Design and Implementation of Mobility Based Network Reconfiguration System to Enhance Security in Wireless Sensor Networks

Nupur Gupta
Research Scholar, Department of Computer Science, CEC, LANDRAN, India.

Gagangeet Singh Aujla
Associate Professor, Department of Computer Science, CEC, LANDRAN, India.

Ranbir Singh
Assistant Professor, Department of Computer Science,SUSCET, Mohali, India.

Sahil Vashist
Associate Professor, Department of Computer Science, CEC, LANDRAN, India.

Abstract – In this work, it proposes mobility based dynamic reconfiguration system in WSN. By providing access for the user to construct different virtual fields, proposed protocol accomplishes the goal of meeting the need of different applications and different network conditions. In this work, an environmental data collection scenario is taken. In this, all nodes are in dynamic nature and moves randomly. Sensor nodes are prone to failure due to energy depletion and their deployment in an uncontrolled or even hostile environment, also providing a convenient method for the administrator of the WSN to reconfigure the system just by a remote application. It can achieve the goal that adopt to different applications and different network conditions. This protocol will give the administrator of the WSN a powerful ability. With this great ability, the administrator can reconfigure remotely to adopt different applications and different network conditions. Reconfiguration is performed when the QoS attributes exceed a set threshold. The proposed mechanism was implemented with MATLAB. The time required for a particular network to reconfigure its components is around 15 to 20 seconds, which is very less when compared to the cost of manually stopping and restarting the application with the correct components.

Index Terms – QOS, sensor nodes, Network reconfiguration, WSN.

1. INTRODUCTION

A Wireless Sensor Network (WSN) consists of hundreds or thousands of these sensor nodes. Wireless Sensor Networks (WSNs) have considerable interest from the research community due to their varied applications. They have found applications in military use as well as other applications including traffic monitoring, habitat monitoring, etc [1, 17, 18]. A wireless sensor network (WSN) is a self-organized system of small, independent, low cost, low powered and wirelessly communicating nodes distributed over a large area with one or possibly more powerful sink nodes gathering readings of sensor nodes and, may handle a variety of sensing, actuating, communication act, signal processing, computation, and communication tasks, deployed in the absence of permanent network infrastructure and in environments with limited or no human accessibility. The sink serves as the gateway between the user application and the sensor network. The WSN nodes have no fixed topology, but can configure themselves to work in such conditions. In addition, wireless sensor nodes themselves are exceptionally complex systems where a variety of components interact in a complex way.

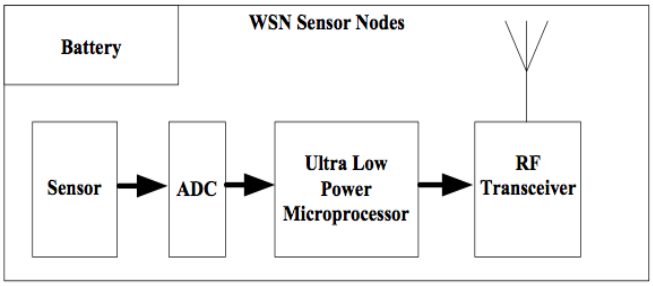

Figure 1: The system block diagram for Wireless Sensor Network nodes

A wireless sensor network (WSN) uses a number of autonomous devices to cooperatively monitor physical or environmental conditions via a wireless network. The design of wireless sensor networks requires consideration for several disciplines such as distributed signal processing, communications and cross-layer design [2]. It Provide a bridge between the real physical and also worlds. It allows the ability to observe the previously unobservable at a fine resolution over large spatio-temporal scales [3].

Wireless sensor networks processing sensitive data are facing the risks of data manipulation, data fraud and sensor damage or replacement. Sensor networks hold the promise of facilitating large-scale and real-time data processing in complex environments. Security is a very complex procedure for many sensor network applications, such as target tracking and security monitoring in military. Providing the security and privacy to small sensor nodes is challenging task, because of limited capabilities of sensor nodes in terms of computation, communication, storing data, and supplied energy [4].

From the above survey, it can be obtained that a routing protocol designed for WSN should have the ability of adapting to different applications and different network conditions. If we can change the routing protocol remotely according to the applications' requirement and the network conditions, we can achieve this goal. Currently, it is very difficult, if not impossible, to change a routing service in a large scale sensor network because the service is statically pre-configured into each node, which is often unattended. So, it proposes a mobility based network reconfiguration system in WSN which can be dynamically reconfigured. Then we present the mechanism of dynamic reconfiguration. The dynamic reconfiguration at node level sought to minimize energy consumption by dynamically adjusting hardware platforms of sensor nodes. The utilization of reconfiguration technique have to consider dynamic factors, such as changes in user requirements, variations in communication channel quality, application changes etc.

The paper is ordered as follows. In section II, it provides the information about network reconfiguration system in sensor networks. In Section III, It defines proposed work & implementation of system. The results are provided in section IV. Finally, conclusion is explained in Section V.

2.DYNAMIC NETWORK RECONFIGURATION SYSTEM

Achieving automatic reconfiguration requires some intelligent component to reason about when to change which components. In the larger area of computer science, artificial intelligence has been a research topic for many years and has branched into many subcategories. Due to advances in hardware technology, several reconfiguration techniques have been developed on the sensor node level. These include Dynamic modulation scaling (DMS) (used to reconfigure modulation schemes in communication), dynamic voltage scaling (DVS) (used to reconfigure voltages and operating frequency of processors), adaptive sampling rate (used to change the sampling rate of sensors), and intelligent node activation (used to change sensor node status). The energy efficiency achieved by these dynamic reconfiguration techniques can be categorized into two different types. At node-level reconfiguration, the DVS, DMS, and adaptive sampling rate are used to minimize the energy consumption of sensor nodes. At network-level reconfiguration, intelligent node activation determines node activity to minimize redundant energy usage within the network [6].

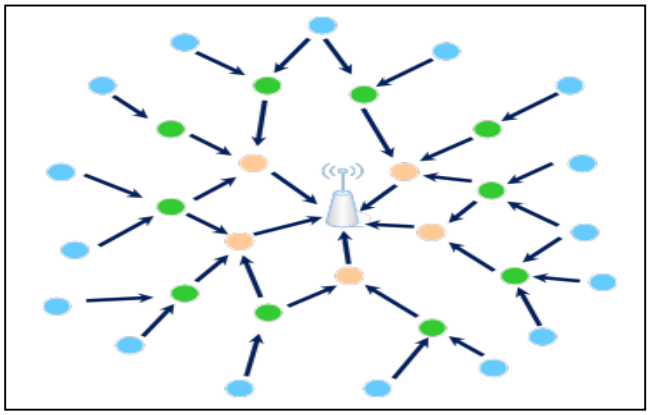

Figure 2: Communication Pattern in WSN [7]

The reconfiguration is the important task related in WSN. The main objective of reconfiguration is to maintain the working of the system in all the conditions even when the problems occur [5].Centralized approach is a common solution to identify and localize the cause of failures or suspicious nodes in WSNs. the central node easily becomes a single point of data traffic concentration in the network, as it also causes all the fault detection and fault management. This causes a large number of message transfer and quick energy depletion in certain regions of the network, especially the nodes which are more close to the base station. Distributed approach encourages the concept of local decision-making, which distributes fault management into the network. The goal is to allow a node to make certain levels of decision before communicating with the central node. The control Centre should not be informed unless there is really a fault occurred in the network.

Dynamic network reconfiguration is described as the process of replacing one routing function with another while the network keeps running. Reconfiguration techniques can be either static or dynamic. The routing algorithm used after the reconfiguration process is not similar. All the paths for each source destination pair need to be computed. Owing to the network time, may cause strong performance degradation during the reconfiguration process, static reconfiguration largely impacts on the message latency.

In dynamic reconfiguration the transition from one routing function to another is performed while the functional parts of the network are fully operational. The problem in this approach exists in the fact that, in general, two different and individually deadlock-free routing functions may be prone to deadlock if they coexist in the network. In a dynamic reconfiguration, there will be a transition phase between the old and new routing functions where reconfiguration-induced deadlocks may occur.

Another drawback of using dynamic reconfiguration is that it usually requires extra resources [6].

3. PROPOSED WORK AND IMPLEMENTATION

From the survey, it can be stated that a routing protocol designed for WSN should have the ability of adapting to different applications and different network conditions.

The actual system presented a routing protocol for WSN, which can be dynamically reconfigured by the remote administrator. It could be able to achieve the goal that adopt to different network conditions and different applications. This protocol would give the administrator the ability to change the routing protocol remotely to adopt different applications and different network conditions. In order to get this ability though protocol, they supported commands for the administrator to change the routing protocol running on the sensor network platform. The nodes change their routing protocol after receiving the commands. When commands come into play on the nodes, a set of mechanisms is provided. These commands and mechanisms help this routing protocol get the great ability of adapting to different applications and different network conditions [7].

Collecting the environmental data, at the network level by having a large number of nodes sense and transmit data back to a set of base stations that store the data using traditional methods continuously. Tree-based routing topologies are used by Environmental data collection applications, where each routing tree is rooted at high-capability nodes that sink data. After the network is configured, each node samples its sensors and transmits its data up the routing tree and back to the base station. In order to meet lifetime requirements, each communication an event must be precisely scheduled.

3.1. Proposed Algorithm

Step 1: Generate no. of sensor nodes (N)
Step 2: Create a random topology
Step 3: Provide random movement in nodes
Step 4: Compute the shortest distance between nodes & all nodes are communicating with each other.
Step 5: Provide head in network for giving commands & monitoring the nodes.
Step 6: Head collect data about environmental conditions like temperature
Step 7: If temperature > threshold then
Nodes move & change their locations immediately for security purposes
Else
Continue their work
Step 8: If locations get changed then check the reconfigure the network.
Step 9: Compute reconfiguration time & other parameters.
Step 10: End

3.2. Placement of Nodes

In above figure, the first step describes the sensors are being deployed in a disaster area. Sensors are randomly spread over the area. Each sensor has a sensor ID shown along with it. It will be used to address any sensor throughout the process. Here we take large number of sensors so that proposed scheme will evaluate easily. No two nodes overlap each other.

3.3. Discover a Topology

In typical usage scenario, the nodes will be evenly distributed over an outdoor environment. This distance between adjacent nodes will be minimal yet the distance across the entire network will be significant. They create a random topology initially.

3.4. Provide Random Mobility

Then provide random mobility in nodes to show that all nodes are dynamic in nature. All nodes move here & there depends upon their speed. We can change the speed of nodes manually.

3.5. Provide Head & Initiator

After the deployment of the sensor nodes, there is a Head node selection by polling method. In a sensor network, the basic sensors are simple and perform the sensing task, while some other nodes, often called the heads, are more powerful and focus on communications and computations.

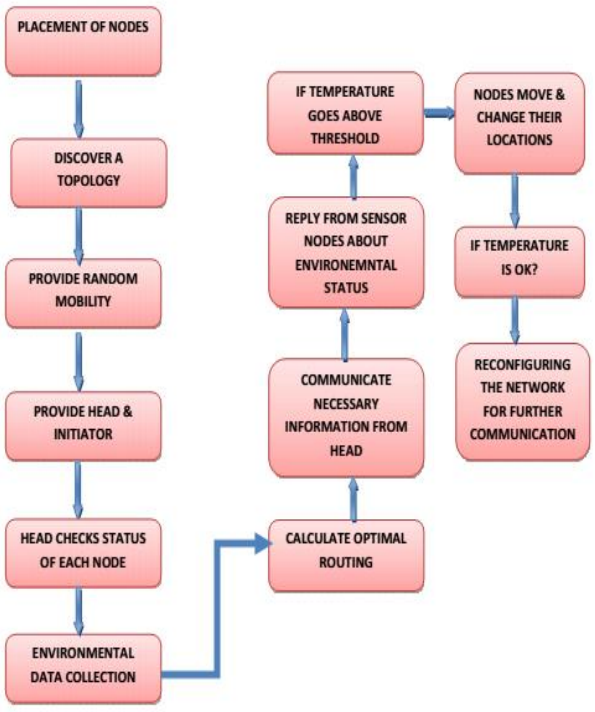

Figure 3 Proposed System Model of Reconfiguration System

3.6. Environmental Data Collection

All nodes are communicating with each other on the basis of shortest path calculated. Then head check the status of each node and collects the environmental data from sensor nodes. All nodes collect data like temperature or any disaster affect from environment.

3.7. Communication between Head & Nodes

For this, there is a direct communication between head & nodes. Head asks the nodes about environment conditions, and then nodes reply back to head about status. For this, there is no loss of data because there is direct transfer of packets from head & all nodes.

3.8. Temperature Effect

Now if temperature goes above threshold due to any disaster effect, the nodes sense data and tells to the head and starts moving from their locations. Then they collect to any other location and when the disaster under control then head orders the nodes to repositioning or reconfigure their locations within minimum time. This reconfiguration is done by self-reconfigurable protocol used. The nodes are moving to same locations after control of disaster.

4. RESULTS

Results are carried out on MATLAB using GUI toolbox. A GUI represents the information and actions available to a user through graphical icons and visual indicators such as secondary notation.

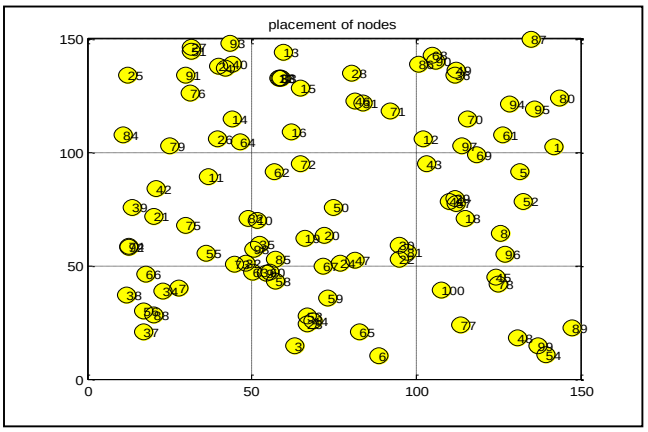

Figure 4: Placement of Nodes

The above figure 4, displays how the sensors are being deployed in an area. Sensors are randomly spread over the area. Each sensor has a sensor ID shown along with it. No two nodes overlap each other. In typical usage scenario, the nodes will be evenly distributed over an outer environment. This distance between adjacent nodes will be minimal yet the distance across the entire network will be significant.

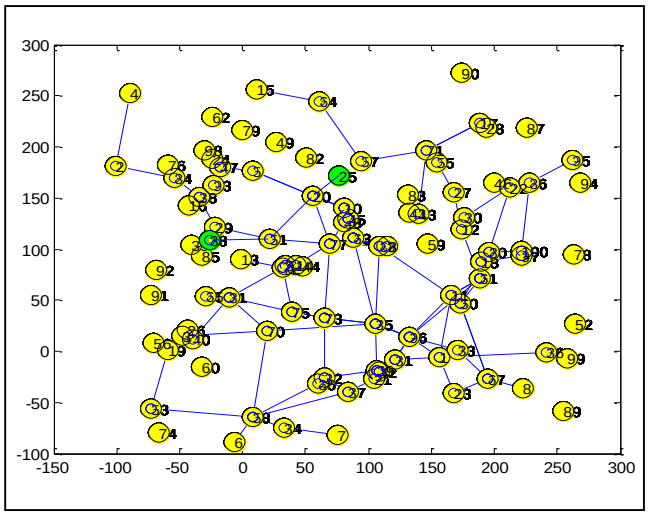

Figure 5: Environmental Data Communication by Nodes

After the deployment of the sensor nodes, there is a Head node selection by polling method. Polling is a method in which the cluster heads request each node one by one to send the data back to the cluster head. The objective of polling is to avoid interference from multiple nodes transmitting to the cluster head simultaneously. After mastering the node, it sends the signal to each node for knowing the distance between them as shown in fig 5.

The routing consists of two basic mechanisms: Route Discovery and Route Maintenance. Route Discovery is the mechanism where a node wishing to send a packet to a destination obtains a source route. To reduce the cost of Route Discovery, each node has to maintain a Route Cache of source routes it has learned or overheard.

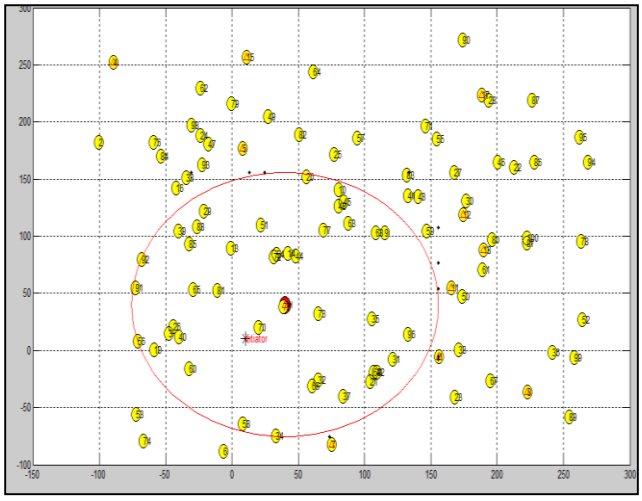

Figure 6: Message Transfer by Head to Nodes

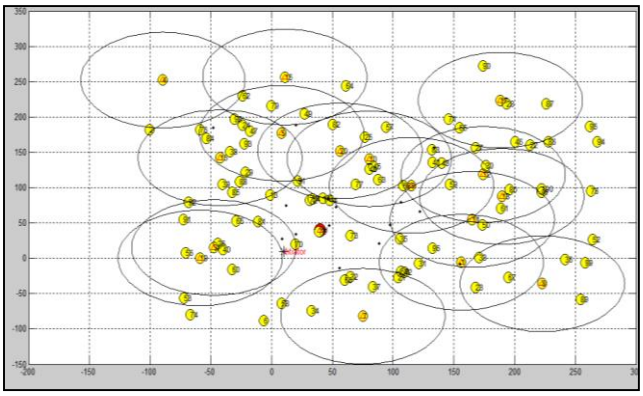

Figure 7: Message Reply Transfer by Nodes to Head

Environmental data collection scenario belongs to data gathering application class. Sensor nodes deployed in such applications are expected to operate.

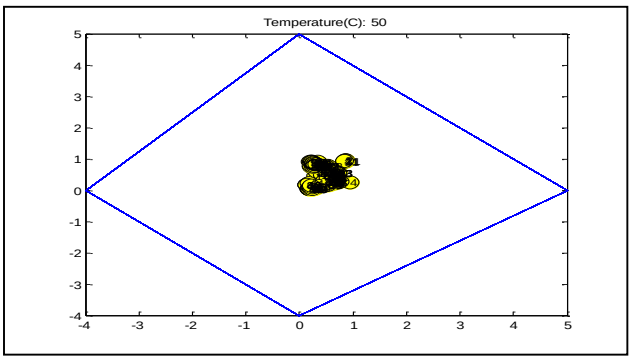

Figure 8: Change of Locations of Nodes for Security

Reconfiguration is intended to adapt the software's components such that it can operate in a changing context. The quicker the middleware responds to a change, the lesser the application is interrupted and the more time the application spends in an optimal configuration.

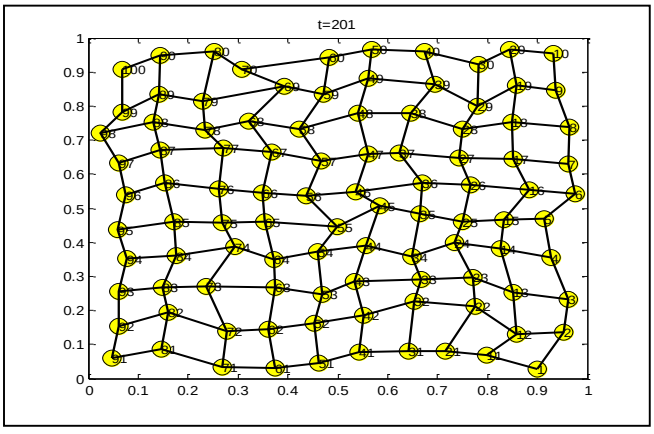

Figure 9: Self Reconfiguring Network Output

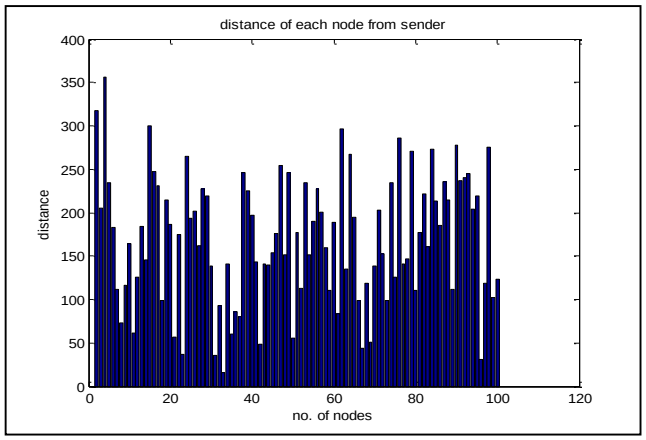

Figure 10: Shortest Distance from Sender

A main issue again relates to the energy consumption: because it is unknown if and when a change in the vibration pattern occurs, it is difficult to assess how long the WSN should run. When a node is low on energy, it could increase the time between measurements, which decrease its energy consumption in exchange for fewer measurement samples.

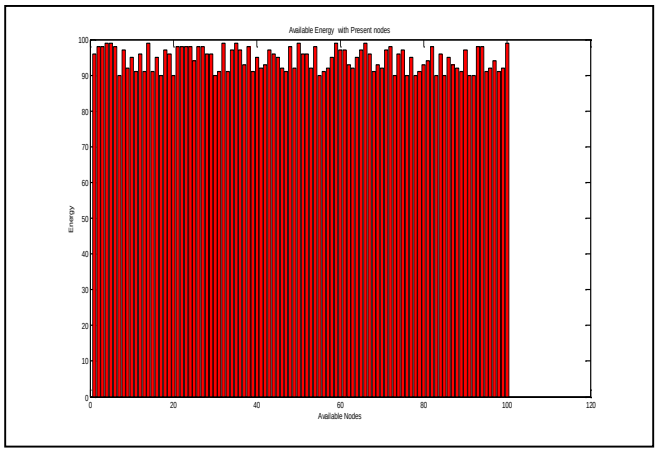

Figure 11: Available Energy in System

Parameter	Proposed	Actual
Throughput	60 (Max)	45 (Max)
Reconfiguration Time	18 Sec	

Table 1: Performance Comparison of System

The time required for a particular network to reconfigure its components is around 15 to 20 seconds, which is very less when compared to the cost of manually stopping and restarting the application with the correct components. The network throughput is the main parameter that is used to reflect the network capability. It is the amount of traffic that is leaving the "Network". We measure these statistics in bits per second unit.

It is also clear that throughput is inversely proportional to mobility i.e. throughput decrease and on other side mobility increase.

5. CONCLUSION

All scenarios of the dynamic reconfiguration infrastructure have been evaluated. In this work, all nodes are communicating with each other. A head is provided for giving the instructions to all nodes. The need for reconfiguration architecture for sensor network applications is apparent from the results of even a simple environmental monitoring algorithm. The time required for a particular network to reconfigure its components is around 15 to 20 seconds, which is very less when compared to the cost of manually stopping and restarting the application with the correct components. In sensor network applications running over a long duration, the ability to reconfigure the components, resulting in a change in the behaviour of the application, in response to external stimuli, in such a short time is of special significance. The automatic reconfiguration of components expressed in a user friendly modelling environment on a base station in response to changing operating conditions in the field. Reconfiguration is performed when the QoS attributes exceed a set threshold. These thresholds may be different for different application domains. Also energy is saved by using dynamic reconfiguration system. In this, shortest distance is calculated between each node so that an optimal routing is performed in network and also direct communication between head to nodes is also provided.

REFFERENCES

[1] Linden, Reddy, Handbook of Batteries, McGraw-Hill Professional: New York, 2002.
[2] Ananthram Swami, Qing Zhao, Yao-Win Hong and Lang Tong, Wireless Sensor Networks: Signal Processing and Communications, Wiley-Blackwell Publication, 2007.
[3] Bhaskar Krishnamachari," An Introduction to Wireless Sensor Networks", 2nd International Conference on Intelligent Sensing and Information Processing, Chennai, January 2005.
[4] Xiaojiang Du and Hsiao-Hwa Chen, "Security in wireless sensor networks", IEEEWireless Communications, Vol.15, Issue 4, pp.60-66, August 2008.
[5] Petra Perner, Advances in Data Mining. Applications and Theoretical Aspects, In proc. 12th Industrial Conference, ICDM, Berlin, July 2012.
[6] MajedValadBeigi, FarshadSafaei and BaharehPourshirazi,"DBR: A Simple, Fast and Efficient Dynamic Network Reconfiguration Mechanism Based on Deadlock Recovery Scheme", International Journal of VLSI design & Communication Systems (VLSICS), Vol.3, No.5, pp.13-26, October 2012.
[7] Gao, Piao, "DRRP: A Dynamically Reconfigurable Routing Protocol for WSN", IEEE 2014.
[8] Aron, Al-Khateeb, "An Enhancement of Fault-Tolerant Routing Protocol for Wireless Sensor Network", International Conference on Computer and Communication Engineering (ICCCE), 11-13 May 2010.
[9] Lin, Wu, Li, "A Selfish Node Preventive Real Time Fault Tolerant Routing Protocol for WSNs", IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, February 2011.
[10] Wang, Feng, Kim, "Catching Packet Droppers and Modifiers in Wireless Sensor Networks", IEEE Transactions on Vehicular Technology, Vol. 62, No. 1, January 2009.
[11] Bruneo and Scarpa, "Adaptive Swarm Intelligence Routing Algorithms for WSN in a Changing Environment", IEEE SENSORS Conference, 2010.
[12] Shih, Ho, Liao, "Fault Node Recovery Algorithm for a Wireless Sensor Network" IEEE Sensors Journal, Vol. 13, No. 7, July 2013.
[13] Kullaa, "Detection, identification, and quantification of sensor fault in a sensor network", Elsevier Journal of Network and Computer Applications, June 2013.
[14] Akkaya, Senturk, Vemulapalli, "Handling large-scale node failures in mobile sensor/robot networks", Elsevier Journal of Network and Computer Applications, June 2013.
[15] Karim, Nasser, "Reliable location-aware routing protocol for mobile wireless sensor network", IET Communication, Vol. 6, Iss. 14, pp. 2149–2158, 2012.
[16] Nguyen, Defago, Beuran, Shinoda, "An Energy Efficient Routing Scheme for Mobile Wireless Sensor Networks", IEEE 2008.
[17] A. Anuba Merlyn and A. Anuja Merlyn, "Energy Efficient Routing (EER) for Reducing Congestion and Time Delay in Wireless Sensor Network", International Journal of Computer Networks and Applications, volume 1, Issue 1, pp. 1-10, November – December (2014).
[18] Sercan VANÇİN, Ebubekir ERDEM, "Design and Simulation of Wireless Sensor Network Topologies Using the ZigBee Standard", International Journal of Computer Networks and Applications (IJCNA), Volume 2, Issue 3, May – June (2015).