



## International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

# Secure and Performance Analysis of Data Transaction in Clustered Wireless Sensor Networks

Pradeep G<sup>1</sup>, Prithi S<sup>2</sup>, Gowri G<sup>3</sup>

P.G. Scholar, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore, India<sup>1</sup>.

Assistant Professor, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore, India<sup>2</sup>.

P.G. Scholar, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore, India<sup>3</sup>.

**ABSTRACT:** In Wireless Sensor Network adding security is a crucial issue, the system performance is improved by clustering the Network. The Clustering are formed periodically and dynamically by using Position based Aggregator Node Election for Wireless Sensor Network (PANEL). We propose two protocols called SET-IBS and SET-IBOOS using Id-Based Digital Signature and ID-Based Online-Offline Digital Signature respectively which will add the authentication to the sensed data. For Security the data is encrypted at sender (Leaf Node) and Decrypted at receiver (Base Station). The Security is analysed by investigating various attacks are Passive Attack, Active Attack, and Node Compromising Attack. The Calculating and Simulation show the efficiency and security of the protocol and the result also shows that the proposed protocol have better performance and security than the Existing Protocols.

**KEYWORDS:** Clustered Wireless Sensor Network, SET-IBS, SET-IBOOS, Digital Signature, and Cryptography.

### I. INTRODUCTION

Wireless Sensor Network is a collection of sensor nodes which are specially distributed for monitoring physical or environmental condition such as temperature, sound, pressure, motion, etc. Each node are capable of sensing the environment locally and sending the data to another sensor node or a base station in Wireless Sensor Network. Performance and efficient data transaction is a major issue in Wireless Sensor Network. the most certain applications of Wireless Sensor Network are Process Management, Health Care Monitoring, Air Pollution Monitoring, Forest Fire Detection, Natural Disaster Prevention and Military Applications. The Secure and Efficient Data Transmission (SET) is necessary in Wireless Sensor Network.

In Wireless Sensor Network the clustering is achieved for Network Scalability and Management which increase the lifetime of the sensor node and reduces the energy consumption. In the clustered Wireless Sensor Network, every cluster has a Cluster Head (CH) and the remaining nodes in the cluster are Leaf Nodes (Non Cluster Head Sensor Node), the data aggregated by the Leaf Node (Non Cluster Head Sensor Nodes) sends to the Cluster Head (CH) and the Cluster Head (CH) then transmits the data to the Base Station. The Low Energy Adaptive Cluster Hierarchy (LEACH) is most probably used for Low Energy Consumption of sensor node in Wireless Sensor Network. To avoid the quick energy consumption of CH's the LEACH protocol will randomly rotates the CH's among the sensor nodes which will leads to improving the Network lifetime. The Protocols which are similar to LEACH are APTEEN and PEACH.

Implementing Security to the LEACH like protocol is the challenging because the data link and Network Clusters are dynamically, randomly and periodically rearranged. So the common key distribution and Node to Node trust was lacking in the protocols like LEACH (The distributed Wireless Sensor Network are existing solution but not for the Clustered Wireless Sensor Network (CWSN). The most similar protocols to LEACH like protocol are SecLEACH, GS-LEACH and RLEACH, these protocols are most probably uses symmetric key management for security in which will cause so called orphan node problem. The orphan node is a problem in which any node which does not share the pairwise key with the other nodes in the preloaded key ring.



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

To reduce the storage cost of symmetric key, the key ring was not enough for sharing pairwise symmetric key with all the nodes in the Wireless Sensor Network so the orphan node will elects themselves as a Cluster Head. It does not share with any other node then it often decrease energy of the node often a long operation. If the CH's are elected by themselves so the energy consumption is more in every Cluster Head's. The possibility of asymmetric key management (PANEL) had been recently used in Wireless Sensor Network which compensates the disadvantages from symmetric key management. The cryptography offering one of the most crucial security services was the Digital Signature in asymmetric key management, the id and public key was obtained from Digital Certificate. The Id-based Digital Signature is based on factoring integer from Id-based Cryptography. IBOOS is proposed to reduce computational overhead in the signature process. We proposed two protocols for clustered Wireless Sensor Network called IBS and IBOOS by IBS scheme and the IBOOS scheme. The proposed and the key idea behind the proposed protocol IBS and IBOOS are to authenticate the encrypted data by using digital signature to the sensed data (Message Packet) which are efficient in communication and applying asymmetric key management for security. The secret key and paring parameters are preloaded and distributed in all sensor node by the base station initially which will overcomes key escrow problem. Finally we just compare the proposed protocol with the existing protocol for efficiency and security.

## II. RELATED WORK

In Wireless Sensor Network the clustering is achieved for Network Scalability and Management which increase the lifetime of the sensor node and reduces the energy consumption. The Low Energy Adaptive Cluster Hierarchy (LEACH) is most probably used for Low Energy Consumption of sensor node in Wireless Sensor Network. To avoid the quick energy consumption of CH's the LEACH protocol will randomly rotates the CH's among the sensor nodes which will leads to improving the Network lifetime. The Protocols which are similar to LEACH are APTEEN and PEACH. Implementing Security to the LEACH like protocol is the challenging because the data link and Network Clusters are dynamically, randomly and periodically rearranged. So the common key distribution and Node to Node trust was lacking in the protocols like LEACH (The distributed Wireless Sensor Network are existing solution but not for the Clustered Wireless Sensor Network (CWSN). The most similar protocols to LEACH like protocol are SecLEACH, GS-LEACH and RLEACH, these protocols are most probably uses symmetric key management for security in which will cause so called orphan node problem. The orphan node is a problem in which any node which does not share the pairwise key with the other nodes in the preloaded key ring.

## III. PROPOSED ALGORITHM

The proposed and the key idea behind the proposed protocol IBS and IBOOS are to authenticate the encrypted data by using digital signature to the sensed data (Message Packet) which are efficient in communication and applying asymmetric key management for security. The secret key and paring parameters are preloaded and distributed in all sensor node by the base station initially which will overcomes key escrow problem.

### A. Design Considerations:

- Create a Network model.
- Initialization of Protocol (IBS).
- Operation of Protocol (IBS).
- Initialization of Protocol (IBOOS).
- Operation of Protocol (IBOOS).
- Performance Evaluation.

### B. Description of the Proposed Algorithm:

Aim of the proposed protocol is to add Security and Authentication of the sensed data and also the reduction of energy consumption of sensor nodes. The proposed protocol having the following steps.

#### Step 1: Create a network model.

An undirected graph  $G(V,E)$  where the set of vertical  $V$  represent the sensor node in the network and  $E$  represents set of edges in the graph which represents the physical and logical links between the sensor nodes.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Let  $n$  denotes the Number of sensor nodes of  $n_1, n_2, \dots, n_m$  and  $D$  is the data of  $d_1, d_2, \dots, d_n$ , the sender and receiver node which is represented as  $N_i$  and  $N_j$ .  $t_{ij}$  Denotes the delay of data transmission.

## Step 2: Initialization of Protocol (IBS):

**Setup Phase:** Base Station will predistribute the key to all the Sensor Node.

- Generate a Encryption key  $K$ , where  $k \in [m - 1]$
- Generate the pairing parameters  $(p, q, \frac{E}{F_p}, \mathbb{G}_1, \mathbb{G}_2, e)$
- Choose two hash function  $\mathbb{G}_1$  and  $h$
- Pick a random integer as the master key set  $P_{pub} = \tau P$
- Sensor Nodes are preloaded by system parameters  $param = (k, m, p, q, \frac{E}{F_p}, \mathbb{G}_1, \mathbb{G}_2, e, H, h, P, \tau)$

**Extraction Phase:**  $sek_j = \tau H(ID_j || t_j)$  from master key and  $ID_j$  where  $ID_j$  and  $t_j$  is the time stamp of node  $j$ 's time interval in the current round that is generated by its CH's I from the TDMA control.

**Signature Signing:** The sensor node  $j$  picks a random number  $\alpha_j \in \mathbb{Z}_q^*$  and computes  $\theta_j = e(P, P)^{\alpha_j}$ . The sensor node further computes

$$c_j = h(C_j || t_j || \theta_j).$$

$$\sigma_j = c_j sek_j + \alpha_j P,$$

**Verification Phase:** The Base Station finally authenticate the data by current time interval  $t_j$  whether the received Message is currently sent

$$\theta_j = e(\sigma_j, P) e(H(ID_j || t_j), -P_{pub})^{c_j}$$

## Step3: Operation of Protocol (IBS)

Once the Initialization of protocol is over, the communication was done in rounds by the following steps. In the verification phase the CH I sends the message to all the leaf nodes in the cluster.

The leaf node will send the aggregated data by encrypting and adding digital signature with it by the param to its Cluster Head. Cluster Head sends the aggregated data to the Base Station. Finally the Encrypted data is decrypted in the Base Station.

## Step 4: Initialization of Protocol (IBOOS)

**Setup Phase:** Base Station will predistribute the key to all the Sensor Node.

- Generate a Encryption key  $K$ , where  $k \in [m - 1]$
- Generate the pairing parameters  $(p, q, \frac{E}{F_p}, \mathbb{G}_1, \mathbb{G}_2, e)$
- Choose two hash function  $\mathbb{G}_1$  and  $h$
- Pick a random integer as the master key set  $P_{pub} = \tau P$
- Sensor Nodes are preloaded by system parameters  $param = (k, m, p, q, \frac{E}{F_p}, \mathbb{G}_1, \mathbb{G}_2, e, H, h, P, \tau)$

**Extraction Phase:**  $sek_j = \tau H(ID_j || t_j)$  from master key and  $ID_j$  where  $ID_j$  and  $t_j$  is the time stamp of node  $j$ 's time interval in the current round that is generated by its CH's I from the TDMA control.

**Offline Signing Phase:** Node will generate the offline value with the time stamp

$$g^{s_j} = g^{r_j} g^{H(R_j, ID_j) \tau \text{mod } q} = R_j X^{H(R_j, ID_j) \text{mod } q}$$

$$\hat{\sigma}_j = g^{-t_j}$$

**Online Signing Phase:** Node will generate the online value

$$h_j = H(C_j, ID_j)$$

$$z_j = \hat{\sigma}_j + h_j s_j \text{mod } q$$

$$\sigma_j = g^{\hat{\sigma}_j}$$

**Verification Phase:** The Base Station finally authenticate the data by current time interval  $t_j$  whether the received Message is currently sent

$$\theta_j = e(\sigma_j, P) e(H(ID_j || t_j), -P_{pub})^{c_j}$$



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

## Step5: Operation of Protocol (IBOOS)

Once the Initialization of protocol is over, the communication was done in rounds by the following steps. In the verification phase the CHI sends the message to all the leaf nodes in the cluster.

The leaf node will send the aggregated data by encrypting and adding digital signature with it by the param to its Cluster Head. Cluster Head sends the aggregated data to the Base Station. Finally the Encrypted data is decrypted in the Base Station.

## Step6: Performance Evaluation

The existing and the proposed protocols performance are evaluated.

In the existing protocol the LEACH, SecLEACH are used for providing security and authentication of sensed data in the Wireless Sensor Network. In the proposed protocol we have proposed protocol Id-Based digital Signature (IBS) and Id-Based digital Signature (IBOOS) which are used for security and authentication. Here we are comparing the proposed protocol with the existing protocol for the performance evaluation.

## IV. SIMULATION RESULTS

The simulation studies involve the deterministic small network topology with 30 nodes as shown in Fig.1. The proposed secure and performance of clustered Wireless Sensor Network is implemented in NS-2. the simulation results of message size for transmission and energy consumption is measured for the proposed secure and efficient data transmission (SET) protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS. Number of nodes is defined as number of nodes is taken in the network setup. Energy Consumption which refers to the amount of energy consumed in a WSN. Message size for transmission which is defined as the message packet size for data transmission in the wireless sensor networks.

In the above Fig.2. Shows the energy consumption graph. The X-axis denotes the number of nodes. Y-axis denotes the energy consumption. In the proposed method secure and efficient data transmission (SET) protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS. In this method, the number of nodes is increased, the energy consumption is increased. In the above Fig.3 Shows the message size graph. The X-axis denotes the number of nodes. Y-axis denotes message size. In the proposed method secure and efficient data transmission (SET) protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS. This graph clearly shows that the number of nodes is increases the message size is increases in the proposed methods.

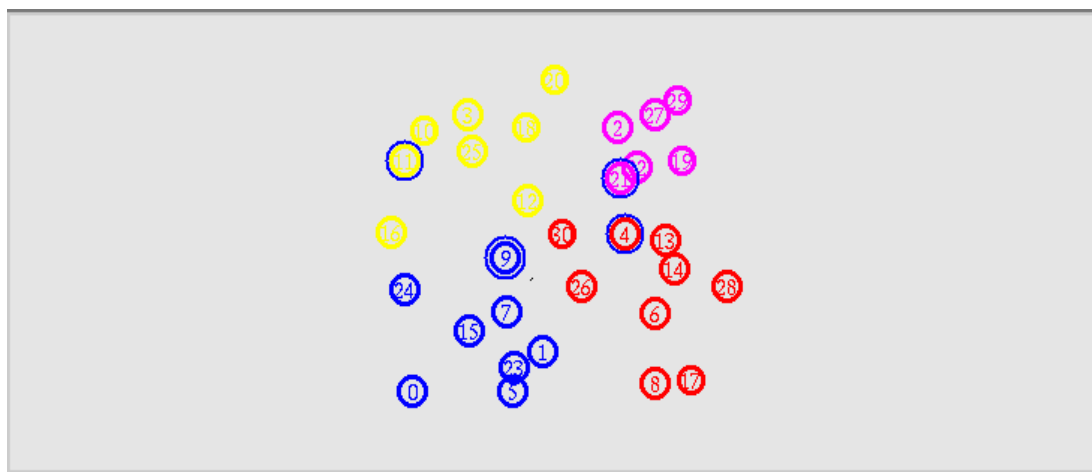


Fig.1 DEPLOYMENT OF WSN

In the above Fig.1 Shows the Deployment of Wireless Sensor Network using the Network Simulator OMNeT++ 3.0

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

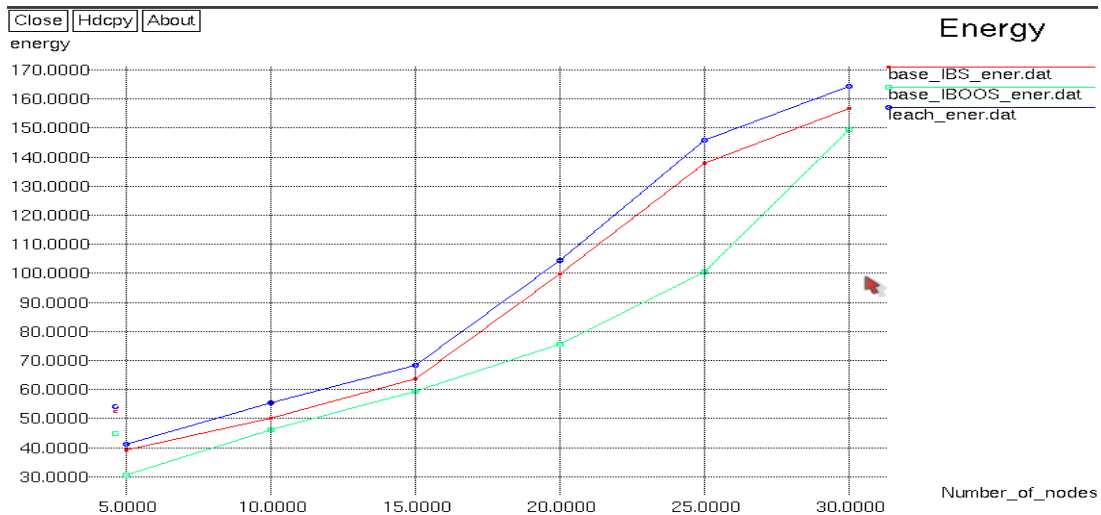


Fig.2 Energy Consumption Graph of three protocols

In the above Fig.2. Shows the energy consumption is shown in this graph. In the X-axis denotes number of nodes. Y-axis denotes energy consumption is taken. In the existing system, LEACH protocol is used. The low-energy adaptive clustering hierarchy (LEACH) protocol is presented which is a widely known and effective one to reduce and balance the total energy consumption for cluster-based Wireless sensor networks. In the proposed method secure and efficient data transmission (SET) protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS. In this method, the number of nodes is increased, the energy consumption is increased.

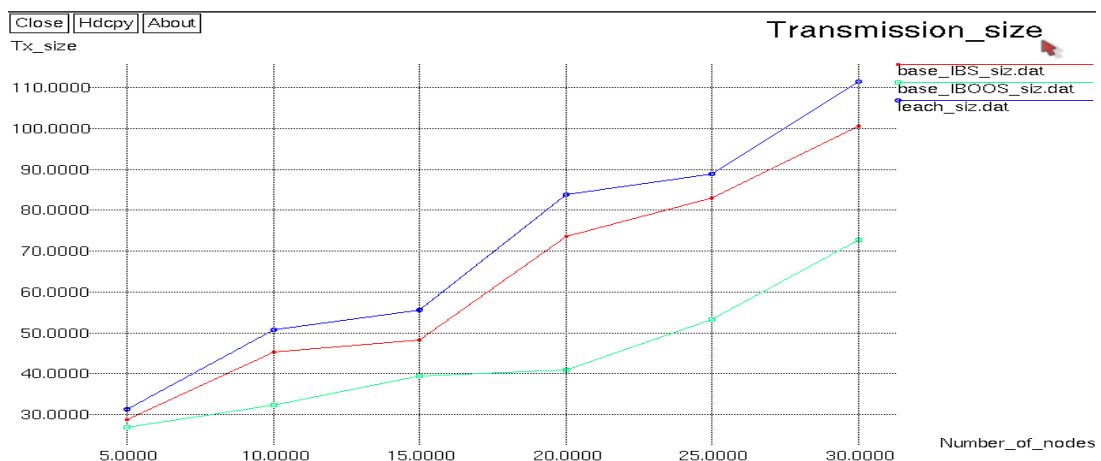


Fig.3. Message size for transmission

In the above Fig.3 shows The message size is shown in this graph. In the X-axis denotes number of nodes. Y-axis denotes message size. In the existing system, LEACH protocol is used. The low-energy adaptive clustering hierarchy (LEACH) protocol is presented which is a widely known and effective one to reduce and balance the total energy consumption for cluster-based Wireless sensor networks. In the proposed method secure and efficient data transmission (SET) protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS. This graph clearly shows that the number of nodes is increases the message size is increases in the proposed methods.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

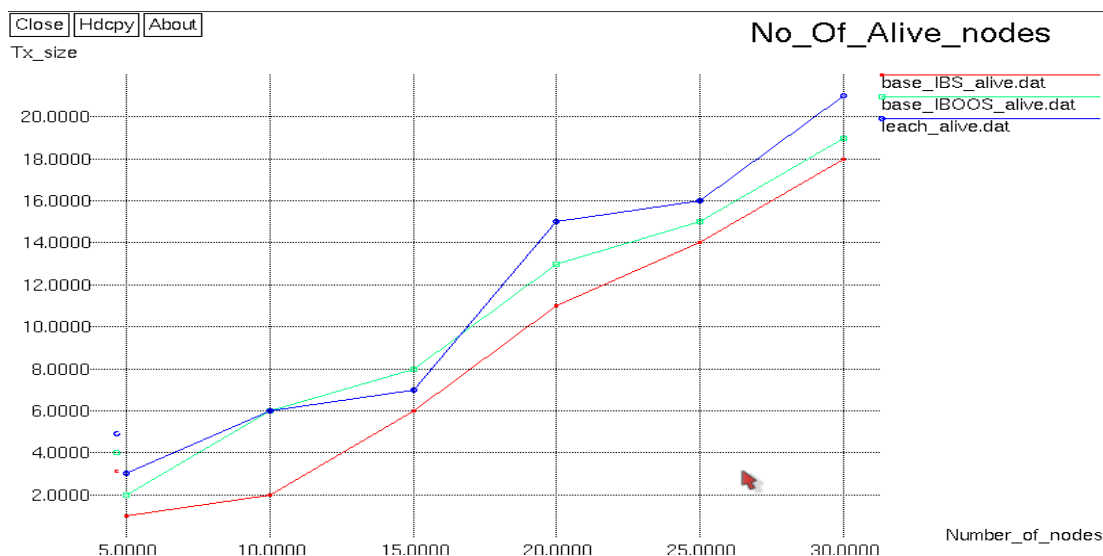


Fig.4. Number of alive nodes

The number of alive nodes is shown in this graph. In the X-axis denotes number of nodes. Y-axis denotes number of alive nodes. In the existing system LEACH protocol is used. The low-energy adaptive clustering hierarchy (LEACH) protocol is presented which is a widely known and effective one to reduce and balance the total energy consumption for cluster-based Wireless sensor networks. This shows that the comparison graph of alive nodes of protocols of LEACH, SET-IBS and SET-IBOOS protocols. The results demonstrate that the proposed SET-IBS and SET-IBOOS protocols consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS and/or IBOOS process.

## V. CONCLUSION AND FUTURE WORK

The simulation results showed that the proposed algorithm performs better than the existing algorithm with secure data transmission and energy consumption. In the existing method, the data transmission issues and the security issues is analysed in CWSNs. The insufficiency of the symmetric key management for secure data transmission has been discussed. Then the two secure and efficient data transmission protocols are presented which is called SET-IBS and SET-IBOOS for CWSNs. The proposed algorithm provides energy efficient path for data transmission and maximizes the lifetime of Wireless Sensor Network. The proposed algorithm can be compared with other energy efficient algorithm. We have used very small network of 30 nodes, as number of nodes increases the complexity will be too.

For future work in order to provide efficient security some of the modifications are considered in the SET-IBS and SET-IBOOS protocols.

## REFERENCES

1. A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," *Computer Comm.*, vol. 30, Issue nos. 14/ 15, pp. 2826-2841, 2007.
2. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans. Wireless Comm.*, vol. 1, no. 4, pp. 660- 670, Oct. 2002.
3. A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," *IEEE Trans. Parallel & Distributed Systems*, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
4. S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," *Computer Comm.*, vol. 30, nos. 14/15, pp. 2842-2852, 2007.
5. K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," *Int'l J. Computer Applications*, vol. 47, no. 11, pp. 23-28, 2012.
6. L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," *Signal Processing*, vol. 87, pp. 2882-2895, 2007.








# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

7. P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.

## BIOGRAPHY

	<sup>1</sup> <b>Pradeep G</b> is a P.G. Scholar, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore. He received Bachelor of Engineering in 2012 from Anna University, Chennai India.
	<sup>2</sup> <b>Prithi S</b> is a Research Scholar and Assistant Professor, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore. She received Master of Engineering in 2007 from Anna University, Coimbatore. India.
	<sup>3</sup> <b>Gowri G</b> is a P.G. Scholar, Department of CSE, R.V.S. College of Engineering and Technology, Coimbatore. He received Bachelor of Engineering in 2012 from Anna University, Chennai India.