ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

Development of an Enhanced Efficient Secured Multi-Hop Routing Technique for Wireless Sensor Networks

Rijin I.K[1], Dr.N.K.Sakthivel[2] , Dr.S.Subasree[3]

Student II Year M.E, Dept. Of CSE, VSB Engineering College ,Tamilnadu, India[1]

Professor, Dept. Of CSE, VSB Engineering College, Tamilnadu, India[2]

Professor, Dept. Of IT, VSB Engineering College, Tamilnadu, India[3]

Abstract: Wireless Sensor Networks use numbers of sensors to send data from sender to base station. Wireless Sensor Nodes are battery-powered devices. Power saving is always vital to increase the lifetime of Wireless Sensor Networks. There are many Protocols has designed and proposed for WS Networks to increase its performance in terms of throughput, network lifetime and security, An efficient secured multi-hop routing technique for wireless sensor networks (ES-MHRT) was proposed recently, which was a two contemporary hybrid Multi-Hop Routing Techniques, namely, Flat Multi- Hop Routing Technique and Hierarchical Multi-Hop Routing Technique for providing trustworthy and efficient routing in WS networks. It demonstrates the effective performance in terms of Network Lifetime and superior connectivity. However, from the literature survey, it is observed that in ES-MHRT the sender understand the status of delivery report from receiver only, which costs more time to understand the reliable route. Thus Sender couldn't forward the data in fast manner, which affects the Network Performance in terms of Throughput and Bandwidth Utilization. This is the major issue. To address this issue, this project work is planned to design an efficient Distributed Monitoring System, which will help the ES-MHRT to push more volume of Data with Secured Route.

Keywords: Routing protocols, Wireless sensor networks, Security, Trust, Sink node.

I. INTRODUCTION

A wireless sensor network contains large number of wireless sensors used to take environmental measurements. Typical examples include light, temperature, sound, and humidity. These nodes readings are transmit through wireless medium to a application that perform decisions from these sensor readings. A WSN consist of number of battery-powered sensors having limited processing power. With a limted communication range, a sensor node wirelessly transmits information to a receiver through multihop path. The multihop path of WSNs commonly becomes the target of attacks. An attacker will attack nodes physically, and create traffic collision for valid transmission, drop or mislead messages in routes, or make communication jam on the channel by creating radio interference

The past decade has witnessed an explosive growth in the use of wireless technologies. In particular, WSNs is a very wide research area[5]. There are many diverse and interesting aspects of this technology which demand further research to produce the innovative solutions needed to make WSNs a viable technology. Routing plays a important role in the WSNs. Particularly, the inherent characteristics of WSNs, routing security is a important area of research. Network attack [4] is the one of the way which causes network failure. Although many WSN routing protocols have been proposed, none have been developed for security purpose [6]. Due to its broadcast nature of the communication medium WSNs are vulnerable to different type of attacks[3] .

Here we are focusing routing security in wireless sensor networks. Recent proposals in Wireless sensor networks overcome for the limited capacity of the SN nodes and the nature of the networks, but do not consider security. These protocols is not developed with security as a important factor, we feel it is important to analyze their security properties.

In this paper, an Enhanced Efficient Secured Multi-Hop Routing Technique is proposed. our proposal is focus different type of attacks on Hybrid Multi-hop routiNg (HYMN) [1]which adversaries misdirect network routing traffic by identity deception technique through replaying information of routing. Using identity deception technique, the adversary can capable of performing hard-to identify and harmful attack against the data path, such as selective forwarding, sinkhole attacks, wormhole attacks and Sybil attacks

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

II. RELATED WORKS

In WSNs, information collecting using multi-hop communication generally make a problem to WS nodes that are near to the Base Station that, because of acting as intermediaries for information transmission, their power will reduce faster. It wii call as self-induced black hole attack or energy hole problem, To address this issue and to make an energy efficient routing mechanisms Ahmed E.A.A. Abdulla, et al presented A Novel Hybrid Multi-Hop Routing Algorithm which is used to Improve the Longevity of Wireless Sensor Networks(HYMN),Heinzelman, et al. proposed the LEACH (Low- Energy Adaptive Clustering Hierarchy) WS Network protocol for WSNs of hierarchical-based architecture, which is commonly known and elegant hierarchical algorithm, by selecting the CHs in each rounds. LEACH algorithm achieve improvement compared to the direct communication, which will measure in terms of sensor nodes' lifetime, In this paper, for convenience, we call this kind of routing algorithms.
In data aggregation, trust management field and a cluster-based transmission mechanism with dynamic changes in the path has been proposed in [8]. In [7], a trust management frame work is proposed, heree the trust decision of each node has determined by using two parameters, that are, data transmission and data fusion. RDAT [9] presented a aggregation protocol, that enables the aggregators to determine the action of each sensor node using functional reputation. so, this WSN protocol will increase the accuracy of the trust management system. in cluster WS Networks (WSNs) such as LEACH [10], EC [12], EEHC [11], and HEED [13], the clustering algorithms will increase network throughput and scalability. Providing trust management in clustered environment will have number of advantages [11], [12], [13], such as helping a CH to identify faulty or malicious sensor nodes within a group [12]. In multi-hop clustering [11], a trust management system helps in the selection of trusted path for nodes through which a cluster member (CM) can forward data to the Cluster Head. in inter-cluster transmission, a trust system will help for the selection of trusted path gateway sensor nodes or other trusted Cluster Heads through which the sender node will send data to the station [12].
Multihop routing in WSNs provide less security in identity deception by replaying routing datas. An attacker may identify this fault to launch different harmful attacks to the routing protocols, such as sinkhole, wormhole, and Sybil attacks. To address this issue Guoxing Zhan,et al. proposed A Trust-Aware Routing Framework for Wireless Sensor Networks Follows the idea of TARF protocol, there are number of protocol has been presented in this work it use these kinds of frame works for providing security in the WSNs system

III. PROPOSED ENHANCED EFFICIENT SECURED MULTI-HOP ROUTING TECHNIQUE FOR WIRELESS SENSOR NETWORK (EES-MHRT)

This research work is planned to enhance the efficient secured multi-Hop Routing Technique with Distributed monitoring system, which will increase the performance of WS Networks in terms of trustworthy and Network Lifetime.

A. Architecture For Ees-Mhrt

EES-MHRT secures the hybrid multi hop routing in Wireless Sensor against attacker misdirecting the hybrid multi hop path by calculating the trustworthiness of neighbouring sensor nodes. It also identifies attacker by their less trustworthiness and routes information through paths passing those intruders to achieve satisfactory throughputt.ES-MHRT is also high energy efficient, scalable, and adaptable.

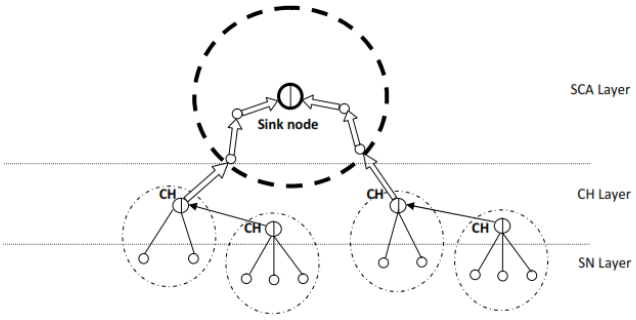

Fig .1 Architecture for Ees-Mhrt

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

Our trust management framework contains three level of trust such as Sensor Node-*level* trust, Cluster Head-*level* trust and Sink *level* trust.

Sensor Node layer: Each Sensor Node evaluates all other Sensor Nodes in the same group and all Cluster Head evaluates all other Cluster Heads and Sensor Nodes in its group. The p-to-p trust evaluation is continuously upgraded on the basis of either *direct* or *indirect node* observations. In WSNs two nodes are neighbours within communication limit, they will evaluate sensor node each other on the basis of direct observations through snooping or overhearing. In this each Sensor Node forward its trust results to other Sensor Nodes in the same group to its Cluster Head.

CH layer: Each Cluster Head execute trust evaluation to other Sensor Nodes within its cluster. And also each Cluster Head forward its trust execution value to all other Cluster Heads in the WSNs to a "Cluster Head commander" it is either locate on the base station if anyone is present, or on a Cluster Head selected whether a BS is not available. The Cluster Head commander of WSNs performs trust evaluation to all Cluster Heads in the WSN system.

SCA layer: In WSN each Sensor Node evaluates all other Sensor Nodes in the SCA and sends its trust evaluation results towards the base station. This trust management framework will use different WSN consist of heterogeneous Sensor Nodes with closely different starting energy levels and different types of malicious or selfish attacks. We are applying the trust management framework to the sensor node in the clustered WSN might dynamically adjust there behaviour according to environmental conditions and its own execution state

IV. PROPOSED TECHNIQUES

In hybrid wireless networks, the sensor nodes in the Sink Connectivity Area will be commonly less than that sensor node outside the Sink Connectivity Area, and also the volume of information that they are getting is less than the information they relay.

A. Hierarchical Trust Management Protocol

Trust management protocol contains three levels of trust: Sensor Node-*level* trust, Cluster Head-*level* trust and Sink *level* trust .in SN level Each Sensor Node evaluates other Sensor Nodes in the same group and also each Cluster Head evaluate other Cluster Heads and Sensor Nodes in its group. The p-to-p trust evaluation will automatically update based on the technique such as d*irect* or *indirect* observations. In this network two sensor nodes are near within communication range, they will execute each other based on the direct observations. Each Sensor Node forwards their trust evaluation value to all other Sensor Nodes in the same group to its Cluster Head. In Cluster Head level Each Cluster Head execute trust evaluation to all Sensor Nodes in its group. And also, each Cluster Head forward its trust information to all other Cluster Heads in the Wireless Sensor Network to a "Cluster Head commander" that is present on the BS if anyone is present, or on a Cluster Head selected if a base station is not present. The Cluster Head commander also executes trust evaluation to all Cluster Heads in the system. In Sink Connectivity Area level Each Sensor Node evaluates all other Sensor Nodes in the SCA and sends its trust evaluation results towards the base station.

Trust value:

$T_{ij}(t)=w_1T_{ij}^{intimacy}(t)+w_2T_{ij}^{honesty}(t)+w_3T_{ij}^{energy}(t)+w_4T_{ij}^{unselfishness}(t)$

The trust of that sensor node *i* evaluates towards sensor node *j* at a particular time *t* is represented as the natural number in the range of 0and 1 where 1 represents complete trust of the node, 0.5 ignorance of the node , and 0 distrust node.

P-to-P Trust Evaluation:

$T_{ij}(t)=(1-\alpha)T_{ij}(t-\Delta t)+ \alpha T_{ij}^{direct}(t)$, were I and j are 1-hop neighbor

$T_{ij}(t)=avg_{k\varepsilon Ni}\{(1-Y)T_{ij}(t- \Delta t)+ Y\ T_{kj}^{recom}(t)\}$,Otherwise

p-to-p trust calculation is conducted, for two peer Sensor Nodes or two peer Cluster Heads. A trustworthy (node *i*) find a trustee (node *j*) at a particular time *t*, it will update T_{ij} (*t*) when sensor node *i* is a 1-hop near of sensor node *j*, sensor node *i* would take its new trust value on the basis of direct observations (T_{ij},*directij* (*t*)) and also its old trust value from past execution experiences (T_{ij} ($t - \Delta t$)) here Δt is trust update interval toward the sensor node *j* to update $T_{ij}(t)$. A parameter α ($0 \leq \alpha \leq 1$) is using here for weigh these two trust result values and to consider trust decay over the particular time, that is the decay of the past trust result and the contribution of the newer trust value. A increased value of α means its trust evaluation result rely large on direct observations In the other hand, when sensor node *i* is not a 1-hop near of sensor node *j*, sensor node *i* would use their old execution T_{ij}^{X} ($t - \Delta t$) and recommendations for its 1-hop neighbors T^{recom} s_j (*t*) (where s is a recommender) to update T_{ij} (*t*). Sensor Node *i* only use their 1-hop near (*Ni*) as recommend for energy scalability and conservation. When *Ni* is an null set, hence node *i* is orphan for which $\gamma = 0$ and sensor node *i* would not be able to gives to p-to-p trust management. Here the attribute γ is used to weigh recommendations with old experiences. CH-SN Trust Evaluation:

$T_{chj}(t)=avg_{i\varepsilon Mc}\Lambda T_{chi}(t)\geq T^{th}\{T_{ij}(t)\}$

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

Tchj (*t*) represents a Cluster Head, *ch*, for finding a Sensor Node, *j*, where *Mc* is the set of Sensor Nodes in the group. Cluster Head *ch* will say *j* as compromised node when *Tchj* (*t*) is smaller than *T th*; else, node *j* will not be compromised node.

Station-to-CH Trust Evaluation:

Every Cluster Head reports its trust execution result to all other Cluster Heads in the Wireless Sensor Network to the BS that is infallible with all other physical security. The Cluster Head commander is located on the BS then applies the similar statistical evaluation technique as CH-SN Trust Evaluation

V. IMPLEMENTATION AND RESULTS

We used a reconfigurable emulator for this work The maximum sensor node capacity for the network is 50 and each nod in the WSN will launch as a separate window all the nodes default launching state will be ACTIVE, user can manually change the operational states of the node or system will automatically set the different operational state, and the battery power and trust level of all the nodes initially equal to 100%.There are mainly four operational states are there in a wireless sensor networks which are given below

ACTIVE: In this active state, all the sensor node sensing circuitry will on and that forward information to the gateway node or the Base Station, TRANSIVE: The node state at which it perform both the transmission and reception operation, IDLE: The node do not perform any operation is called idle state.

TRANSMIT: Node which initiates the transmission and it forward information to the gateway WS node or the Base Station, RECEIVE: The sensor node in which it receives the sensed data, SLEEP: Sensor Node is treat inactive and will turn off the nodes sensing and transmission circuitry.

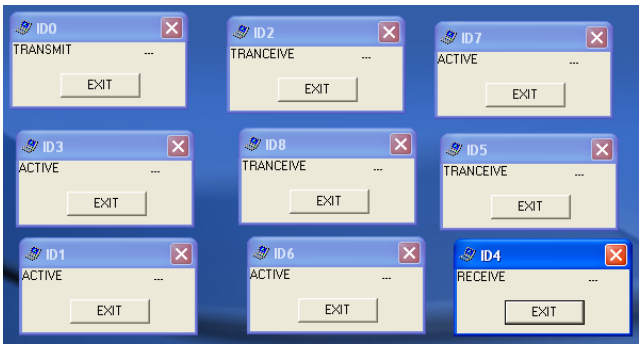

Fig.2. states of WSN nodes

The node in a WS node is categories into four important categories: *sensing sensors*, *relaying sensors*, *sensing-relaying sensors*, and *inactivity*. The active node state, the sensor node sensing circuitry will turn-on and it forward information to the gateway Wireless sensor node or to the Base Station. Here in the relaying node state, the sensor node will relays the information from all other active sensor nodes. Here a node is having both active the target and also the node is relaying information from all other sensor nodes, this will consider as the sensing-relaying node state. Else, the node as treat inactive and will turn off their sensing and transmission circuitry. The hierarchical Wireless sensor cluster-base architecture, all the Cluster Head in a group would be in the status of relaying and sensing- relaying. By the non-Cluster Head wireless sensor nodes will be in all states of the other main four states, the execution contains two phases deploying the Wireless network and it will running the tool. After deploying the Sensor network, the features of the sensor network shall be set by using the network properties buttons. Network configuration properties will set automatically.

Network Configuration: It will determine the hardware feature of the network. The following variables can be configured. Network Size: The number of sensor node in the Wireless network if set to a large value, and the sensor network will have hundred nodes; and since it will increase the density of the WS network and also the number of Sensor network connections; this may bog down the simulation. Sensor Radius: The maximum transmission limit of the wireless sensors in the wireless network, Sensor Period: IT is the delay period for sensor detection events. If set to a less value, a wireless network sensor will fire immediately as object enters into their sensor radius (thereby consuming lots of energy.) If set to a large value, the wireless network sensor would wait for a long time for firing a second data packet, Sensor Cost: It is the sensor energy cost in finding an object and generating a data packet, Transmission Radius: it is the maximum amount of distance in which any of the two network sensor nodes will exchange information. If set to a high value, nodes located on opposite sides may be able to reach each other; if set to a low value, sensor nodes must be very near to transmit, Transmitter Period: It is the amount of time required to forward a data packet. Transmit

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

Cost: It is the energy cost in forwarding a data packet. Setting this value very high will cause nodes to be depleted after sending only a few packets; setting this value very low allows the nodes to send many hundred packets, Receive Cost: energy cost in receiving a packet.

Number of nodes	9
Transmitter node	Node 0
Receiver node	Node 4
Encryption algorithm	RAC
Data Size	14186 B

Table.1 Experimental Data

Once the network has been deployed, run the hack tool & motes emulator then select the source and destination folder for the file to be transmitted(use encryption and decryption button for providing security for the data) the simulation may be run by clicking "Start button."

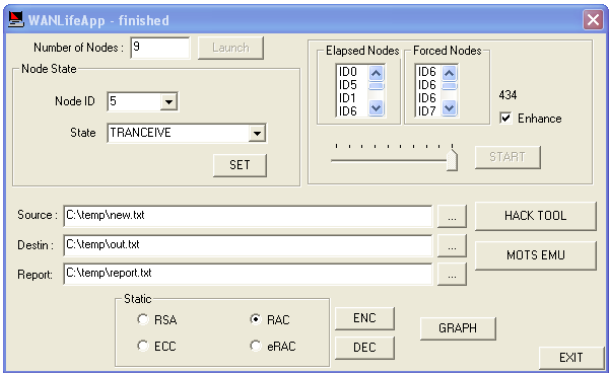

Fig.3 Final window

The wireless sensors may execute out of power and it will fall out of the network, and eventually, all sensor node power will be down. The progress of the network can be monitored via the elapsed nodes and forced nodes box, and also we can view the execution report on the report file.

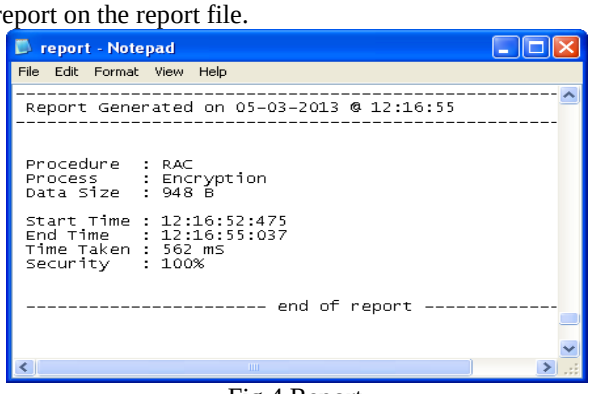

Fig.4 Report

A. Network Lifetime

The lifetime in a wireless sensor network is mostly defined as the time to which first wireless sensor node failure It has been shown that network lifetime of EES-MHRT network is increasing compared to ES-MHRT.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

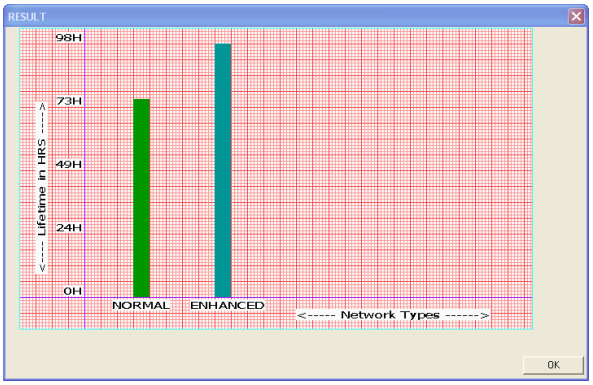

Fig.5 Network Lifetime

B. Security Level

Security is an essential feature for EES-MHRT. The EES-MHRT should be able to handle both wormhole attack and sink whole attack. it has been shown that the total Security level in a EES-MHRT network is increased compared toe ES-MHRT network**.**

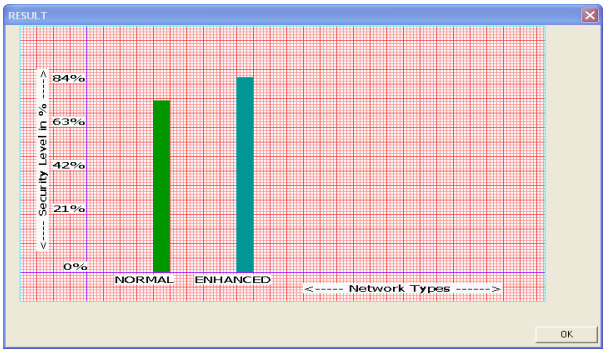

Fig.6 Security Level

C. Energy consumption

Saving power is important in WS networks (WSNs) for wireless sensor nods these are powered by batteries with a less charge carrying capacity, sending/receiving of information will be limited. In this work, it has been shown that the total energy consumption in a EES-MHRT network is reduced compared to ES-MHRT.

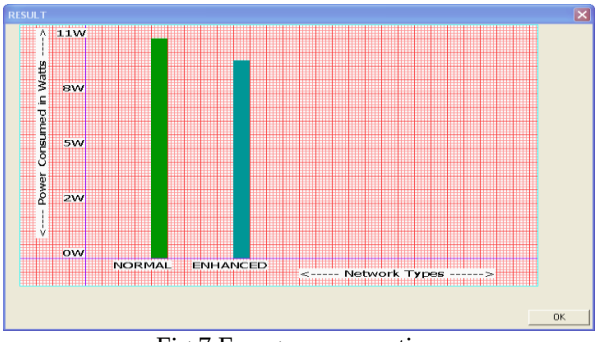

Fig.7 Energy consumption

VI. CONCLUSION

We have designed and implemented EES-MHRT (Enhanced Efficient Secured Multi-Hop Routing Technique), an efficient trust aware routing technique for WS Networks, to protect Hybrid multihop routing in WS Networks against malicious attackers revelling the replay of sensor routing information. EES-MHRT mainly looking on trustworthiness of WSN and energy efficiency of WSN, it is important to the survival of a Wireless Sensor Networks in different

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3,May 2013

environment. By using the technique of trust management frame work, ES-MHRT enables a sensor node to keep track of the trustworthiness of their neighbours and will select a reliable path.

REFERENCES

[1]. Ahmed E.A.A. Abdulla, "HYMN: A Novel Hybrid Multi-Hop Routing Algorithm to Improve the Longevity of WSNs," IEEE Transactions On Wireless Communications, Vol. 11, pp. 7, July 2012.
[2]. Guoxing Zhan, Weisong Shi, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," IEEE Transactions On Dependable And Secure Computing, Vol. 9, pp. 2, March/April 2012.
[3]. Padmavathi, G., & Shanmugapriya, D.A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security (IJCSIS)*: Vol.4, pp.1 & 2 March 2009.
[4]. Hanapi,. Z.M. Ismail,. M,. Jumari,. K. & Mahdavi,. M. (2009). Dynamic window secured implicit geographic forwarding routing for wireless sensor network. *World Academy of Science, Engineering and Technology Vol.4 pp4*
March 2010.
[5]. Kavitha, T., & Sridharan, D. Security vulnerabilities in wireless sensor networks: a survey. *Journal of Information Assurance and Security* 5,pp31-44 June 2010.
[6]. Unoma N. Okorafor, and Deepa Kundur, "Security-Aware Routing and Localization for a Directional Mission Critical Network" ieee Journal On Selected Areas In Communications, Vol. 28, pp. 5, June 2010.
[7]. R.A. Shaikh, H. Jameel, B.J. dAuriol, H. Lee, S. Lee, and Y. Song, "Group-Based Trust Management Scheme for Clustered Wireless Sensor Networks," IEEE Trans. Parallel and Distributed Systems, vol. 20, no. 11, pp. 1698-1712, Nov. 2009.
[8]. Yan Sun, and Sajal K. Das, "A Trust-Based Framework for Fault-Tolerant Data Aggregation in Wireless Multimedia Sensor Networks" ieee Transactions On Dependable And Secure Computing, Vol. 9, pp. 6, November/December 2012.
[9]. Dan Wu and Man Hon Wong," Fast and Simultaneous Data Aggregation Over Multiple Regions in Wireless Sensor Networks" ieee Transactions On Systems, Man, And Cybernetics—Part C: Applications And Reviews, Vol. 41, pp. 3, May 2011
[10]. Zhe Cao, Rong Zhu, and Rui-Yi Que. "A Wireless Portable System With Microsensors for Monitoring Respiratory Diseases" ieee Transactions On Biomedical Engineering, Vol. 59, pp. 11, November 2012.
[11]. Y. Jin, S. Vural, K. Moessner, R. Tafazolli, An Energy-Efficient Clustering Solution for Wireless Sensor Networks , *IEEE Trans. Wireless Comm.*. vo. 10, no. 11, pp. 3973-3983, Nov. 2011.
[12]. Dali Wei,and Rahim Tafazolli," An Energy-Efficient Clustering Solution for Wireless Sensor Networks" ieee Transactions On Wireless Communications, Vol. 10, pp. 11, November 2011.
[13]. Fenye Bao, Ing-Ray Chen," Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection" ieee transactions on network and service management, vol. 9, pp. 2, june 2012.