An Energy Efficient Approach in Heterogeneous WSN

[1]P. Durga Prasad, [2]R. Naveen
[1,2]Dept. of CSE, SBIT, Khammam, AP, India

Abstract
Intrusion detection plays an important role in the area of security in WSN. Detection of any type of intruder is essential in case of WSN. WSN consumes a lot of energy to detect an intruder. Therefore we derive an algorithm for energy efficient external and internal intrusion detection. We also analyse the probability of detecting the intruder for heterogeneous WSN. This paper considers single sensing and multi sensing intruder detection models. It is found that our experimental results validate the theoretical results.

Keywords
Intrusion Detection, Node Density, Sensing Range, Wireless Sensor Network (WSN)

I. Introduction

WSN is common in different types of application scenarios. It includes a set of sensor nodes deployed over a geographical area to monitor a variety of phenomenons. However, challenges and difficulties still exist. The sensor nodes own limited power, processing and sensing ability. The sensor nodes are prone to failure because of lack of power, physical damage etc. Since the information generated by a single node is usually incomplete or inaccurate, and the applications need collaborative communication and computation among multiple sensors multiple sensing models can be used. A Heterogeneous WSN is more complex as compared to homogeneous WSN and which consists of a number of sensor nodes of different types deployed in a particular area and which are collectively working together to achieve a particular aim. The aim may be any of the physical or environmental condition. For e.g. the wireless sensor network is mainly used in military applications such as in borders for finding out the infiltrations. It is also used in industrial process monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation and traffic control [1]. WSN become increasingly useful in variety critical applications, such as environmental monitoring, smart offices, battlefield surveillance and transportation traffic monitoring.

The sensor nodes are tiny and limited in power. Sensor types vary according to the application of WSN. Whatever be the application, the resources such as power, memory and band width are limited. More over, most of the sensor nodes are throw away in nature. Therefore it is vital to consider energy efficiency so as to maximize the life time of the WSN.

Great efforts have been devoted to minimizing the energy consumption and extending the lifetime of the network. One common way is to put some sensor nodes in sleep mode to save energy and wake them up under some strategies.

Work towards maximizing the life time of WSN has been studied in many research works. Some of them lead to the need of heterogeneous WSN deployment. Lee et al. [2] analyse heterogeneous deployments both mathematically and through simulations in different deployment environments and network operation models. In [3], Hu et al. investigate some fundamental questions for hybrid deployment of sensor network, and propose a cost model and integer linear programming problem formulation for minimizing energy usage and maximizing lifetime in a hybrid sensor network. Their studies show that network lifetime can be increased dramatically with the addition of extra micro-servers, and the locations of micro-servers can affect the lifetime of network significantly.

Intrusion detection plays an important role in the area of computer security, in particular network security, so an attempt to apply the idea in WSNs makes a lot of sense. However, there are currently only a few studies in this area. Da Silva et al. [4] and Onat and Miri [5] propose similar IDS systems, where certain monitor nodes in the network are responsible for monitoring their neighbours, looking for intruders. They listen to messages in their radio range and store in a buffer specific message fields that might be useful to an IDS system running within a sensor node.

The sensor nodes in WSNs are usually static after deployment, and communicate mainly through broadcast instead of point-to-point communication. Sensors are deployed in a variety of domains and some application should be secure from all types of attacks. A lot of security protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure data confidentiality, two-party data authentication, and data freshness and authenticated broadcast for sensor network [6]. LEAP (Localized Encryption and Authentication Protocol), is designed to support in-network processing bases on the different security requirements for different types of messages exchange [7]. INSENS is an intrusion tolerant routing protocol for wireless sensor networks [8]. In general, security solutions in the network can be divided into two categories: prevention and detection. Prevention techniques, such as encryption, authentication, firewalls, physical isolation, as the first line of defence, are usually to prevent attacks from outside.

The goal of intrusion detection is that when preventive measures fail, WSNs can identify and resist the attacks by means of intrusion detection techniques. An intrusion detection system (IDSs) is an important tool for the security of networks. Although, there have existed several intrusion detection techniques in wired networks, they are not suitable for WSNs and cannot transfer directly to WSNs. Therefore, these techniques must be modified or new techniques must be developed to make IDSs work well in WSNs. It is defined as a monitoring system for detecting any malicious intruder that is invading the network domain [9], [10], [11], [12]. For this purpose, a number of sensors, N, are deployed in an area of interest, A, to monitor the environmental changes by using optical, mechanical, acoustic, thermal, RF and magnetic sensing modalities . In this way, possible intruder approaching or travelling inside the deployment field can be detected by the WSN if it enters into the sensing range(s) of one or multiple sensor.

The rest of this paper is organized as follows. There are six sections. First section includes the related works. The papers which we referred to start this work are mentioned in this. Following this contribution section is there, which specifies our idea to intrusion detection. Next is problem definition, assumption made for simulation. Intrusion detection in heterogeneous wsn includes the algorithm and probability analysis. The simulation results are specified in simulation and verification section. Finally, the paper is concluded in the last Section.

II. Related Works

There exist several tools for security in networks and IDSs are important tools. Many solutions have been proposed in traditional networks but it cannot be applied directly to WSN because the resources of sensor nodes are restricted. Ad-hoc and WSNs security has been studied in a number of proposals. Zhang and Lee [13] are among the first to study the problem of intrusion detection in wireless Ad-hoc networks. They proposed architecture for a distributed and cooperative intrusion detection system for Ad-hoc networks; their scheme was based on statistical anomaly detection techniques. But the scheme need much time, data and traffic to detect intrusion. In WSNs, the nodes can not afford the cost.

Detecting a moving intruder is a crucial application in wireless sensor networks, thus, attracting considerable research attention in the literature. Intrusion detection is defined as the first contact time when the intruder hits the sensing range of a sensor belonging to the large sensor cluster. To date, most of the existing work focus on the problem of network configuration for efficiently detecting the intruder within a pre-specified time threshold, under the constraints of tight power saving and/or cost efficiency. Liu et al. [14] have explored the effects of sensor mobility on sensing coverage and detection capability in a mobile WSN. It is demonstrated that sensor mobility can improve the sensing coverage of the network, and provide fast detection of targeted events.

Wang et al. [15] have provided a unifying approach in relating the intrusion detection probability with respect to the intrusion distance and the network parameters (i.e., node density, sensing range and transmission range), under single-sensing detection and multiple-sensing detection models, in both homogeneous and heterogeneous WSNs. A straight line or linear motion intrusion path is assumed for an intruder.

An intruder can attack the network following a curved path or even a random walk in order to improve its attacking probability. Yun Wang, Yoon Kah Leow, and Jun Yin[16] have provided an approach where the intruder takes a curved path. They propose a novel Sine-curve mobility model to explore the effects of different intrusion paths on the intrusion detection probability using single-sensing and K-sensing detections in a given wireless sensor network.

Xi Peng et al[17] proposed a security management model for self organizing wireless sensor networks based on intrusion detection. It can prevent most of attacks. Then an analysis of each layer of networks in security model is discussed and the security management measures in the data link layer and network layer are described in detail especially. Such a structure is built based on the existing encryption and authentication protocols, and can detect most types of attacks in the sensor networks. In this paper, intrusion detection strategy is deployed in the form of layers.

Typically a wireless sensor network uses cryptography to secure itself against unauthorized external nodes gaining entry into the network. But cryptography can only protect the network against the external nodes and does little to thwart malicious nodes that already possess one or more keys. Brutch and Ko classify intrusion detection systems (IDS) into two categories: host-based and network-based. They further classify intrusion detection schemes into those that are signature based, anomaly based, and specification based [18].

Byunggil Lee et al., [19] have developed management platform and security framework for wsn. The proposed framework has advantages as regard secure association and intrusion detection. This also provides the background an wsn, its security issues and requirements.

Qi wang et al., [20] have developed a intruder detection algorithm of low complexity for static wireless sensor network. The intrusion detection model includes characteristics that determine the average frequency of execution of order. A distributed algorithm in which the sensor collects the information from the neighbouring nodes to analyses the anomalies if any from the neighbours. The intrusion detection algorithm on detecting anomalies packets received from its neighbours basic alarms to report the anomaly.

III. Contribution

Here we have developed an algorithm which helps the WSN in detecting the intruder with energy efficiency and there by increasing the life time of the network .More over, we have carried out the probability analysis for intrusion detection. Two things are considered in this work.

Energy consumed for the intrusion detection process Whether this technique can be used for both external and internal intrusion detection.

The algorithm is developed by keeping these two things in our mind. We cannot separate internal and external intrusion detection as separate fields because most of the applications need both in the network. The internal intrusion detection includes the analysis of data send by each node. The algorithm proposed by us can be used for internal data analysis. This algorithm selects a set of nodes among the entire nodes and activates its IDS module.

IV. Problem Definition

The life span of wireless sensor network directly depends on the power. The power required to transfer a data from sensor is more compared to its internal processing. All sensors are performing the intrusion detection and passing this information to base station may cause unnecessary usage of power. It is better to activate only few sensors within a region of WSN at a time for intrusion detection. So in the case of intrusion detection, if we are able to save battery power of each sensor, then it is very easy to increase the WSN life span. In this paper, we are proposing a new technique of energy efficient Intrusion detection, which will maximize the network life time, and its probability analysis .

V. Assumptions

The sensors we are considering here are static sensors. The intruder is considered as a moving object. Each node has omni antenna properties for sensing. The sink node knows each nodes location and its neighbour list. The algorithm is executed at the sink node and it sends packet to the selected nodes to activate its IDS module.

VI. Heterogeneous WSN

The heterogeneous WSN consists of different types of sensors with different sensing and transmission range. So while selecting the sensor nodes for intrusion detection , we need to consider these inequality of sensing and transmission range. For example, if two nodes have different transmission range it is better to select the one whose transmission range is higher. In this paper, we are considering N types of sensors. Here the sensing range and transmission range is high for Type 1 compared to Type2 and so on. The sensors are uniformly and independently deployed in a area A = LxL. Such a random deployment results in a 2D Poisson point distribution of sensors. A sensor can only sense the intruder within its sensing coverage area that is a disk with radius rs centered at the sensor.

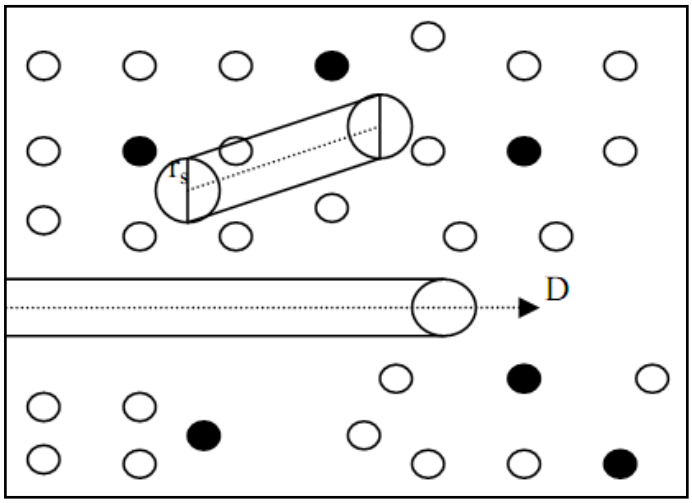

Fig. 1: Area Moved by Intruder

Consider figure 1, here the intruder is coming from the boundary and the distance moved by the intruder is D, the intruder is detected only when there is any sensor in the area moved by the intruder.In this paper we are considering only straight path. Figure 1 shows the case when the intruder enters from the boundary. Here the area moved by the intruder

$S=2*D*r_s+ \Pi r_s^2 /2$ (1)

If the intruder is entering the WSN area from a random point, i.e , the intruder is dropped from the air, then the area moved by the intruder is also shown in figure 1.This area is given by

$S=2*D*r_s+ \Pi r_s^2$ (2)

A. 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 neighbours 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)<(rsi/2)}

If |SN|>1

S=S-(SN U a)

Else

S= S-a

Until S is null set.

The algorithm select a certain set of nodes that cover the entire area based on type of node, its transmission range and sensing range.

B. Single Sensing Detection Model

As we explained before, the intruder is detected only when it enters the sensing range of any one sensor nodes. When the intruder enters the area through the boundary and the boundary is covered by the sensors, then the intruder will be detected as soon as it enters the WSN area. Otherwise it has to move a certain distance D before detected by any of the sensors.

Theorem 1

The probability P(D) that an intruder can be immediately detected once it enters a heterogeneous WSN can be given by

$$p(D=0)=1-\prod_{i=1}^{N} e^{-n_i}$$

where n_i is the number of type i nodes activated in the area πrsi2/2.

Proof

Here the area we need to consider when the intruder enter from the boundary is $A_1=(\pi r_{s1}^2)/2, A_2=(\pi r_{s2}^2)/2 ,\ldots A_N=(\pi r_{sN}^2)/2$ as shown in fig. 2. So P (0, A_1) , P (0, A_2)….P(0, A_N) gives the probability that there is no Type 1,Type 2…type N sensors in that area. the probability that neither type 1 nor type 2….nor type N are given P(0, A_1) , P (0, A_2)….$P(0.A_N)=1-e^{-n1}\, e^{-n2}\ldots\, e^{-nN}$ where $n_1,n_2,\ldots n_N$ are the number of selected nodes from each type. So the probability of detecting the intruder when it enters the boundary is given by complement of P(0, A_1) , P (0, A_2)….$P(0.A_N)=1-e_{-n1}\, e_{-n2}\ldots\, e_{-nN}$.

Theorem 2

Suppose η is the maximal intrusion distance allowable for a given application, the probability P(D) that the intruder can be detected within η in the given heterogeneous WSN can be derived as

$$p(D<=\eta)=1-\prod_{i=0}^{N} e^{-n_i},$$

where ni is the number of sensors participating in intrusion detection area

$A_i= 2\,\eta r_{si}+(1/2)\pi r_{si}^2$

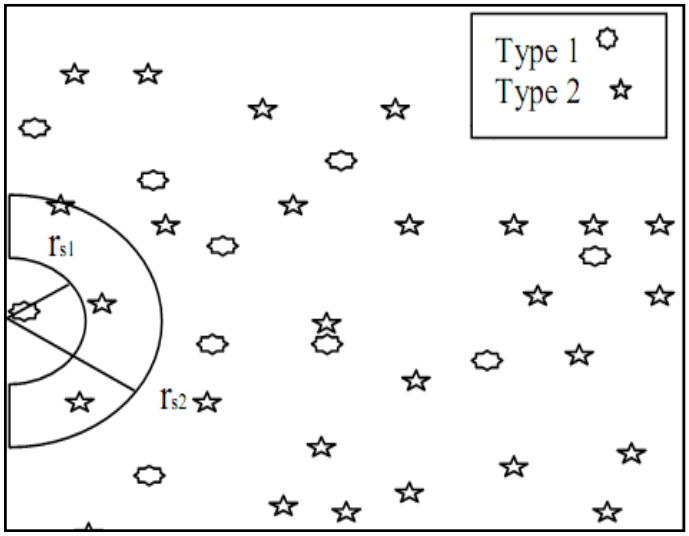

Fig. 2: The Area Covered by Sensors at the Boundary

Proof

This can be proved just like above theorem.

C. Multi Sensing Detection Model

Multi sensing in a heterogeneous WSN is explained in fig. 3. Here multiple sensors have to detect a intruder at the same time. Three sensors are considered. The intruder is within the sensing range of three sensors. In the k-sensing detection model of a heterogeneous WSN with two types of sensors, at least k sensors are required to detect an intruder. These k sensors can be any combination of any type of sensors.

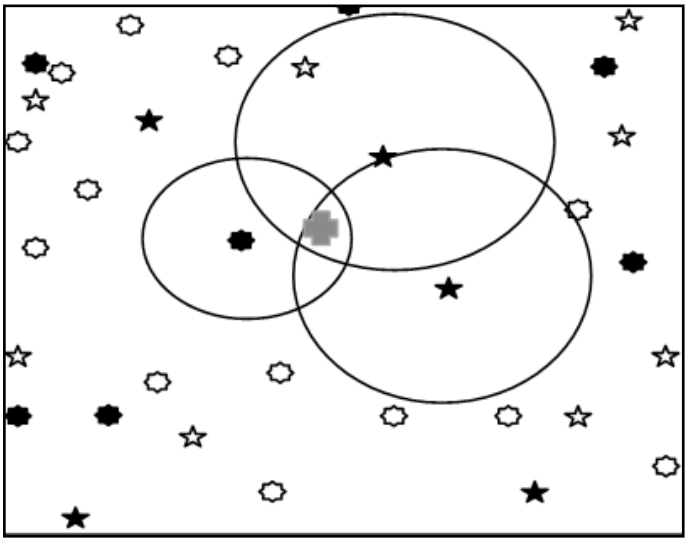

Fig. 3: Multisensing

Theorem 3

Let Pm (D = 0) be the probability that an intruder is detected immediately once it enters a WSN in multi sensing detection model.

It has

$$\text{Pm (D=0)} = 1 - \prod_{j=1}^{N} \sum_{i=0}^{m-1} P(i, Aj) \ ,$$

where A_j is the area covered by type j sensor and we are assuming that n_j of type j sensors are activated in the area A_j.

Proof

This theorem can be proved just like above theorems. Here the area is only one half circles with radius rs.P(i,A) gives the probability of detecting the intruder with i sensors.

$$\sum_{i=0}^{m-1} P(i, A)$$

gives the sum of the probabilities of detecting the intruder with less than m sensors. So the complement will give the multi sensing probability.

VII. Simulation and Verification

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. The fig 4 shows Single-Sensing detection. It is evident that the single sensing detection probability is higher than that of multi sensing- detection probability .This is because the multi-sensing detection imposes a stricter requirement on detecting the intruder (e.g., at least 3 sensors are required).

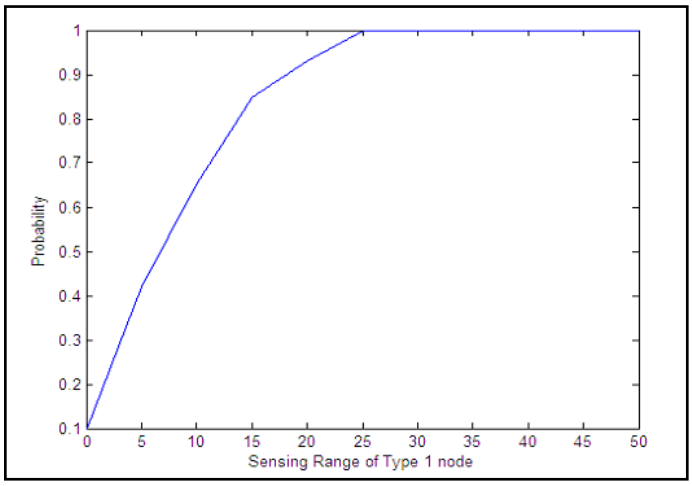

Fig. 4: Probability Analysis
Type 1 node

Here the graph is obtained by changing the sensing range from 0 to 40. The each point in the graph is a result of 100 simulations. That is to get each point we need to execute our simulation and find out the probability from the result of this 100 executions. Here we can see that single sensing is possible at lower ranges also. But for multi sensing it will take a little time to get the result. Because it needs more than one sensor (here , in this simulation 3 sensor information)information to detect the intruder.

Fig. 5 demonstrates the average number of nodes selected by using this algorithm specified above. The density of type 1 nodes is varied to check how many nodes are activating its IDS module. Here the simulation is done by fixing the number of Type 2 sensors to 300. The sensing range and transmission range are set to 30. The sensing and transmission range of Type 1 is set to 45. The numbers of type 1 nodes are varied in each execution and find out how it will affect the selection process.

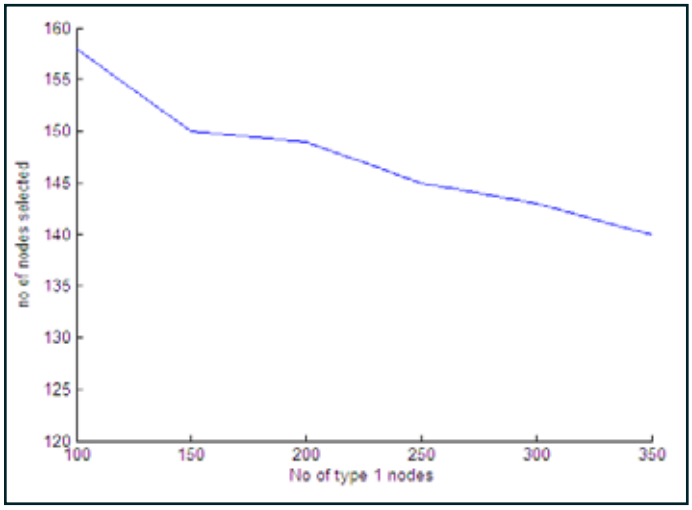

Fig. 5: Number of Node Selected

The energy used by this algorithm is analyzed in the fig. 6, 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.

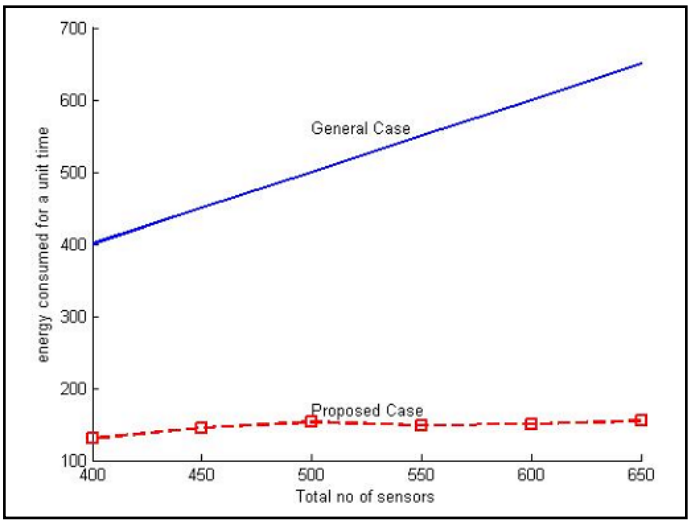

Fig. 6: Energy Used

VIII. Conclusions

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

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. 2002.

[2] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.,"Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks", (IEEE SECON). (2004)

[3] Hu, W., Chou, C.T., Jha, S., Bulusu, N.,"Deploying Long-Lived and Cost-effective Hybrid Sensor Networks", Elsevier Ad-Hoc Networks, Vol. 4, Issue 6. (2006) 749-767.

[4] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, 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] I. Onat, A. Miri,"An intrusion detection system for wirelesssensor networks", in Proceeding of the IEEE InternationalConference on Wireless and Mobile Computing, Networking and Communications, Vol. 3, Montreal, Canada, August 2005, pp. 253–259.

[6] A. Perrig, et al.,"SPINS: Security Protocols for Sensor Networks", Wireless Networks, 8(5) pp. 521- 534, Sep. 2002.

[7] S. Zhu, S. Setia, 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. 2003.

[8] J. Deng, R. Han, 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, 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, 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.

P. Durga Prasad received his MCA degree in Computer Science in the year 2005 from Kakatiya University, Warangal and pursuing M.Tech in Computer Science from JNTUH in 2010-12. At present working as Assistant Professor in MCA department at Swarana Bharathi Institute of Management Science Khammam, AP, His research interest includes Network Security and Web Technologies.

R. Naveen received his M.Tech degree in Computer Science in the year 2006 from Acharya Nagarjuna University, Guntur. At present working as Assistant Professor in CSE department at Swarana Bharathi Institute of Science & Technology (SBIT), Khammam, AP, His research interest includes Network Security and Web Technologies.