ISSN:0975-9646



# Intrusion detection: an Energy efficient approach and Data loss estimation in Heterogeneous WSN

Mahipal Reddy.G [1] ,Ananda Raj.S.P [2] ,Ramana.V [3] ,Poornima.S [4]

[1]*M.Tech in CSE Dept*
[2] *Senior Assistant Professor*
[3]*Assistant Professor*
*CSE Dept, S.R ENGINEERING COLLEGE*
*Warangal, ANDHRA PRADESH,INDIA*

[4]*Assistant Professor in IT Dept, S.R ENGINEERING COLLEGE*
*Warangal, ANDHRA PRADESH,INDIA*

*Abstrac:t*-**Due to the innovations in sensor technologies, Heterogeneous Wireless Sensor Networks (WSNs) are playing key role in many applications with monitoring phenomena. With increasing popularity of the WSNs, the security risks are also growing and that is evident in the incidents of intrusions in terms of various kinds of attacks recorded in this domain. Therefore it is essential to have intrusion detection systems built into the framework of the WSN. Research in this area has revealed that intrusion detection demands more energy. As wireless sensors have restrictions with respect to energy and memory resources, paramount importance has to be given to energy efficient intrusion detection mechanisms in WSN. This paper presents mechanisms that help in detecting intrusions with less energy consumption and also estimates the data loss occur in transmission. The empirical results revealed that the energy efficiency of our approach for intrusion detection in WSN is competitive and that can be used in real time sensing applications.**

*Key Words:*-**WSN, energy efficiency, intrusion detection, Data loss, Energy consumption, Heterogeneous**

## I. INTRODUCTION

Wireless Sensor Networks (WSNs) witnesses rapid growth due to the technology innovations in this domain. As the work implies, in a network of Wireless sensor nodes is located in centre, here the Sensors are connected to base station in turn it gets associated with a server where the sensing information gets recorded and from other places queries can be made to this. The sensor nodes once deployed have to live with the energy levels they have. Once energy levels are consumed completely, that sensor live is said to be completed. Thus the network lifetime and usefulness of the WSN depends on how efficiently the network uses energy. This is because the sensor nodes in such network have limited memory, processing and energy resources that are vital for the life of overall functioning of the network. In WSNs often multi sensing communication models are used. It is also common to have heterogeneous WSN with different types of sensing nodes and with various kinds of sensing models. There are many applications of WSN in civilian and military related environment monitoring. There are applications that are used in monitoring military borders for detection of infiltration.

Sensor nodes are small and have constraints with respect to resources. The resources include processing power, data loss and energy. With the limited resources, the nodes are to work to achieve the aim of the WSN. This is very challenging to have certain mechanisms in place that ensure that the nodes work in collaboration with each other and reduce the cost of communication, cost of computations that leads to maximizing network lifetime. There were many efforts made in terms of research and implementation of mechanisms that minimize the usage of energy in wireless sensor networks so as to increase the lifetime of network. There were many strategies already in place to overcome the short lifetime problem of wireless sensor networks. One such technique is to let some nodes to go into sleeping mode while the other nodes continue functioning actively. The nodes which are in sleeping mode will be waked up whenever required. This results in efficient energy consumption. Collaboration with other nodes also improves overall energy saving in such networks. In many research works, the maximization of network lifetime as considered as a problem and solutions are suggested. According to Hu et al. [10] hybrid deployment of sensor networks, usage of cost models, implementation of different computational approaches such as linear programming can maximize the life of WSN. Lee et al. [6] also analyzed WSN in heterogeneous network environment under various kinds of deployments for maximizing lifetime of network. Their studies revealed that life time of WSN can be maximized by using certain mechanisms and especially by adding micro-servers that affect life time of network positively.

Intrusion detection is essential in WSN for ensuring security in communications. The IDS is generally heavy weight and its functionality ensures fool proof security for WSN. However, its downside is that it consumes more energy of WSN. In network some of the nodes are given IDS responsibilities that monitor the incoming and outgoing traffic in order to ensure that there are no intrusions or the intrusions are detected and prevention mechanisms are applied. There is another approach in WSN to ensure

security. This is achieved by using a distributed IDS mechanism where every node has IDS capabilities and nodes are collaborated in order to make the intrusion detection process energy efficient. In [7] and [8] proposal of such IDS is made in which nodes has IDS responsibilities and observe conversations in their radio range and the messages are kept in buffer for IDS to detect any intrusion occurred. Here the system function supports only small networks.

The nodes in WSN are generally static and they are deployed in a field for monitoring. They mostly used broadcasting for communication. They are supposed to withstand all types of security attacks such as man in the middle, replay and DoS (Denial of Service). The security solutions can be classified into two categories. They are known as prevention and detection. The detection category is to detect intrusions in the network while prevention mechanisms really prevent the intrusion attacks make on WSN. The prevention techniques in WSN include physical isolation, firewalls, authentication and encryption. There are certain protocols also existing to prevent various kinds of attacks in WSN. The SPINS [2] is actually a set of protocols to prevent various security threats such as impersonation, authentication, data confidentiality etc. LEAP is for serving different security requirement in WSN based on different types of exchange of messages [3] while INSENS is a special intrusion tolerant routing protocol for WSN [4].

Intrusion detection has gained significance importance and there are many researches on this area of interest. The researches reviewed in literature such as [5], [11], [12] and [13] are proposing good mechanisms for intrusion detection. However, they are very suitable to computer networks but not ideal for the purpose of detection of intruders in WSN. It is required to modify these techniques or new techniques are to be proposed for the purpose of WSN. The review of literature in this area is done in the ensuing section. The rest of the paper presents related work and other sections of this journal.

## II. RELATED WORK

With respect to security, there are many tools that are used to ensure security in ID systems. The IDSs are very important tools since they can detect intrusions in networks. Many techniques that are result of research are pertaining to network security in general. They are developed for the nodes that have lot of resources in place. For this reason they can't be directly applied to WSN. That led to further research in the area of WSN for modifying techniques or inventing new ones that are best suited for WSN where nodes are energy constrained. Among the researchers on WSN Zhang and Lee [1] are first in researching on security issues of Ad hoc networks. Their IDS which is distributed in nature works based on the detection techniques of statistical anomaly. This technique assumes much traffic and the time taken for detection of intrusion is high and thus not efficient. The cost of this model can't be afforded by any WSN.

At times intruders might be moving and detecting such intruder is also important in WSN. This has attracted research in this domain. When nodes are in transit, the mechanisms and techniques are to be altered. The moving objects, their direction and probability of intrusion, detection etc. are to be considered. The intrusion detection in this environment also has to be considering energy efficient approaches. Most of the research that has been done in this area focuses on detection of intrusions under assumptions and criteria. The sensor coverage and sensing capabilities for detection of intrusions has effect are impacted by mobility according to Liu et al. [9]. His work demonstrated with the mobility of sensor increases the coverage of network and provides fast detection of intrusions and targeted events.

Sensing models are of two types. They are single sensing model and multi sensing model. Intrusion detection process in these two models is explored by Wang et al. [13]. In his work, the combination of detection probability and network parameters such as transmission range, sensing range, and node density are considered for experiments under single sensing models**.**

A security management model is proposed by [15] where intrusion detection in WSN assumes that the nodes in the network are self organizing and the model is based on the layers in network. The cryptography used by WSN can only prevent external attacks while it can't do it with already compromised nodes.

## III. PROPOSED WORK

Here the contribution towards intrusion detection in WSN is an algorithm which detects intrusions with energy efficient way. The following things are considered in this work.

- The consumption of energy for the purpose of intrusion detection.
- Exploring the mechanism for internal and external detection.

The proposed algorithms keeps these two in mind as they are essential in WSN because the intrusions might be from within the network or from outside of it.

## IV. PROBLEM DEFINITION AND ASSUMPTIONS

Intrusion detection is essential in WSN. The nodes that take this responsibility have to consume lot of energy in delivering their duties in terms of intrusion detection. This leads to drastic loss of energy and over a period of time that node will be devoid of energy resulting in the death of the node. The early demise of nodes in the network leads to the reduction of network lifetime. This is the problem to be solved by inventing a new mechanism that can perform energy efficient intrusion detection. The assumptions considered in this paper are that the sensors nodes are static; intruders are moving objects; the sensor nodes and their location are known to sink node; the algorithm is expected to work at sink node and the select node is given instruction to activate its IDS for detection of intruders.

### *A. Multi sensing Detection Model*

Fig. 1 shows multi sensing concept in heterogeneous WSN. An intruder is detected by multiple sensors at the same time. In fig. 1, three sensors are considered for intrusion detection. The intrusion is in the sensing range of those three sensors in

WSN. As a general guideline, with two types of sensors, at least k-sensors are needed in order to support in the k-sensing detection model with any type of sensors.

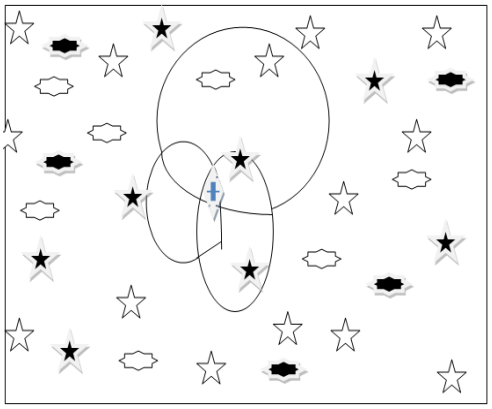

Fig.1 Shows multi sensing in heterogeneous WSN

*B. The estimation for energy consumption and energy efficient algorithm*

The below algorithm as said before runs in sink node that has details about all other sensor nodes in the WSN. This algorithm is responsible to find out suitable node among the sensor nodes for choosing it as a candidate node for activating IDS in that node. However, this mechanism has to be done keeping energy in mind.

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

Fig.2 shows proposed algorithm

The algorithm considers sensors in WSN, neighbors of given node. Based on the distances energy consumption is estimated and energy efficient intrusion detection is achieved.

## V. IMPLEMENTATION

The implementation environment has software such as JDK 1.6 running in Windows XP operating system which is in a PC with 2GB RAM and 2.x MHz processing power. The system uses Java technology such as RMI (Remote Method Invocation). Java's SWING API is used to build user interface. The RMI technology lets nodes to communicate remotely. The simulation has three kinds of nodes namely centralized server, server and client.

The purpose of centralized server is to monitor the server and client communication. The data sent by server to client is routed through centralized server. If any intruder is detected in server to client communication, that is detected by centralized server. The centralized server runs the algorithm in order to detect the intrusions. Data will not be sent to destination but it will be sent through any centralized server. Server acts as source.

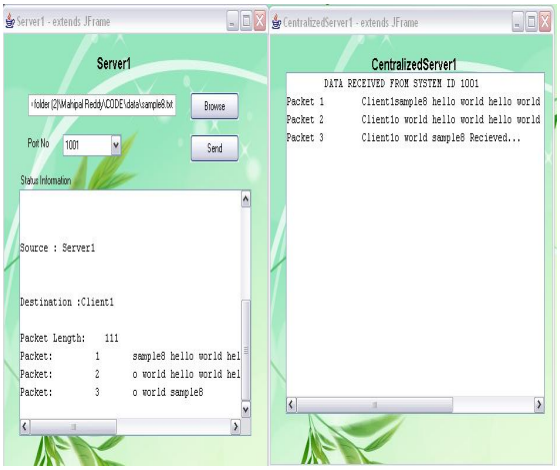


Fig.3 screen shot for centralized server

It selects the required data and sends it to a particular client. The data is sent in the form of packets with length 48 bytes. The server has to use specific IP address and port number based on the centralized server through which it is to send the messages to client. Server checks whether the port number matches that of the client or destination.

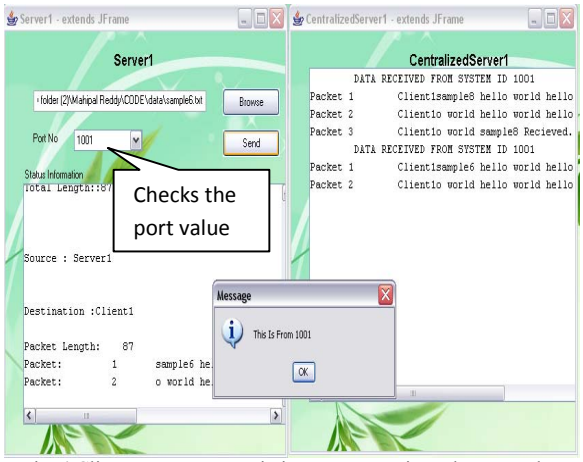


Fig .4 Client server communiction server monitors the port value

Identify the destination and data is send to selected destination. Client acts as destination node. Server sends the data to client. The sent data successfully received by the client through centralized server chosen with balancing features. Client sends acknowledgement to the server.

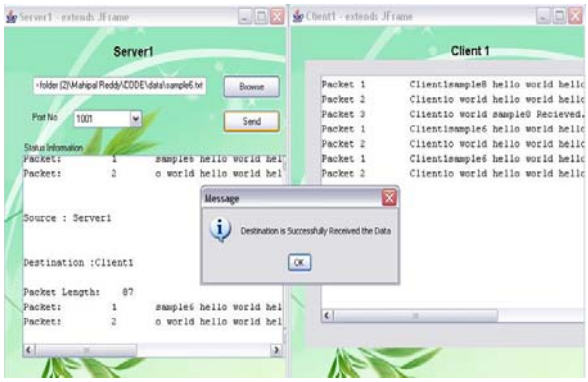


Fig.5 Acknowledgment for sent data from server to client

If intruder is detected data sent by server is not reachable to client or destination in that situation data will be sent to any centralized server for further analysis. The intrusion detection is identified when data sent from source to destination is delayed because of obstruction created in the flow.

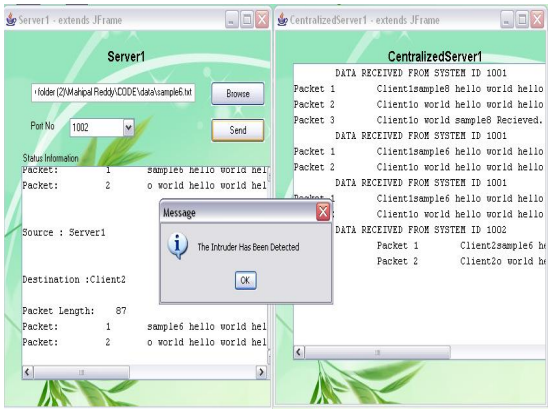


Fig.6 Detection of intruder while the communication process in centralized server

In the communication process if data is missing (packet loss) that is considered as another kind of intrusion. In case of packet loss, the percentage of packet loss is also calculated and displayed in centralized server which monitors the whole communication.

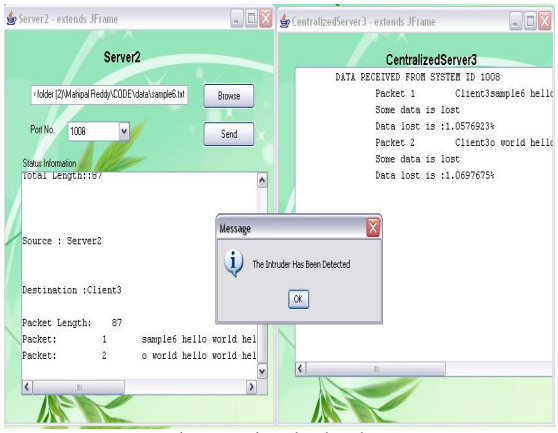


Fig.7 Monitor the data loss

*A. Centralized Server*

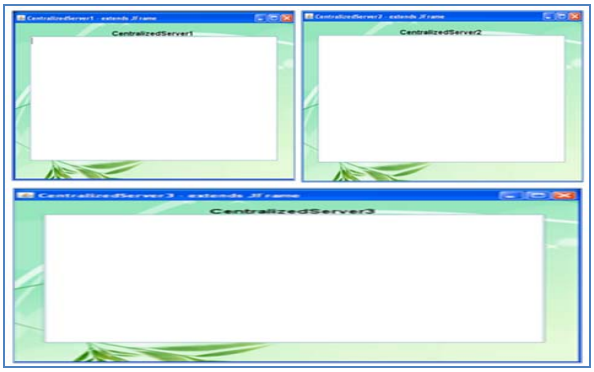


Fig.8 Centralized server 1, 2, and 3 are listening to servers

As can be seen in fig. 8, the three centralized servers with remoting capabilities are ready and running on specific port numbers. The servers when they want to communicate with clients are supposed to communicate with centralized servers for secure communication.

*B. Server*

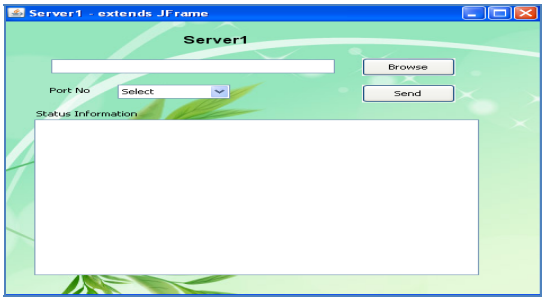


Fig. 9 The main view UI of server node.

For simulation of communication in WSN, the server node is able to send messages to client nodes based on the port number and the communication is routed through one of the centralized servers. Here user is able to select a file by clicking browse button and select port number from the drop down list. The Send button is to be initiated by user in order to send messages to client based on port number. The message or file selected is broken into packets with length 48 bytes.

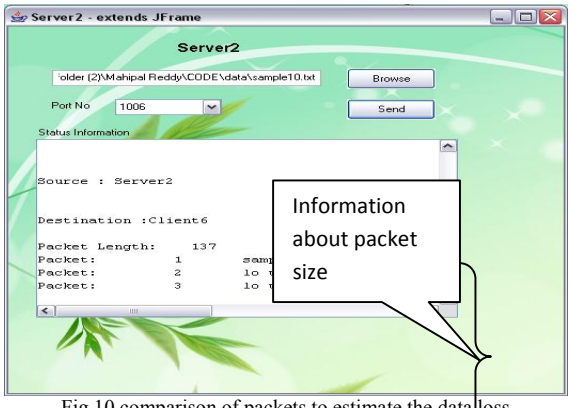


Fig.10 comparison of packets to estimate the data loss

The status information text area is meant for presenting status messages.

*C. Client*

In the proposed simulation model, the client acts as receiver or destination node. However, it can send acknowledgements back to its sender. The UI of the client is as shown in fig. 11.

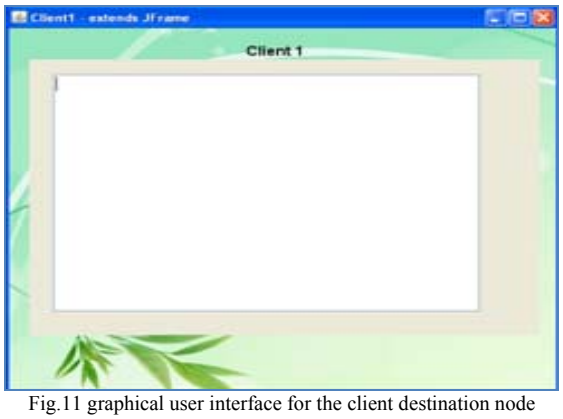


Fig.11 graphical user interface for the client destination node

As can be seen in fig. 11, the client node has no UI controls except the text area where the received messages are presented. However, it has a mechanism to acknowledge the server on successful communication implicitly.

*D. The Experiments and Communication*

Experiments are made with three centralized servers, two server nodes and six receiver nodes or destinations. The communication flow starts when server decides to send messages to client. It chooses a file and breaks it into many packets of size 48 bytes each and sends them through randomly selected centralized server. The server monitors communication and detects any intrusions. In case of intrusion observed because of loss in packets transmitted, the ratio of loss is calculated and presented at centralized server. The successful communication is presented in fig. 12.


Fig.12 End view of successful communication

As can be seen in fig. 12, the file sample1.txt is selected at server and sent it to client1 using port number 1001.

When data is sent from server to client through centralized server, the centralized server monitors data transfer for any possible attacks or intrusions. It can analyze the traffic and also find whether the attack is made or not. It considers packet loss as well. It is assumed that due to attack or intrusion delay in sending packets may occur and in turn it results in data loss or packet loss. Fig. 13 shows this case the percentage of data loss also.

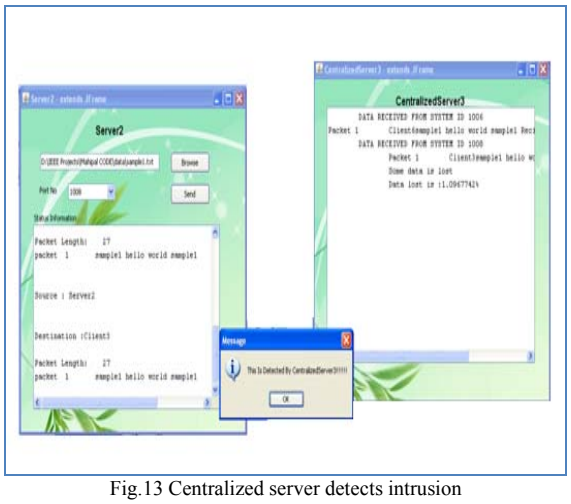


Fig.13 Centralized server detects intrusion

As seen in fig. 13, the server2 is sending packets to a client. However, the data transfer is subjected to an intrusion attack. As some data is lost, the centralized server suspects it as an intrusion attack and provides appropriate message.

## VI. CONCLUSION

Wireless Sensor Networks have resource constraints. They need to have security systems such as intrusion detection system. However, an IDS running in wireless sensor node consumes more energy which leads to early demise of network. This paper presents an energy efficient intrusion detection mechanism that improves life of WSN. The effectiveness of the simulation model is tested with simulations using a custom-built simulator developed in Java programming language. The results revealed that the proposed analytical model is effective and can be used in real world applications.

## REFERENCES

[1] Y. Zhang and W. Lee. *Intrusion Detection in Wireless Ad-Hoc Networks.* In Proc. ACM MobiCom, pages [275-283], 2000.

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

[3] 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. 2003.

[4] 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.

[5] H. Kung and D. Vlah, "Efficient location tracking using sensor networks," in *IEEE Wireless Communications and Networking Conference*, ser. 3, vol. 3, March 2003, pp. 1954– 1961.

[6] Lee, J.J., Krishnamachari, B., Kuo, C.C.J.: Impact of Heterogeneous Deployment on Lifetime Sensing Coverage in Sensor Networks (IEEE SECON). (2004).
[7] 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.*
[8] I. 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 2005, pp. 253–259.
[9] B. Liu, P. Brass, O. Dousse, P. Nain, and D. Towsley, "Mobility improves coverage of sensor networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, 2005.
[10] 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. (2006) 749-767.
[11] 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.
[12] C.-Y. Lin, W.-C. Peng and Y.-C. Tseng, "Efficient in-network moving object tracking in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 8, pp. 1044– 1056, 2006.
[13] 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.
[14] Yun Wang, Yoon Kah Leow, and Jun Yin," Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks," in 15th International Conference on Parallel and Distributed Systems, 2009.
[15] Xi Peng, Zheng Wu, Debao Xiao, Yang Yu," Study on Security Management Architecture for Sensor Network based on Intrusion Detection," in 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing ,2009.
[16]Mohammad Mubarak, Syed Abdul Sattar, Appa Rao, Sajitha, "Intrusion Detection: An Energy Efficient approach in Heterogeneous WSN" ,IEEE ICETECT 2011.

**G.Mahipal Reddy** received the B.Tech Degree in Computer Science and Engineering from Ganapathy Engineering College, Rangasaipet, Warangal, A.P, India. Currently pursuing M.tech in Computer Science and Engineering at SR Engineering College, Warangal, India. His research interest includes bandwidth estimation in networks, Mobile Adhoc networks.

**S.P.Anandaraj** received B.E (CSE) degree from Madras University, Chennai in the year 2004, M.Tech (CSE) with Gold Medal from Dr.MGR Educational and Research Institute, University in the year 2007 (Distinction with Honors). Now Pursuing Ph.D in St. Peter's University, Chennai. He has 8 Years of Teaching Experience. His areas of interest are Information security and Sensor Networks. He has published papers in International Journal, International Conference and National Conference and attended nearly15 National Workshops/FDP/Seminars etc. He is a member of ISTE, CSI, IEEE, Member of IACSIT and Member of IAENG.

**V.Ramana** received B.Tech (CSE) degree from JNTU, Hyderabad in the year 2006.M.Tech (AI) from university of Hyderabad in the year 2010, He has2 Years of Teaching Experience. His area of interest is Artificial Intelligence and Machine Learning. He has published papers in International Journal, International Conferences and National Conferences and attended National Workshops/FDP/Seminars etc., He is a member of CSI.

**S.Poornima** received B.Tech (IT) degree from Anna University in the year 2005. She has 6+ years of experience in teaching field. Her areas of interest include Neural Networks and Wireless Sensor Networks. She has published research papers in various National and International Journals, National and International Conferences. She also attended many National Seminars/FDP/Workshops Etc., She is a life member of ISTE.