Deterministic Key Distribution in Wireless Sensor Network using Finite Affine Plane

Nagendra Nath Giri,
Govt. Women's College,
Hassan-573201, INDIA

G. Mahadevan,
AMC Engineering College,
Bangalore-560077, INDIA

ABSTRACT

Security of large scale densely deployed and infrastructure-less wireless networks of resource limited sensor nodes requires efficient key distribution and management mechanisms. Key management is an important area of research in Wireless Sensor Networks (WSN), because resource constraints make security protocols difficult to be implemented. Key predistribution, a new combinatorial scheme for key distribution that makes use of finite plane. This gives rise to a new type of combinatorial design. Which involves preloading keys in sensor nodes, has been considered as the best solution when sensor nodes are battery powered and have to work unattended.

Key words- Security, Key Management, Affine plane,

1. Introduction

Wireless sensor networks consist of many tiny sensing devices, with very limited memory and power, and are scattered randomly in large numbers over a target area. The networks are used for both military and civilian purposes like monitoring seismic activities, ocean-water temperature, military surveillance, smoke detection, wild fire detection in forests, to name only a few. These sensor nodes communicate via radio waves within a certain range called Radio Frequency range. Sensor nodes work in a self organized way and are prone to adversarial attacks. So, secure communication is very important for many applications. Cryptographic keys can be established between two parties in many ways.

The conventional way using protocols like Kerberos [1] is expensive for sensor networks, which are resource constrained. The other method using public keys is being explored [2], [3] but not preferred because of costly operations involved. Key predistribution is a method to preload cryptographic keys in sensor nodes, even before they are deployed in the area of operation. It is a symmetric key approach, where two communicating nodes share a common secret key. The sender encrypts the message using the secret key and the receiver decrypts using the same key.

Key predistribution consists of three main algorithms:

1) Key assignment by a central authority before deployment

2) Shared-key discovery by a pair of nodes, after deployment and

3) Path-key establishment, establishing a path-key to communicate, when nodes do not have a common key.

2. Motivation

Wireless Sensor Network, consists of large number of sensor nodes having the capability of wireless communication, limited computation and sensing. WSN was initially developed for military and disaster rescue purposes but because of the availability of ISM band (2.4 GHz), the technology is now emerging in public applications. The salient features in Wireless Sensor Network makes it different from other network; self-organize, low power, low memory and low bandwidth for communication, large-scale nodes, self-configurable, wireless and infrastructure-less.

Therefore, WSN design must encounter these features in order to provide a reliable network. However each sensor node is equipped with its own sensor, processor and radio transceiver, so it has the ability of sensing, data processing and communicating with each other.

Past researches on sensor network routing have been focused on efficiency and effectiveness of data dissemination. Current routing protocols in sensor networks are susceptible to sinkhole attacks. This is because these protocols were not designed having security threats in mind. It has been proposed that a secure routing protocol against sinkhole attacks based on mobile agents in mobile wireless sensor networks.

The proposed protocol does not require encryption and authentication mechanisms. Moreover, it provides another route against such an attack. Recently, a critical component of research in the networking area has been Wireless Sensor Networks (WSNs). Numerous civilian and military applications are possible with wireless sensor networks. Towards this extent, a vast amount of theory in the realm of sensor deployment, data dissemination, sensor mobility, localization, tracking, security etc. have been developed by researchers.

3. Existing System

The existing system focus on randomized key distribution in which keys are assigned randomly from a large key pool and preloaded in the sensors. It was widely believed that randomized key distribution works better than deterministic key predistribution during adversarial attack but only with marginal factor.

3.1 Problem Identification

Key management is an important area of research in Wireless Sensor Networks (WSN), because resource constraints make security protocols difficult to be implemented. Key predistribution, using a new combinatorial scheme for key distribution that makes use of finite plane in Zq, where q is a prime number. A group of four points in a finite plane represent a node and the lines passing through these points represent the keys. This gives rise to a new type of combinatorial design. Which involves preloading keys in sensor nodes, has been considered as the best solution when sensor nodes are battery powered and have to work unattended.

4. Proposed System

To address the above problem and enhance connectivity and security, a deterministic key predistribution scheme in WSN is proposed, in which sensor nodes are deployed randomly. This scheme relies on affine planes for key predistribution. This scheme offers a better security to node compromise, than other deterministic predistribution schemes. It has the same storage requirements as other predistribution schemes for large networks of thousands of nodes.

It can be shown that this scheme performs better than non deterministic schemes when communication overheads are considered. In this paper it is proposed a new combinatorial scheme for key distribution that makes use of finite plane in Zq, where q is a prime number. A group of four points in a finite plane represent a node and the lines passing through these points represent the keys. This gives rise to a new type of combinatorial design. Then studying and comparing the connectivity and security of the proposed scheme with respect to existing schemes.

Studying the security of such a network in terms of two parameters. One of the parameters considers the proportion of nodes disconnected when a certain number of nodes are compromised. The other parameter considers the proportion of links broken under node compromise. The proposed design results in much better connectivity and resiliency compared to other schemes and shows that the connectivity and security results outperform all these schemes.

4.1 Key Predistribution.

Key predistribution is a method to preload cryptographic keys in sensor nodes, even before they are deployed in the area of operation. It is a symmetric key approach, where two communicating nodes share a common secret key. The sender encrypts the message using the secret key and the receiver decrypts using the same key.

Key predistribution algorithms are classified into two groups:

1) Deterministic key predistribution where the key assignment follows certain pattern and 2) Randomized key distribution, in which keys are assigned randomly from a large key pool and preloaded in the sensors. It was widely believed that randomized key predistribution results in high security during adversarial attacks. However, Xu et al [4] showed that randomized scheme perform only marginally better than deterministic schemes. The supporters of deterministic approach [5], [6] point out that the patterns used in key assignment, makes it simpler to find the common keys during the shared-key discovery phase.

A deterministic design using combinatorial structures called affine planes. Several deterministic schemes have been proposed in literature. Chan and Perrig [7] proposed PIKE. Combinatorial designs have been used in a number of designs like [8], [9], [10], [11], [12], [6]. A new combinatorial scheme for key distribution that makes use of finite plane in Zq, where q is a prime number. A group of four points in a finite plane represent a node and the lines passing through these points represent the keys. This gives rise to a new type of combinatorial design.

The comparative study of the connectivity and security of the scheme is given with respect to existing schemes. The security of such a network is in terms of two parameters. One of the parameters considers the proportion of nodes disconnected when a certain number of nodes are compromised. The other parameter considers the proportion of links broken under node compromise. It can be shown that proposed design's results is much better in connectivity and resiliency compared to [8], [10], [12], [13] .

5. Performance Metrics

These sections explain about the key Predistribution using finite affine plane and are evaluated by simulation. It illustrates the advantages of the scheme along with combinatorial design. To make a performance evaluation, several measurable metrics are defined.

5.1. Proportion of Nodes Disconnected

V (s) is defined as the proportion of nodes disconnected, when s nodes are compromised as given by the Eq 10.1. That is, if N is the total number of nodes in the network as in table 1.1 and t, the number of nodes disconnected when s nodes are compromised then,

V (s) =t/N – s……..Eq 10.1

It has been noted that no nodes are disconnected if the number of compromised nodes s is such that $s \leq (q+1)/4$. Experimental results of the values of V (s) are given in Table 1.1.

5.2 Proportion of Link Exposed

E(s) is defined as the fraction of links exposed when s nodes are compromised as shown in the figure 1.1. If t is the total number of links in the network as given by the Eq 10.2 before s nodes were compromised and x is the number of links after s nodes are compromised then,

E(s) = 1 –x/t……...Eq 10.2

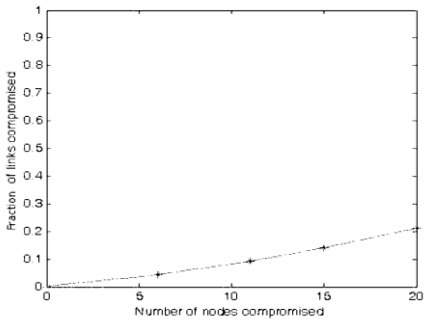

Fig 1.1 Experimental results for E(s)

6. Simulation Setup

The simulations experiments of wireless sensor networks and the performance evaluation of key predistribution using finite affine plane and compare them with non affine or random key distribution has been done. In this special topology, a node can only communicate with its direct neighbors. We can manually position both source and destination in the deployment area. The node with maximum number of nodes is selected as group leader. The group leader then sends the packet based on AODV algorithm. The same simulation is repeated for deploying N number of nodes. The average values of the performance metrics are calculated.

6.1 Simulation Results.

When comparing this scheme with non-deterministic schemes as shown in the figure 1.2, it can be seen that this scheme

requires computation of O(1), to calculate the shared keys, whereas non-deterministic schemes require O(k log k) (k is the number of keys per node) as in table 1.2. The communication expense is O(logN) in this scheme, whereas it is O(k log v) in case of non-deterministic schemes.

This is because the proposed scheme broadcasts only the node identifier, whereas the probabilistic schemes have to share key identifiers. Comparing the security of this scheme with the basic scheme of random key distribution. It can seen from Table 1.3 that the connectivity of the networks under different schemes. N represents the size of the network and k represents the number of keys. It is observed that, this scheme is highly secure compared to all of those schemes discussed earlier. This scheme requires more memory in this example. However for networks which deploy huge number of sensors, this scheme has O(logN) keys, which is the same as all the other schemes.

Table 1.1 -Experimental value of v (s), when n is the total number of nodes, s is the number of nodes compromised.

N	V(s)
870	1
870	0.98
1980	0.92
1980	0.86
1980	0.88
1980	0.89

Table 1.2-Experimental value of e(s), when n is the total number of nodes; s is the number of nodes compromised

N	Q	s	E(s)
870	59	5	0.068958
870	59	10	0.157406
1980	89	11	0.090639
1980	89	15	0.139159
1980	89	12	0.139159
1980	89	10	0.212303

Table 1.3-Schemes with parameters that chooses for comparisons and connectivity

Scheme	N	K	Full Connectivity
Basic [14]	2415	136	No
Camtepe-Yener [8]	2417	48	Yes
Linear [5]	2209	30	No
Quadratic [5]	2219	12	No
CMR [13]	2550	28	No
PBIBD I[12]	2415	136	Yes

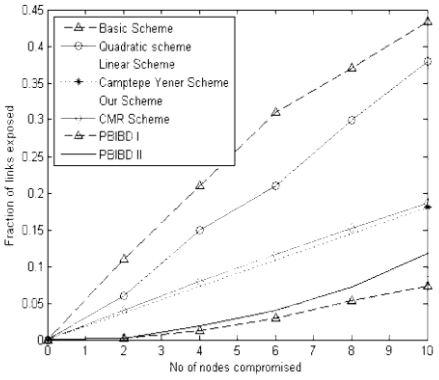

Fig. 1.2 Comparison of the fraction of links broken for different schemes

7. Conclusion

In this paper it is discussed a new key predistribution technique using combinatorial strategy. Key predistribution, which involves preloading keys in sensor nodes, has been considered as the best solution when sensor nodes are battery powered and have to work unattended. In deterministic key predistribution scheme in WSN, in which sensor nodes are deployed randomly. This scheme relies on affine planes for key predistribution. It offers a better security to node compromise, than other deterministic predistribution schemes.

This scheme has the same storage requirements as other predistribution schemes for large networks of thousands of nodes**.** Discussing some properties of this design, have proven a lower as well as an upper bound for the number of distinct keys in a particular node. Again a bound can be seen for the number of distinct keys between two separate nodes. Studying the resiliency of this design with respect to the model .Then comparing the experimental values of resiliency of the scheme with several deterministic schemes and shown that, it outperforms them. Then an algorithm for shared key discovery that works in time O(1) is provided.

8. Future Enhancement

The concept of key predistribution can be expanded in several directions. A simple method for clubbing 4 points for any node N is used. In future it can generalize this to clubbing arbitrary number of points. If Clubbing more points, then the size of the key ring will increase through the resilience to compromise will be stronger. It is important to find the optimal number of points being clubbed. Further research can be done to invent efficient clubbing technique. This scheme can be extended from Zq to GF(qm) where m is a positive integer.

9. References

[1] J. Evans, D. Raychaudhuri, and S. Paul, "Overview of Wireless, Mobile and Sensor Networks in GENI," GENI Design Document 06- 14, Wireless Working Group, 2006.

[2] S. Olariu and I. Stojmenovi_c, "Design Guidelines for Maximizing Lifetime and Avoiding Energy Holes in Sensor Networks with Uniform Distribution and Uniform Reporting," Proc. IEEE INFOCOM, 2006.

[3] Ian F. Akyildizon, Weilian Su, Yogesh Sankasubramanium and Erdal Cayirici, A Survey on Sensor Networks, IEEE communications Magazine, August 2002, pp 102 - 114

[4] H. Zhang and H. Shen, "Balancing Energy Consumption to Maximize Network Lifetime in Data-Gathering Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 10, pp. 1526-1539, Oct. 2009.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy- Efficient Communication Protocols for Wireless Micro sensor Networks," Proc. Hawaiian Int'l Conf. Systems Science, 2000.

[6] O. Younis and S. Fahmy, "HEED: A Hybrid, Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks," IEEE Trans. Mobile Computing, vol. 3, no. 4, pp. 366-379, Oct.-Dec. 2004.

[7] M. Singh and V. Prasanna, "Energy-Optimal and Energy-Balanced Sorting in a Single-Hop Wireless Sensor Network," Proc. First IEEE Int'l Conf. Pervasive Computing and Comm., 2003.

[8] H. Lin, M. Lu, N. Milosavljevic, J. Gao, and L.J. Guibas, "Composable Information Gradients in Wireless Sensor Networks," Proc. Seventh Int'l Conf. Information Processing in Sensor Networks (IPSN), pp. 121-132, 2008.

[9] Y. Xu, J. Heidemann, and D. Estrin, "Geography-Informed Energy Conservation for Ad-Hoc Routing," Proc. ACM MobiCom, 2001.

[10] V. Rodoplu and T.H. Meng, "Minimum Energy Mobile Wireless Networks," IEEE J. Selected Areas in Comm., vol. 17, no. 8, pp. 1333- 1344, Aug. 1999.

[13] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. ACM MobiCom, 1999.

[11] D.H. Armitage and S.J. Gardiner, Classical Potential Theory. Springer, 2001.

[12] C. Schurgers and M. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks," Proc. Military Comm. Conf. (MILCOM), 2001.

[13] K. Kalpakis, K. Dasgupta, and P. Namjoshi, "Maximum Lifetime Data Gathering and Aggregation in Wireless Sensor Networks," Proc. IEEE Int'l Conf. Networking (ICN), pp. 685-696, 2002.

[14] D.H. Armitage and S.J. Gardiner, Classical Potential Theory. Springer, 2001.