International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 04, April-2015

Robust Heterogeneity in WMN: Powerful Neighbor Pair wise Scheme

Prakruthi H S
PG in DECS
SJC Institute of Technology
Chickaballapur, India

Veena S
Asst. prof. ECE Dept.
SJC Institute of Technology
Chickaballapur,India

***Abstract* - The security plays an important role in WMN due to vulnerability of network. Powerful neighbour pair wise scheme is one of the fundamental issue in securing WMNs. This paper presents the new pair wise key establishment scheme. The pair wise key is required for the secure communication link between the two nodes which are ready for communicating. Pre-distribution of secrete key for all the nodes in a larger area of network consumes more memory so to avoid this we proposed a random key pre-distribution scheme that exploits the deployment knowledge and avoids unnecessary usage of memory. We show that the performance including communication, usage of memory and network resilience against the node capture attack of the mesh network can be improved with our proposed scheme. The scheme and detailed performance evaluation is presented in this paper.**

Keywords - *Wireless mesh network, pair wise key, sensor nodes, deployment knowledge.*

I. INTRODUCTION

Key establishment is the first step to provide the security mechanisms. Because some security mechanisms depends on keys to operate correctly and provide desirable security measures. sensor networks are networks that consist of tiny electronic devices called sensor nodes that are capable of sensing the environmental conditions such as temperature, pressure, humidity, sound, vibration, fog level and monitors pollution levels, etc. [2]. the sensor network consist of: sensor nodes-device designed to sense various environmental conditions, microcontroller-device which is used to interface with the sensor node, radio transceiver-used to transmit and receive the data using external and internal antenna, energy source- a battery that provide energy for working of sensor nodes [1].

WMN are self configured and self organized, with the nodes in the network participating in routing by forwarding data for other node and maintain mesh connectivity [3]. Mesh network consist of two types of nodes: mesh clients and mesh routers. Mesh clients are either stationary or mobile stations and mesh router is a back bone to the mesh clients. Different types of key distribution scheme that exist are: (1) network keying (2) pair Wise keying (3) group keying [6]. In this paper we are using the pair wise key distribution scheme. Because this is the best keying in terms of robustness, authentication as well as in Storage efficiency. We have proposed a key management scheme that is based on Blom's scheme [3].

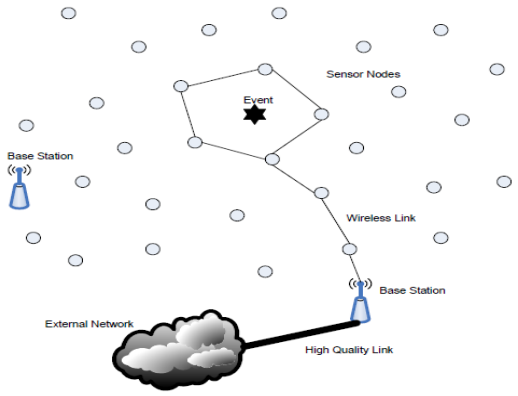

Fig 1: wireless sensor network

The key distribution scheme proposed by blom's allow any pair of nodes in a network can find the secrete pair wise key [5]. The network consists of N number of nodes termed as N users. λ is a threshold treated as a security parameter i.e., larger the λ value more will the security provided to the network. Another use of λ is that amount of memory needed to store key information. Higher λ value leads to higher memory usage. The network is said to be secure as long as no more than λ node is compromised. This is called the λ-secure property.

II. REVIEW ON RELATED RESEARCH

Key management protocol based on either symmetric or asymmetric key functions. Asymmetric key cryptographic algorithms are infeasible for computations and communication. Because sensor nodes are not able afford asymmetric cryptographic operation. Hence symmetric key management functions are favorable to WMN [6].
Different key management protocols base on pair wise key establishment scheme are [7]:

Eschenauer and Gligor proposed a random key pre-distribution scheme, here they pre-distribute a random subset of key to all the nodes from a large pool of keys before the deployment. To agree on a key for communication, two node find a common key from their subset and use that key as a shared secrete key for communication [7]. Though it is robust and require less storage it suffer from less authentication and low accessibility with no support to cluster operation.

Chan, Perrig and Song [8]. This scheme is based on q-composite random key pre-distribution. In this scheme they used q common keys (q>=1) instead of a single one, for the establishment of communication between the pair of nodes. This scheme provides a better security for small scale attack while trading off increased vulnerability in the case of large scale physical attack on network node.

Due, Dan, Hang and Vershney proposed a new key pre-distribution scheme [9]. Where they used the number of private matrices instead of one and use k key matrices in each node.

Perrig et al. proposed SPINS [10]. In SPINS each sensor nodes shares a secrete key with the base station. Two sensor nodes cannot directly establish secret key. However they use the base station as a trusted third party to set up a secret key.

Apart from these many other schemes have been proposed. Our scheme is based on Blom's scheme [3] and we use this scheme as a basic scheme throughout the paper. Blom presented a symmetric key generation system based on MD5. In a network of N users K users as to cooperate to get the information. The public matrix G is choose from the field GF(q) and central authority generate the symmetric secrete matrix D and computes the key and distribute to all users. The public matrix is generated using vandermonde matrix [12].

Modified Blom's scheme [6]: instead of using the Vandermonde matrix as a public matrix here we use the adjacency matrix. Adjacency matrix is a matrix in which the neighboring nodes of a particular node are filled with 1's and other nodes are filled with q-1 value. q is a prime number chosen from GF(q) and q should be (q>N).

$$\begin{vmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{vmatrix}$$

Fig 2: Adjacency matrix

III. PROPOSED SYTEM

This section briefly describes the steps from the network creation to till the pair wise key establishment phase.

Figure-3 shows the block diagram of the proposed system. Here the network creation indicates the creation of the sensor nodes. Once the sensor nodes are created it is necessary to initialize the sensor nodes with the configuration details. Then a group of sensor nodes are assigned with the cluster head, which is designated as region. Next the total target development area is divided into regular hexagons. Then the base station generates the key seeds for each nodes in the region. After this the central authority (base station) generates a secrete matrix G and also generates the symmetric matrix D for pair wise key establishment. This pair wise key will be established using the modified blom's algorithm. After all these the the nodes can communicate with each other.

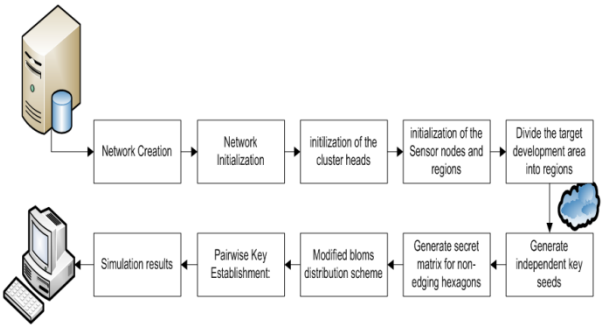

Fig-3: block diagram of proposed system

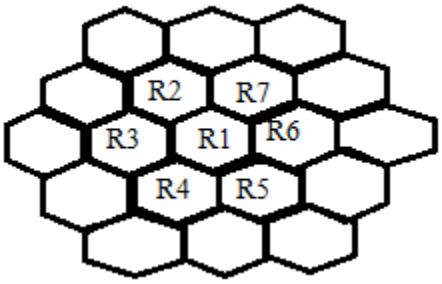

Fig-4: target development area divided into regular hexagons

I. KEY ESTABLISHMENT IN WMN

This section denotes the description of our full scheme. In this section will see the preliminaries requrired for the scheme, basic Blom scheme and then our full scheme.

A.PRELIMINARIES

There are three phase in Blom's scheme: system setup phase, key pre-distribution phase and pair wise key establishment phase.

System setup phase: the central authority generates the required parameters and the matrices.

Key pre-distribution phase: the central authority pre load each node including mesh router and mesh client with a key information.

Pair wise key establishment phase: with the use of mesh router the two sensor nodes can establish pair wise secrete key.

B.BASIC SCHEME

Our basic scheme is a blom's scheme [13]. In blom's scheme with λ as a security parameter it takes large storage cost [14]. To reduce the storage cost at each sensor node, we modified the Blom's scheme as follows.

System setup: central authority

- The central authority choose N independent key seeds s1,s2…sN and use the identifier to indicate the key seed, let id_i be the identifier of key seed s_i .
- Generate a public matrix G of size (λ+1)×N:

$$G = \begin{pmatrix} S_1 & S_2 \ldots\ldots\ldots S_N \\ (S_1)^2 & (S_2)^2 \ldots\ldots (S_N)^2 \\ (S_1)^3 & (S_2)^3 \ldots\ldots (S_N)^3 \end{pmatrix}$$

- Generate a symmetric matrix D of size (λ+1)×(λ+1) in GF(q).

Key pre-distribution phase: In this phase the central authority completes the following operations.

- Operation associated with sensor nodes: store each key seeds s_i and its identifier id_i to the ith sensor node.
- After the generation of symmetric matrix computes the public matrix $A=(D.G)^T$.
- Pre-load the mesh router with a matrix A.

Pair wise key establishment phase:

- After the deployment all sensor node broadcast the key seed identifier id_i and keeps track of neighbours key seed identifier.
- Any two sensor nodes can directly establish the pair wise key after broadcasting the matrix A by the mesh router.
- Suppose node i and node j want to establish a pair wise key with each other then,

Calculation at the ith node:

- node i uses its key seed s_i to generate the ith column of the G matrix $(s_i\ s_i^2 \ldots\ldots s_i^{\lambda+1})^T$.
- Let $(a_j\ a_j^2 \ldots\ldots a_j^{\lambda+1})$ be the jth row of the A matrix which is broadcast by the mesh router.

$K_{ji}=(a_j\ a_j^2 \ldots\ldots a_j^{\lambda+1})\ .\ (s_i\ s_i^2 \ldots\ldots s_i^{\lambda+1})^T$

Calculation at jth node:

- node j uses its key seed s_j to generate the jth column of the G matrix $(s_j\ s_j^2 \ldots\ldots s_j^{\lambda+1})^T$.
- Let $(a_i\ a_i^2 \ldots\ldots a_i^{\lambda+1})$ be the ith row of the A matrix which is broadcast by mesh router.

$K_{ij}= (a_i\ a_i^2 \ldots\ldots a_i^{\lambda+1})\ .\ (s_j\ s_j^2 \ldots\ldots s_j^{\lambda+1})^T$

- From this we can say that $K_{ij}=K_{ji}$.

C.OUR FULL SCHEME

In our scheme we use the adjacency matrix as a public matrix G. from figure-2 we can see that the adjacency matrix consist of only two numbers 1's and q-1. q is the prime number. The key generation is same as that in blom's scheme. The following steps are use for calculating keys.

Generation of matrices:

First select a prime number q (q>N). Then generate a G matrix of size N. Then generate a G matrix of size N×N. Modify the G matrix by selecting λ+1 row and N columns from the original G matrix.

G_j is the jth column of the G matrix it is loaded to the node j in original blom's scheme but in our scheme each node knows its neighbor nodes so there is no need of storing it once again. This avoids the large 0memory consumption.

The central authority generates ω random secrete symmetric matrix $D_1\ D_2 \ldots\ldots D_\omega$ of size (λ+1)×(λ+1). Then computes $A_i=(D_i.G_i)^T$.

Computation of key:

The central authority will stores each row of matrix A to all the nodes in the region. If node I want to communicate with node j then node i multiply ith row of A matrix and the jth column of G matrix.

Implementation:

The following example shows the working of the modified Blom's scheme. Let the number of nodes are N=6, security parameter λ=3 and the prime number q=29. Which says no more than 3 nodes in the network are compromised it is not possible to find the keys of other users (nodes).

Consider the node structure,

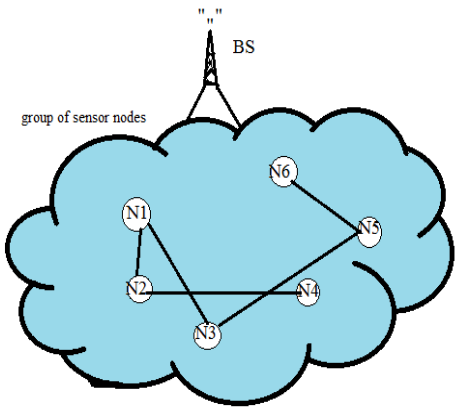

Fig-5: example of sensor nodes structure

From fig-5 the adjacency matrix is,

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Modified adjacency matrix is,

$$\begin{pmatrix} 28 & 1 & 1 & 28 & 28 & 28 \\ 1 & 28 & 28 & 1 & 28 & 28 \\ 1 & 28 & 28 & 28 & 1 & 28 \\ 28 & 1 & 28 & 28 & 28 & 28 \\ 28 & 28 & 1 & 28 & 28 & 1 \\ 28 & 28 & 28 & 28 & 1 & 28 \end{pmatrix}$$

Public matrix G of size (4×6),

$$\begin{pmatrix} 28 & 1 & 1 & 28 & 28 & 28 \\ 1 & 28 & 28 & 1 & 28 & 28 \\ 1 & 28 & 28 & 28 & 1 & 28 \\ 28 & 1 & 28 & 28 & 28 & 28 \end{pmatrix}$$

Secrete symmetric matrix D of size (4×4),

$$\begin{pmatrix} 3 & 5 & 2 & 7 \\ 5 & 6 & 9 & 1 \\ 2 & 9 & 3 & 5 \\ 7 & 1 & 5 & 4 \end{pmatrix}$$

$A=(D\times G)^T \bmod 29$ is,

$$\begin{pmatrix} 26 & 9 & 5 & 24 \\ 3 & 20 & 24 & 5 \\ 18 & 18 & 14 & 26 \\ 22 & 20 & 28 & 14 \\ 16 & 26 & 16 & 22 \\ 12 & 8 & 10 & 12 \end{pmatrix}$$

Once matrix A is calculated each sensor nodes are filled with the row corresponding to the index.

Key generation:

Suppose let node-3 want to communicate with node-5, in order to obtain the shared secrete key node-3 multiplies its private row which is provided to it by matrix A which is 3rd row of A with the column of public matrix G which is 5th column of G.

$K_{35}=A_3G_5$

$$K_{35}=\begin{bmatrix} 18 & 18 & 14 & 26 \end{bmatrix}\begin{pmatrix} 28 \\ 28 \\ 1 \\ 28 \end{pmatrix} = 175 \bmod 29$$

$K_{35} = 10$

Similarly,

$$K_{53} = \begin{bmatrix} 16 & 26 & 16 & 22 \end{bmatrix}\begin{pmatrix} 1 \\ 28 \\ 28 \\ 28 \end{pmatrix} = 1808 \bmod 29$$

$K_{53} = 10$

We can observe that $K_{35}=K_{53}$ which is node-3 and node-5 share a common secrete key therefore they can communicate with each other.

IV. LINK ESTABLISHMENT

In wireless mesh network, according to the blom's scheme the keys are generated and distributed randomly to each sensor nodes in the network. The node which shares a common key will establish link between the nodes. In this scheme a new approach has been proposed to establish a secure communication between the nodes with desire scalability and resiliency.

When two nodes share more than one shared key, the amount of data transferred will be high when compared to one shared key and bandwidth consumption will also less when compared to others.

Fig-6 shows how link will be establish between the nodes using the blom's algorithm. If there is a common key then link will be establish ,if there is no common key between the nodes then no link will be establish, it will look again with other nodes for the common key.

Flow chart that describes the link establishment is,

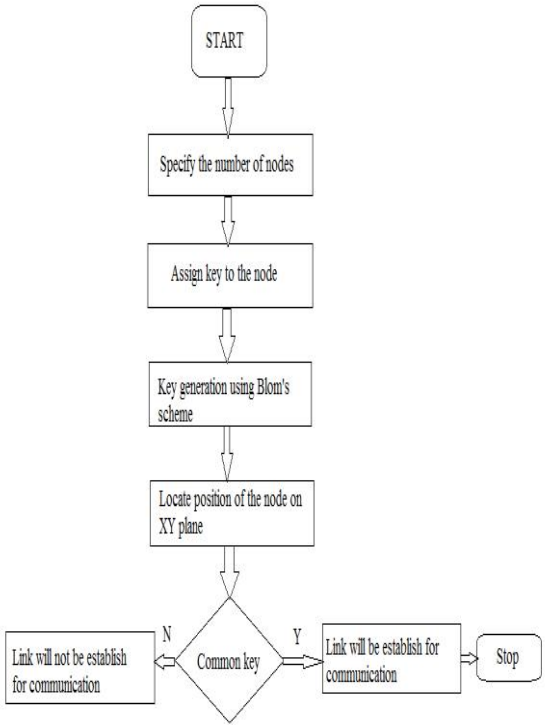

Fig-6: Flowchart for link establishment

Fig-6 shows how link will be establish between the nodes using the blom's algorithm. If there is a common key then link will be establish ,if there is no common key between the nodes then no link will be establish, it will look again with other nodes for the common key.

V. ANALYSIS

This section devote the analysis of our scheme, by comparing it with others [6],[7],[8].

Consider total number of sensor nodes N=100, the security parameter is taken as λ=29, target area divided into 10 sub regions r=10 and the total number of nodes in each sub region is β=100. Figure-7 shows how the number of sensor nodes spread over network size of 5000.

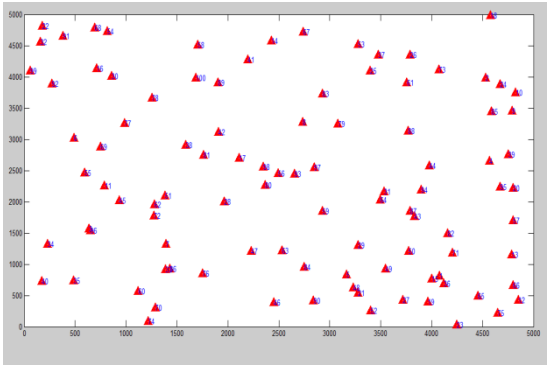

Fig-7: sensor nodes spread across the network

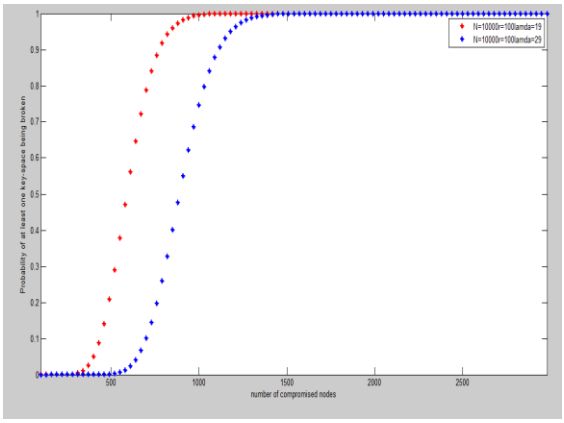

Fig-8: probability of at least one key space being broken after x nodes are compromised

Figure-8 indicates that: when the system security parameter is λ=19, the adversaries have to randomly capture about 300 nodes in order to break at least one key space with reasonably high probability. When security parameter increase to λ=29 the adversary have to randomly capture minimum of 600 nodes to break at least one key space. From this we can say that larger the security parameter more will be the security.

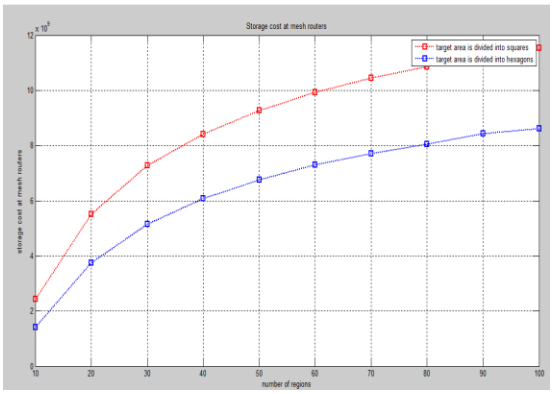

Fig-9: storage cost

Figure-9 indicates that: the storage cost of mesh router is high when the total target area is divided into square. When the total target area is divided into regular hexagons the storage cost is comparatively low.

VI. OTHER ANALYSIS

SCALABILITY: new node can be added to the network to replace the old node or to extend the network.

To add the new node to replace an existing node in region R_j, central authority follow these steps:

1. Select a new key seed $S_{j(\beta+1)}$ and an identifier $id_{j(\beta+1)}$
2. Update G matrix associated with R_j and its 6 neighbouring regions
3. Update A matrices stored in router.
4. Load each node with $S_{j(\beta+1)}$, $id_{j(\beta+1)}$ and with set identifier $N_{j(\beta+1)}$.

After all these the new node can establish pair wise key with other nodes as described in key establishment phase.

KEY UPDATING: we can update the pair wise keys when needed to increase the network resilience.

VII. CONCLUSION

Security by establishing a pair wise key is a fundamental issue in WMN. This paper presents a new design of pair wise key establishment scheme. This new scheme reduce the computational cost of sensor nodes for their communication and reduce memory required for storage. Furthermore our scheme has the ability perform even in non-uniform condition and neighbor nodes can directly establish pair wise keys. Our scheme can be scalable, updateable and it gives robust heterogeneity in wireless mesh network.

VIII. REFERENCE

(1) S.R.Murthy, B.S.Manoj, Ad Hoc wireless networks: Architecture and protocol, 1st ed. Pearson education, 2004, ch.12, wireless sensor network.
(2) A. Habib, "sensor network security issues at network layer," in 2nd international conference on advances in space technologies, Islamabad, pakisthan, 29th-30th November 2008.
(3) R.Blom, " an optimal class of symmetric key generation system," in proc. Of EUROCRYPT' 84, pages 335-338.
(4) G.J.Pottie, W.J.Kaiser, "wireless integrated network sensors," in communication of the ACM, 2000, vol. 43(5), pages 51-58.
(5) Rohithi singh reddy, "key management in wireless sensor networks using a modified Blom scheme," arXiv, 1103,5712.
(6) L.Eschenauer and V.D.Gligor, "a key-management scheme for distributed sensor networks," in proceeding of the 9th ACM conference on computer and communication security, Washington DC, USA, November 18-22 2002, pp. 41-47.
(7) H.chan, A.Perrig and D.Song, "Random key pre-distribution scheme for sensor networks," in IEEE symposium on security & privacy, Berkley California, may 11-14 2003, pp. 197-213.
(8) W.Du, J.Deng, Y.S.Han, and P.K.Varshney, "A pair wise key pre-distribution scheme for wireless sensor networks," in proceeding of the 10th ACM conference on computer & communications security (CCS), Washington DC, USA, October 27-31 2003, pp. 42-51.
(9) H.Chan, A.Perrig and D.Song, "random key pre-distribution schemes for sensor networks," in IEEE symposium on security & privacy, Berkeley California, May 11-14 2003, pp. 197-213.
(10) A.Perrig, R.szewczyk, V.Wen, D.Cullar, and J.D.Tygar, "SPINS: security protocols for sensor networks", in proceedings of the 7th annual computing &networking (Mobicom), Rome, Italy, July 2001, pp. 189-199.
(11) W.Du, J.Deng, Y.S.Han, and P.K.Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," IEEE Trans Dependable secure comput, vol.3, nol, pp.62-77 Jan/Mar. 2006.
(12) B.Zhou, S.Li, Q.Li, X.Sun & X.Wang, "an efficient & scalable pair wise key pre-distribution scheme for sensor networks using deployment knowledge," Comput. Commun., Vol. 32, no.1, pp. 124-133, 2009.