# ISRA IN WIRELESS NETWORK USING VIRTUALIZATION

*A.Josephine Jeena[1], P.Loganathan[2], P.G.Vajravel[3], N.Mohammed Anis[4]*
*UG Scholars, Dr.NGP Institute of Technology*
*Josephinejeena2@gmailcom[1] , nathanogre@gmail.com[2], vajravel13@gmail.com[3]anisdoa@gmail.com[4]*

***Abstract-*** ***Wireless Sensor Networks additionally include a concept called Virtualization. Virtualization is an emerging concept in all technologies including storage, networks and examples like Virtual Reality, Virtual Storage, Virtual Machines and Virtual Networks. Here, in our project we took Virtualization concept in general Wireless Networks and implementing that concept in Wireless Sensor Networks. Unlike in Virtual Sensor Networks, Virtualization can be applicable to the fixed sensor nodes in target application areas. But it has some issues like Node isolation, control signaling, resource discovery and allocation, mobility management, network management and operation and security. We took two issues Node Isolation and Resource Allocation, tried to solve that by implementing our ideas by referring some algorithms and techniques. This project reduces the complexity in isolating the nodes for better communication between nodes and gateway and also it will optimize the resource allocation. By managing the above mentioned issues in a given way can increase the efficiency of the network isolation and resource allocation.***

***Keywords-Virtualization, Sensor nodes, isolation, resource allocation.***

## INTRODUCTION

Nowadays, a Sensor networks are involved in many application usages including detecting the change in the temperature of the environment, tracking and monitoring the pollution and also it has been used in many sectors like industries, military services, data communication in environmental research areas, security as well. Since the technology has made the making of sensors and implementing the sensor in the networking side. In our project we used virtualization concept in WSN and also it has some technical issues, among them and for this project two issues are taken Isolation and Resource Allocation. For Isolation, Data Size based technique is used for increasing the performance and for Resource Allocation, Emergent Co-ordination Mechanism is used for better utilization of resource[1]. The implementation of the project is done by using Network Simulation tools and further details are mentioned in the following.

### 1.2 Wireless Sensor Network

Initially the sensor networks were wired one but after introducing the wireless networking, the wireless sensor network has become very popular because its scalability, stability, reliability, easy implementation, cost effective and compact in size. On the other side of networking the introduction of new technologies is not yet attained its stabilization[2].

As before mentioned a WSN is used in various sectors and it is used for many applications, A Wireless sensor network (WSN) is a hardware and software package that typically consists of Four parts and are mentioned below.

#### a. Components of WSN

- Nodes
- Sensors
- Gateway
- Base Station

Nodes – Nodes are systems or device that carries the sensor components and transmit/receive the data from the base station. That nodes has a capability of storing the data in memory and process the data collected with a help of processor and also it has power station as Battery.

Sensors – Sensors are responsible for collecting the data such as moisture, temperature, wind flow and any changes or movement in the place where it installed. It has sensor components that embedded with coding and processing functionalities.

Gateway – A gateway is an interface between the application platform and the wireless nodes on the wireless sensor network. All information received from the wireless nodes is aggregated/manipulated (e.g. translation between network packet formats) by the gateway and forwarded to the application. That application may run on a local computer or a networked computer. In the reverse direction, when a command is issued by the application program to a wireless node, the gateway relays the information to the wireless sensor network.

Base Station –Base Station is where the collected data are organized and used. Base Station can be computer which is connected with the internet.

A WSN has a collection of nodes that why it called as Network, similarly a single nodes contains several components and basic architecture and components are described below,

### b. Components of Sensor Nodes

- Micro – Controller
- ADC
- Sensor
- Transceiver
- Memory
- Battery

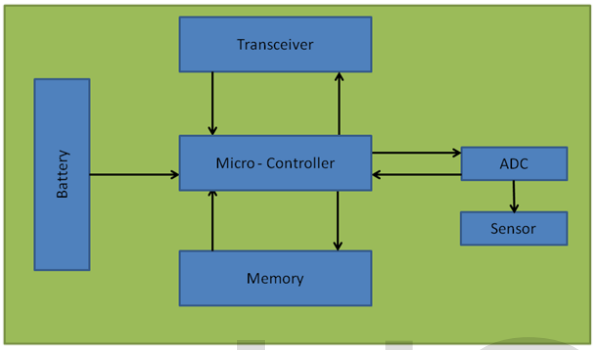



Figure 1.1 Architecture of Sensor Nodes

Micro – Controller is also called as processor which process data to store it in memory which is embedded with coding for processing the data collected by sensors.

ADC – Analog to Digital Convertor is a section where sensed analog signals are converted into Digital signal and sent to the micro-controller.
Sensor – Sensor are devices with ability of sensing the required data like moisture, temperature in the installed area.

Transceiver – It is responsible for transmitting and receiving data from the node and from the base station and gateway.

Memory – The processed data from the micro-controller will be stored in the memory and further used while transmitting the data.

Battery – For functioning, sensor nodes requires power. It will be provided in the Battery as a resource, but it will be a limited one.

## 1.2 Virtualization

Virtualization is a concept introduced and implemented for a while in other sectors in Computer Science. Virtualization is a simple concept that makes use of the physical component and applies the logical concept over it, to produce some good result. It includes some application areas like Virtual Data Centre, Virtual Machines, Virtual Reality, Virtual Storage and Virtual Networks.
In our project, we implemented a Virtualization concept used in Wireless Network in Wireless Sensor Networks. So that it will be easy for processing the data in a quite efficient manner. Usually virtualization can be done in two ways,

1. Node Level Virtualization
2. Network Level Virtualization

### a. Node Level Virtualization

In node level Virtualization, multiple tasks can be done in a sensor node which has single operating system. By using Virtual Machine/Hypervisor some other operating systems can be installed and it is represented in Figure 1.2. Sequential execution can be termed a weak form of virtualization, in which the actual execution of application tasks occurs one-by-one (in series). The advantage of this approach is its simple implementation, while the obvious disadvantage is that applications have to wait in a queue. In simultaneous execution, application tasks are executed in a time-sliced fashion by rapidly switching the context from one task to another. The advantage of this approach is that application tasks that take less time to execute will not be blocked by longer running application tasks, while the disadvantage is its complexity.

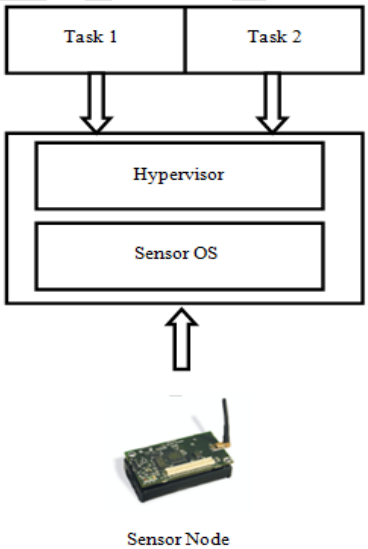



Figure 1.2 Node Level Virtualization

### b. Network Level Virtualization

For Network Level Virtualization, infrastructure of the network is sliced and nodes in the WSN will be virtually

separated in desired group or section, and it can be done by using, The generic cell rate algorithm (GCRA) and the representation of the general WSN and Virtualized WSN are represented in Figure 1.3 (a) and (b).A Virtualized WSN is formed by a subset of a WSN's nodes that is dedicated to one application at a given time. Enabling the dynamic formation of such subsets ensures resource efficiency, because the remaining nodes are available for different multiple applications (even for applications that had not been envisaged when the WSN was deployed), although not necessarily simultaneously.

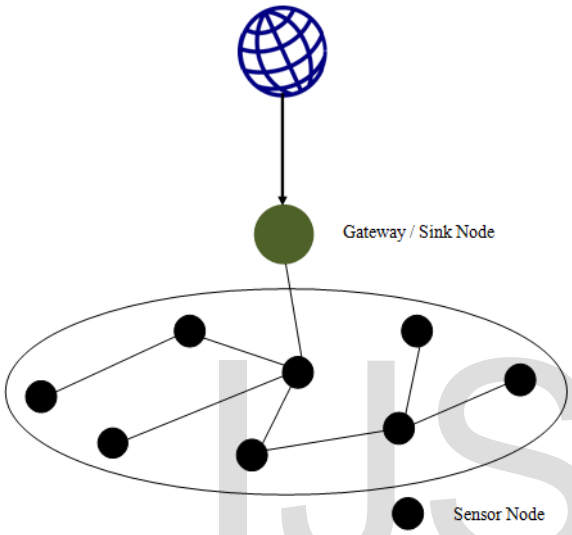



Figure 1.3(a) Wireless Sensor Network

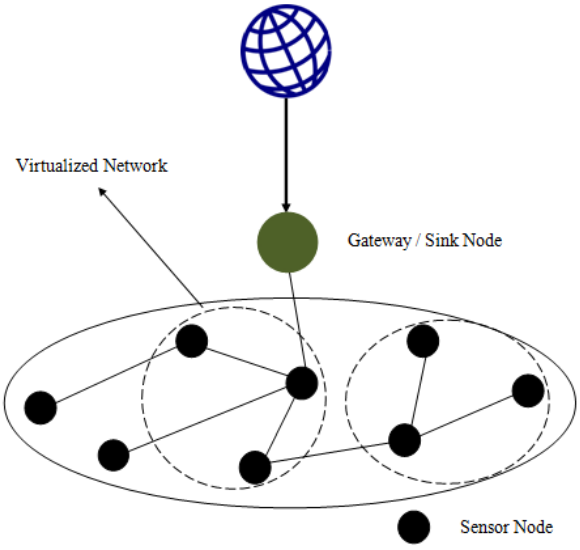



Figure 1.3(b) Virtualized Wireless Sensor Network

### 1.3 Issues in Virtualization

Since Virtualization concept is much efficient and useful, it also has some issues and challenges to face. Basically the Wireless Network Virtualization requires some requirements to be enabled, and such a requirements are:

- Coexistence: In wireless network virtualization, physical infrastructures should allow that multiple independent virtual resources coexist on substrate physical networks. Actually, it is clear that the purpose of virtualizing network is to make multiple systems to run on the same physical resources.

- Coexistence: The network is virtualized to help multiple systems run on the same physical resources.In case of wireless networks, multiple independent virtual resources should coexist on substrate physical networks, permitted by physical infrastructures.

- Flexibility, manageability and programmability: Freedom in different aspects of networking needs to be provided in wireless network virtualization through the decoupling customized control protocols from the underlying physical networks and other coexisting virtual networks. However, since different virtualization may have different levels, ranging from flow level, sub-channel or time-slot level, to antennas level, flexibility depends on the level of virtualization. Higher level virtualization may reduce the flexibility of virtualization while better multiplexing of resources across slices (and hence increased utilization with fluctuating traffic) and simplicity of implementation, but can reduce the efficacy of isolation and the flexibility of resource customization, whereas virtualization at a lower level leads to the reverse effects. Manageability and programmability are other two basic requirements. Since virtual slices or virtual networks are assigned to SPs and the management of these virtual wireless resources are decoupled from substrate networks, wireless network virtualization needs to provide complete end-to-end control of the virtual resource to the SPs. SPs are able to manage configuration, allocation of virtual networks, e.g., routing table, virtual resource scheduling, admission, and even modifying protocols, etc.

- Isolation: Isolation ensures that any configuration, customization, topology change, mis-configuration and departure of any specific virtual networks will be not able to affect and interfere other coexisting parts. In other words, isolation means that any change in one virtual slice, such as the number of end users, mobility of end users, fluctuating of channel status, etc., should not cause any change in resource allocation for other slices. Indeed, virtual slices or virtual networks are transparent to each other, or we can say that they never know the existence of other virtual slices. It is similar to the multiplexing among users in modern mobile networks but not the same. Since many virtual networks should coexist, isolation is the basic issue in virtualization that guarantees fault tolerance, security, and privacy. In addition, in wireless networks, especially cellular networks, any change in one cell may introduce high interference to neighbor cells, and the mobility of end users may create instability of a specific area. Therefore, isolation becomes more difficult and complicated in wireless networks compared to the wired counterparts. So, the above requirements are basic for the virtualization but sometimes these requirements are get violated by some issues and they are listed below:

- **Isolation:** The basic issue in virtualization is Isolation that enables sharing of resources on an abstract level. The changes made to the topology of any virtual network must not affect with any coexisting nodes. The concept of isolation is easier in wired networks than in the wireless networks. Because of the inherent broadcast nature, the radio resource abstraction and isolation is not straight-forward in wireless communication. It also experiences fluctuations in the quality of the wireless channel.

- **Control signaling:** Connectivity needs to be established between SPs and InPs before a virtual network can be created. With this connectivity, SPs can express their requirements of resources to serve end users. In addition, since virtualization can happen among InPs, a standard language to express explicit sharing information among InPs becomes necessary. Moreover, the communication between SPs and end-users is also needed. This introduces a circularity where networks connectivity is a prerequisite to itself. Thus, proper control signaling and interface considering delays and reliability need to be designed carefully to enable the communication among different parties involved in wireless network virtualization. Due to the particular properties of wireless networks, SPs or end user may require different QoS attributes. In contrast to functional service features, there is less agreement regarding the specification of QoS attributes. Therefore, the control signaling and interface should be compatible with different kinds of requirements.

- **Resource discovery and allocation:** To realize wireless network virtualization, InPs or MVNOs should discover the available active and passive resources in the underlying physical wireless networks. InPs need to decide the physical resources used to virtualized, which means InPs may reserve some resource for their own usage. Since resource may be shared among multiple InPs, an efficient coordination mechanism should be designed appropriately.

Resource allocation is another significant challenge of wireless network virtualization. Resource allocation schemes need to decide how to embed a virtual wireless network on physical networks (e.g., Which nodes, links and resources should be picked and what should be optimized ). As defined in, resource allocation in a network virtualization environment refers to static or dynamic allocation of virtual nodes and links on physical nodes and paths, respectively.

In resource discovery and allocation, the time granularity(i.e., how often should resource discovery and allocation be performed?) needs to be carefully designed. If the time interval is too small, the cost of overload and signaling may increase significantly. However, long time interval would lead degradation to static architecture of traditional networks.

- **Mobility management:** Mobility management is an important issue in wireless networks that ensures successful delivery of new communications to users and maintains ongoing communication with minimal disruptions, while users move freely and independently. There are two components immobility management: location management and handoff (also referred to as handover in the literature) management. Location management enables the network to deliver communications to users by tracking their locations. Handoff management maintains service continuity by keeping a user connected when its point of connection to the network moves from one access

point (or base station) to another. With wireless network virtualization, tracking a user's location is challenging, since it may perform location update with different VMNOs or InPs.

- **Network management:** Network management is always a big challenge for the carriers. Management of wireless network virtualization is crucial to guarantee the proper operation of the physical infrastructure, the host virtual wireless networks and the wireless services supported by the virtual networks. Asa (virtual) network may span over multiple underlying physical networks, network management and operation face new challenges.
- **Security:** A widely used assumption in wireless network virtualization is that different parties are always trusted. Therefore, in addition to the vulnerabilities and threats of traditional wireless networks, the involvement of intelligence in wireless network virtualization present new security challenges. For many security issues, authentication is an important requirement, which is crucial for integrity, confidentiality and non-repudiation. In addition, the experience in security of traditional wired and wireless networks indicates the importance of multi-level protections because there are always some weak points in the system, no matter what is used for prevention-based approaches (e.g., authentication). This is especially true for wireless network virtualization, given the low physical security autonomous functions of mobile devices.

Among these challenges, Node Isolation and Resource Allocation is taken in account to rectify the problems using our techniques which is obtained from literature survey regarding this problems. By applying the given algorithms and techniques it can improve the performance of the WSN considerably.

## LITERATURE REVIEW

### 2.1 For Virtualization

**a.** Rogerio V. Nunes, Raphael L. Pontes, and Dorgival Guedes, "Virtualized Network Isolation Using Software Defined Networks" in Isolation on IEEE Journal.

**Description**

In this work they propose DCPortals, a system which addresses those issues without requiring new hardware. Their solution is based on packet header rewriting, done in a way to hide real traffic origins and destinations from the core of the network (hardware), also hiding traffic from each virtual network from any VMs not belonging to the same tenant. To do that, they use the virtual switches present in the virtualization monitors (hypervisors) of each physical machine1, which already implement the OpenFlow architecture. With Open-Flow, each virtual switch exports a programming interface to their forwarding tables. Using that interface, a controller can tell the switch to inform it of any packets that do not match previously identified flows. This led to the creation of
the network hypervisor, a software controller that can isolate tenants' network traffic as machine hypervisors isolate CPU and memory bettheyen VMs. The use of such a controller to centralize the network view is called a Software Defined Network (SDN).

**Disadvantage**

- Need to improve the system and considering its integration with OpenStack, it must intend to study the integration of our solution directly with Quantum, the new OpenStack component for network configuration.
- It needs some working on integrating DCPortals, which provides network isolation, with Gatekeeper, a system designed to provide network traffic guarantees in a datacenter Environment.

**b.** Andreas Blenk, Arsany Basta, Martin Reisslein and Wolfgang Kellerer, "Survey on Network Virtualization Hypervisors for Software Defined Networking" in SDN on IEEE Journal.

**Description**

Software defined networking (SDN) has emerged as a promising paradigm for making the control of communication networks flexible. SDN separates the data packet forwarding plane, i.e., the data plane, from the control plane and employs a central controller. Network virtualization allows the flexible sharing of physical networking resources by multiple users (tenants). Each tenant runs its own applications over its virtual network, i.e., its slice of the actual physical network. The virtualization of SDN networks promises to allow networks to leverage the combined benefits of SDN networking and network virtualization and has therefore attracted significant research attention in recent years. A critical component for virtualizing SDN networks is an SDN hypervisor that abstracts the underlying physical SDN network into multiple logically isolated virtual SDN networks (vSDNs), each with its own controller. They comprehensively survey hypervisors for SDN networks in this article. They categorize the SDN hypervisors according to their architecture into centralized and distributed hypervisors. They furthermore sub-classify the hypervisors according to their execution platform into hypervisors

running exclusively on general-purpose compute platforms, or on a combination of general-purpose compute platforms with general- or special-purpose network elements. They exhaustively compare the network attribute abstraction and isolation features of the existing SDN hypervisors. As part of the future research agenda, they outline the development of a performance evaluation framework for SDN hypervisors.

**Disadvantage**

- There is a wide gamut of important open future research directions for SDN hypervisors. One important prerequisite for the future development of SDN hypervisors is a comprehensive performance evaluation framework and more research is necessary to refine this framework and grow it into widely accepted performance benchmarking suite complete with standard workload traces and test scenarios.
- Establishing a unified comprehensive evaluation methodology will likely provide additional deepened insights into the existing hypervisors and help guide the research on strategies for advancing the abstraction and isolation capabilities of the SDN hypervisors while keeping the overhead introduced by the hypervisor low.

**c.** Mao Yang, Yong Li, Depeng Jin, Lieguang Zeng, Xin Wu, Athanasios V. Vasilakos, "Software-Defined and Virtualized Future Mobile and Wireless Networks: A Survey" on SDN Survey in IEEE Journal.

**Description**

With the proliferation of mobile demands and increasingly multifarious services and applications, mobile Internet has been an irreversible trend. Unfortunately, the current mobile and wireless network (MWN) faces a series of pressing challenges caused by the inherent design. In this paper, we extend two latest and promising innovations of Internet, software-defined networking and network virtualization, to mobile and wireless scenarios. We first describe the challenges and expectations of MWN, and analyze the opportunities provided by the software-defined wireless network (SDWN) and wireless network virtualization (WNV). Then, this paper focuses on SDWN and WNV by presenting the main ideas, advantages, ongoing researches and key technologies, and open issues respectively. Moreover, we interpret that these two technologies highly complement each other, and further investigate efficient joint design between them. This paper confirms that SDWN and WNV may efficiently address the crucial challenges of MWN and significantly benefit the future mobile and wireless network.

**Disadvantage**

- NFV and middlebox optimizing Recently, NFV enabling middlebox has captured increasing attention. Plenty of network functions may be implemented in middlebox running on the commodity hardware by virtualization. Meanwhile, middlebox may be effectively managed and controlled though SDWN. However, several key issues need to be addressed, including middle box placement problem, flow path optimizing, dynamic resource allocation, and etc.
- Software-defined multi-dimension virtualization There are multiple dimensions of virtualization in WNV, such as spectrum resources, access devices, and forwarding devices. Various dimensions of virtualization call for quite different implementation approaches. Achieving one unified software-defined virtualization control covering all the dimensions is obviously challenging.
- Mobile and wireless environment Mobile and wireless environment is complicated and varies continuously, which makes it quite difficult to implement just one technology of SDWN and WNV, let alone the combination of both of them.
- Trade-off between fine-grained and implementation difficulties Fine-grained sofware-defining and virtualization may achieve higher performance. On the other hand, this also extremely causes implementation difficulties and further makes the vendors and operators hesitate to undertake the design and implementation. Therefore, a reasonable trade-off between fine-grained and implementation difficulties should be found.

## 2.2 FOR ISOLATION

**a.** Kalaiselvan. K, Gurpreet Singh, "Detection and Isolation of Black Hole Attack in Wireless Sensor Networks", in IJIRSET

**Description**

The proposed model for the identification and isolation of blackhole node involves the following steps. The wireless sensors are deployed in the field randomly. The K mean clustering method is applied for creating the clusters in the sensor network. The clusters are formed so the sensor nodes within that cluster will forward the sensed data to the cluster head of the corresponding cluster not directly to the sink node. The cluster head for each cluster are selected on the LEACH (Low Energy Adaptive Cluster Hierarchy) protocol. This protocol allows the sensor nodes the possibility to

be selected as the cluster head. The network performance of the sensor network is analyzed for the presence of the black hole node. If the network performance is lower than the threshold, then the black hole node is present in the Network. The sensor nodes broadcast the route request messages to transmit to the other node in the network. Within the cluster, the cluster head gathers the sensed data from the sensor nodes and it will transmit to the sink. The source sensor node will wait for the reply messages to the route request messages sent by the source sensor node. If the black hole is present in the sensor network, the black hole node will send the fake reply packet with the distance to the destination node value is less. The source sensor node will acknowledge the black hole node as the neighbor node and it will transmit the data to the black hole node. The black hole node simply discards or drops the packet. The sensor nodes will check for the fake reply packets and identify the black hole node and it will inform the other nodes in the network that particular node is the black hole node. Thus, the black hole node is isolated from the network and if the black hole node transmits the reply packets to other sensor nodes, the nodes simply discard the reply messages. The proposed methodology is implemented in a simulated environment and the results are compared with the existing technique. The parameters which are considered in the proposed methodology for the detection and isolation of the black hole node are packet delivery ratio and the throughput of the sensor network.

**Disadvantages**

- Above does not provide isolation for collaborative black hole attacks where the nodes act in coordination with each other and it is lacking in the detection of black hole attacks. It simply provide cure for the after attack, it does provide early detection and it is complicated for the simple isolation algorithms.

**b.** Rashad Eletreby and Osman Yagan, "Node Isolation of Secure Wireless Sensor Networks under a Heterogeneous Channel Model" in Carnegie Mellon University.

**Description**

Ya˘gan introduced a new variation of the Eschenauer and Gligor (EG) key redistribution scheme , referred to as the heterogeneous key predistribution scheme. The heterogeneous key predistribution scheme accounts for the cases
when the network comprises sensor nodes with varying level of resources and/or connectivity requirements, e.g., regular nodes vs. cluster heads, which is likely to be the case for many WSN applications. According to this scheme, each sensor node belongs to a specific priority class and is given a number of keys corresponding to its class. More specifically, Given r classes, a sensor node is classified as a class-i node
with probability _i, resulting in a probability distribution _ = f_1; _2; : : : ; P _rg with _i > 0; for i = 1; : : : ; r and r i=1 _i = 1. Sensors belonging to class-i are each given Ki keys selected uniformly at random (without replacement) from a key pool of size P. As with the EG scheme, pairs of sensors that share key(s) can communicate securely over an available channel after deployment. Let K(n;_;K; P) denote the random graph induced by the heterogeneous key pre-distribution scheme described above, where K = fK1;K2; : : : ;Krg and n denotes the number of nodes. Pair of nodes are adjacent as long as they share a key. This model is referred to as the inhomogeneous random key graph in wherein, zero-one laws for the properties that
K(n;_;K; P). i) has no isolated nodes and ii) is connected are established under the assumption of full visibility. Namely, it was assumed that all wireless channels are reliable and secure communications among participating nodes require only the existence of a shared key. Our paper is motivated by the fact that the full visibility assumption is too optimistic and is not likely to hold in most WSN applications; e.g., the wireless medium of communication is often unreliable and sensors typically have limited communication ranges. To that end, we study the secure connectivity of heterogeneous WSNs under a heterogeneous on/off communication model; wherein, the communication channel between two nodes of class-i and class-j is on with probability _ij . The heterogeneous on/off communication model induces the inhomogeneous Erd˝os-R´enyi (ER) graph [9], [10], denoted hereafter by G(n;_). The overall WSN can then be modeled by a random graph model formed by the intersection of an inhomogeneous random key graph and an in homogeneous ER graph. We denote the intersection graph K(n;_;K; P) \ G(n;_) by H(n;_;K; P;_). Our main contribution is as follows. We present conditions (in the form of zero-one laws) on how to scale the parameters of the intersection model H(n;_;K; P;_) so that it has no secure node which is isolated with high probability when the number of nodes n gets large. Our result generalizes several results in the literature, including the zero-one laws for absence of isolated nodes in inhomogeneous random key graphs intersecting homogeneous ER graphs, and in homogeneous random key graphs intersecting homogeneous ER graphs.

**Disadvantage**

- The above mentioned isolation techniques involves mathematical functionalities which increases the complexity of the algorithm and it is difficult to implement in the real time project,

since the results are just simulated and it cause some unwanted difficulties in implementation.

### 2.3 FOR RESOURCE ALLOCATION

**a.** Aram Galstyan, Bhaskar Krishnamachari & Kristina Lerman, "Resource Allocation and Emergent Coordination in Wireless Sensor Networks",

**Description**

In this paper, they explore the paradigm of emergent coordination as an efficient distributed control mechanism for WSN. Instead of concentrating on a specific sensor coordination problem, they present their results for rather general settings of repeated games. Specifically, they treat nodes as autonomous self-interested agents that utilize a simple reinforcement learning scheme and achieve coordination by playing repeated resource allocation (load balancing) games with changing resource (load) capacities. Their results indicate that for a range of parameters the system as a whole adapts efficiently to these changes. More importantly, the range of parameters for which coordination arises is independent of the number of nodes in the system. This property
Was very important for the WSN where the number of nodes might change in time (e.g., some nodes will run out of the power, while other nodes might be introduced to an already existing system).

**Disadvantages**

- Above paper, actually has some more complicated algorithms such as Resource Allocation Games with Changing Resource Capacity, Multi Choice games. For our convenient, we select only few concept from the paper not completely derived one.

**b.** Andrew T. Zimmerman And Jerome P. Lynch, University Of Michigan Frank T. Ferrese, Naval Surface Warfare Center, "Market-Based Resource Allocation for Distributed Data Processing in Wireless Sensor Networks".

**Description**

The work presented in this study builds upon the price and utility-based resource
allocation methodologies mentioned above. However, it differs from previous work in
WSN resource management in two distinct ways. First, in order to account for a greater emphasis on embedded data processing, this study broadens the previous utility function focus on optimal communication and data flow in order to include computational speed and efficiency. Second, the resource allocation algorithm developed in this study is implemented directly on a network of wireless sensor prototypes, allowing the performance of the proposed algorithm to be evaluated directly on the sensing system it was designed for instead of in a simulated environment.

**Disadvantage**

- The paper applied for prototypes and it has yield a good result, but it is not applicable and suitable for our project content. And nodes act as a buyer and seller, so for large number of nodes it may result in complex & time consuming process.

## METHODOLOGY

### 3.1 IMPLEMENTATION TECHNIQUES

For implementing our projects, we referenced some papers and obtained Basic ideas from those papers, then we made our ideas and implemented in this paper. Basically the modules implementation is carried out in three steps,

1) Virtualization
2) Node Isolation
3) Resource Allocation

### 3.2 ALGORITHM FOR VIRTUALIZATION

For virtualization we use generic cell rate algorithm which is based on leaky bucket mechanism. The leaky bucket mechanism may be considered un buffered or buffered. 'K' size of token pool consists by un buffered leaky bucket mechanism, as shown in figure 3.1(a). Fixed rate tokens are generated. In particular time if the token pool is full then a token will be lost. when the cell enters the network it takes a token from the token pool. After this process the number of tokens reduced by one from the token pool. The cell may be noncompliant cell or violating cell. If token pool is empty then cell will be arrive. Next we discussed about buffered leaky bucket is shown in figure3.1(b). It is similar to the un buffered leaky bucket but here we take 'M' size of input buffer. When the token pool is empty a cell can wait if it arrives at a time. Violating cells are may be dropped or tagged based on the parameters (K, token generation rate and M, if it is a buffered leaky bucket) leaky bucket is defined. The main difficulty in the leaky bucket is fixing its parameters. When the source adheres to its contract leaky bucket is transparent, and when the source exeeds its contract it catches all the violating cells. An arrival process of cells to the UNI, in leaky bucket it is possible to fix the parameters using queueing based models. In catching violating cells, the leaky bucket can be very ineffective. Dual leaky bucket mechanism suggested for more capable policing. The first leaky bucket polices is violation of the peak cell rate, and the next one polices

violations of the sources burstiness. GCRA catch all violating cells, but it needs an additional traffic parameter.

In addition to GCRA, using a traffic shaper a source can shape its traffic in order to the stream of cell it transmits to the network of desired characteristics. peak cell rate reduction, burst size reduction, and reduction of cell clumping are involved in traffic shaping by suitable spacing out the cells in time.

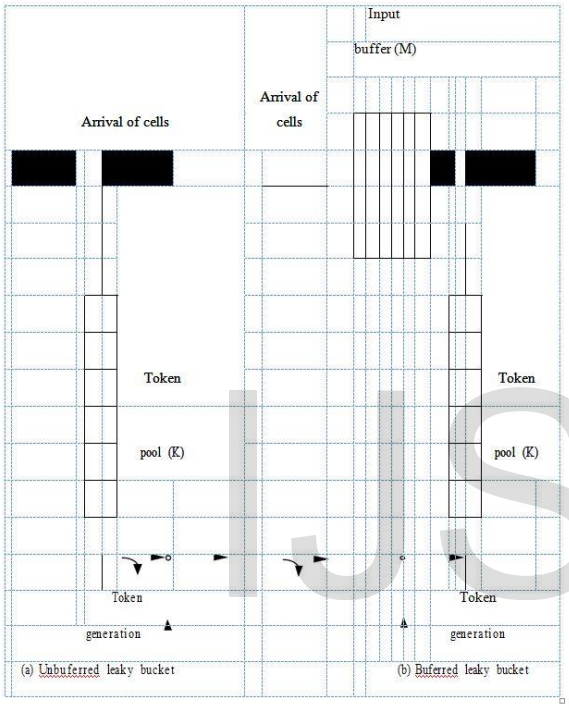
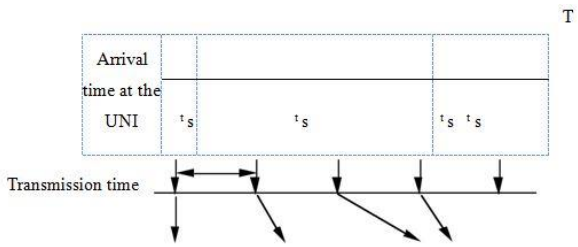



Figure 3.1: The leaky bucket

### a. The generic cell rate algorithm (GCRA)

GCRA is a deterministic algorithm it is not similar to the leaky bucket mechanism and it does catch all the violating cells. However, the additional parameter known as the cell delay variation tolerance (CDVT) is for GCRA requires. This additional parameter is not to be complicated with the peak to peak cell delay variation parameter described.




Let us assume that a source is transmitting at peak cell rate and it produces a cell every T units of time, where T = 1/PCR. As shown in figure 3.2, due to multiplexing with cells from other sources and with signalling and network management cells, it is possible that the inter-arrival time of successive cells belonging to the same source at the UNI may vary around T. That is, for some cells it may be greater than T, and for others it may be less than T. In the former case, there is no penalty in arriving late! However, in the latter case, the cells will appear to the UNI that they were transmitted at a higher rate, even though they were transmitted conformally to the peak cell rate. In this case, these cells should not be penalized by the network. The cell delay variation tolerance is a parameter that permits the network to tolerate a number of cells arriving at a rate which is faster than the agreed upon peak cell rate. This parameter does not depend upon a particular source. Rather, it depends on the number of sources that use the same UNI and the access to the UNI, and it is specified by a network administrator. GCRA can be used to monitor the peak cell rate and the sustained cell rate. There are two implementations of GCRA, namely, the virtual scheduling algorithm and the continuous-state leaky bucket algorithm. These two algorithms are equivalent to each other.

### 3.2 NODE ISOLATION (Data Size Based Technique)

Usually, sensor nodes carry a various sized nodes, size of the node may be range from kilo bytes to Mega bytes. So in a WSN, say there are 50 nodes are installed. All the nodes are installed at various place, there is considerable distance between the nodes. Each node has a certain sensed data like moisture, temperature, humidity. They started to send those collected data to the gateway, but there will be a chance for occurrence congestion. Though it can be neglected by congestion control protocols and other communication protocols, those are applicable for certain amount of nodes. But in our case, we took 100 nodes. Even the protocols reduce the network traffic and also performance of nodes. Nodes cannot wait for long period, since the sensed data could be changed, updated frequently. And also the nodes may lose the power unnecessarily which may result in reduced life time and performance of nodes. This scenario is represented in figure 3.3.

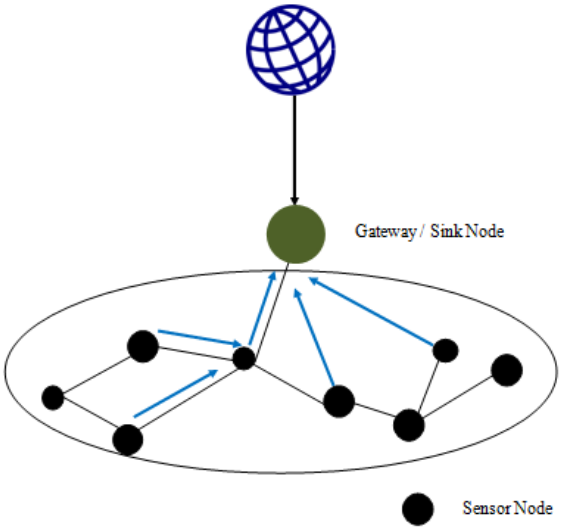



Figure 3.3 Before Isolation

So by applying virtualization and isolating the nodes is one of the solutions for this problem, we used Data Size Based Technique.

### a. Data Size Based Technique

As already mentioned, each sensor node has certain amount of data. Data can be varying from large one to small. Threshold value is set on the inter communication protocol, so gateway can know which nodes are below and above the threshold value. If nodes fall below the threshold value is isolated into a Virtual network and if nodes falls above the threshold value is isolated into another Virtual network. Usually, data packets have the details about destination, source and length of the data. So obviously, gateway came to know about the details about each sensor node. Then rest of the thing is separating the node in virtual network by virtualization. The representation of this technique is represented in figure 3.4.

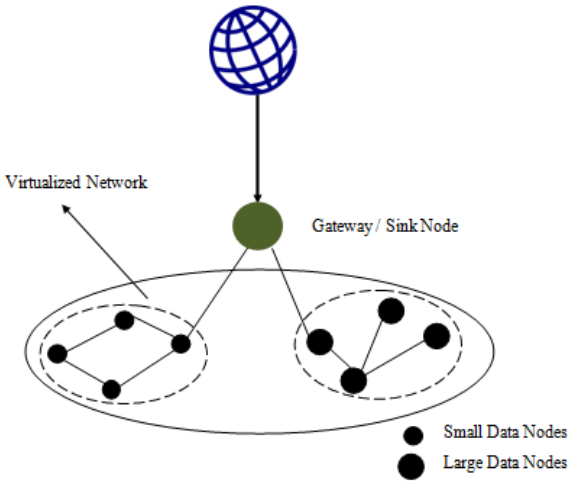



Figure 3.4 After Isolation

## 3.3 RESOURCE ALLOCATION (Emergent Coordination Mechanism)

In a WSN, resource is not only the data transmitted, it includes bandwidth, data, battery power, utilization of communication channel. So Resource must be used efficiently. For our project, we took how to preserve the Battery resource during the communication. A battery is only resource to the nodes and it must be utilized optimally. Unnecessary usage of resource may lead to loss of node. A WSN node usually uses protocols like MACA, CSMA-CD. We used those protocols as a medium to implement our concept called emergent coordination mechanism in that.

### a. Emergent Coordination Mechanism

Emergent Coordination Mechanism is similar to the normal CSMA-CD, MACA protocol. Before establishing the connection, sensor nodes send Request-To-Send (RTS) signal to neighbourhood nodes, so that those nodes will not involve in the communication channel. In general, during that waiting time all the nodes were in operating status (i.e Nodes will be waiting to establish connection) but in our concept the nodes that ready to data will RTS signal to all nodes along with time period. So that, until the nodes completes its communication rest of the nodes will go to idle state. So there is a efficient utilization of battery power. Here, after the isolation the network is virtually separated, so it will be applicable for both side of the virtual network. Node that tries to communicate with the gateway, before that it sends RTS to nearby nodes and it is given in Figure 3.5 and after receiving the Message the rest of the nodes will be in a idle state, and its representation is given in figure 3.6

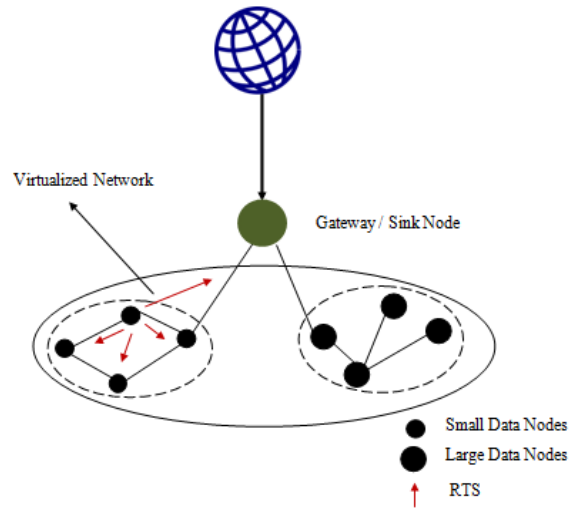



Figure 3.5

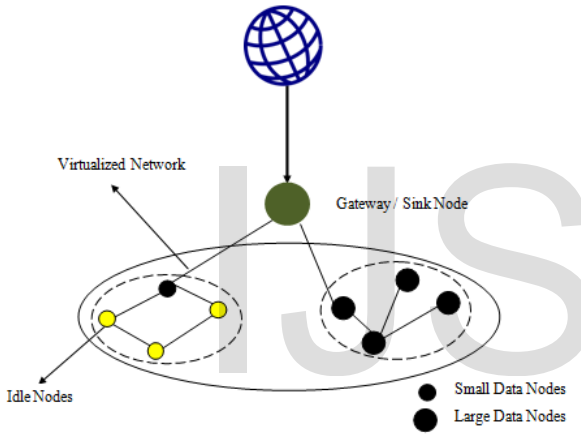



Figure 3.6

Above Mechanism is applicable to both networks and it maximizes the performance in a considerable way.

## MODULE IMPLEMENTATION

### 4.1 MODULES

Our project modules are divided into three major sections and they are given below as follow as:

- Network Setup & Virtualization
- Isolation of Nodes
- Resource Allocation

All the three modules requires coding part that has to be done in C, TCL language.

### 4.2 REQUIREMENTS

- NS-2 (Network Simulation Tool)
- Operating System – Linux

### 4.3 ABOUT THE TOOL

Since the real time implementation of the WSN may cost, so we decided to go on with simulation tools. Simulation tools are used to attain the real time results without using complex hardware. For our project we used a Tool Called NS-2.

#### a. NS-2 (Network Simulator)

The NS-2 simulation environment offers great flexibility in investigating the characteristics of sensor networks because it already contains flexible models for energy-constrained wireless ad hoc networks. In this environment a sensor network can be built with many of the same set of protocols and characteristics as those available in the real world. The mobile networking environment in NS-2 includes support for each of the paradigms and protocols. The wireless model also includes support for node movement and energy constraints.

NS-2 has many and expanding uses including:

- To evaluate the performance of existing network protocols.
- To evaluate new network protocols before use.
- To run large scale experiments not possible in real experiments.
- To simulate a variety of IP networks.

NS is an object-oriented, discrete event driven network simulator that simulates a variety of IP networks, written in C++ and OTcl . It is primarily useful for simulating local and wide area networks. It implements network protocols such as TCP and UDP, traffic behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBR, routing algorithms such as Dijkstra, and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. NS develops tools for simulation results display, analysis and converters that convert network topologies to NS formats. And the architecture of NS-2 is represented in figure 4.1

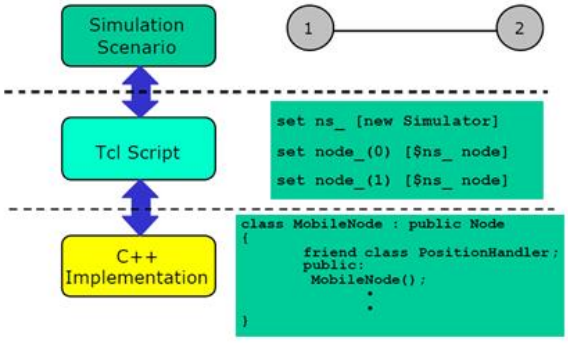



Figure 4.1 Architecture of NS-2

After the coding part, compiled tcl scripts are simulated and viewed using Nam. Nam is Network Animator tool that shows animated output of the script written. And the figure 4.2 will have NAM output.

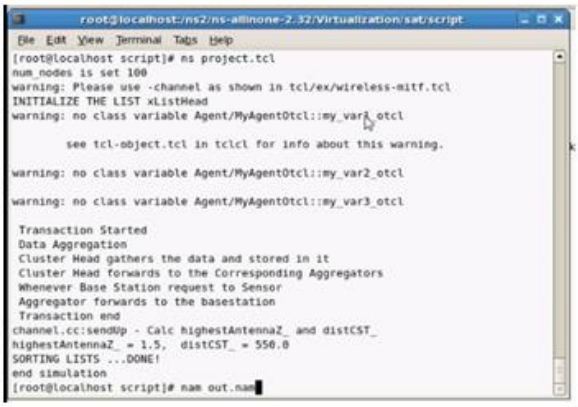



Figure 4.2 (a) Calling NAM

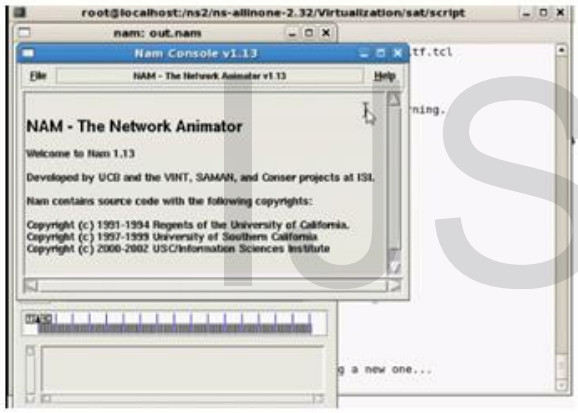



Figure 4.2 (b) Opening of NAM

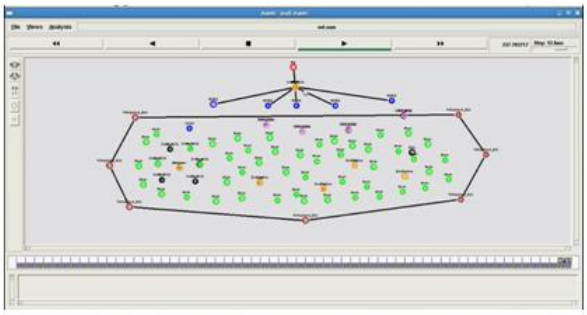


Figure 4.2 (c) NAM final output screen.

And for obtaining the results in a statically data by using Xgraph represented in Figure 4.3 and ploting and tracing can be done in Xgrpahs

### b. Installation of NS-2

NS-2 can be installed in both Linux and Windows platform, but NS-2 is suitable for Linux. Because installation in Windows does not produce the expected results. So we chose Linux platform for the installation. And installation of NS-2 Requires some packages since its combined with simulation for network terms like protocols, packets and also associated with animation. The packages are given below,

- **Automake**
- **Make**
- **Patch**
- **Perl**
- **X86 libraries**
- **Window Maker**
- **All GCC components**
- **Nano Text editor** (Optional… If you are not used to VI or other UNIX editors)
- **Xgraph** (optional, but needed for test suites)

## RESULT & DISCUSSION

The above tool requires Linux based operating system, so in our project we used Virtualization in operating System using Virtual Machine. Virtual Machine is software that helps to run a various platforms in one single system. It allocated memory for working of host operating system. Here, guest operating system used is Cent OS.

Cent OS is an open source operating system that can be used in Virtual Machines and VMware is a Virtual Machine that we used for our project. Steps for using VMware and working of Cent OS are given below:

- Open and Run VMware.
- Download the ISO file of Cent OS.
- In VMware choose option called Existing file and open the ISO file of Cent OS where its downloaded.
- Allocate the memory size for Guest OS and power on the machine.

The results are obtained from Xgraph that has the bandwidth usage for resource allocation and packet delivery ratio for better isolation. The results are

compared with traditional routing and resource allocation technique with our technique, and results are mentioned below, but here we used general wireless network implemented with virtualization, isolation and resource allocation technique

For virtualization in wireless network, the result has obtained from MNO and DSR. MNO has the result of usual wireless network and DSR has virtualized network result.

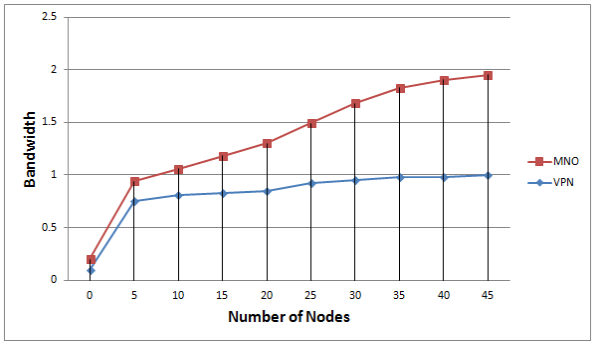



Figure 5.1 Efficient Bandwidth usages

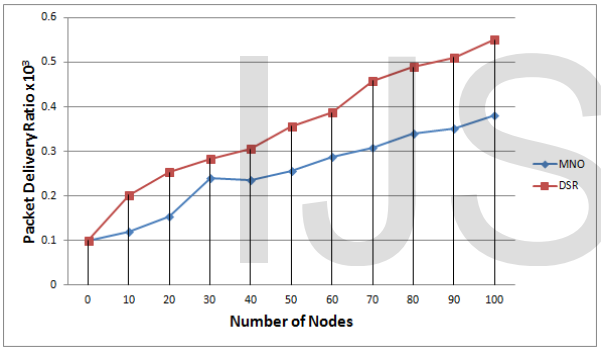



Figure 5.2 Better packet delivery ratio of DSR

e

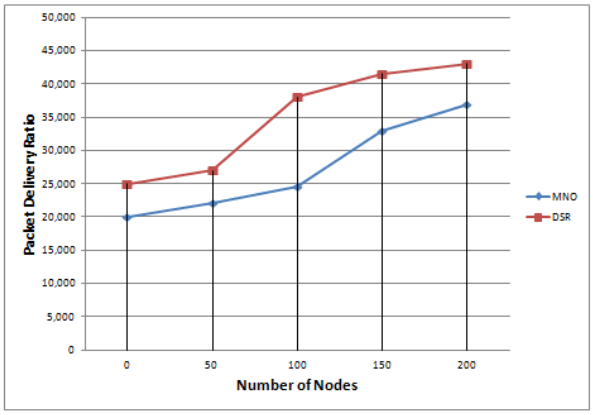



Figure 4.3 Energy & Life time performance

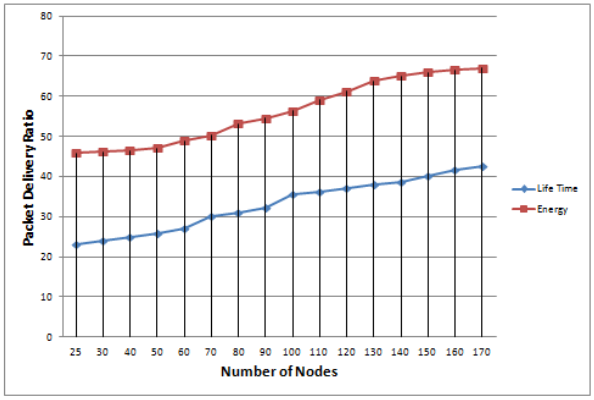



Figure 4.4 Overall Performance

And obtained results are compared with the papers that we have mentioned in Literature Survey. It yields a better result in bandwidth and packet delivery ratio.

## CONCLUSION

So far, our project has a better output than the surveyed paper and the above papers deals with wireless sensor network and as well as wireless networks. The simulation of the WSN done in our project is completely based on WSN not wireless network so there might be some issues, when the above methodologies implemented in general wireless networks, but the methodologies that we used will surely yield a good result in WSN. Virtualization plays a important role in this project which is the only thing derived from wireless networks and existing concepts are suitable for WSN in some scenarios which not includes virtualization of WSN, but this proposed concept will work for virtualization. Future work of this project is to make the mentioned concepts work under all kind of situations.

## REFERENCE

[1] Michal Michalik, (2013) , Base station for Wireless sensor network, Diploma thesis, Brno.

[2] Miguel Angel Erazo Villegas, Seok Yee Tang, Yi Qian (2010) Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring.

[3] Springer International Publishing Switzerland 2014, J. Cecílio, P. Furtado, *Wireless Sensors in Heterogeneous Networked Systems*,Computer Communications and Networks.

[4] Wireless Network Virtualization: A Survey,Some Research Issues and Challenges, Chengchao Liang and F. Richard Yu, Senior Member, IEEE, IEEE COMMUNICATION SURVEYS & TUTORIALS, 2015.

[5] Wireless Network Virtualization,(2013), Xin Wang, Prashant Krishnamurthy, and David Tipper, Graduate Telecommunications and Networking Program, University of Pittsburgh, Pittsburgh, USA.

[6] A Survey of Network Virtualization, (2008), N.M. Mosharaf Kabir Chowdhury and Raouf Boutaba David R. Cheriton School of Computer Science, University of Waterloo.

[7] Design and Simulation of Wireless Sensor Network in NS2, Genita Gautam, Biswaraj Sen, *International Journal of Computer Applications, March 2015*.

[8] Market-Based Resource Allocation for Distributed Data Processing in Wireless Sensor Networks, (2013),Andrew T. Zimmerman and Jerome p. Lynch, University of Michigan Frank T. Ferrese, Naval Surface Warfare Center.

[9] Scheduling And Resource Allocation In WirelessSensor Networks, (2014), Yosef Alayev, *Graduate Center, City University of New York.*

[10] Resource Allocation and Emergent Coordination in Wireless Sensor Networks,(2013), Bhaskar Krishnamachari, Kristina Lerman, Aram Galstyan, University of Southern California.

[11] A.Suresh (2014), "Privilege based Attribute Encryption System for Secure and Reliable Data Sharing", International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), ISSN(Online):2320-9801, ISSN(Print): 2320- 9798, *Vol. 2, No.5, May 2014*, pp. 4099 – 4102.