Delaunay Triangulation Based Key Distribution for Wireless Sensor Network

Monjul Saikia
Computer Science and Engineering Department, North Eastern Regional Institute of Science and Technology, Nirjuli-791109, Arunachal Pradesh, India
Email: monjuls@gmail.com

Md. Anwar Hussain
Electronics and Communication Engineering Department, North Eastern Regional Institute of Science and Technology, Nirjuli-791109, Arunachal Pradesh, India
Email: ah@neris.ac.in

Abstract—The key distribution in a wireless sensor network is a security phase, which involves distribution secret keys among sensor nodes prior to deployment. The distributed keys are used for encryption and decryption process in later stages. There are mainly two types of key distribution strategies namely location independent and location dependent. Location independent key distribution scheme is used when the location of the sensor nodes are not known prior. If the expected locations of sensor nodes are known prior to deployment, the location dependent key distribution scheme is used. Here in this paper, we proposed a location dependent key distribution scheme using Delaunay Triangulation (DTKPS). Delaunay triangulation is a triangulation method which forms a set of triangles for a given set of points such that no point falls inside the Delaunay disk of any triangle. Implementation of the key distribution scheme is done using Matlab software and results were presented.

Index Terms—Wireless sensor network; key distribution; security; delaunay triangulation; secure communication; connectivity.

I. Introduction

Wireless sensor networks are used for many application where direct human interaction not possible. Sensor nodes collect data and send the collected data to a control center called base station. The sensor nodes are consisting of a sensing device, wireless communication equipment with transmitter and receiver controlled by a small micro-controller. Sensor nodes are powered by a small energy source usually in the form of battery or solar powered. Sensor nodes have several limitations such as limited storage capacity, low computation power and speed and limited bandwidth etc. Sensor nodes are designed with limited cost with minimal size. In many applications security is an essential requirement. In a wireless sensor network, sensors are highly prone to malicious attacks such as mimicking, camouflaged or capture for misleading. A sensor network is not guarded with a physical protection and an unattended deployment is done. Therefore, other means of the security is to be done for such networks. However, the exclusive properties of a wireless sensor network make the implementation very challenging and the existing security system cannot directly apply on such network. Thus, a portable version of the security mechanism often becomes a necessity. Symmetric key cryptography is considered due to its simplicity and cost efficiency. For this purpose key management protocols are the preliminary steps for the secure communications, where keys are distributed in such a way that a proper connectivity retains at later phase of deployment. The objective of a key management system is to form secure links between neighbor sensor nodes at the formation of the network. Following figure shows pairwise key distribution for three sensor nodes. Nodes S_1 and S_2 shares a common key K_1, therefore they can communicate with the help of K_1. Similarly, S_1 and S_3 and S_2 and S_3 can communicate securely with the help of key K_2 and K_3 respectively.

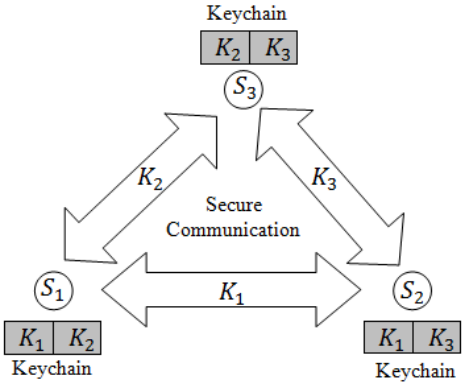


Fig. 1. Key distribution and secure communication

Several key management schemes have been developed in the recent for the wireless sensor network. L. Eschenauer and B. D. Gligor [1] the first to propose a key management system for distributed sensor networks. They use simple random key distribution method in their proposed model. H Chan *et al*. [2] also proposed a random key predistribution schemes which randomly distributes secret keys for wireless sensor networks. D. Liu and P. Ning [3] introduced key predistribution with

Manuscript received November 1, 2018; revised June 1, 2019.
doi:10.12720/jcm.14.7.530-537

deployment knowledge in static sensor networks also proposed pairwise key distribution scheme in distributed sensor networks [4]. J. Zhang *et al.* [5] studied key management taxonomy and discuss the merits of key distribution in sensor network. X. Zheng *et al.* [6] proposed a neighborhood prediction based decentralized key management for mobile wireless networks. Various version of combinatorial design based key distribution have been proposed in the literature. In combinatorial designed based key distribution, they used balance incomplete block design as building block for arrangement of key chain. M. F. Younis *et al.* [7] gave a location-aware combinatorial key management scheme for clustered sensor networks. S.A. Camtepe *et al.* [8] first proposed Combinatorial Design based Key Distribution Mechanisms for Wireless Sensor Networks. They proposed a deterministic and hybrid approaches based on Combinatorial Design and uses Balanced Incomplete Block Designs (BIBD) and Generalized Quadrangles (GQ) to obtain an efficient key distribution scheme. R. Blom [9] an Optimal Class of Symmetric Key Generation Systems method for wireless sensor network. F. Piper *et al.* [10] discuss efficient use of Combinatorics in Key Management for sensor network. C. Intanagonwiwat *et al.* [11] used directed diffusion technique for a scalable and robust communication paradigm for sensor networks. R. Perrig *et al.* [12] proposed a security protocol for sensor networks namely SPIN. S. Zhu *et al.* [13] pair-wise keys for secure Communication in Ad Hoc Networks. S. Zhu *et al.* [14] proposeda scheme called LEAP: an efficient security mechanism for Large-Scale Distributed Sensor Networks. W. Stallings [15] discussed various security issues in wireless sensor network and usability of Cryptography for security. M. Saikia *et al.* [16] proposed a combinatorial group-based approach for key predistribution scheme for wireless sensor network. M. Saikia *et al.* [17] used prior location information for key predistribution for square and hexagonal grid of sensor network. C. Blundo *et al.* [18] proposed a perfectly-secure key distribution for dynamic conferences.

Delaunay triangulation is a special triangulation over a set of planer points, named after Boris Delaunay for his work on this topic from 1934 [19]. There are numerous applications of Delaunay triangulation in data analysis, sensor network deployment and clustering techniques etc. Two simple construction model of Delaunay triangulation is given by D. Lee *et al.* [20]. W. Schroeder *et al.* [21] proposed a geometry based fully automatic mesh generation and the Delaunay triangulation. Chun-Hsien *et al.* [22] proposed a Delaunay triangulation-based method for wireless sensor network deployment.

Organization of the paper:

Section-I gives an introduction to key distribution. Section-II gives properties of Delaunay Triangulation and its usability in key distribution. In section-III we discuss the proposed key distribution scheme. The implementation is given in section-IV and results were shown in section-V. Section-VI concludes the paper.

II. Delaunay Triangulation and Properties

Triangulation of a Point Set $P:=\{p_1, p_2, \cdots, p_n\}$ is the maximal planar subdivision S, that no edge connecting two vertices can be added to the subdivision without destroying its planarity [19]. In other words, any edge that is not in the subdivision S intersects one of the existing edges. Therefore, a triangulation of P is defined as a maximal planar subdivision whose vertex set is P. It is obvious that there exist a triangulation for a set of points.

If P be a set of n not all collinear points in the plane, and let k denote the number of points in P that lie on the boundary of the convex hull of P. Then any triangulation of P will give $2n-2-k$ triangles and $3n-3-k$number of edges [21].

Delaunay Triangulation is a special case of triangulation, which satisfies some properties. Delaunay triangulation can be defined as triangulation T of a set of points P in the plane is a Delaunay triangulation of P if and only if the circum-circle of any triangle of T does not contain a point of P in its interior. This is shown in the Fig. 2.

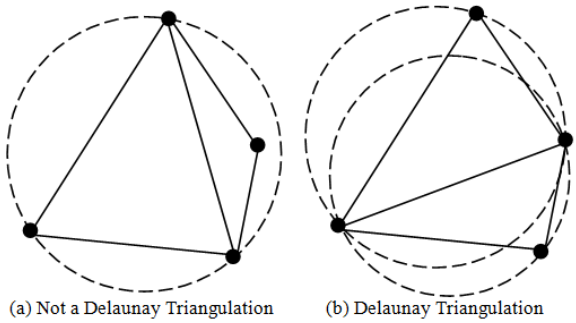


Fig. 2. Two ways of triangulation

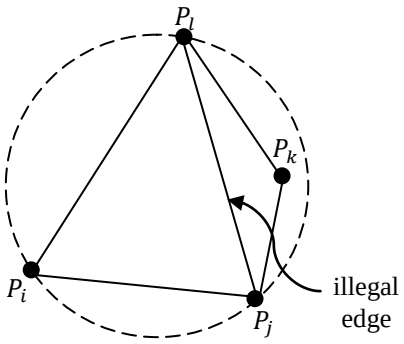


Fig. 3. Delaunay triangulation illegal edge identification

There are various methods for computing Delaunay triangulation. One of these is *LEGALIZEEDGE*. Where, first random triangulation is computed, and then the algorithm flips an edge if it is found to be an illegal edge. If we have a convex quadrilateral, then either of the two diagonals makes a valid Delaunay triangulation. The Fig.

3 shows the edge flip method or simply *LEGALIZEEDGE* method of Delaunay triangulation.

Let P_i, P_j, P_k and P_l form a convex quadrilateral and do not lie a common circle, then exactly one or the diagonal is an illegal edge of Delaunay triangulation. Let edge $\overline{P_jP_l}$ be incident to both triangles $P_iP_jP_k$ and $P_jP_kP_l$and let the circle through P_i, P_j and P_l. The edge $\overline{P_jP_l}$ is illegal if and only if the point P_k lies in the interior of circle C. If any edge is found to be illegal the edge is flipped and this makes triangulation a legal Delaunay triangulation.

III. The Proposed Key Distribution Scheme

Here we proposed a location dependent key predistribution scheme. We use the expected location (coordinates) the sensor nodes to form a set of Delaunay triangles. Each edge of the triangle is then assigned a paired key. The following flow diagram [Fig. 4] shows the proposed scheme. The algorithm first takes the expected location of the sensor nodes. Then with these set of points Delaunay triangulation is generated. Then keys are assigned to the sensor nodes sharing a triangle edge that are within the communication range.

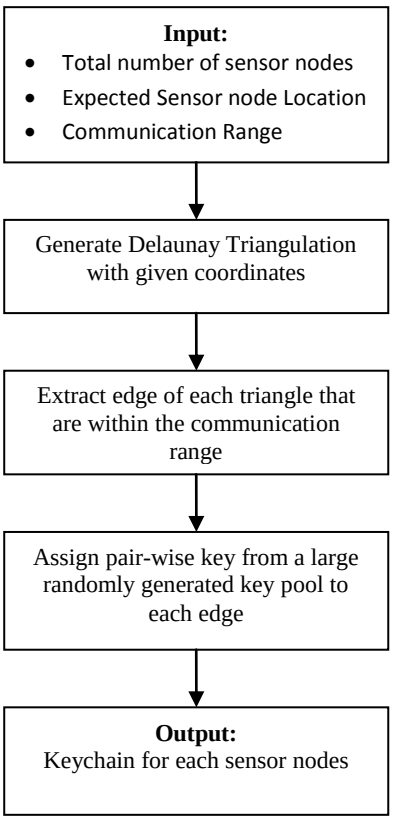


Fig. 4. Proposed scheme flow diagram

Example: Let us consider 4 sensor nodes S_1, S_2, S_3 and S_4. The figure 5 shows the Delaunay triangulation of these nodes. We assign pairwise keys between the pairs $\{S_1, S_2\}$, $\{S_2, S_3\}$, $\{S_3, S_4\}$, $\{S_4, S_1\}$ and $\{S_3, S_1\}$ according to the edges in the triangulation. It is seen that there is no key share between the pair $\{S_2, S_4\}$ as there is no edge between them [Fig. 5].

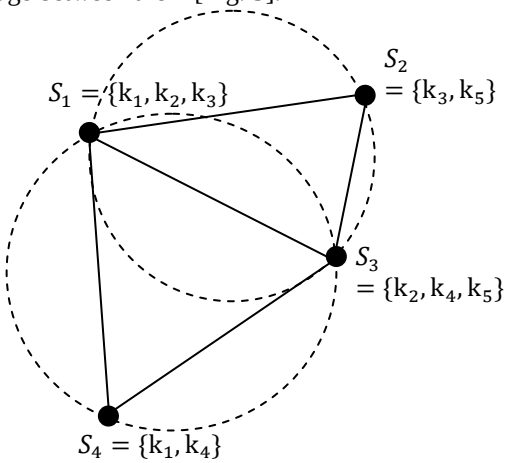


Fig. 5. Delaunay triangulation of four points

IV. Implementation of the Proposed Key Distribution Algorithm

First, we generate a set of random locations for the sensor nodes. These locations are considered to be the expected post-deployment coordinate position for the sensor nodes. With these set of nodes, we generate Delaunay triangulation. In the next step, we assign a shared key for each edge in the triangulation.

Algorithm 1: DTKPS	
Step 1:	Random location for each sensor nodes
Step 2:	Delaunay triangulation for the set of node
Step 3:	Identify each edge associated with two triangles
Step 4:	Assign random keys from key pool

Equivalent pseudo-code is as follows:

Pseudo-code 1: $DTKPS(N, X, Y)$

Input: *Number of sensor Nodes=**N**,*
*Expected locations **X**-cord, **Y**-Cord,*
*Sensing Range=**R***
Output: *KeyRing[][]*

Step 1. *triangles= Delaunay(X,Y)*
Step 2. *k=1;*
for** i=1 to no_of_triangles **do
edge[k][1]=triangle[i][1];
edge[k][2]=triangle[i][2];
k=k+1;
edge[k][1]=triangle[i][2];
edge[k][2]=triangle[i][3];
k=k+1;
edge[k][1]=triangle[i][3];
edge[k][2]=triangle[i][1];
k=k+1;
endfor
Step 3. *//Removal of Duplicates edges*
k=1;
edges[]=[0,0];
for** i=1 to no_of_edges **do
temp=edge[i];
***if** ismember(Edges, temp) != 0*
// ismember function test existence of the edge
edges[k]=temp;
k=k+1;

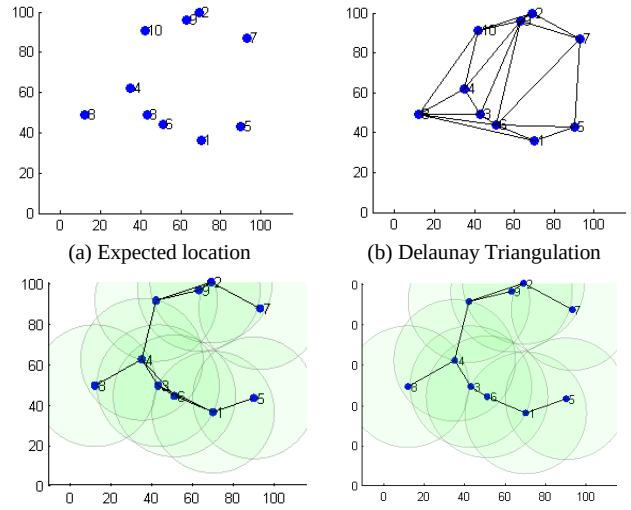
```
        endif
      endfor
Step 4. for i=1 to no_of_edges do
        S=edges[i][1];
        D=edges[i][2];
        if dist(s,d)<=R then % R= Sensing Range
          index=1;
          while keyRing[S][index] !=empty
              index= index+1;
          endwhile
          keyRing[S][index]= k;
           index=1;
          whilekeyRing[D][index] !=empty
              index=index+1;
          endwhile
          keyRing[D][index]=k;
          k=k+1;
        endif
      endfor
Step 5. Return keyRing;
```

V. Simulation Results and Analysis

Simulations on various network scenarios were performed and evaluated the following for analysis of our proposed scheme.

- Average number of usable keys per sensor node
- Average number of unused keys per sensor node
- Average number of key storage
- Percentage of Connected nodes after deployment
- Resilience

A. Simple Experiment



(a) Expected location (b) Delaunay Triangulation

(c) Sensor in sensing range (d) Secure connectivity

Fig. 6. Experiment with $N = 10$ units, $R = 30$ uints, $A = 100 \times 100$ sq. units

For our first experiment, we take 10 sensor nodes with sensing radius of 30 units in an area of 100×100 sq. units. Fig. 6(a) shows the expected location of the sensor nodes. Fig. 6(b) shows the Delaunay triangulation, Fig. 6(c) show the sensor nodes that are within the sensing range and Fig. 6(d) shows the actual connectivity after deployment. The set of keys distributed to a sensor node is called the *Key Ring*. Table I shows the key ring for each of the sensor nodes. The numbers indicated key identifiers, for example, sensor node S_1 stores three keys $\{17, 8, 9\}$, using which it can establish secure communication with a sensor node having key id 17, 8 or 9. In this case, S_1 can communicate with S_5, S_7 and S_8 using key id 17, 8 and 9 respectively.

TABLE I: KEY RING FOR EACH SENSOR NODES

	S_1	S_2	S_3	S_4	S_5	S_6	S_7	S_8	S_9	S_{10}
S_1					17	8		9		
S_2							21		14	15
S_3				6		1		2	5	
S_4			6					7	12	10
S_5	17					16	18			
S_6	8		1		16		19	3	4	
S_7		21			18	19			20	
S_8	9		2	7		3				11
S_9		14	5	12		4	20			13
S_{10}		15		10				11	13	

TABLE II: ANALYSIS RING SIZE AND USABLE KEYS

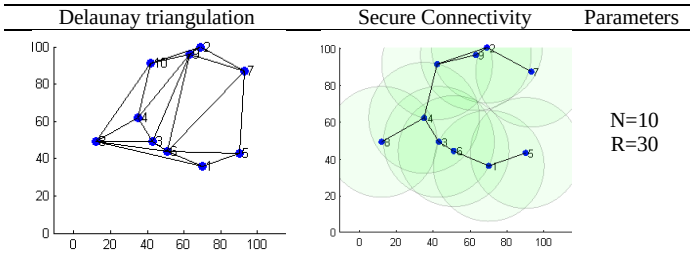
Sensor Node	Ring size	Usable key	Unused key
s_1	3	2	1
s_2	3	3	0
s_3	4	2	2
s_4	4	3	1
s_5	3	1	2
s_6	6	2	4
s_7	4	1	3
s_8	5	1	4
s_9	6	2	4
s_{10}	4	3	1
avg.=	4.2	2	2.2

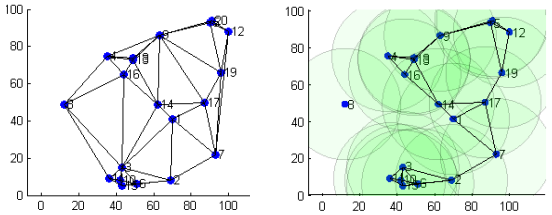
Simulation over various network scenarios:

The following table describes the value/range of parameters used for various simulations. Simulation outcome is shown in Fig. 7.

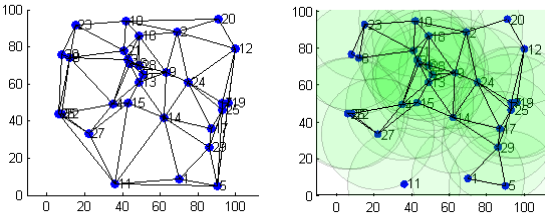
TABLE III: SIMULATION PARAMETERS

Sl.	Parameters	Value/ Range
1.	Number of Sensor Nodes	N= 10 to 100
2.	Communication Range	R= 30 units
3.	Deployment Area	A=100×100 sq. units

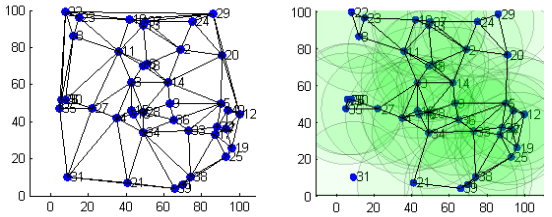




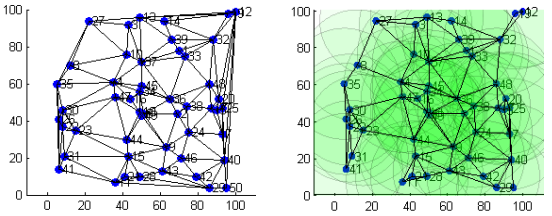
N=20
R=30



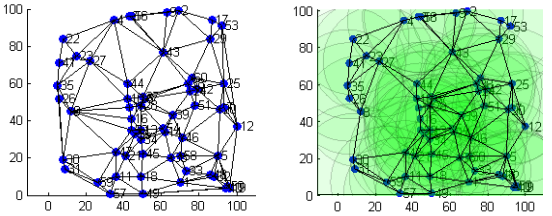
N=30
R=30



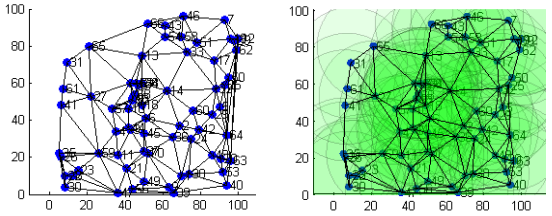
N=40
R=30



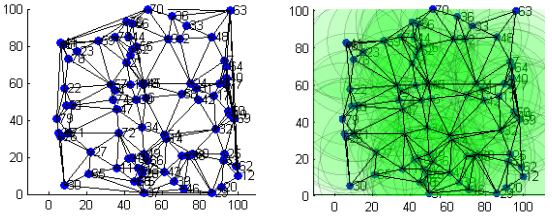
N=50
R=30



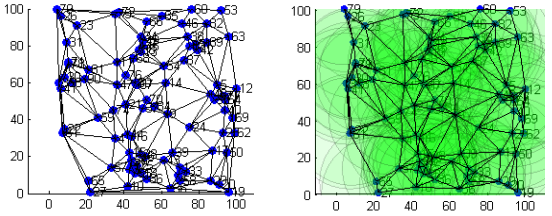
N=60
R=30



N=70
R=30



N=80
R=30



N=90
R=30

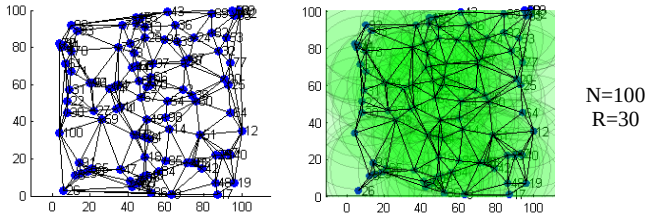


Fig. 7. Simulations

Average Keychain size, usable keys and unused keys:

As key distribution is done based on Delaunay triangulation edges incident on a node therefore keychain is variable sized. After performing simulations, we find out the average size of the key ring, usable keys, and unused key. The results are shown in a bar graph as in Fig. 8. Average number of keychain size for large network is found to approximately 4 to 5. Number of usable keys is found to be high for larger network and a there is negligible unused keys.

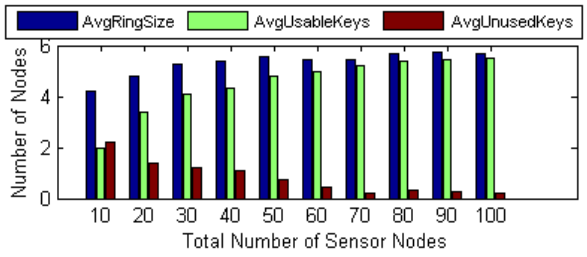


Fig. 8. Average key ring size, Average number of usable keys and unused keys

Average secure communication links per node:

Keeping key chain size 4 for the above simulation scenarios with combinatorial design based and random KPS the average number of secure communication link found per sensor node is shown in plot in Fig. 9.

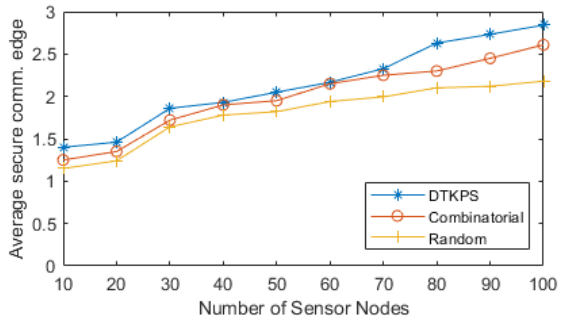


Fig. 9. Average secure communication links per node

Resilience:

Resilience is the measure of network performance in case of node failure or node capture. This is a measure of fraction for the network that is operable after a fraction of network fails. Resilience $fail_s$ is calculated as follows.

$$fail_s = \left(1 - \left(1 - \frac{k}{|K|}\right)^s\right)^q$$

where q= Number of key shares between two randomly selected uncompromised node and $|K|$ is key pool size.If number of compromised node s=1 and key share q=1, then

$$fail_1 = \frac{k}{|K|}$$

Resilience $fail_1$ is computed as the fraction of the network that can work when a single node fails. Similarly $fail_2$ and $fail_3$ are computed as the workable fraction of the network when two and three sensors are failed respectively. The figure 10 shows $fail_1$, $fail_2$, $fail_3$ and $fail_4$ for the simulations performed above.

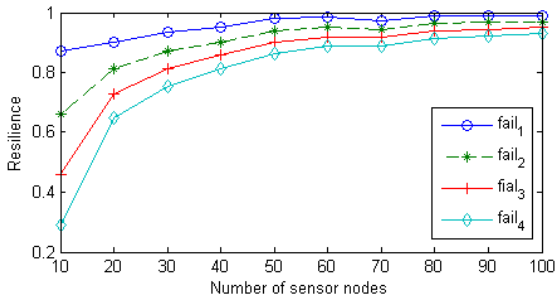


Fig. 10. Resilience:$fail_1$, $fail_2$, $fail_3$and $fail_4$

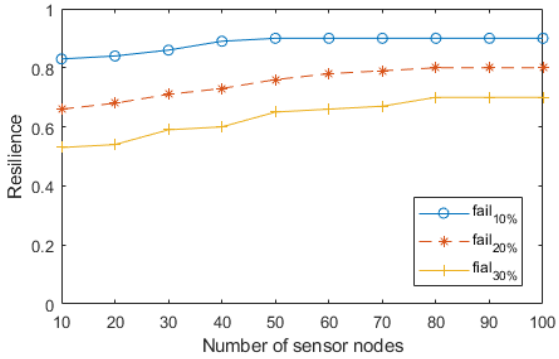


Fig. 11. Resilience with fraction of network failure

Resilience for same ratio of node failure for various sized network is evaluated. Experiments are done for 10%, 20% and 30% node failure and this is shown in the plot in Fig. 11.

VI. Conclusion

In this paper, a key pre-distribution scheme using Delaunay triangulation method is proposed. The scheme is location dependent in the sense that expected coordinates of the sensor nodes are assumed to be known prior to deployment. For various experiments, it can be

claimed that the algorithm guarantees an assignment of secret shared keys among the nodes if two nodes are within their communication ranges. We performed various experiments to evaluate the performance and found that the algorithm distributes shared keys among nodes that are nearby to the nodes and avoids assigning keys to a node that is far away. Also, it is seen that the average key ring size is minimal and for large sensor network unused keys are found to be very low. For a larger sized network, the algorithm is found to be efficient in terms of resilience, average key storage as well as minimal unused keys. The key distribution using Delaunay triangulation can be extended to 3D wireless sensor network by incorporating Delaunay tetrahedralization.

REFERENCES

[1] L. Eschenauer and B. D. Gligor, "A key management scheme for distributed sensor networks," in *Proc. 9th ACM Conference on Computer and Communication Security*, Washington, DC, USA, 2002. p. 41–47.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symposium on Security and Privacy*, 2003, pp. 197–213.

[3] S. Liu and P. Ning, "Improving key predistribution with deployment knowledge in static sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 2, pp. 204–239, 2005

[4] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM conference on Computer and communication security-CCS '03*, New York, 2003, p. 52.

[5] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, March 2010.

[6] X Zheng, Y. Chen, H. Wang, H. Liu, and R. Liu, "Neighborhood prediction based decentralized key management for mobile wireless networks," *Wireless Networks*, vol. 19, no. 6, pp. 1387–1406, 2013.

[7] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-Aware combinatorial key management scheme for clustered sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865–882, 2006.

[8] S. A. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," in *Proc. IEEE/ACM Transactions on Networking*, Springer, 2007.

[9] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. Workshop Advances in Cryptology: Theory and Application of Cryptographic Techniques*, 1984, pp. 335-338.

[10] F. Piper and P. Wild, "The use of combinatorics in key management," *IMA J. Math. Applied in Business and Industry*, vol. 7, pp. 207-218, 1996.

[11] C Intanagonwiwat, R Govindan, and D Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proc. 6th Annual International Conference on Mobile Computing and Networking*, ACM New York, NY, USA, 2000, pp. 56-67.

[12] Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," in *Proc. of MOBICOM*, 2001.

[13] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," in *Proc. IEEE 11th Int. Conf. Network Protocols*, 2003, pp. 326-335.

[14] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," in *Proc. ACM CCS Conference*, 2003, pp. 62-72.

[15] W. Stallings, *Cryptography and Network Security-Principles and Practices*, 3rd ed. Upper Saddle River, NJ: Prentice Hall, 2003.

[16] M. Saikia and M. A. Hussain, "Combinatorial group based approach for key predistribution scheme in wireless sensor network," in *Proc. Int. Conf. on Computing, Communication and Automation*, India, May 5-6, 2017, pp. 502-506.

[17] M. Saikia and M. A. Hussain, "Location dependent key predistribution scheme for square grid and hexagonal grid," *Indian Journal of Science and Technology*, vol. 10, no. 9, pp. 1-6, March 2017.

[18] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure key distribution for dynamic conferences," in *Proc. 12th Ann. Int'l Cryptology Conf. Advances in Cryptology*, 1993, vol. 740, pp. 471-486.

[19] B. Delaunay, "Sur la sphere vide," Izv. Akad. Nauk SSSR, Otdelenie Matematicheskiii Estestvenny ka Nauk, 1934.

[20] D. T. Lee and J. B. Schachter, "Two algorithms for constructing a delaunay triangulation," *International Journal of Computer & Information Sciences*, vol. 9, no. 3, pp. 219-242, 1980.

[21] Schroeder, J. William, and M. S. Shephard, "Geometry - Based fully automatic mesh generation and the delaunay triangulation," *Int. Journal for Numerical Methods in Engineering*, vol. 26, no. 11, pp. 2503-2515, 1988.

[22] W. Chun-Hsien, K. C. Lee, and Y. C. Chung, "A delaunay triangulation based method for wireless sensor network deployment,' *Computer Communications*, vol. 30, no. 14-15, pp. 2744-2752, 2007.

Monjul Saikia is Assistant Professor in Computer Science and Engineering department of NERIST (North Eastern Regional Institute of Science and Technology) a Deemed University under the Govt. of India, in Arunachal Pradesh, India since July 2007. He has completed his Masters of Technology in Computer Science in the year of 2011. He did his Bachelor of Engineering from Jorhat Engineering C-ollege, Assam, in 2005 in Computer Science discipline. Currently he is pursuing PhD in the field of wireless sensor network. His major research

interests include Information Security, Cryptography, Signal Processing, Sensor Network etc. He is a member of professional societies like IEEE, CSI (India), IEI (India) and ISTE (India).

Md. Anwar Hussain is Professor in the department of Electro--nics and Comminication Engineering, NERIST (North Eastern Regional Institute of Science and Technology) a Deemed University under the Govt. of India, in Arunachal Pradesh, India. His area of research includes: High data rate wireless communication & network Routing & scheduling in Multi-hop wireless networks, Key distribution in Sensor networks, Multimedia data encryption & security, Mobile computing security, Time-series data modeling and prediction, Low power VLSI design, Climate change & modeling, Networks-on-Chip.