Volume 2, No. 4, July-August 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Nodes Deployment Model and Key Predistribution in Wireless Sensor Networks

Subash T.D
Assistant Professor,
Department Of ECE
Infant Jesus College of Engineering and Technology
Tamilnadu,India
tdsubash2007@gmail.com

Abstract— in wireless sensor network key management is one of the crucial aspects of security. Although existing key managaement schemes are enough to solve most of the security constraints on wireless sensor networks, a hexagonal based deployment model with asymmetric based key predistribution scheme has recently evolved as an efficient solution for sharing keys between sensor nodes.The existing scheme makes use of symmetric matrices in order to establish a secret key between the sensor nodes. It results in the establishment of a single key for communication between two sensor nodes. If it is captured by an adversary then the network is compromised, thus the resilience of the network is reduced. . In this paper the deployment model is improved by making use of hexagonal based deployment and the key pre-distribution scheme is improved by using asymmetric matrix. An asymmetric matrix generates two secret keys for two nodes. Thus bidirectional communication links are established between the nodes. Though one of the links gets compromised by an attacker, there exists another link for secure communication between the nodes. Thus the resilience of the sensor network is improved. The result shows that the number of times network gets compromised is less and the connectivity is high in our method compared to the existing scheme.

Keywords— Key Pre-Distribution**,** Key Pool, Key Ring, Wireless Sensor Networks.

I. INTRODUCTION

Wireless sensor networks have recently received remarkable attention. A sensor network contains a large number of tiny sensor nodes that sense data specific to that environment and report them to other nodes over a flexible architecture. Sensor networks are best suited to be deployed in hostile environments and over large geographical regions. In other words, sensor networks are suited to be deployed over unattended areas. When sensor networks are deployed in hostile environments, security becomes a very important problem to be resolved. Sensor networks are subjected to different types of attacks [1] (physical capture of a node, intentionally providing misleading information, impersonation, eavesdropping, etc.). In order to provide security for sensor networks, key management is applied. Security services like authentication and confidentiality are critical to secure the communication between sensors in hostile environments. For these security services, key management is the fundamental building block. Since each node has constrained resources and can be captured, traditional key management techniques using public key infrastructure or centralized key management techniques may not be appropriate for sensor networks. Secret key pre-distribution for symmetric encryption is one of the practical approaches for establishing secure channels among sensors.

Key management lays the foundation to ensuring the security of network services and applications in WSNs. The goal of key management is to establish the required keys between sensor nodes that exchange data. Due to the constraints of sensor nodes, symmetric key management systems should be the only option for WSNs [2]–[6]. According to the underlying network structure, the key management protocols for the symmetric cryptography can be divided into two categories: 1) hierarchical key schemes and 2) distributed key schemes. The hierarchical key scheme depends on the trusted controller for key assignment and exchange between nodes. This scheme is vulnerable since compromise of the controller can render the entire network vulnerable. Furthermore, the network may become too large to be managed by some single entities, thus affecting scalability. In the distributed key management protocol, the keys distributed among all sensor nodes minimize the risk of the trusted entity failures and allow for better scalability. As keys are assigned to the nodes before deployment, the schemes are called “key predistribution.”

EG [2] proposed a key predistribution scheme based on the concept of probabilistic key sharing among nodes contained in a random graph. In the key setup phase, a large pool of keys is generated; each sensor key ring consists of m keys, which are randomly drawn from the key pool without replacement. In the shared-key discovery phase, two neighboring nodes exchange and compare their key rings for matching messages from each node within its signal range. With the advantage that a random graph is connected with high probability if the average degree of its nodes is above a threshold, key establishment only needs to be probabilistically performed. This is done such that two neighboring nodes have a certain probability of sharing at least one key after deployment. An attractive feature of EG is that each sensor incurs small communication overhead for key establishment, regardless of the network size. However,EG suffers from two major problems: First, it requires a high deployment density to ensure connectivity. If the node density is nonuniform, performing probabilistic key establishment could result in an unreachable part. Second, there is a requisite for high network connectivity when the key rings are big (e.g., 200 keys for 10 000 nodes for a connectivity of 0.33).

This shortcoming seems avoidable for random key predistribution schemes. In this paper, we propose a new scheme that uses signal range knowledge to solve the two aforementioned drawbacks.

To resolve to a high density requirement, Chan *et al.* proposed a grid-based scheme called PIKE [3], where the keys are preloaded to the sensor based on the location of each node.The core idea is that each sensor shares its key with the other sensors that are located in the same row or column of the grid. PIKE offers a better tradeoff between the communication overhead and the memory cost per sensor node. However, the disadvantage of PIKE is that each pair of sensor nodes having common keys is probably not within the signal range of each other. Therefore, the probability of key sharing is not really high. In addition, PIKE requires trust from the third intermediary for key establishment. This involves the security weakness of the scheme.

Liu and Ning.,[4] proposed the Polynomial Pool-Based Key Pre-Distribution Scheme. This scheme offers several efficient features the other schemes lack, including: Any two sensors can definitely establish a pair-wise key when there are no compromised sensors. Even with some nodes compromised, the others in the distributed sensor network can still establish a Pair-Wise Key and thereby help reduce communication overhead.

Du et al., proposed a new key pre-distribution scheme [5], which improves the resilience of the network. It has a threshold property that the probability of nodes other than the compromised ones is close to zero while the number of compromised nodes is less than the threshold. This makes the adversary to attack a significant portion of the network.

The major drawback in the existing scheme is generating a single key for communication between two sensor nodes. If the single key is captured by an adversary the communication between the node pair is permanently destroyed and thus the resilience of the network is less. To overcome this drawback two secret keys are generated for communication between the node pairs. Thus two separate links are established between the nodes. If one of the links gets compromised by an adversary, there exists another link to communicate between the nodes. Thereby the resilience of the network gets increased.

The paper is designed as follows. The proposed scheme is presented in the next section. The simulation result is discussed in the section III. Section IV gives the conclusion of the proposed scheme.

II. PROPOSED SCHEME

In this paper the Blom's scheme is modified by making use of asymmetric matrix instead of symmetric matrix and the deployment model is modified as hexagonal based model.The keys were generated using asymmetric matrices which improve the resilience of the sensor network. It generates two secret keys to communicate between any two sensor nodes (say nl and n2). One key is used to communicate from node nl to n2 and another to communicate from node n2 to nl. Two separate communication links are established between a pair of nodes. If one of the communication links gets compromised by an adversary, still there exists another link to communicate between the nodes. Thus increases the resilience of the sensor network.

A. Model For Hexagon Based Deployment

The sensor field is in the shape of hexagon as in fig.1. the centre of the grid is the deployment point, which is the desired location of the group of nodes. the location of sensor node over the entire sensor field follows some distribution with a probability density function. in hexagon based scheme, all adjacent sensor nodes have the same distance. the hexagon system has some advantages over the rectangular system. first, when a sensor node transmits data over wireless links, its signal range would form a circle that is centered around its deployment location with the radius being the distance of signal propagation. therefore, a hexagon can be used to express and simulate the signal range more appropriately than a square can. Second, a hexagon can be used to describe equal distance between two neighboring sensor nodes. In a common rectangular coordinate system, the distance between neighboring sensor nodes differs, which depends on whether the neighboring node is located directly adjacent (in which case the distance is 1 unit) or diagonal (in which the distance is square root of 2 units) to it. Under the hexagonal coordinate system, all adjacent sensor nodes have that same distance which is normally 1 unit.

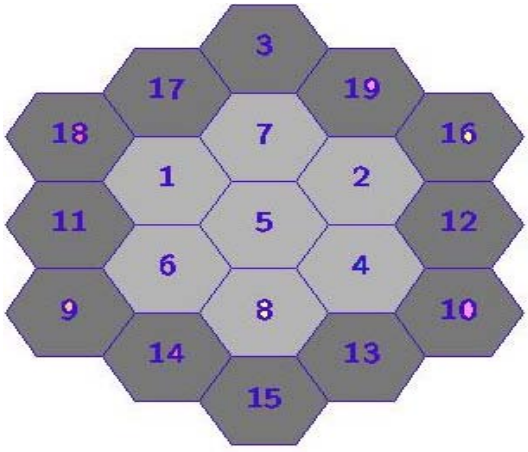

Figure 1. Hexagon co-ordinate system

There are many different ways to deploy sensor networks, for example, sensors could be deployed using an airborne vehicle. For example, if the number of nodes is too large, e.g. more than 10^4, divide them into groups and deploy one group each time. Each group of nodes may be deployed into a local area or to just a single deployment point, which is the desired location of nodes. Such kind of deployment methods into a group-based deployment model can be summarized as follows:

a. An arbitrary sensor field S_f is divided into t grids equally, where the shape of grids may vary.
b. N nodes are also divided into t groups equally. Each group has $n = N / t$ nodes and is to be deployed into a grid, i.e. group i is deployed to grid i (i = 1 . . . t), where i is called the group ID.
c. The center of a grid is a deployment point, which is the desired location of a group of nodes. However, due to the randomness in deployment process, assume that the real location of nodes of each group *i* follows some distribution (PDF) $f_i(x, y) = f(x, y, \mu_{xi}, \mu_{yi})$, where $(\mu_{xi}, \mu_{yi}) \in S_f$ is the coordinate of deployment point of the group.

In a group-based deployment model, there are two generally used distributions. In most cases, sensor nodes are often assumed to be uniformly deployed i.e. Uniform distribution. Due to randomness the group of nodes may

spread around the deployment point. It is observed that more nodes are residing in the areas closer to the deployment point, and the number of nodes in different directions and within the same distance from the deployment point are almost the same. Hence, such deployment can be modeled by a normal distribution i.e. two dimensional Gaussian distribution is given

$$f(x,y \mid k \in G_{i,j}) = \frac{1}{2\Pi\sigma^2} e^{-\left[(x-x_i)^2+(y-y_j)^2\right] / 2\sigma^2}$$

In the hexagon based scheme, each sensor node takes its deployment hexagon as the center and share keys with the sensor nodes deployed in its 19 adjacent hexagons. In Fig.1. all sensor nodes deployed in shaded hexagon can share key with the sensor nodes deployed in hexagon 5. The hexagon based predistribution scheme also has three phases similar to grid based scheme.

Without loss of generality, let's label the center of a hexagon 5 in the hexagonal coordinate system. Then all other points in the hexagon are located around hexagon 5 counter-clockwise as shown in Fig 1. According to the numbering rule, the numbers in the nth circle of the hexagon should be from $\sum_{i=1}^{n-1} 6(i-1)+1$ to $\sum_{i=1}^{n} 6(i-1)$. Consequently, a hexagon's location and its adjacent hexagons in a hexagonal coordinate system are determined based on the above numbering rule.

B. Key Distribution Scheme

Consider the sensor nodes are deployed into a hexagonal sensor field. The detailed procedure in Key Pre-Distribution Phase is as follows:

a. Generate a public matrix *G* for all groups and a secret matrix A_i for each group i (i = 1, . . . , t). Each node j (j = 1, . . . , n) of group i picks the jth row from A_i, where j is called node ID.
b. Suppose there are totally t1×t2 grids, where t1×t2 = t. Each group i can be located by a pair of row and column index (r_i,c_i), where r_i = 1, . . . , t1 and c_i = 1, . . . , t2.
c. For each group i, if "r_i%2 = 0 and c_i%2 = 0, but r_i%4 ≠ 0", OR, "r_i%4 = 0 and c_i%2 = 1", select it as the basic group and assign it a distinct matrix F. Repeating this step for all groups until all basic groups are found.
d. For each non-basic group, look up all F matrices assigned to its neighboring basic groups and assign these F matrices to the non-basic group.
e. Each node i of a group picks the ith row from every matrix F assigned to its group.
f. Set an identical transmission range r (how to compute r will be discussed later) for all nodes and deploy them into the sensor field.

After deployment, sensor nodes enter into Key Discovery Phase. The detailed procedure is as follows:

a. Each node broadcasts its group ID, a row of matrix F and column of G in plain text and also receives these ID's from its neighbors within the transmission range r.
b. Each node checks the IDs of every neighbor to see if any ID equals to one of its own. If two nodes have the same group IDs, then either of them derives a pairwise key by computing the dot product of its row of A and the column of the other's.
c. If two nodes only have one common F ID (a row of matrix F), then either of them derives a pairwise key by computing the dot product of its row of that shared F and the column of the other's.
d. If two nodes have more than one common F IDs, then they randomly select a shared F and derive a pairwise key from the selected F.
e. If no ID equals, two nodes stop the direct communications with each other.

III. SIMULATION RESULTS

Resilience is defined as the fraction of secure links that are compromised when a certain number of nodes are captured by the adversaries. The adversary can attack a sensor node after it is deployed. The aim is to find how many links are compromised by an adversary.The comparison between symmetric and asymmetric matrix for a network of size N=100 is shown in Fig.3.The resilience analysis was made by introducing some malicious nodes into the network and there by the number of links gets compromised is analyzed. The figure shows that for asymmetric matrix the number of times network getting compromised is reduced since bidirectional link exist between the nodes.

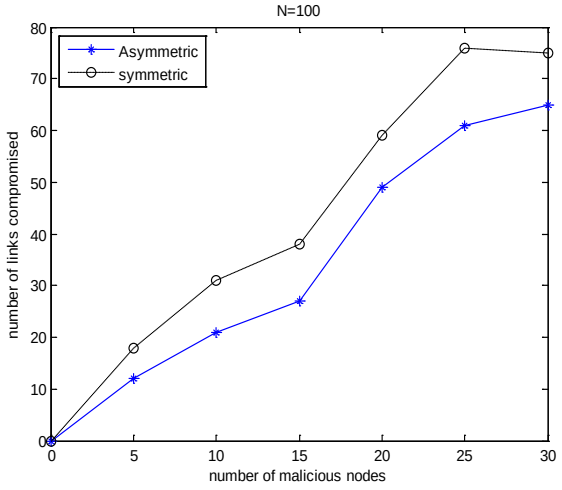

Figure.3Resilience analysis of symmetric and asymmetric matrix for a network of size N=100

The connectivity analysis is the probability that any two neighbouring nodes share one key and it is depicted in Fig 4.

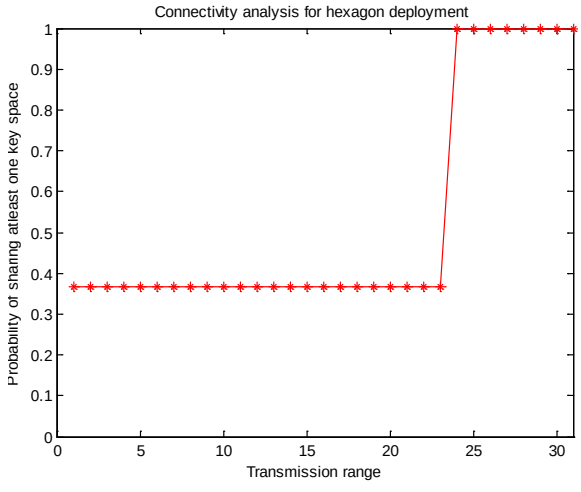

Figure.4 Connectivity analysis

Fig.4. shows the connectivity analysis of hexagon based scheme based on transmission range with 10000 nodes requiring P_c =0.9999 and the transmission range as 24m. From the plot it is inferred that P_c =0.9999 is achieved at the transmission range of 24m. But in literature it is already proved that the basic scheme requires 40m to achieve a connectivity of 0.9999.

IV. CONCLUSION

This paper presents asymmetric matrix scheme hexagonal based deployment. A secret key can be derived from this scheme and it can be used to communicate between node pairs. Two different keys were used for communication between the nodes. This decreases the number of communication links compromised. The result shows that the resilience of the key pre-distribution scheme using asymmetric matrices has been improved.

V. REFERENCES

[1] C.Karlof and D. Wagner "Secure Routing In Wireless Sensor Networks: Attacks And Countermeasures", First IEEE International Workshop On Sensor Networks Protocols and Applications, 2003.

[2] L. Eschenauer and V. D. Gligor, "A Key Management Scheme for Distributed Sensor Networks", 9th ACM Conference on Computer and Communication Security Washington DC, 2002, pp. 41–47.

[3] H.Chan,A.Perrig, and D.Song,"Random Key Pre-distrib-ution Schemes for Sensor Networks", IEEE Symp.on Security and Privacy, Berkeley CA. 2003, pp.197-213.

[4] D. Liu, P. Ning, andW. Du, "Group-based key predistribution for wireless sensor networks," ACM Trans. Sensor Netw., vol. 4, no. 2, pp. 1–30, Mar. 2008.

[5] W.Du,J.Deng, Y. S.Han, and P. K.Varshney, "A Pairwise Key Predistribution Scheme for Wireless sensor network" 10th ACM Conference on Computer And Communications Security, Washington DC, 2003,pp.42- 51.

[6] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in Proc. 23rd IEEE Annu. Joint Conf. IEEE Comput. Commun. Societies, Mar. 2004, pp. 586–597.

[7] Shaila K, S H Manjula, Aruna R, Anupama K R. Venugoal, L M Patnaik ," Resilience Key Predistribution Scheme using Asymmetric Matrices for Wireless Sensor Networks" IEEE International Advance Computing Conference(2009).