the following description to make it suitable for sensor networks. [13]

During the pre-deployment phase, the base station creates a (λ+1)N matrix G over a finite field *GF*(q), where *N* is the network size. *G* is considered public information; any sensor, including adversaries, is permitted to know its contents. The base station then generates a random (λ+1) (λ+1) symmetric matrix *D* over *GF* (q) and computes a *N*(λ+1) matrix A=$(DG)^{T,}$ where $(DG)^T$ is D G's transpose.

Matrix *D* must be kept secret and not revealed to adversaries or any sensor node (though, as discussed later, one row of $(DG)^T$ will be revealed to each sensor node). Because *D* is symmetric, it is simple to see:

$$A \cdot G = (D \cdot G)^T \cdot G = G^T \cdot D^T \cdot G = G^T \cdot D \cdot G = (A \cdot)^T .$$

As a result, *AG* is a symmetric matrix. If we assume *K* = *AG*, we can deduce that *Kij* = *Kji*, where *Kij* is the element in K in the *i*th row and *j*th column. *Kij* (or *Kji*) is used as the pairwise key between nodes *i* and *j*.

Multiple-Space Key Pre-Distribution Scheme

We propose a new key pre-distribution scheme that uses Blom's method as a building block to achieve better resilience against node capture. Our hypothesis is founded on the following observations: Blom's method ensures that any pair of nodes can discover a secret key between them. We use graph theory concepts to represent this, drawing an edge between two nodes if and only if they can find a secret key between themselves. We will obtain a complete graph (every node pair has an edge). Although complete connectivity is desirable, it is not required. We only need a connected graph, not a complete graph, to achieve our goal of key agreement. Our hypothesis is that *by limiting* the *graph to only connected nodes, each sensor node must carry less critical information.*

Before we get into our proposed scheme, we define a key space (or space in short) as a tuple (*D,G*), where *D* and *G* are the matrices defined in Blom's scheme. A node is said to pick a key space (*D,G*) if it carries the secret information generated by (*D,G*) using Blom's scheme. If two nodes have chosen a common key space, they can calculate their pairwise key. [14-16]

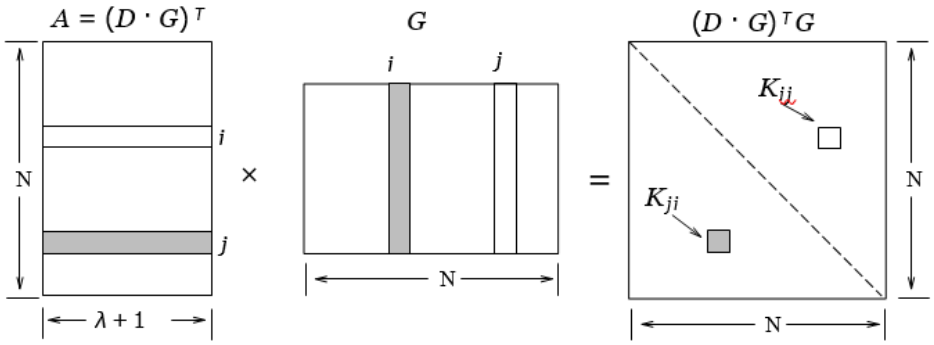

Figure 4: Generating Keys in Blom's Scheme

We now discuss various schemes for key pre-distribution in WSNs.

1. Polynomial based key pre-distribution

We go over how to pre-distribute pairwise keys.

The (key) setup server generates a bivariate t-degree polynomial *f*(x,y) = at random.

$$\sum_{i,j=0}^{t} a_{ij} x^i y^j$$

over a finite field Fq, where q is a prime number large enough to hold a cryptographic key

and has the property f(x,y)=f (y,x). (Without explicit statement, we assume that all bivariate polynomials have this property.) In this system, each sensor is assigned a unique ID. The setup server computes a polynomial share of f(x,y) for each sensor 'i', that is, f(i,y). Node i can compute the common key f(i,j) by evaluating f (i,y) at point j, and node j can compute the same key f (j,i) = f (i,j) by evaluating f(j,y) at point i for any two sensor nodes i and j. [17]

2. Polynomial pool based key pre-distribution

As the name implies, we have a pool of randomly generated bivariate polynomials in this technique; the method used to generate these bivariate polynomials is based on the polynomial-based key pre-distribution discussed above. The polynomial pool has two instances. When there is only one polynomial in the polynomial pool, the general framework degenerates into the polynomial-based key pre distribution. The polynomial pool degenerates into a key pool Random Subset assignment key pre-distribution when all of the polynomials are 0-degree ones. [17-19]

3. Grid based key pre-distribution

Assume you have a sensor network with N sensor nodes. The grid-based key pre distribution scheme then builds a $m \times m$ grid with a set of 2m polynomials $\{ f_i^c(x,y) , f_j^r(x,y)\}_{i=0,\ldots,m-1}\}$,where $m = \lceil \sqrt{N} \rceil$. Each row j in the grid is associated with a polynomial $f^{i^r}(x,y)$, and each column i is associated with a polynomial $f_i^c(x,y)$, as shown in Figure below. The setup server assigns a unique intersection in this grid to each sensor in the network. The setup server assigns the polynomial shares of $f_i^c(x,y)$ and $f_j^r(x,y)$to the sensor at coordinate (i, j). As a result, sensor nodes can use this information to perform share and path discovery, and eventually pre-distribute the keys. [20]

4. Hyper-cube multivariate Scheme (HMS)

It is essentially a Threshold-based scheme in which a number of multivariate polynomials are assigned to each point on the hypercube and a hypercube is designed in multidimensional space. The sensors are assigned to specific points on the hypercube. A direct key is established between any two sensors at a Hamming distance of one from each other using this technique. Other sensors can also generate indirect keys.[21]

5. A Robust Key Pre-distribution protocol for Multi-phase WSN

We can see from the sensor node components that they are battery operated, and their life time is much shorter than the lifetime of the entire network, so we need to deploy new sensor nodes to replace the disappearing ones in the network to ensure good network connectivity. Generations refers to the process of deploying new sensors on a regular basis. The generation period is the time between two successive generations. Gw- Window of generation:- a number based on the assumption that a sensor's lifetime is bounded by generations. The generation period is set to one. In this scheme, the time it takes for a node deployed at generation j to establish a secret channel with any other sensor deployed is |j- k,j+k|, where k is an integer and it is assumed that k = Gw. If k is less than Gw, a newly deployed node can establish a secure channel with a subset of network sensors. Each sensor is assigned one of two key rings: FKRA and BKRA, where a key ring is a subset of the key pool, namely $FKR_A \subset FKP$ and $BKR_A \subset BKP$. The abbreviation and full form are as follows: [22-23]

Gw: generation window, n:last generation of the network, A: sensor A, $kr^j_A = (FKR^j_A, BKR^j_A)$: key ring of A at gen. j, FKR^j_A: forward key ring of A at gen. j, BKR^j_A: backward key ring of A at gen. j, m:key ring size, FKP^j: Forward key pool at gen. j, BKP^j: Backward key pool at gen. j, P:key pool size, $fk^j_t \in FKP^j$: t-th f key at gen j, $bk^j_t \in BKP^j$: t-th b key at gen j, h:secure hash function $h:\{0,1\}^* \rightarrow \{0,1\}^{160}$, f:hash function $f:\{0,1\}^* \rightarrow \{0,1\}^{\log_2(P)}$, RKP: keymanagement defined in [2], Rok: Robust key pre-distribution scheme.

Conclusion:

A survey of key distribution schemes for wireless sensor networks was presented in this paper. Due to resource constraints in sensor nodes, key management protocols based on public key cryptographic (asymmetric functions) are not appropriate; thus, key pre-distribution a particular symmetric approach is deployed in WSNs, which reduces the cost of key establishment. However, it appears that the piggy bank version of public key cryptography, by pre-distributing key elements, can be adapted for sensor networks.

References:

1. M. Moshtaghi et al. An adaptive elliptical anomaly detection model for wireless sensor networks Comput. Networks (2014)

2. Maguluri, Lakshmana & Basha, Shaik & Ramesh, S. & Amanatulla, Md. (2015). A Distributed Secured Localization Scheme for Wireless Sensor Networks. Advances in Intelligent Systems and Computing. 309. 115-120. 10.1007/978-81-322-2009-1_14.
3. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro,and M. Yung. Perfectly-secure key distribution for dynamic conferences. In Advances in Cryptology – CRYPTO '92,LNCS 740, pages 471–486, 1993
4. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, 2003
5. L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proc. of the 9th ACM Conf. on Computer and Communications Security, pages 41–47, November 2002.
6. Donggang Liu , Peng Ning. Establishing Pairwise keys in Distributed Sensor Network. CCS'03, October 27–31, 2003, Washington, DC, USA
7. Farshid Delgosha , Faramarz Fekri. Key Pre-distribution in Wireless Sensor Networks Using Multivariate Polynomials. 0-7803-9012-1/05/$20.00 (C) 2005 IEEE
8. A. Parakh and S. Kak, Matrix based key agreement algorithms for sensor networks. Proceedings of IEEE Advanced Networks and Telecommunications Conference (ANTS 2011), Bangalore.
9. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci : Wireless sensor networks: a survey 2002 Elsevier Science
10. S. A. Camtepe and B. Yener, Key Distribution Mechanisms for Wireless Sensor Networks: a Survey. Technical Report TR-05-07 (March 23, 2005).
11. M. Jakobsson, S. Wetzel, B. Yener, Stealth attacks on ad-hoc wireless networks, in: IEEE Vehicular Technology Conf., 2003, pp. 2103{2111.
12. C. Karlof, D. Wagner, Secure routing in wireless sensor networks: Attacks and counter-measures, in: IEEE Int. Workshop on Sensor Netw. Protocols and Appl., 2003, pp. 113{127.
13. Gao Weimin and Zhu Lingzhi; Distributed Data Storage in Wireless Sensor Networks Gao Weimin. International Journal of Database Theory and Application. Vol.8, No.4 (2015), pp.179-182
14. R. Blom. An optimal class of symmetric key generation systems. Advances in Cryptology: Proceedings of EUROCRYPT 84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), Lecture Notes in Computer Science, Springer-Verlag, 209:335–338, 1985.
15. Claude Castelluccia, Angelo Spognardi: A Robust Key Pre-distribution Protocol for Multi-Phase Wireless Sensor Networks. Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007.

16. Sushmita Ruj, Jennifer Seberry, Bimal Roy, Key predistribution schemes using block designs in WSN's. Key predistribution schemes using block designs in wireless sensor networks. In Computational Science and Engineering, 2009. CSE '09., 873- 878.
17. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro,and M. Yung. Perfectly-secure key distribution for dynamic conferences. In Advances in Cryptology – CRYPTO '92,LNCS 740, pages 471–486, 1993
18. H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, 2003
19. L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In Proc. of the 9th ACM Conf. on Computer and Communications Security, pages 41–47, November 2002.
20. Donggang Liu , Peng Ning. Establishing Pairwise keys in Distributed Sensor Network. CCS'03, October 27–31, 2003, Washington, DC, USA
21. Farshid Delgosha , Faramarz Fekri. Key Pre-distribution in Wireless Sensor Networks Using Multivariate Polynomials. 0-7803-9012-1/05/$20.00 (C) 2005 IEEE
22. A. Parakh and S. Kak, Matrix based key agreement algorithms for sensor networks. Proceedings of IEEE Advanced Networks and Telecommunications Conference (ANTS 2011), Bangalore.
23. Chao Xiong et al 2019 J. Phys.: Conf. Ser. 1229 012066