www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-5, Issue-4, August 2017
Research Paper

Int. J. Sc. Res. in
Network Security
and Communication

ISSN: 2321-3256

NCPKS- Neighbourhood Connectivity Predicted Key Distribution for Location Dependent Sensor Network

M. Saikia[1*], A. Hussain[2]

[1*]Dept. of CSE, NERIST, Itanagar, India
[2] Dept. ECE, NERIST, Itanagar, India

Corresponding Author: msk@nerist.ac.in, Tel.: +91-94022-75949

Received 29th Jul 2017, Revised 11th Aug 2017, Accepted 24th Aug 2017, Online 30th Aug 2017

***Abstract*—** Prior knowledge of positions of sensor network helps in key predistribution of a sensor network. Key predistribution is an important phase for ensuring security and it is done prior to deployment of sensor nodes into a specific target field. Intelligent robot can be used to deploy such nodes in their predetermined location. There are various key predistribution schemes (KPS in short) for wireless sensor network proposed earlier. Here in this paper, we propose a KPS by neighbour node connectivity prediction key predistribution technique to enhance probability of key share among nodes. The proposed algorithm is implemented and various simulations were done over different network scenario. The performance of the proposed scheme is discussed with the help of experimental results.

***Keywords*—** Wireless Sensor Network; Key Pre-distribution; CPKS; Connectivity; Resilience; Neighbourhood connectivity

I. INTRODUCTION

Wireless Sensor Networks (WSN) comprises of a large number of tiny, inexpensive, low computation powers and resource constrained devices called sensor nodes (SN) whose purpose is to sense or monitor changes in critical parameters such as sound, environmental pressure and temperature and communicate the observations locally or to the Base Station (BS) in a single or multi-hops routes. In recent days, wireless sensor network is broadly used in numerous applications such as health care, environment monitoring, military surveillance and many more [1]. In all those application security is a crucial issue as wireless sensor network is prone to adversarial attacks due to limited computation power of sensor nodes, lack of fixed infrastructure and uncontrolled environment. Heavy security scheme cannot be incorporated in those networks [2][3]. To enable safe communication among any two sensor nodes communication confidentiality, authentication and integrity are basic norms. From cryptographic point of view a simple possible ways in which secure communication can be established involves sharing a single key (symmetric key encryption) or sharing of different keys (asymmetric key encryption). However asymmetric key system is infeasible because it requires a lot of computation overhead. A symmetric encryption scheme is mostly chosen as a solution in this case and that lead to finding a proper way to upload keys on the sensor nodes. Since the network topology is not known prior to sensor deployment in the target area uploading keys prior to deployment is a challenging task. The keys that are stored in the memory of the sensors must be carefully chosen so that two neighbouring sensor nodes within their communication range must share at least one common key. Nodes which do not share a common key have to communicate through a path where a key is shared between each pair of adjacent nodes. In order to provide better performance, a key predistribution scheme depends on a number of attributes like local connectivity, global connectivity and resiliency etc. [5][14].

A key predistribution scheme has mainly three phases. In first phase keys are loaded to sensor nodes such that there is high probability of immediate key share. In second phase, when a node wanted to send some data securely they use their common shared key uses symmetric key encryption and in third phase, if two nodes do not have a common shared key then need to find a secure link via other nodes that share common keys among themselves i.e. establish a secure link between source node to destination node.

Several schemes have been developed for the key management, where Eschenauer and Gligor's [6][13] first pioneered a randomized key pre-distribution scheme is the foundation of the subsequent key distribution schemes. In this scheme, a large key pool of symmetric keys is generated by the key setup server then for each sensor node keys are randomly picked up from the key-pool and loaded into the sensor nodes before deployment. These keys along with their identities form a key-chain. Chan et al. [7] proposed a modification to the basic scheme of Eschenauer et al. Here the number of key requirement for key set up is increased, i.e. q common keys are required instead of one for establishing secure communication two neighbouring nodes. This scheme needs a larger key ring and smaller key pool as compared to the original Eschenauer et al scheme.

Blundo et al [8] proposed the polynomial pool-based key distribution scheme in order to establish pair-wise keys for a group of sensor nodes. The key setup server randomly generates λ -degree polynomial $f(x,y)=\sum_{i,j=0}^{\lambda} a_{i,j}x^i y^j$ over a finite field F_q, where q is a prime number that is large enough to accommodate a cryptographic key, such that it has the property of $f(x,y)=f(y,x)$.

Du et al. [9] and Liu et al. [8] recommend a threshold based key pre-distribution schemes, where links between uncompromised nodes remain unaffected, when number of compromised nodes is less than the predefined threshold. However, when number increases above threshold then entire network gets affected. Du et al. scheme is built to guarantee that any pair of nodes can establish a key among them and involves use of matrices and modular multiplications. Liu et al. scheme generated bivariate *t-degree* polynomials pool where nodes which shares same polynomial can compute pairwise key by evaluating the polynomial. Both schemes certainly enhance security but on the stake of huge computation and storage overhead for their coefficient.

A common inference drawn from the above discussed key predistribution schemes is that there is no priori deployment knowledge available while in some practical cases, certain deployment knowledge is available prior to sensor deployment. Prior knowledge availability gives advantage for a key predistribution scheme by exploiting deployment knowledge and avoids unnecessary key assignments to reduce memory overhead. Sensors are assumed to be deployed in a two dimensional target field to their expected location [9][11]. Two sensor nodes communicate with each other if they reside within their communication range. The geometric location of a sensor can be represented by a coordinate system in the deployment region [12]. Using the coordinate system and their communication range connectivity can be computed and accordingly keys can be assigned to those nodes which are within their communication range.

The paper is organized as follows: Section-I gives introduction to the key predistribution, section-II states the proposed scheme with algorithm and flow diagram. Section-III gives simulations results; section-IV gives analysis of the proposed scheme and section-V concludes the paper.

II. Proposed Scheme

A KPS scheme has been proposed by D. Liu and P. Ning named Closest Pair Key Distribution scheme [4], where they assign keys to neighbour nodes based on their coverage range. The basic scheme assigns pairwise keys to those nodes that are in its communication range and the number of key share limits by memory constrains of the sensor nodes. The CPKS scheme assumes that the setup server have knowledge of signal range, deployment error and expected position of the sensor nodes. The server assigns a unique sensor ID to refer to a particular sensor and a pairwise key that can form a direct secure link between two neighbour nodes.

The improvement over the existing CPKS is done with neighbour node's statistics of connectivity. If a node with less connectivity is found in its neighbour then highest preference is given to that node by assigning a key pair. Flow diagram of the proposed scheme is as shown in figure 1.

The algorithm Improved CPKS with neighbour connectivity prediction is as follows:

Algorithm:

```
Input: Key Ring Size, Network Size, Coverage Area,
Node Locations
OutPut: Key Ring
Initialize KeyIdentifyer:=1;
from i=1 to N
  from j=1 to N
   find neighbour nodes connectivity
   sort nodes in ascending order
   assign $K_{ij}$ =KeyIdentifyer;
  KeyIdentifyer:= KeyIdentifyer + 1;
    end
  end
end
```

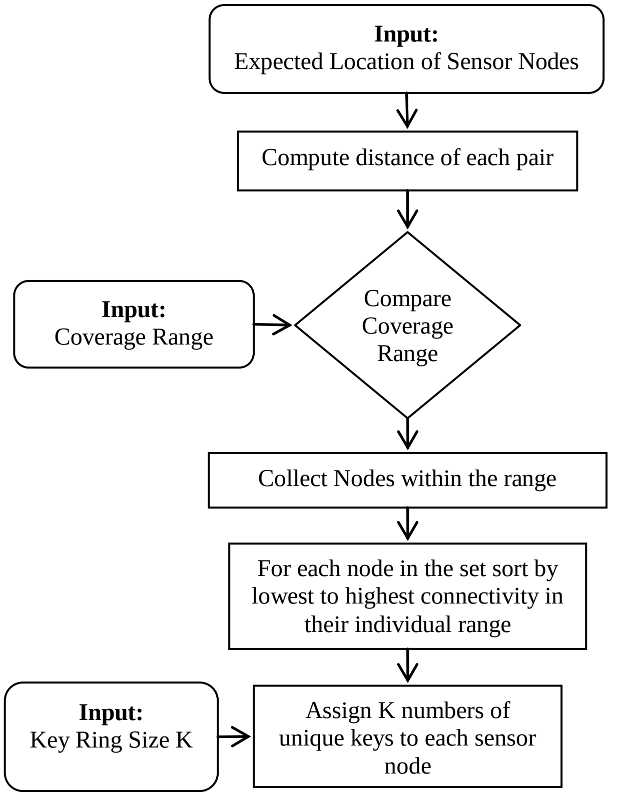
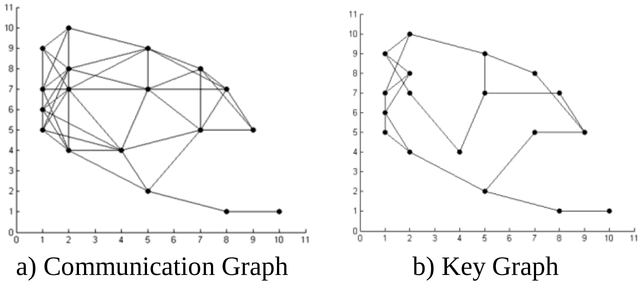

Input:
Expected Location of Sensor Nodes
Compute distance of each pair
Input:
Coverage Range
Compare
Coverage
Range
Collect Nodes within the range
For each node in the set sort by lowest to highest connectivity in their individual range
Input:
Key Ring Size K
Assign K numbers of unique keys to each sensor node

Fig.1. Basic Model of CPKS with Connectivity Probability

III. SIMULATOIN AND OUTCOME

Simulation of the algorithm was done for various network scenario of different size of network with different connectivity coverage range and location. Expected location of the sensor nodes are randomly generated and deployed over a specific region. Coverage range of each sensor node is assumed to be same. Two nodes within is communication range can communicate the same is shown in figure 2(a) as a communication graph. On application of the CPKS-NCP algorithm we restrict the number of keys that can hold by any sensor node to a fixed number, therefore secure communication can happen among the nodes that share a common key the resultant graph called a key graph obtained after applying the algorithm is shown in fig 2 (b).



a) Communication Graph b) Key Graph

Fig.2. Simulation Results with N=20 Coverage Range=3

meter in an area of 10 meter sq.

IV. ANALYSIS OF RESULTS

To find performance analysis the following metric have been considered.

Local Connectivity (Pr_1): Local connectivity or simply probability is the measure of immediate key share among nodes and is calculated as

$P_{r_1} = 1 - \frac{\binom{|K|-k}{k}}{\binom{|K|}{k}}$ Where $|K|$= Key pool size and k= key ring size.

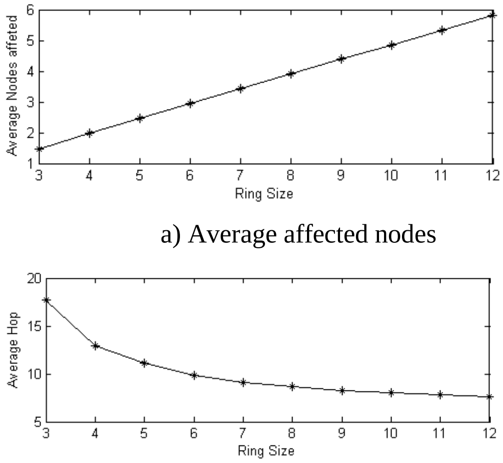
Global connectivity: The part of nodes that are in the largest connected graph over the number of all nodes is referred to as Global connectivity.

Resiliency: Resiliency is the ability of the network to protect the links when a number of nodes are dead or attacked. Other performance attributes related to the design of WSN are computational cost and hardware cost. Computational cost is the summation of the overall computation performed in the phases of a Key Predistribution Scheme (KPS) and hardware cost include the cost of the memory and battery in all nodes. *Number of affected nodes:* In case node failure or node compromise how the network can survive is measured using number of nodes affected.

Resilience (fails): Resilience is the measure of how a network is survive in case of attack or node compromise and is calculated as $fail_s = \left(1 - \left(1 - \frac{k}{|K|}\right)^s\right)^q$ Where *q*= no. of key share, *s* is no. of node fails.

Average Hop Count: Average hop count refers to collective information from the entire sensor network. It is a measure of average number of required hops to communicate between any two nodes in the network. The average path length or average hop count is also considered as a performance evaluation metric for key pre-distribution scheme.

The network is simulated for large number of nodes ranging from 100 to 1000 nodes over an area of 100 square meters. The algorithm assigns keys to a sensor node based on neighbour connectivity probability and forms a key ring/ key chain. The table-1 shows probability, average hop count, affected nodes, resilience using improved CPKS. From the table it is seen that the probability of key share decreases when network size increases while keeping same ring size and deployment area. Average hop count and affected number of nodes increases along with increase in network size. A plot is also shown in figure 4 (a) average affected nodes vs. key ring size and (b) average hop count vs. ring size. As nodes can communicate securely with each other through multi-hop path, an experiment result shows number of multi-hop path with key ring size 3, 4, 5 and 6 in the figure 5. It is observed that for high value of key ring size nodes can communicate in smaller hop count.



a) Average affected nodes

b) Average hop count

Fig. 4. Affected Nodes and Average Hop Plot N=1000

Table 1: Probability, Average hop count, Affected Nodes, Resilience using improved CPKS

Nodes	Key Pair	Probability	Avg. hop	Affected Nodes	Resilience
100	138	0.027	0.325	1.380	0.986
200	547	0.027	2.209	2.735	0.986
300	1101	0.024	8.228	3.670	0.987
400	1711	0.021	7.479	4.277	0.989
500	2230	0.017	7.524	4.460	0.991
600	2804	0.015	7.635	4.673	0.992
700	3322	0.013	7.470	4.745	0.993
800	3777	0.011	7.765	4.721	0.994
900	4332	0.010	8.035	4.813	0.994
1000	4849	0.009	7.985	4.849	0.995

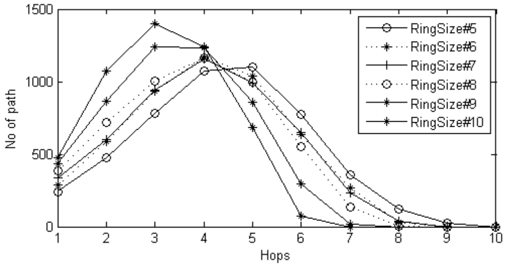


Fig.5. Multi-hop path in network of 100 nodes

A comparison of probability of key share in traditional CPKS vs. our improved proposed scheme is shown in figure 6. Figure 7 show a comparison of average hop in both the schemes, where is seen that higher value of average hop count requires to establish a secure link in case of non key share among nodes.

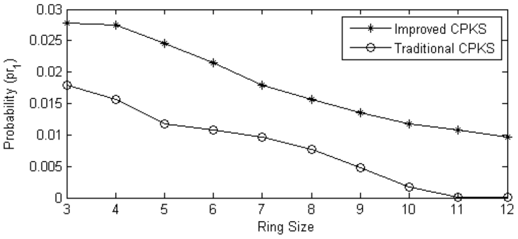


Fig.6. Probability comparison in traditional CPKS vs Improved CPKS

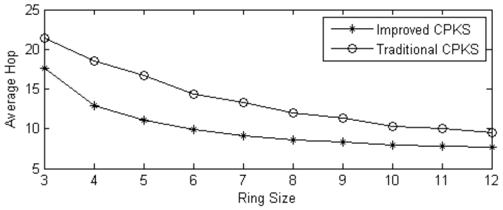
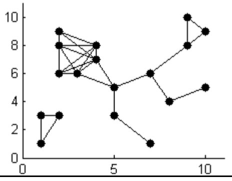
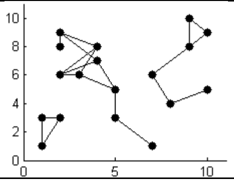


Fig.7. Average hop comparison in traditional CPKS vs Improved CPKS

V. Conclusion

High connectivity is desirable with minimum number of secret keys stored in sensor nodes. Closest pair key predistribution with neighbour node probability (CPKS-NCP) gives a better performance with smaller number of key storage in the sensor nodes. Resilience is found to be high as compared to various existing schemes as capture of one node affects only a few links in the key graph as seen from various experiments. Experiments have been performed to show its multi-hop path establishment that can give security in packet routing. Furthermore the proposed scheme ensures high connectivity with every node within its communication range. Nodes not lying in its communication range can always find a path via other nodes resulting high global connectivity.

Exp. No.	Communication Graph	Key Graph	Topology
1			Nodes=20 Key Ring size=3

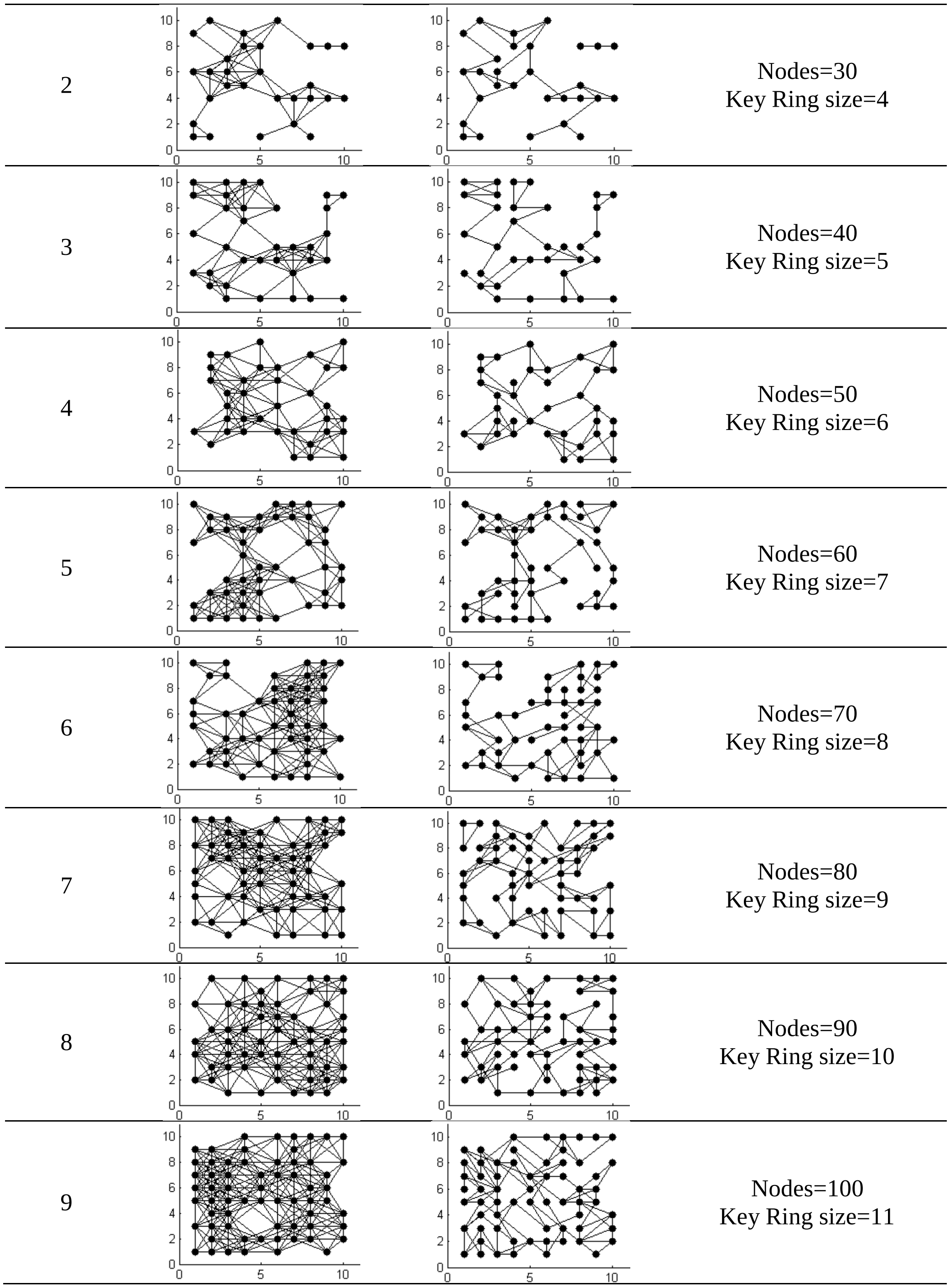


Fig.3. Communication graph and key graph

REFERENCES

[1] Hussain, M. A., Khan, P., Kwak kyung, "*WSN Research Activities for Military Application*", 11th International Conference on Advanced Communication Technology, pp.271–274, 2009.

[2] Virali Girdhar and Gaurav Banga, "*A Comparative Analysis of Different Movement Models in MANET*", International Journal of Computer Sciences and Engineering, Vol.3, Issue.6, pp.9-13, 2015.

[3] Zhu, S., Setia, S., Jajodia, S., *"LEAP+: Efficient security mechanisms for large-scale distributed sensor networks",* ACM Transactions on Sensor Networks, Vol.2, Issue.4, pp.500–528, 2006.

[4] D. Liu and P. Ning, "*Location-based pairwise key establishments for static sensor networks*," in Proceedings of 1st ACM

Workshop on security of ad-hoc and sensor networks, Fairfax, Virginia, pp. 72–82, 2003.

[5] Neetu Rani and Manik Gupta “*Review on key predistribtion schemes in Wireless Sensor Networks*” International Journal of Advanced Smart Sensor Network Systems (IJASSN), Vol 6, No.1, 2016

[6] Eschenauer, L., & Gligor, V. D., “ *A key-management scheme for distributed sensor networks*”, Proceedings of the 9th ACM Conference on Computer and Communications Security, pp.41–47, 2002.

[7] Chan, H., Perrig, A., & Song, D., “*Random key predistribution schemes for sensor networks*”, In Proceedings - IEEE Symposium on Security and Privacy, Vol. 2003, pp. 197–213, 2003.

[8] Blundolz, C., Santis, A. De, Herzberg, A., Kutten, S., Vaccaro, U., Yung, M., & Salerno, U., “*Perfectly- Secure Key Distribution for Dynamic Conferences*”, Advances in Cryptology — CRYPTO’ 92, 23, 471–486, 1993.

[9] Du, W., Han, Y. S., Deng, J., & Varshney, P. K., “*A pairwise key pre-distribution scheme for wireless sensor networks*”, In Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, pp. 42–51, 2003.

[10] A. K. Das, A. Das, S. Mohapatra and S. Vavilapalli, "*A Location-Aware Scheme for Key Establishment in Wireless Sensor Networks*", 2006 1st International Conference on Communication Systems Software & Middleware, New Delhi, 2006, pp. 1-5, 2003.

[11] Anjum, F., “*Location dependent key management using random key predistribution in sensor networks*”, In proceedings of WiSe, 2006.

[12] Aditya Singh Mandloi and Vinita Choudhary, "*An Efficient Clustering Technique for Deterministically Deployed Wireless Sensor Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.6-10, 2013.

[13] Sanchita Gupta and Pooja Saini, "*Modified Pairwise Key Pre-distribution Scheme with Deployment Knowledge in Wireless Sensor Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.21-23, 2013.

[14] Saikia, Monjul; Acharjamayum, Irani; Hussain, Md.A., "*A review on desirable measures for good Key Pre-distribution Scheme in wireless sensor network,*" (ICGCIoT), 2015 pp.129-134, 8-10 Oct. 2015 doi: 10.1109/ ICGCIoT.2015.7380443.

Author's Profile

Mr. Monjul Saikia has been serving as an Assistant Professor in the department of Computer Science and Engineering, 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 from the Department Computer Science and Engineering, NERIST in the year of 2011. He did his Bachelor of Engineering from Jorhat Engineering College, Jorhat Assam, in 2005 in Computer Science discipline. Currently he is pursuing PhD in the Department of Electronics and Communication Engineering, NERIST. His major research interests include Information Security, Cryptography, and Wireless Sensor Network. He is a member of professional societies like IEEE, CSI (India), IEI (India) and ISTE (India).

Prof. Md. A. Hussain, Professor, Department of Electronics and Communication Engineering, North Eastern Regional Institute of Science and Technology. Ph.D (in Engineering), Optical Fiber Communication from Jadavpur University, Kolkota in 2002 (Feb.) in 2002. His area of research includes: High data rate wireless communication & networks, Routing & scheduling in Multi-hop wireless networks, Key distribution in Sensor networks, Multimedia data encryption & security, Mobile computing security, Time-series data modelling and prediction, Low power VLSI design, Climate change & modelling, Networks-on-Chip.