ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Survey on Various Matrix Based Key Management Scheme in WSN.

S Abinaya*, B Kiruthika, R Ezhilarasie, and A Umamakeswari.

School of Computing, SASTRA University, Tirumalaisamudram, Thanjavur-613401, Tamil Nadu, India.

ABSTRACT

Wireless Sensor Network (WSN) involves sensor nodes, deployed for monitoring the hostile environment in which the sensor nodes are spatially. The sensor nodes communicates with each other and exchanges information about the environment. Securing this information is one of many issues in WSN. It requires a secuirty mechanism using a secret key to protect the data. This is focused as the prime factor for surveying the various key management schemes Though many metrics are there for evaluating KMS, Key Connectivity plays a vital role. Since most matrix based scheme establish 100% connectivity this paper presents a comparison analysis on various matrix based key management schemes for WSN.

Keywords: Wireless sensor network (WSN), Key Management Scheme (KMS), Probabilistic, Matrix.

**Corresponding author*

INTRODUCTION

Wireless sensor networks (WSN) consists of sensor nodes that are arranged in a random manner. These sensors monitor and gather information about the deployed environment and transmit data to a base station or to other nodes in the network [1]. These nodes possess less processing and computation capabilities. Primarily, WSN are mainly utilized for military surveillance later they were extended to serve for commercial applications such as medical and environmental monitoring, machinery monitoring in manufacturing applications, home automation, traffic control, etc. The sensor nodes in these environments are subject to periodical surveillance. In many cases WSN is deployed in hostile environments so the security of WSN becomes a common concern. It becomes an easy task for an attacker to obtain the information exchanged in the network. In order to protect this information, various cryptographic techniques are used. These cryptographic techniques often involve a key used as a seed to mask the information transferred in the network. The data obtained as a result of these techniques proven to be secure. However, maintaining the key used for encryption is the major concern. Key Management is a method for establishing and maintaining the key relation between authorized parties in the network involved in cryptography. Secured communication between the nodes can be obtained by implementing KMS.

KMS can be implemented in two ways: Symmetric and Asymmetric Key Management Scheme [1,2]. The key used in symmetric method is unique between sender and receiver, whereas in asymmetric method, public key is used for encryption and private key is used for decryption. Since sensor nodes are resource constrained deploying asymmetric method is difficult, so most of the KMS is concentrating on symmetric methodology. Based on the symmetric based communication style the KMS in general classified as:

- Network wide key based method- Single key is used throughout the network.
- Pairwise key based method - For a network containing of N nodes, each node store (n-1) distinct keys
- Probabilistic key based method-Nodes are distributed with a subgroup of keys from a key pool. To establish a communication between sensor nodes, the initiating node has to broadcast the key. The nodes communicate only if the key matches at the receiving node. It requires less number of keys than the keys required for the pair wise method
- Combinatorial key based method- Direct or indirect key path is established among the nodes by combinatorial theorem [1].
- Matrix key base method- A key is generated based on two matrices, of which one is public and the other is private.

SURVEY ON MATRIX BASED KEY MANAGEMENT SYSTEM

For any KMS, achieving a good key connectivity is more complex than generating and distributing an efficient key. The key connectivity depends on the number of keys stored in each node. For a higher number of keys, the probability [3] of key connectivity is high. As the pairwise key method stores n-1 keys in each node, it provides better connectivity than other method such as probabilistic method which stores keys in high number but comparatively lesser than pairwise scheme. Considering the factor that all the nodes in the wireless sensor networks are resource constrained, the performance of the above methods is poor. In order to overcome this, matrix based schemes are proposed which takes less storage and less computation to establish a symmetric key between the nodes. In general matrix schemes are performed on symmetric matrices. Various matrixes based KMS are: Blom's scheme and LU decomposition.

BLOM'S SCHEME

Blom's scheme is the first matrix based KMS. Any node that wants to communicate with other nodes in the network will split the keying information and distribute among the nodes. In this scheme two matrixes are used, one with public information and the other one are private. A symmetric key is established between two nodes with the use of matrixes.

CONSTRUCTION OF BLOM'S SCHEME:

Blom's scheme [4] is a Symmetric Key

Generation System (SKGS). Any node in a network will interact with any other node with less information. This scheme is a threshold secret sharing method.
Construction of Blom's scheme explained as below,

Step 1: Construct a private symmetric matrix $D_{\lambda,\lambda}$over a GF (q) is the power of prime
For example assume λ =5 , then $D_{5,5}$ is :

$$D = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 7 & 5 \\ 3 & 3 & 5 & 6 & 7 \\ 4 & 7 & 6 & 1 & 2 \\ 5 & 5 & 7 & 2 & 1 \end{pmatrix}$$

Step 2: Construct a public matrix $G_{\lambda,\ N}$ over GF(q). In general G matrix is of type Vandermonde which is of the form:

$$G = \begin{bmatrix} 1 & \cdots & 1 \\ s & \ddots & s^N \\ s^\lambda & \cdots & (s^N)^\lambda \end{bmatrix}$$

For Eg., if seed S = 2, then the matrix G is

$$G= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 2 & 4 & 8 & 16 & 32 & 64 \\ 4 & 16 & 64 & 256 & 1024 & 4096 \\ 8 & 64 & 512 & 4056 & 32768 & 262144 \\ 16 & 256 & 4096 & 65536 & 1048576 & 16777216 \end{pmatrix}$$

Step 3: Compute the private matrix as $A = (D.G)^T$

$$\text{For example } A= \begin{pmatrix} 129 & 158 & 189 & 82 & 75 \\ 1593 & 1794 & 2271 & 704 & 521 \\ 227370 & 24290 & 32091 & 9148 & 5613 \\ 344865 & 357186 & 484659 & 136820 & 5613 \\ 5377089 & 5475458 & 7541851 & 2136292 & 1121465 \\ 84947073 & 75733634 & 119034051 & 33841604 & 17330501 \end{pmatrix}$$

Step 4: Key pre deployment phase:

Load each sensor node with a row from A matrix and also the seed value S to generate the column of G matrix.

Step 5: Key agreement phase:

Each sensor node transmits its seed to the neighboring node which wants to communicate and thereby the sensor nodes compute the column itself and generate the symmetric key with the help already preloaded row value of A matrix and the regenerated column value is shown in figure 1.

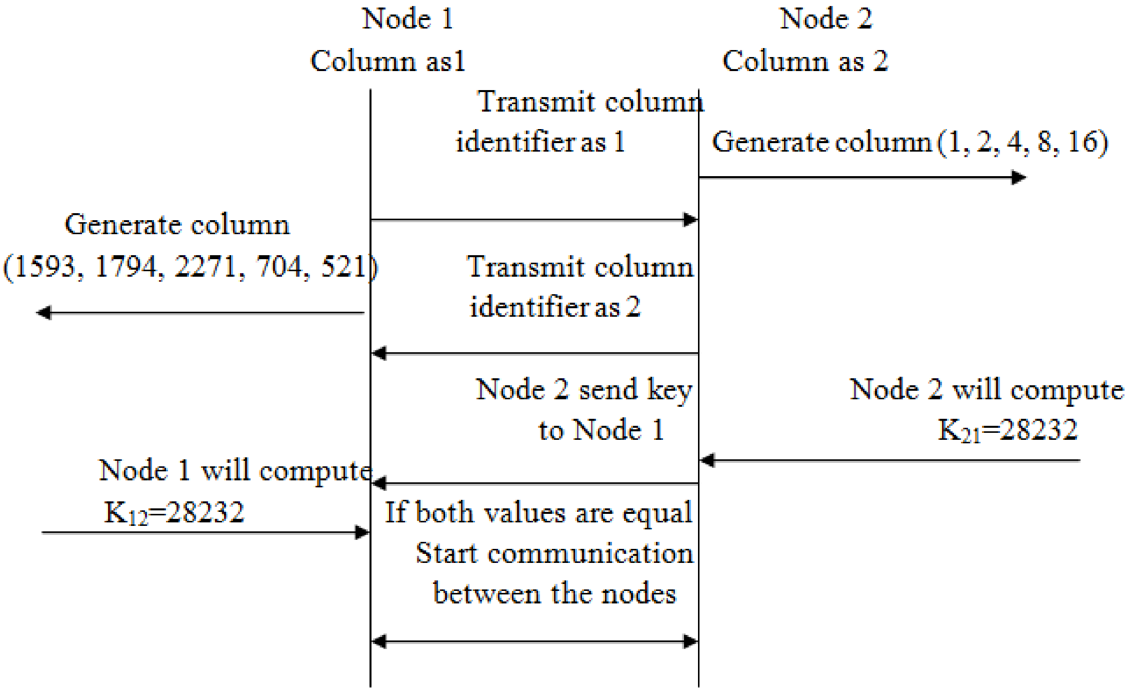
Node 1
Column as1
Node 2
Column as 2
Transmit column identifier as 1
Generate column (1, 2, 4, 8, 16)
Generate column (1593, 1794, 2271, 704, 521)
Transmit column identifier as 2
Node 2 send key to Node 1
Node 2 will compute K21=28232
Node 1 will compute K12=28232
If both values are equal Start communication between the nodes

Figure1: Key generation for Blom's scheme

The advantage of Blom's scheme [4]: since it generates pairwise key node authentication and revocation are easy this scheme provides 100% key connectivity between nodes. The drawback of Blom's scheme is a threshold (λ) secret sharing method i.e., up to λ nodes the attacker cannot recover any keys from the other nodes. If more than λ nodes are captured the attacker can recover any keys in the network. So while choosing λ it has to be large enough, but parallely affects the storage cost.

MULTI SPACE KEY DISTRIBUTION SCHEME

The single symmetric matrix is used for the entire network to establish the symmetric key between the nodes i.e.,.Single key space method in Blom's scheme [5]. When the attacker captures more than a threshold the whole network is revealed. To overcome this Multi Space key distribution scheme is proposed where multiple symmetric matrices D_1, D_2, $D_{3\ldots\ldots}$ D_n is generated and matrix A_1, A_2, $A_{3\ldots\ldots}A_n$ are computed. From the key spaces, load ω key spaces (ω rows) and key space identifier into the node. The nodes which want to communicate will broadcast the key space identifier. The node which shares the common key space will communicate each other. The advantage of this scheme is attaining security at the cost of storage and communication overheads. Scalability is a big issue with matrix based scheme because the number of nodes is fixed prior to the determination of the matrix size.

Chen et al.,suggested a key management scheme for cluster [6] architecture using Blom's scheme. The reason to go for clusters is because of the limited resources in nodes. The cluster head will have more resources when compared to sensor nodes. The base station which takes entire control of the network have unlimited resources. It is assumed that the range of communication for all the sensor nodes will reach the cluster heads. This scheme gets both key pre distribution phase and key agreement phase. In key pre distribution phase, we have to assign the key information to each sensor node. After the nodes are deployed it will find the secret key between the nodes. Each sensor node will directly communicate with the cluster head. It communicates with other cluster heads to share the information. In key agreement phase, each node will establish the key using inter cluster and an intra cluster key mechanism. In inter cluster mechanism cluster head share the key with other cluster head and for intra cluster mechanism the key is established between each nodes and cluster head. Disadvantage of this scheme is when cluster head compromised the number of rekeying message to connect the orphan sensor node to another cluster head is more.

Zhang and Wang proposed ID based Pairwise key pre distribution [7] scheme is using Blom's scheme. In this scheme the network is divided into zones. For each zone symmetric matrix is generated. In key pre distribution phase the nodes are loaded with the row and identifier of the symmetric matrix. The nodes which share the same symmetric matrix identifier will communicate each other.

Mesh topology [8] is another way used to secure the information using Blom's scheme. In this method by using the pair of mesh the client will directly establish key in pairwise manner, and will compare with other matrix which will secure the information using mesh structure. Therefore the client will access the network using mesh network, during the setup phase λ and it is used for security and M=PQ for node to node communication. It selects a secure key from independent key S1, S2, S3………Sn and computes $A=(D.G)^T$ where G is the secure matrix and A is public symmetric matrix. After which it establishes the pairwise key between the two nodes. Connectivity is high, but storage and communication network is low.

RohithSingi Reddy proposed KMS to diminish the reckoning and memory overhead in Blom's scheme. As opposed to utilizing Vandermonde network [9], a method utilizing non-parallel Hadamard lattice is used as shown in fig 3

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

Figure 2. ParallelHadamard

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

Figure 3. Non ParallelHadamard

The original parallel Hadamard is shown in fig 2. As, the Hadamard lattice is a square grid with 1s and -1s, it lessens complexity for computing for all the components in Vandermonde network. It also reduces the storage requirements for saving the columns as the Hamdamard network [4] generates column of known size . The operation depends on the prime number that provides the required key length as that of the Blom's scheme.

Generating pair wise keys and providing authentication for nodes at the deployment phase and are few properties of Blom's scheme. In addition, it provides better connectivity and the resilience can be refined by selecting appropriate parameters.

LU DECOMPOSITION

LU decomposition matrix based key distribution technique suitable for large-scale sensor networks. In wireless sensor networks this scheme provides comprehensive analysis in terms of network resilience, scalability and overhead. It also improves the network initializing stage by establishing the pairwise key. The LU decomposition solves the linear equation, A=LU where A is the product of both L and U, L is Lower triangular Matrix, U is Upper triangular Matrix

$$\begin{bmatrix} l_{11} & \cdots & 0 \\ \vdots & \dots & \vdots \\ l_{1n} & \cdots & l_{nn} \end{bmatrix} \begin{bmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & u_{nn} \end{bmatrix} = \begin{bmatrix} k_{11} & \cdots & k_{1n} \\ \vdots & \ddots & \vdots \\ k_{1n} & \cdots & k_{nn} \end{bmatrix}$$

This decomposition simplifies solution because of a triangular matrix. LU matrix assures that pairwise key is shared between two nodes and it provides by using the secret information assigned from the lower and upper triangular matrices. All the keying information shared between the different nodes is distinct from each other.

Steps to construct the symmetric matrix A,

Step 1: Construct lower triangular matrix using the key from the key pool GF (q).

$$L= \begin{pmatrix} 96 & 0 & 0 & 0 & 0 \\ 118 & 209 & 0 & 0 & 0 \\ 155 & 31 & 193 & 0 & 0 \\ 199 & 138 & 75 & 108 & 0 \\ 178 & 54 & 190 & 51 & 47 \end{pmatrix}$$

Step 2: Based on the assumption that product of L and U yields symmetric matrix, the upper triangular matrix U is generated as follows

$l_{11}.u_{11} = k_{11}$; $l_{11}.u_{12} = k_{12}$; $l_{11}.u_{13} = k1_3$; $l_{21}.u_{11} = k_{21}$; $l_{31}.u_{11} = k_{31}$
$l_{21}.u_{12} + l_{22}.u_{22} = k_{22}l_{21}.u_{13} + l_{22}.u_{23} = k_{23}l_{31}.u_{12} + l_{32}.u_{22} = k_{32}$
$l_{31}.u_{13} + l_{32}.u_{23}+ l_{33}.u_{33} = k_{33}$

Since K is symmetric, K_{ij} will be equal to K_{ji}

$k_{12} = k_{21} = l_{11}.u_{12} = l_{21}.u_{11} \Rightarrow u_{12} = (l_{21}.u_{11}) / l_{11}$
$k_{13} = k_{31} = l_{11}.u_{13} = l_{31}.u_{11} \Rightarrow u_{13} = (l_{31}.u_{11}) / l_{11}$
$k_{23} = k_{32} = l_{21}.u_{13} + l_{22}.u_{23} = l_{31}.u_{12} + l_{32}.u_{22} \Rightarrow u_{23} = (l_{31}.u_{12} + l_{32}.u_{22} - l_{21}.u_{13}) / l_{22}$

$$U_= \begin{pmatrix} 209 & 257 & 337 & 433 & 386 \\ 0 & 236 & 35 & 156 & 61 \\ 0 & 0 & 60 & 23 & 59 \\ 0 & 0 & 0 & 6 & 3 \\ 0 & 0 & 0 & 0 & 8 \end{pmatrix}$$

Step 3: Randomly generate the values for u_{11}, u_{22}, u_{33} and compute the remaining elements in a U matrix

Step 4: Pre deployment phase: Load the sensor node with row from the L matrix and corresponding column from the U matrix.

Step 5: Key agreement phase: the node which wants to communicate transmits its column and symmetric key is generated is shown in figure 4.

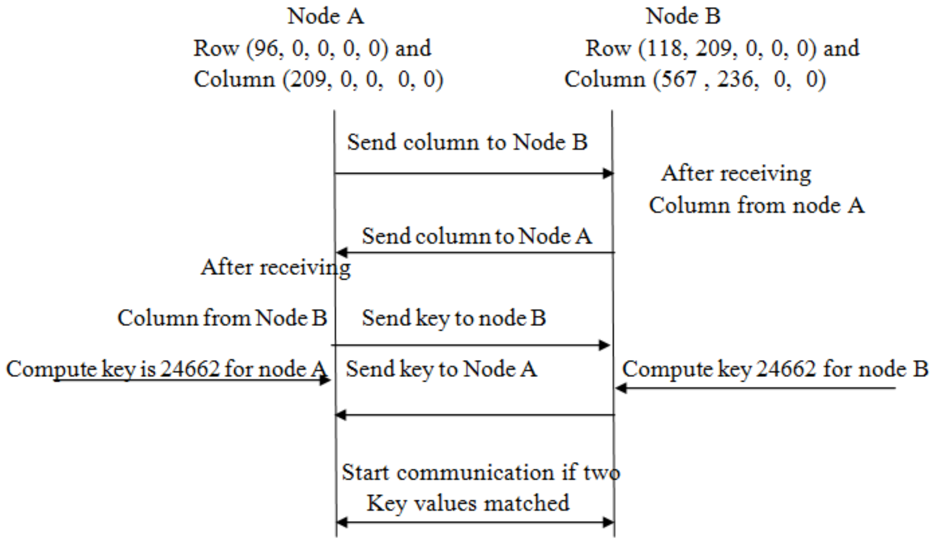

Figure 4: Key Generation using LU decomposition

Eric Ke Wang and Yunming Ye proposed effective and secure [10] key pre distribution using LU matrix scheme provides the mutual authentication between the pairwise nodes. Integrated along with Elliptic Curve and Diffie- Hellman technique, it is used to secure the key path establishment by using tree based LU matrix. LU composition key exchange protocol is used for group key agreement and management using tree based LU matrix. The row is assigned i for A matrix in L, whereas column of B matrix is assigned j after which decomposition takes place. Both will communicate with $A_{ij} = B_{ji}$ using symmetric value. After the key is generated it will be used for distribution to the sensor nodes. Elliptic curve Hellman protocol is used for key agreement to share the key in unsecured areas. The key is established in both group wise and path wise protocol.

Chang et al., LU decomposition [5] scheme is proposed for distributed sensor network. This scheme additionally utilizes the three pre deployment stages. Once deployed in the network, the following steps are used to generate the communication key:

- On the off chance that Node A begins to communicate with Node B by sending its U matrix column.
- Node B sends hash value with the column and its row
- Likewise Node A also computes the hash value.
- After hashing value is computed check whether the two values are similar, start communication between the nodes.

Wen et al., proposed a key management scheme for Hierarchical [11] sensor network using LU decomposition. This scheme will form the layered architecture in the first level base station shaping, in the middle layer cluster head and the final layer is sensor nodes. It will form the two distinctivesymmetric matrices for communication. Communication between the base station and cluster head is performed by SMBS-CH and by using SMCH-SN cluster head and sensor nodes are used between the group head and the sensor nodes. Pre deployment and post deployment stages are the same as in Chang et al., scheme. The disadvantage of this scheme is a row and column are arbitrarily chosen from the L and U matrices , have the changes to selecting same row and column in the same network will form the largest. Due to this many communication of the node having the similar row and column of L and U matrix will be uncovered.

Manivannan et al., proposed cluster [12] based mechanism using LU matrix. This scheme will achieve the node to node communication within the cluster. The row will be exchanged between nodes to get the secret key. For secure communication between cluster head and base station, ElGamal public key encryption scheme is used. And for group communication the cluster will be divided into cluster groups because to reduce the overhead between the group and cluster head. The advantage of this scheme is perfect resilience and full connectivity between the nodes and network.This scheme archives node to node communication and group communication.

In LU decomposition having lacks in some features like as the row and column are arbitrarily chosen from L and U, the likelihood of selecting the same column and row when the nodes are added to the system gets to be higher. Due to this, when a node is compromised, numerous connections of the nodes having the same column and segment of L and U network will be uncovered.

Table1: Key Management Schemes

Methods	Connectivity	Scalability	Efficiency	Resilience
Symmetric generation–Blom’s scheme	High	Low	High	High
Cluster structure based Blom’s scheme	High	Low	High	Low
Multi Space Blom’s scheme	High	Low	High	Medium compare with Blom’s scheme
ID pairwise –Bolm’s scheme	High	Low	Low	High
Mesh topology-Blom’s scheme	High	Low	High	High
Modified Blom scheme	High	Low	High	High
LU-decomposition	High	Low	High	High
Heriarhical LU decomposition	High	Low	Medium	High
Clustering LU decomposition	High	High	High	Low
Hybrid based LU scheme.	High	Medium	High	Medium

CONCLUSION

The key management scheme is essential for wireless sensor network as it improves the security and resilience. In this paper, the survey is made for various matrix based key management. The pros and cons of various methods are discussed briefly. The analysis is made on connectivity, resilience, scalability and efficiency is shown the table 1.

REFERENCES

[1] Lopez J, Zhou J. Overview of wireless sensor network security. Wireless sensor network security IOS Press, incorporated. 2008:1-21.

[2] Zhang J, Varadharajan V. J Network Comp App 2010;33(2):63-75.

[3] Simplício MA, Barreto PS, Margi CB, Carvalho TC. Computer Networks 2010;54(15):2591-612.

[4] Blom R, editor An optimal class of symmetric key generation systems. Advances in cryptology; 1985: Springer.

[5] Camtepe SA, Yener B. Key distribution mechanisms for wireless sensor networks: a survey. Rensselaer Polytechnic Institute, Troy, New York, Technical Report. 2005:05-7.

[6] Cui X, Zhang Y, editors. A key management scheme based on cluster radiation matrix in WSN. Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on; 2012: IEEE.

[7] Li-Ping Z, Yi W, editors. An ID-based pairwise key predistribution scheme for wireless sensor networks. Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on; 2010: IEEE.

[8] Xu L, Zhang Y. Future Generation Computer Systems 2014;30:140-5.

[9] Reddy RS. Key management in wireless sensor networks using a modified Blom scheme. arXiv preprint arXiv:11035712. 2011.

[10] Wang EK, Ye Y, editors. An efficient and secure key establishment scheme for wireless sensor network. Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on; 2010: IEEE.

[11] Wen M, Zheng Y, Li H, Chen K. A hierarchical composition of LU matrix-based key distribution scheme for sensor networks. Emerging Technologies in Knowledge Discovery and Data Mining: Springer; 2007. p. 608-20.

[12] Doraipandian M, Rajapackiyam E, Neelamegam P, Rai AK. An Efficient and Hybrid Key Management Scheme for Three Tier Wireless Sensor Networks Using LU Matrix. Advances in Computing and Communications: Springer; 2011. p. 111-21.