ISSN 2320 - 2602

International Journal of Advances in Computer Science and Technology (IJACST), Vol.2 , No.5, Pages : 17-20 (2013)
Special Issue of ICACSIT 2013 - Held during 09-10 May, 2013 Malaysia

Efficient Modified Blom Scheme for Key Management in Wireless Sensor Networks

Vishal Gupta[1], M. N. Doja[2], Charu Gupta[3]

[1]Jamia Millia Islamia, Faculty of Engineering, Department of Computer Science, Delhi, India. Email : vishalg26@rediffmail.com

[2]Jamia Millia Islamia Faculty of Engineering, Department of Computer Science, Delhi, India. Email : mndoja@gmail.com

Assistant Professor, SSITM, Aligarh, India. Email: charugupta.mtech@gmail.com

Abstract: Security is an inevitable part in this world. Security plays an important role for applications of WSNs due to the vulnerability of the network. Key management has become one of the main requirements in the field concerned with security of sensor network. Key is required for establishing a secure communication link between the nodes ready for transmitting data. Due to increased interests in sensor network, establishing a secure link between communicating nodes has become a prime area of concern. In this paper we have discussed one of the prominent key management schemes, its modified version and then proposed our own computation efficient key management scheme.

Keywords: Wireless Sensor Network, Security, Key, Vandermonde matrix, Hadamard matrix

INTRODUCTION

Sensor network is the network of various tiny electronic devices called sensor nodes that are capable of sensing the environmental conditions. The sensor network also stores the sensed data and communicates this data to other nodes as well. Sensor networks find a wide variety of applications in the real world as they are designed to sense environmental conditions such as temperature, pressure, humidity, sound, vibration, fog levels and monitor pollution levels, fire alerts [2] and the list is endless.

A sensor network consists of mainly of the following: Sensor nodes - the electronic devices designed to sense various environmental conditions, Micro-controller - electronic device which is used to interface with the sensor nodes, radio transceiver - used to transmitting and receiving the data via internal or external antenna, energy source – a battery to provide energy for the working of sensor nodes and other components of sensor network [1].

Different key distribution schemes that exist are (1) Network keying (2) Pair Wise keying (3) Group Keying [6]. Out of these three, pair wise keying is best in terms of robustness and authentication as well as storage efficiency.

We have proposed a key management scheme that is based on the scheme of Blom [11] and also an improvement on the scheme proposed by Reddy [12].

The rest of the paper is organized as follows: section (II) summarizes the various requirements for WSNs, section (III) summarizes the various constraints on security provisioning in WSNs, section (IV) summarizes the related work on key management in WSNs, section (V) discusses our proposed work, and section (IV) provides the analysis of our proposed scheme. Finally the paper ends with the conclusion.

SECURITY REQUIREMENTS IN SENSOR NETWORK

The various security requirements to sensor networks include the following [3] [4]:

A. **Integrity:** Integrity refers to unmodified data. Data integrity ensures that the data received is not altered or modified by any adversary and is same as the data sent by the sender node. Integrity of data is achieved by using various cryptographic methods.

B. **Authentication:** It is important as the receiving node must be ensured that the received is from a trusted source and not from the adversary.

C. **Confidentiality:** The data being sent should be received only by the intended receiver and should not be exposed to any other node. Hence data travels in a highly secure and encrypted mode.

D. **Availability, Reliability and resiliency:** It ensures proper connectivity of the nodes and that the data and information is available to access at all times whenever and wherever required by the authorized nodes. This ensures protection from attacks such as denial of service attacks etc. It also ensures that the data packet is delivered to its destination.

E. **Data freshness:** Data freshness ensures that the data and information being delivered is fresh and recent. This is one of the most important security aspects as the adversary can send old message and thereby the recently detected data is not communicated.

CONSTRAINTS ON SECURING THE SENSOR NETWORK

Sensor networks provide a powerful technology to monitor and control the physical environment. However it too has some limitations that need to be overcome before to improve its potential to perform better in terms of accuracy, reliability and security. Some of the limitations [5] are:

A. **Energy:** Sensor network consists of tiny sensors which run on batteries. These batteries have limited

International Journal of Advances in Computer Science and Technology (IJACST), Vol.2 , No.5, Pages : 17-20 (2013)
Special Issue of ICACSIT 2013 - Held during 09-10 May, 2013 Malaysia

power supply. Hence there comes the need to conserve energy and transmit data efficiently without consuming much energy.

B. **Computation:** Due to energy constraints, sensors are also limited by low computational capacity. Hence algorithms which require large computations must be avoided to incorporate in sensor networks.

C. **Communication:** Sensors are linked via wireless connection and therefore, the bandwidth is often limited. This also limits the transmission of data and information.

RELATED WORK

Key management protocols can be based on either symmetric or asymmetric management functions. But due to the scarcity of the resources, protocols based on public keys are inefficient. Hence, symmetric algorithm based key management schemes are favored in WSNs [14].
Key management in sensor network includes [6]

1) Key set up: It is a process of generating keys by a central authority or by individual nodes.
2) Key distribution: It refers to the distribution of keys among the sensor nodes in case key is set up by a central authority.
3) Key revocation: It is the process of removing the key from nodes after the data has been transmitted or after a fixed interval of time.

Different key management protocols proposed on pair wise keying can be summarized as below [12]:

1) Eschenauer and Gligor [7] proposed a probabilistic key distribution scheme based on pair wise keying. Though it is robust and require less storage it suffers from less authentication, low accessibility with no support to cluster operations. [6]
2) Chan, Perrig and Song [8] proposed a q-composite random key pre-distribution scheme. This scheme achieved security under small scale attack while trading off increased vulnerability in the face of a large scale physical attack on network nodes.
3) Du, Dang, Han and Varshney [9] proposed a multi space key pre-distribution scheme where it used a number of private matrices instead of one and k key matrices in each node.
4) In SPINS, proposed by Perrig et al, each sensor node shares a secret key with the base station. To establish a new key, two nodes use the base station as a trusted third party to set up the new key.

Apart from these many other schemes have been proposed such as LEAP, SHELL, Heirarchial scheme by Panja et al and so on.

Blom's Scheme [11]: Blom presented a symmetric key generation system (SKGS) based on MD5. In a network of n users, where k users have to co-operate to get information, the public matrix P (n, k) over GF is known to all. The central authority chooses a symmetric secret matrix and computes the key and distribute to all users. Public matrix is constructed using linear Vandermonde matrix [12].

Reddy's scheme [12]: Instead of using Vandermonde matrix, [12] proposed to use a non–binary Hadamard's matrix as the public matrix.
A Hadamard Matrix is a square matrix with values 1s and -1s. It reduces the complexity of calculating values of all the elements corresponding to the columns in Vandermonde matrix. Reddy used the same matrix by replacing the value of -1 with a large prime number p-1.

PROPOSED SCHEME

We have proposed a key management scheme that is based on the scheme of Blom [11] and also an improvement on the scheme proposed by Reddy [12].

Motivation: Sparse Matrix with greater number of zeroes has lesser computation. Hence to reduce the computation and storage head further we proposed a newer scheme based on sparse matrix.

Proposed Scheme: In the public matrix as chosen by taking **t** (secure parameter) **rows** from an N x N Hadamard matrix which contains 1 and -1, we convert it into a sparse Hadamard matrix H, with the following modification:

- The values 1s replaced by 0, And
- The entries -1 replaced by q-1 (modulo q) as proposed by Reddy, Where p is a large prime number greater than the number of nodes in a network.

The rest of whole Blom's scheme and its modified version by Reddy remain same as described by [12].

Example: The following example shows the working of our scheme - the sparse Hadamard matrix. Let the number of nodes in the network be 8, secure parameter t = 6 and prime number (q) = 31.

Hadamard Matrix:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Modified Hadamard Matrix (by Reddy):

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 30 & 1 & 30 & 1 & 30 & 1 & 30 \\ 1 & 1 & 30 & 30 & 1 & 1 & 30 & 30 \\ 1 & 30 & 30 & 1 & 1 & 30 & 30 & 1 \\ 1 & 1 & 1 & 1 & 30 & 30 & 30 & 30 \\ 1 & 30 & 1 & 30 & 30 & 1 & 30 & 1 \\ 1 & 1 & 30 & 30 & 30 & 30 & 1 & 1 \\ 1 & 30 & 30 & 1 & 30 & 1 & 1 & 30 \end{pmatrix}$$

International Journal of Advances in Computer Science and Technology (IJACST), Vol.2 , No.5, Pages : 17-20 (2013)
Special Issue of ICACSIT 2013 - Held during 09-10 May, 2013 Malaysia

Sparse Hadamard Matrix (Proposed):

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 30 & 0 & 30 & 0 & 30 & 0 & 30 \\ 0 & 0 & 30 & 30 & 0 & 0 & 30 & 30 \\ 0 & 30 & 30 & 0 & 0 & 30 & 30 & 0 \\ 0 & 0 & 0 & 0 & 30 & 30 & 30 & 30 \\ 0 & 30 & 0 & 30 & 30 & 0 & 30 & 0 \\ 0 & 0 & 30 & 30 & 30 & 30 & 0 & 0 \\ 0 & 30 & 30 & 0 & 30 & 0 & 0 & 30 \end{pmatrix}$$

Public Matrix (P):

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 30 & 0 & 30 & 0 & 30 & 0 & 30 \\ 0 & 0 & 30 & 30 & 0 & 0 & 30 & 30 \\ 0 & 30 & 30 & 0 & 0 & 30 & 30 & 0 \\ 0 & 0 & 0 & 0 & 30 & 30 & 30 & 30 \\ 0 & 30 & 0 & 30 & 30 & 0 & 30 & 0 \end{pmatrix}$$

Let the secret symmetric matrix (S) be:-

$$S = \begin{pmatrix} 3 & 11 & 15 & 28 & 7 & 5 \\ 11 & 30 & 4 & 1 & 2 & 8 \\ 15 & 4 & 6 & 14 & 18 & 21 \\ 28 & 1 & 14 & 17 & 25 & 6 \\ 7 & 2 & 18 & 25 & 27 & 9 \\ 5 & 8 & 21 & 6 & 9 & 8 \end{pmatrix}$$

$A = (S.P)^T$

$$S.P = \begin{pmatrix} 0 & 1320 & 1290 & 930 & 360 & 1380 & 1650 & 990 \\ 0 & 1170 & 150 & 1260 & 300 & 990 & 450 & 1080 \\ 0 & 1170 & 600 & 930 & 1170 & 1080 & 1770 & 840 \\ 0 & 720 & 930 & 630 & 930 & 1290 & 1860 & 1200 \\ 0 & 1080 & 1290 & 870 & 1080 & 1620 & 2370 & 1410 \\ 0 & 660 & 810 & 1110 & 510 & 690 & 1320 & 1140 \end{pmatrix} \text{ mod } 31$$

$$A = (S.P)^T = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 23 & 23 & 7 & 26 & 9 \\ 19 & 26 & 11 & 0 & 19 & 4 \\ 0 & 20 & 0 & 10 & 2 & 25 \\ 19 & 21 & 23 & 0 & 26 & 14 \\ 16 & 29 & 26 & 19 & 8 & 8 \\ 7 & 16 & 3 & 0 & 14 & 18 \\ 29 & 26 & 3 & 22 & 15 & 24 \end{pmatrix}$$

Now, suppose node 4 and 6 want to communicate. Then the key used by both will be:

$$K_{4,6} = A_4.P_6$$

$$= [0\ 20\ 0\ 10\ 2\ 25] \begin{pmatrix} 0 \\ 30 \\ 0 \\ 30 \\ 30 \\ 0 \end{pmatrix}$$

$$= 960 \bmod 31 = 30$$

$$K_{6,4} = A_6.P_4$$

$$= [16\ 29\ 26\ 19\ 8\ 8] \begin{pmatrix} 0 \\ 30 \\ 30 \\ 0 \\ 0 \\ 30 \end{pmatrix}$$

$$= 1890 \bmod 31 = 30$$

Thus we observe that both the nodes generate a common pair-wise key that will be use for communication.

Now if we compare our scheme with that of Blom's, we observe that we can reduce computation time by eliminating operations on zero elements. Also if we follow the steps of Blom's scheme to pre allocate each of the columns of public matrix (Hadamard matrix) to different nodes according to their index then we can reduce space requirements by taking advantage of the properties of sparse matrix. In Blom's scheme, we require a space proportional to t to save the column of the public matrix in the node where as in our scheme; we require the space proportional to the number of non-zero elements in that column. To add, we only need to store the row index numbers as the non-zero value is fixed i.e. (q-1).

If we compare our scheme to that of Reddy's that favors to generate the public matrix at the node itself rather than storing it in advance, then too our scheme takes the advantage by reducing computation time by eliminating operations on zero elements.

ANALYSIS

Converting the public matrix to a sparse matrix by replacing nearly half of its elements with **0** serves the following purposes:-

1. Using sparse matrix to store data that contains a large number of zero-valued elements can both save a significant amount of memory and speed up the processing of that data.
2. Store only the nonzero elements of the matrix, together with their indices. Thus, Number of bytes of memory stored is much less in sparse matrix**.**
3. In this case, we require even more reduced space proportional to non-zero elements in that column. To add, we only need to store the row index numbers as the non-zero value is fixed i.e. (q-1).
4. Reduce computation time by eliminating operations on zero elements.

CONCLUSION

Our scheme enhances Blom's scheme by minimizing the storage required by using a modified sparse Hadamard matrix & eliminates the run time generation of public matrix to save the computational time & computational energy of the energy scarce sensor nodes.

International Journal of Advances in Computer Science and Technology (IJACST), Vol.2 , No.5, Pages : 17-20 (2013)
Special Issue of ICACSIT 2013 - Held during 09-10 May, 2013 Malaysia

REFERENCES

[1] S.R. Murthy, B.S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocol*, 1st ed. Pearson Education, 2004, ch. 12 Wireless Sensor Networks.

[2] A. Habib, " Sensor Network Security Issues at Network Layer", in 2nd International Conference on Advances in Space Technologies Islamabad, Pakistan, 29th – 30th November 2008.

[3] A. Perrig,, R. Szewczyk, V. Wen, D.Culler, J.D. Tygar , " SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences University of California, Berkeley, Wireless Networks , 2002, pages 521-534.

[4] E. Stavrou, A. Pitsillides, G. Christoforos Hadjicostis, " Security in future mobile sensor networks-Issues and challenges", Department of Electrical and Computer Engineering, University of Cyprus.

[5] J. Kulik, W. Rabiner, H. Balakrishnan, " Adaptive protocols for Information Dissemination in Wireless Sensor Network" , Massachusetts Institute of Technology Cambridge.

[6] J.C. Lee, V.C.M. Leung, K.H. Wong, J. Cao, H.C.B. Chan, " Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments",in IEEE Wireless Communications, October 2007.

[7] L. Eschenauer, V. Gligor, "A key management scheme for distributed sensor networks", in ACM CCS2002, Washington D.C 2002.

[8] H. Chan, A. Perrig, D. Song, " Random key pre-distribution schemes for sensor networks", in proceedings of the 2003 IEEE Symposium on Security and Privacy, May 11-14, 2003, p. l97.

[9] W. Du, J. Deng, Y. S. Han, S. Chen, P. K. Varshney, " A key management scheme for wireless sensor networks using deployment knowledge" , in IEEE INFOCOM 2004, Hong Kong, March 2004.

[10] A. Perrig,, R. Szewczyk, V. Wen, D.Culler, P.K. Tygar , "SPINS: Security protocols for sensor networks", in *Seventh Annual ACM International Conference on Mobile Computing and Networks (MobiCom 2001)*, July 2001.

[11] R. Blom, " An optimal class of symmetric key generation systems", in: *Proc. Of EUROCRYPT* '84, pages 335-338.

[12] Rohithi Singh Reddy, "Key management in wireless sensor networks using a modified Blom scheme", arXiv:1103.5712.

[13] Documentation of sparse matrix by Matlab Inc. (2010 b).

[14] G.J. Pottie, W. J. Kaiser, "Wireless Integrated Network Sensors", in communications of the ACM, 2000, vol 43(5) pages 51-58.