ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

Secure Routing in Heterogeneous Wireless Sensor Networks with Intrusion Detection and a Differential Evolution based Thermal Aware Optimization Algorithms

A.SHAKIL AHMED[1], R.VINOTH[2], M.E.HARIKUMAR[3], AJITH.B.SINGH[4], K.NIVETHITHA[5]

Assistant professor, E & I, Sethu Institute of Technology, Kariapatti, Tamilnadu, India[1,2,3,4,5]

Abstract: Wireless sensor networks and VLSI design are tremendously being used in different environments to perform various monitoring tasks such as search, rescue, disaster relief, target tracking and a number of tasks in smart environments. Node localization is required to report the origin of events, assist group querying of sensors, routing and to answer questions on the network coverage. This paper reviews different approaches of node localization discovery in wireless sensor networks. Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. This paper describes a thermal modeling approach for VLSI Floor planning that is easy to use and computationally efficient. It is based on Differential Evolution (DE) algorithm based thermal-aware floor-planning framework which optimizes both chip area and total wire length. We discuss the network connectivity and broadcast reach ability, which are necessary conditions to ensure the corresponding detection probability in a WSN. Our simulation results validate the analytical values for both homogeneous and heterogeneous WSNs. The experimental result shows that DE can produce good optimal thermal solutions for MCNC benchmarks.

Keywords: Intrusion detection, Wireless Sensor Network (WSN), Differential Evolution algorithm, B*tree, Hotspot tool

INTRODUCTION

Wireless Sensor Network (WSN) is a collection of spatially deployed wireless sensors of small size by which we monitor various changes of environmental conditions(e.g., forest fire, air pollutant concentration, and object moving) in a collaborative manner without relying on any underlying infrastructure support [1].Since most applications depend on a successful localization, i.e. to compute their positions in some fixed coordinate system, it is of great importance to design efficient localization algorithms.

As technology advances, the design complexity increases and the circuit size is getting larger. To cope with the increasing design complexity, hierarchical design and IP modules are widely used. This trend makes module floorplanning/placement much more critical to the quality of a VLSI design than ever. Floorplanning is an important step in VLSI physical design. It can roughly estimate the layout of a given set of functional blocks. The primary objective for floorplanning is to minimize the total area required to accommodate all of the functional blocks on a chip.

Intrusion detection (i.e., object tracking) in a WSN can be regarded as a monitoring system for detecting the intruder that is invading the network domain. Fig. 1gives an example that sensors are deployed in a square area (A=L*L) for detecting the presence of a moving intruder. The intrusion detection application concern show fast the intruder can be detected by the WSN. If sensors are deployed with a high density so that the union of all sensing ranges covers the entire network area, the intruder can be immediately detected once it approaches the network area. However, such a high-density deployment policy increases the network investment and may be even unaffordable for a large area. As shown in Fig. 1, the intrusion distance is referred as D and defined as the distance between the points the intruder enters the WSN, and the point the intruder is detected by the WSN system. This distance is of central interest to a WSN used for intrusion detection. In this paper, we derive the expected intrusion distance and evaluate the detection probability in different application scenarios. Given a maximal allowable intrusion distance D_{MAX}=£, we theoretically capture the impact on the detection probability in terms of different network parameters, including node density, sensing range, and transmission range. For example, given an expected detection
distance E(D), we can derive the node density with respect to sensors' sensing range, thereby knowing the total number of sensors required for WSN deployment. In a WSN, there are two ways to detect an object (i.e., an intruder): single-sensing detection and multiple-sensing detection. In the single-sensing detection, the intruder can be successfully detected by a single sensor. On the contrary, in the multiple-sensing detection, the intruder can only be detected by multiple collaborating sensors [4]

The main contributions of this paper can be summarized as follows:

- Create a network scenario and locate the nodes via energy efficient localization algorithm.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

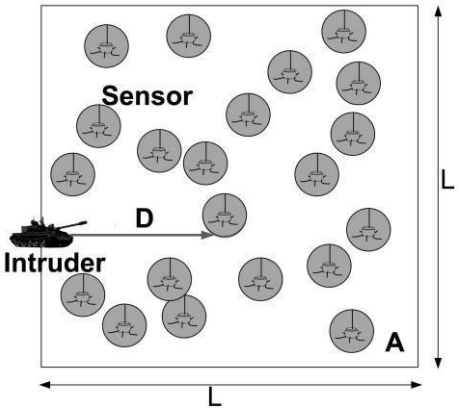


Fig. 1. Intrusion detection in a WSN.

- Developing an analytical model for intrusion detection in WSNs, and mathematically analyzing the detection probability with respect to various network parameters such as node density and sensing range.
- Applying the analytical model to single-sensing detection and multiple-sensing detection scenarios for homogeneous and heterogeneous WSNs.
- Defining and examining the network connectivity and broadcast reachability in a heterogeneous WSN.
- In this proposed work, the tool named HotSpot is used to calculate the maximum temperature amongst all the blocks in the floor plan. The maximum temperature thus calculated is used in the objective function of the Differential Evolution algorithm routine inside the floor planner.

RELATED WORK

Intrusion detection is one of the critical applications in WSNs, and recently, several approaches for intrusion detection in homogeneous WSNs have been presented [3],[4]. The focus of these approaches aims at effectively detecting the presence of an intruder. First, the problem is investigated from the aspect of the network architecture. Kung and Vlah [9] take advantage of a hierarchical tree structure to effectively track the movement of an intruder. the intrusion detection problem has been considered from the constraint of saving network resources.

we provide a comprehensive theoretical analysis on the intrusion detection in both homogeneous and heterogeneous WSNs [10]. The detection probability is theoretically captured by using underlying network parameters. The analytical results indicate the improvement on the detection quality in a heterogeneous WSN, as compared to a homogeneous WSN, either for the single sensing detection or the multiple-sensing detection scenarios.

B*tree representation

B*-trees are based on ordered binary trees representation. By comparing to the properties of ordered binary trees, B*-trees are very easy for implementation and can perform the respective primitive tree operations search, insertion, and deletion. The representations for non-slicing floorplans need at least O(n)time for each of these operations, where n is the number of modules. The transformation between an admissible placement and its induced B*-tree takes only linear time. The B*tree is very flexibe for handling the floorplanning problem with various types of modules. B*tree has fast and easy implementation and also it has a smaller solution space and encoding cost.

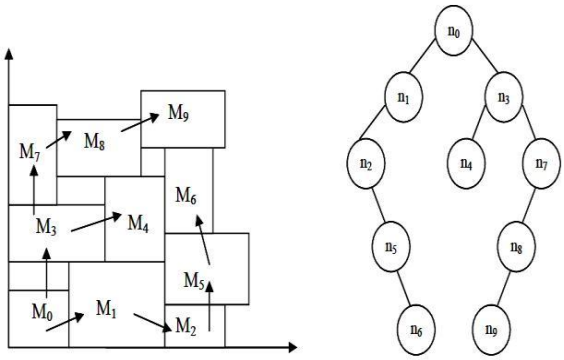


Fig. 2:(a) Admissible Placement (b) B*tree representation

INTRUSION DETECTION AND LOCALISATION MODELS

The localization methods taken for our analysis are:

- ***Time based methods (ToA, TDoA)****:* These methods record the time-of-arrival (ToA) or time-difference-of-arrival (TDoA). The propagation time can be directly translated into distance, based on the known signal propagation speed

- ***Received Signal Strength Indicator (RSSI)****:* RSSI measures the power of the signal at the receiver and based on the known transmit power, the effective propagation loss can be calculated.

In order to evaluate the quality of intrusion detection in WSNs, we define two metrics as follows:

- ***Intrusion distance***: The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time.

- ***Average intrusion distance:*** The average intrusion distance is defined as the expected distance that the intruder travels before it is detected by the WSN for the first time.

NETWORK MODEL

We consider a WSN in a two-dimensional (2D) plane with N sensors, denoted by a set N = (n1, n2, . . . , n_N), where n_N is the N^{th} sensor. These sensors are uniformly and independently deployed in a square area A = L* L. All sensors are static once the WSN has been deployed. Denote the node density of the homogeneous WSN as μ.

We then focus on a heterogeneous WSN with two types of sensors:

- Type I sensor that has a larger sensing range rs1, as well as a longer transmission range rx1
- Type II sensor that has a smaller sensing range rs2, as well as a shorter transmission range rx2.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

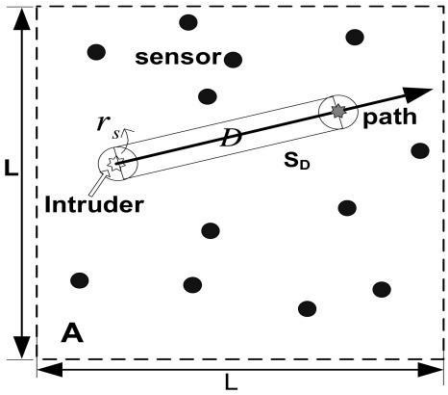
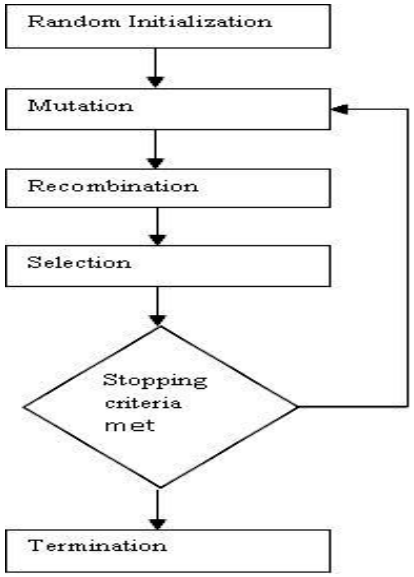


Fig. 3. The intruder starts form a random point in the WSN.

DIFFERENTIAL EVOLUTIONARY OPTIMIZATION ALGORITHM

The DE algorithm is one of the evolutionary algorithms which perform like genetic algorithm using the operators crossover, mutation and selection. The main operation is to find the differences between randomly sampled pairs of solutions in the population. This algorithm first focuses on mutation operation. And also it uses mutation operation as a search mechanism and selection operation to direct the search toward the regions in the search space.

In DE, a population of NP solution vectors is randomly created at the start. This population is successfully improved by applying mutation, crossover and selection operators. The DE algorithm also uses a non-uniform crossover that can take child vector parameters from one parent more often than it does from others. An optimization task consisting of D parameters can be represented by a D-dimensional vector. In DE, a population of NP solution vectors is randomly created at the start. This population is successfully improved by applying mutation, crossover and selection operators. The figure for Differential Evolution is shown below:



HETEROGENEOUS WSN

We consider two types of sensors: Type I and Type II with the node density of μ1 and μ2, respectively. A Type I sensor has the sensing range rs1, and the sensing coverage is a disk of area $S_1 = {}_1{}^2$A Type II sensor has the sensing coverage area S2 with the sensing range rs2. Without loss of generality, we can assume that rs1 > rs2 in our network model. In a heterogeneous WSN, any point in the network domain is said to be covered if the point is under the sensing range of any sensor (Type I, Type II, or both).

Algorithm

The algorithm for node selection trying to select the high capacity nodes compared to other one. High capacity means large sensing range and transmission range.

Si- set of type i sensors in the WSN area.
S - set of all sensors
N (a) - set of neighbors of node a
Repeat
For i=1 to N
Select node a with min N(a) in set Si
If N (a)≠Ø
Select a
SN= {j/the distance between a and
N (a) < (r_{Si}/2)}
If *SN* > 1
S=S-(SN U a)
Else
S= S-a
Until S is null set.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

LOCALISATION MEASUREMENT MODEL

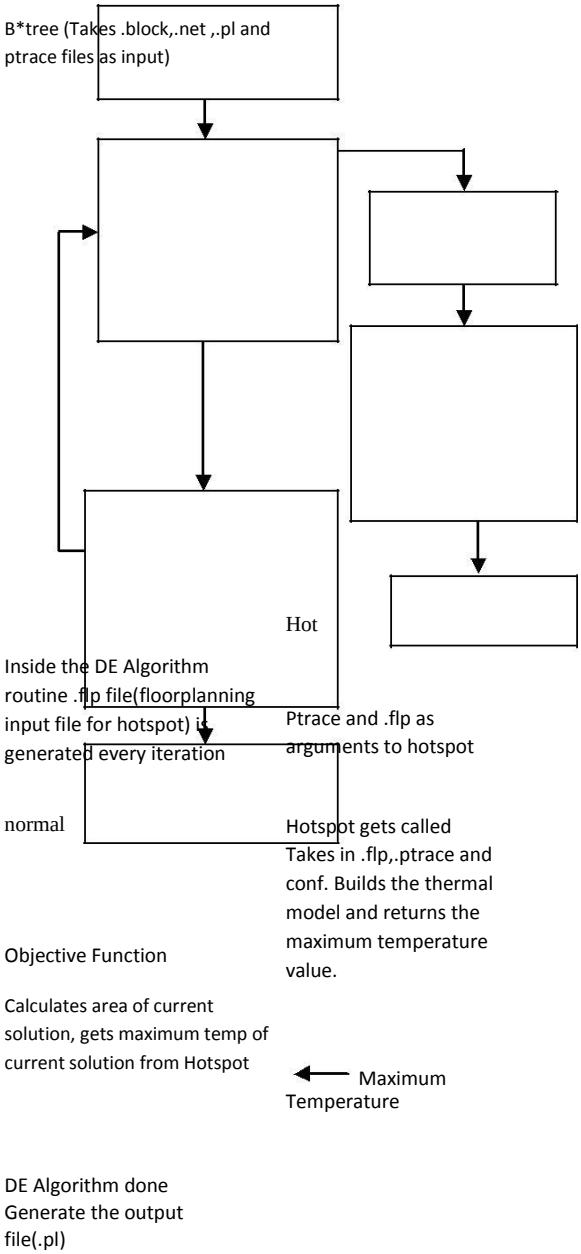


Fig. 5. Hotspot and B*Tree interfacing

A. *Time of Arrival (TOA) method:*

$$T_{i,j} \sim N(d_{i,j}/c, \sigma_T^2)$$

T $_{i,j}$=Average arrival time for 20 trials d $d_{i,j}$=distance between the nodes i and j

c =speed of signal

σ_T^2=variance

B. *Received Signal Strength (RSS) method:*

$$P_{i,j}(dBm) \sim N(Pi,\overline{j}(dBm), \sigma^2_{dB})$$

$$Pi,\overline{j}(dBm) = P_0(dBm)\, 10n_p \log10(d_{i,j}/d_0)$$

P_0 =Average power output after 20 trails $P_{i,j}$=power transfer from i to j node n_p=path loss co-efficient

RSS ALGORITHM

Step-1-Set up the blindfolded device location
Step-2- Define the channel model.
Step-3-Generate a random set of RSS-based distance measurements.
Step-4- Make an initial guess of coordinates.
Step-5- Find optimum locations of neurfons (fixed and relative).
Step-6- Save the resulting estimated coordinates.
Step-7- Plot the location estimates for sensors, one at a time.
Step-8- Calculate CRB vs. estimator performance.

SIMULATION RESULTS

TOA and RSS localization

The simulation considers two types of localization methods, TOA and RSS methods .A network with area 1*1 is created.25 nodes are deployed in the network out of which 4 nodes are assumed to be the reference nodes. The locations of other 21 nodes are estimated via TOA and RSS methods of relative localization. The result shows that TOA method will have less RMS value but not suitable for low cost applications.

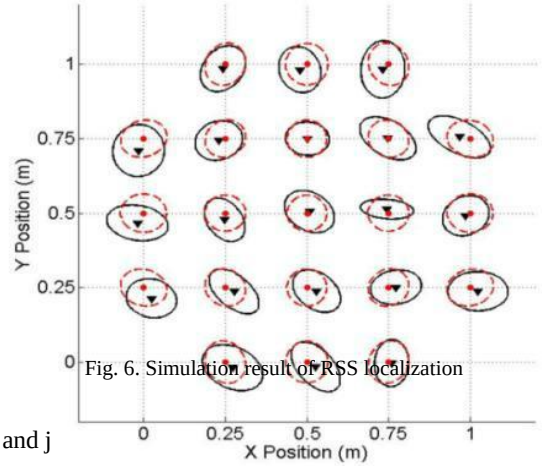


Fig. 6. Simulation result of RSS localization

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

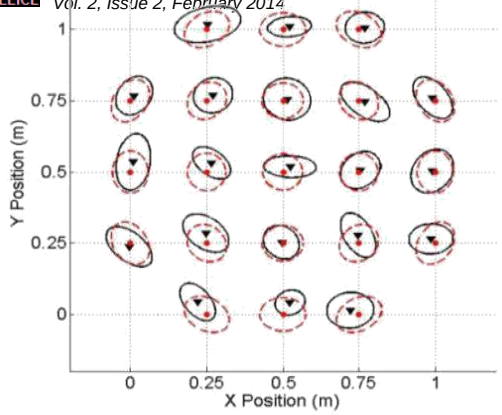


Fig. 7. Simulation result of TOA localization

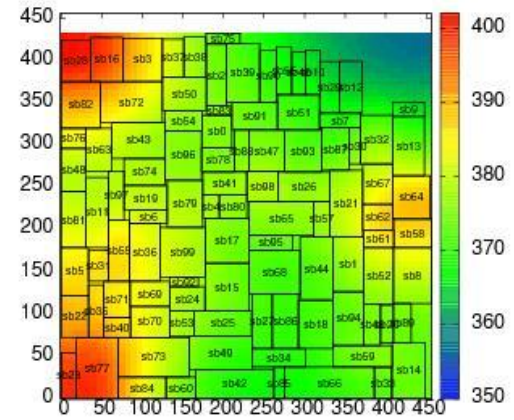


Fig. 8. Floorplan before optimization

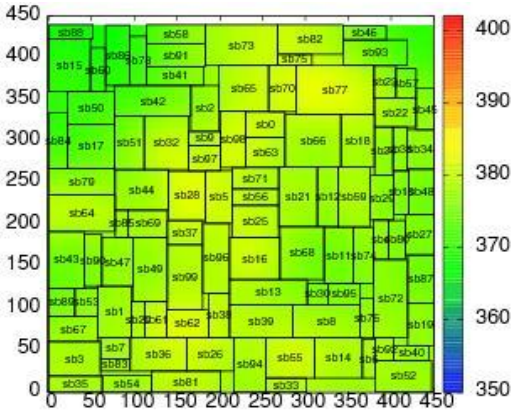


Fig. 9. Floorplan after optimization

HETEROGENEOUS INTRUSION DETECTION

The simulation considers two types of nodes. Here in order to get the result we are varying the parameters such as sensing range, transmission range, number of sensors etc. The sensors are uniformly distributed in a two dimensional space of 1000*1000 meters. The sensing range is varied from 0 to 50 meters and maximal allowable intrusion distance is 50 meters. The graph shows the detection probability. It is found that the detection probability remains same as in the case of analytical results, thus proving the correctness of the analytical model. It is evident that the single sensing detection probability is higher than that of multi sensing detection probability.

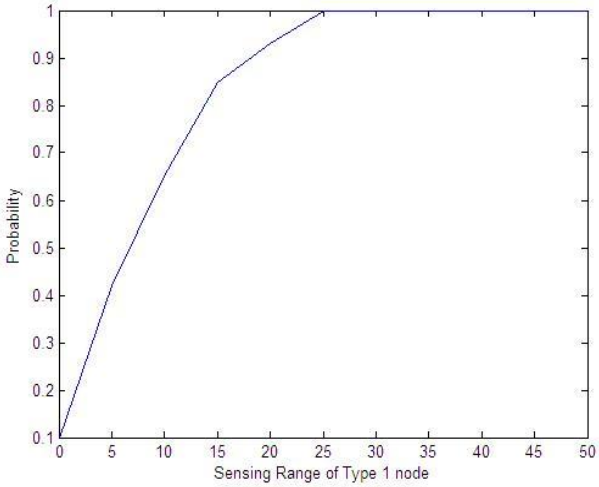


Fig. 10. Probability analysis

The energy used by this algorithm is analyzed in the figure11 given below. Here we compared our paper with the base paper. We assumed that the energy used by one node for a unit time is one unit. The graph clearly shows the energy efficiency. The Intrusion detection performed via the RSS localization will be highly energy efficient in case of heterogeneous wireless sensor networks with both Type I and Type II sensor nodes.The number of sensors are varied in each execution and find out how it will affect the selection process.

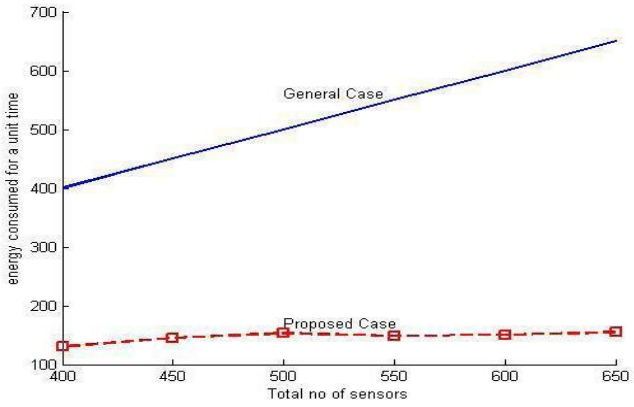


Fig. 11. Energy used

CONCLUSION

This paper speaks about the minimization of external intrusion detection in an energy efficient way and probability of

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 2, February 2014

intrusion detection in a heterogeneous WSN deployed in a two dimensional space. This probability gives an insight in to the required number of sensors in a given deployment, their sensing and transmission range to efficiently detect an intruder in a given WSN. We have developed an analytical model for intrusion detection and applied the same into single-sensing detection and multiple sensing detection scenarios for heterogeneous WSNs. The correctness of the analytical model is proved by simulation. We proposed a floor planner based on the Differential Evolution with B*-tree structures. It is used to search the solution space more efficiently than simulated annealing. DE provides very less computation time and solution space. It is used to get an optimal solution and reducing area compared to simulated annealing algorithm. By using the hotspot tool with this algorithm we can able to reduce the maximum temperature and maintain the constant value throughout the blocks. The experiments results proved that the proposed DE method is used to get the optimal solution compared to simulated annealing method.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, vol. 40, no. 8, pp. 102-14, Aug. 2011.

[2] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2010)

[3] Hu, W., Chou, C.T., Jha, S., and Bulusu, N.: Deploying Long-Lived and Cost-effective Hybrid Sensor Networks. Elsevier Ad-Hoc Networks, Vol. 4, Issue 6. (2010) 749-767.

[4] A.P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. C.

Wong, "Decentralized intrusion detection in wireless sensor networks," in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks.

[5] Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, vol. 3, Montreal, Canada, August 2009, pp. 253–259.

[6] A.Perrig, et al., "SPINS: Security Protocols for Sensor Networks",

Wireless Networks, 8(5):521- 534, Sep. 2008.

[7] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2004.

[8] J. Deng, R. Han, and S. Mishra, "A Performance Evaluation of Intrusion-tolerant Routing in Wireless Sensor Networks", Proc. of the 2nd Int. IEEE Workshop on Information Processing in Sensor Networks (IPSN'03), Apr. 2003.

[9] Y. Wang, X. Wang, B. Xie, D. Wang, and D. P. Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.

[10] O. Dousse, C. Tavoularis, and P. Thiran, "Delay of intrusion detection in wireless sensor networks," in Proceedings of the Seventh ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), 2006.

BIOGRAPHIES

A.Shakil Ahmed is an assistant professor at Sethu Institute of Technology. He received his B.E degree in Electronics and Communication Engineering from K.L.N College of Information Technology and M.E degree in Communication Systems from Coimbatore Institute of Technology. He has been awarded the best student award while doing his master degree. He has attended various national conferences and presented two papers in International Conference and also published one paper in IEEE Explore.

R.Vinoth is an assistant professor at Sethu Institute of Technology. He received his B.E degree in Instrumentation and Control Engineering from Arulmigu Kalasalingam College of Engineering and M.E degree in Industrial Engineering from Thiagarajar College of Engineering. He has attended various national conferences and International Conferences.

M.E.HariKumar is an assistant professor at Sethu Institute of Technology. He received his B.E degree in Electronics and Instrumentation Engineering from Kamaraj College of Engineering and Technology and M.E. degree in Computer and Communication. He is a Student Chapter In-charge in ISOI. He has been awared the Best IEEE Student member while doing masters degree. He has attended various national conferences and presented one papers in International Conference.

Ajith.B.Singh is an assistant professor at Sethu Institute of Technology. He received his B.E degree in Electronics and Instrumentation Engineering from Kamaraj College of Engineering and Technology and M.E degree in Control and Instrumentation from Kalasalingam University. He has presented papers in numerous national and international conferences, and also a book and various international journals.

K.Nivethitha is an assistant professor at Sethu Institute of Technology. She received her B.E degree in Electronics and Communication Engineering from Pandian Saraswathi yadav Engineering College and M.E degree in Communication Systems from Thiagarajar College of Engineering. She has attended various International Conferences and also published in IEEE Explore.