www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-1, Issue-2, June- 2013
Research Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Modified Pairwise Key Pre-distribution Scheme with Deployment Knowledge in Wireless Sensor Network

Sanchita Gupta[#1], Pooja Saini[2]

[#1] Dept. of Comp. Engineering, ACE, Ambala, Haryana, India
[2]Dept. of Comp. Engineering, ACE, Ambala, Haryana, India

Received: 21 March 2013 Revised: 07 May 2013 Accepted: 08 June 2013 Published: 30 June 2013

Abstract— To achieve security in wireless sensor networks it is important to be able to encrypt the messages sent among the sensor nodes. Keys for encryption and authentication purpose must be agreed upon by communicating nodes. Due to the resource constraint (limited memory size), achieving such key agreement in wireless sensor network is extremely difficult. Many key agreement schemes used in general networks, such as Diffie-Hellman and public key based schemes, are not suitable for wireless sensor networks. Pre-distribution of secret key for all the pair of nodes is not possible due to the large amount of memory is used when network size is large. In this paper, we provide a view of pairwise key pre-distribution scheme and the deployment knowledge; and also describe the pairwise key pre-distribution scheme with deployment knowledge as an improvement. Deployment knowledge avoids the unnecessary key assignments and improves the performance of the sensor networks in terms of memory usage.

Keywords- Wireless sensor networks, Pairwise key pre-distribution scheme, Deployment knowledge and security.

I. INTRODUCTION

Recent advancement in electronic and computer technologies have developed the way for the generation of wireless sensor networks (WSN). Sensor networks usually consist of a large number of ultra-small autonomous devices. Each device called sensor node. Sensor node is equipped with integrated sensors, data processing capabilities and short range radio communications. Sensor nodes are spread randomly over the deployment region. Sensor networks are being deployed for a wide variety of applications including military sensing and tracking, environment monitoring, patient monitoring and tracking, smart environment, etc.

To provide the security, communication should be encrypted and authenticated. This problem is known as the key agreement problem. In sensor networks, key agreement is used to set up secret keys between them. There are three types of general agreement schemes: trusted server scheme, self-enforcing scheme, and key pre-distribution scheme.

The trusted server scheme [9] is not suitable for sensor networks because there is no trusted infrastructure in sensor networks. The self-enforcing scheme [10] is also not suitable due to the limited computation and energy resources of sensor nodes often make it undesirable to use public key algorithms, such as Diffie-Hellman key agreement. The third type of key agreement scheme is key pre-distribution. There exist a number of key pre-distribution schemes which do not depend on a priori deployment knowledge. A naive solution is to let all the nodes carry a master secret key. This scheme does not exhibit desirable network resilience: if one node is compromised, the security of the entire sensor network will be compromised. Another key pre-distribution scheme is to let each sensor carry $N - 1$ secret pairwise keys [3], each of which is known only to this sensor and one of the other $N - 1$ sensors (assuming N is the total number of sensors). The resilience of this scheme is perfect. But this scheme is impractical for sensors with an extremely limited amount of memory because N could be large. Moreover, adding new nodes to a pre-existing sensor network is difficult because the existing nodes do not have the new nodes' keys. Eschenauer and Gligor [7], proposed a random key pre-distribution scheme each sensor node receives a random subset of keys from a large key pool; to agree on a key for communication, two nodes find one common key within their subsets and use that key as their shared secret key. The problem with this scheme is that when we pick a large key pool, the connectivity of the sensor networks becomes low. In this paper, we will pick pairwise key pre-distribution scheme as the basic scheme and develop this scheme on the deployment model and show that knowledge regarding the sensor deployment can help us improve the performance of a pairwise key pre-distribution scheme.

The rest of the paper is organized as follows. In section II we have discussed main contribution of our scheme. In section III we have said our proposed work. Then we describe the pairwise key pre-distribution scheme with deployment knowledge in section IV. Section V shows the analytical analysis and finally concludes paper in the section VI

II. MAIN CONTRIBUTION

The main contributions of this paper are as following:

We apply node deployment knowledge [2] in a pairwise key pre-distribution scheme of wireless sensor networks.
B. We show that key pre-distribution with deployment knowledge can substantially reduce the amount of memory required.

III. PROPOSED WORK

To improve the performance of pairwise key pre-distribution scheme in term of memory usage we use this scheme with the deployment knowledge.

In paper [2], Deployment knowledge modeled by using probability density functions. When it is uniform, no information can be gained on where a node is more likely to reside. So, in this paper we look at non-uniform pdf functions. There are many different ways to deploy sensor networks. Sensor deployment distribution is described as a Gaussian distribution (also called Normal distribution).

IV. MODIFIED PAIRWISE KEY PRE-DISTRIBUTION USING DEPLOYMENT KNOWLEDGE

Pairwise key pre-distribution scheme uses Blom's method [4] as a building block. This scheme uses the concepts of graph theory and draws an edge between two nodes if and only if they find a secret key between themselves. Pairwise key pre-distribution scheme with deployment knowledge consists following phases:

A. Key pre-distribution phase

This phase is performed to assign key information to each node before the node deployment. Key pre-distribution phase consist the following steps:

Step 1 Select a primitive element from a finite field GF(q).

Step 2 Create a generator matrix G of size $(\lambda+1) * N$ by using primitive element in which G(j) represents j^{th} column of matrix G and it provides to node j. Each sensor only need to remember one seed element which is used to regenerate all the elements in G(j).

Step3 Generate w symmetric matrices D_1.......D_w of size $(\lambda+1) * (\lambda+1)$.

Step 4 Now call each tuple $S_i = (D_i \,.\, G)$, i = 1……..w a key space of size $(\lambda+1) * N$.

Step 5 Now compute the matrix $A_i = (D_i \,.\, G)^T$ of size $N * (\lambda+1)$. A_i (j) represents the j^{th} row of A_i.

Step 6 Divide the key space pool w into t*n key pools spaces $S_{i,i}$ (for i = 1,……..,t and j = 1,…………..,n), with $S_{i,j}$ corresponding to the deployment group $G_{i,i}$.

Step 7 Now each node select τ distinct key spaces from its corresponding key pool spaces $S_{i,j}$. For each space S_i selected by node j, we store the j^{th} row of A_i and this information is the secret information for a node.

B. Key agreement phase

After deployment, key agreement phase is carried out. In this phase, each node needs to be discover whether it share any space with its neighbors. To do this, each node broadcasts a message containing the following information: (1) the node's id, (2) the indices of the spaces it carries, (3) the seed of the column of G it carries.

Assume that nodes i and j are neighbors, and they have received the above broadcast messages. If they find out that they have a common space. Initially node i has $A_c(i)$ and seed for G(i), and node j has $A_c(j)$ and seed for G(j). After exchanging the seeds, node i can regenerate G(j) and node j can regenerate G(i); then the pairwise secret key between nodes i and j, $K_{ij} = K_{ji}$, can be computed in the following manner by these two nodes independently:

$$K_{ij} = K_{ji} = A_c(i) \cdot G(j) = A_c(j) \cdot G(i).$$

After secret keys with neighbors are set up, the entire sensor network forms the Key-Sharing Graph:
(Key-Sharing Graph): A Key-Sharing graph $G_{ks}(V,E)$ is constructed in the following manner: Let V represents all the nodes in the sensor network. For any two nodes i and j in V, there exists an edge between them if and only if (1) nodes i and j have at least one common key space, and (2) nodes i and j can reach each other within the wireless transmission range.

C. Path establishment phase

We now show how two neighboring nodes, i and j, who do not share a common key space could still come up with a pairwise secret key between them. The idea is to use the secure channels that have already been established in the key-sharing graph G_{ks}: as long as G_{ks} is connected, two neighboring nodes i and j can always find a path in G_{ks} from i to j. Assume that the path is i, v1, . . ., vt, j. To find a common secret key between i and j, i first generates a random key K. Then i sends the key to v1 using the secure link between i and v1; v1 sends the key to v2 using the secure link between v1 and v2, and so on until j receives the key from vt. Nodes i and j use this secret key K as their pairwise key. Because the key is always forwarded over a secure link, no nodes beyond this path can find out the key.

Setting Up Key Pools Spaces
In our scheme, we have:
1) Two horizontally or vertically neighboring key pools share exactly a|Sc| keys[2], where $0 \le a \le 0.25$.
2) Two diagonally neighboring key pools share exactly b|Sc| keys, where $0 \le b \le 0.25$ and $4a + 4b = 1$.
3) Two non-neighboring key pools share no keys.
Where a and b call overlapping factors.

Determine the Size Of Key Pool Space $|S_C|$
We calculate the size of the key pool space |Sc| for each group, given the size of the global key pool space w.

V. ANALYTICAL ANALYSIS

In our analytical analysis, we consider the following assumption:

- Number of nodes N in network is 5 and threshold value (compromised nodes) is 2. So, the size of generator matrix is 3×5.

Corresponding Author : *Sanchita Gupta*

- Number of w matrix is 6 (D_1…….. D_6).
  - The deployment area is 16*16 m^2.
  - The area is divide into a grid of size 4 = t*n = 2*2.
  - The center of each grid cell is the deployment point.

For instance, when w = 6, t = n = 10, a = 0.167 and b = 0.083, we have $|S_c|$ = 2. Therefore, the size of the key pool space for each group is maximum 2. After the key pools space are setup, for each sensor node in the deployment group $G_{i,j}$. We randomly select m keys from its corresponding key pool space $S_{i,j}$ and load those keys into the memory of the node. With the previous pairwise key pre-distribution scheme the size of the key pool space can be upto 6 that is more than twice the modified scheme. The value of N in the network can be larger as much as possible.

VI. CONCLUSION

We describe the pairwise key pre-distribution scheme that uses deployment knowledge. With such knowledge, each node only needs to carry a fraction of keys required by the other key pre-distribution schemes and reduce the usage of memory at any particular node.

REFERENCES

[1] N. Sugathi et al. "Secure key management for dynamic sensor networks", International journal of wireless communications and networking, vol. 3, no. 1, 2011, pp. 83-88.

[2] 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 Proceedings of IEEE INFOCOM 2004, pages 586-597, 2004.

[3] Wenliang Du et al. "A pairwise key pre-distribution scheme for wireless sensor networks", ACM transactions, October, 2003.

[4] H. Chan, A. Perrig, and D. Song., "Random key pre-distribution schemes for sensor networks", in IEEE Symposium on Security and Privacy, Pages 197-213, Berkeley, California, May 11-14 2003.

[5] 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.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks", IEEE Communications Magazine, 40(8):102–114, August 2002.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", in Proceedings of the 9th ACM conference on Computer and communications security, November 2002.

[8] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1996.

[9] B. C. Neuman and T. Tso, "Kerberos: An authentication service for computer networks", IEEE Communications, vol. 32, no. 9, pp.33-38, September 1994.

[10] W. Diffie and M. E. Helllman, "New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, pp. 644-654, November 1976.