

# **A HYBRID TECHNIQUE FOR DEFENSE AGAINST BASE STATION JAMMING IN WSN**

**A DISSERTATION**

*Submitted in partial fulfillment of the  
requirements for the award of the degree*

*of*

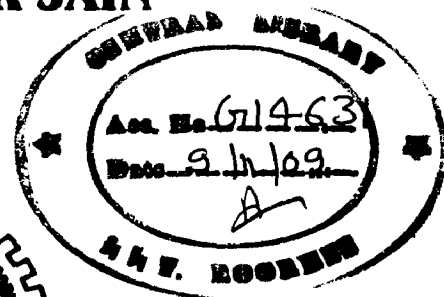
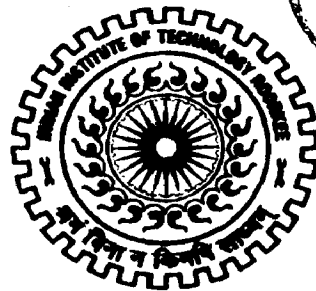
**MASTER OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE AND ENGINEERING**

**By**

**SUSHIL KUMAR JAIN**



**DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING  
INDIAN INSTITUTE OF TECHNOLOGY ROORKEE  
ROORKEE -247 667 (INDIA)**

**JUNE, 2009**

*12*

## **CANDIDATE'S DECLARATION**

---

I hereby declare that the work which is being presented in this dissertation titled, "**A HYBRID TECHNIQUE FOR DEFENSE AGAINST BASE STATION JAMMING IN WSN**" in partial fulfillment of the requirement for the award of the degree of **Master of Technology** with specialization in **Computer Science and Engineering**, submitted in the Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee, is an authentic record of my own original work carried out under the guidance and supervision of **Dr. Kumkum Garg**, Professor, Department of Electronics and Computer Engineering, Indian Institute of Technology, Roorkee.

I also declare that matter embodied in this project report has not been submitted for award of any other degree.

Roorkee

Date: 22.06.09

  
(Sushil Kumar Jain)


---

## **CERTIFICATE**

This is to certify that the above statement made by the candidate is correct to the best of my knowledge and belief.

Date: 22.06.09

Place: Roorkee

  
**Dr. Kumkum Garg**  
Professor, E&CE Department,  
IIT Roorkee,  
Roorkee-247667 (India).

# Acknowledgement

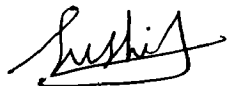
---

I would like to extend my heartfelt gratitude to my guide Dr. Kumkum Garg, Professor, IIT Roorkee, for her able guidance, regular source of encouragement and assistance throughout this dissertation work. It is her vision and insight that inspired me to carry out my dissertation in the field of Wireless Sensor Network. I would state that the dissertation work would not have been in the present shape without her guidance and I consider myself fortunate to have done my dissertation under her.

I also extend my sincere thanks to Dr. S. N. Sinha, Professor and Head of the Department of Electronics and Computer Engineering, IIT Roorkee for providing facilities for the work.

I am also grateful to Raj Khati, staff of Network Security Laboratory of Department of Electronics & Computer Engineering for his sincere co-operation.

Finally, I would like to say that I am indebted to my parents for everything that they have done for me. All of this would have been impossible without their constant support.



Sushil Kumar Jain

# Abstract

---

In Wireless Sensor Networks (WSNs), a large number of distributed sensors collaborate to deliver information to the Base Stations (BSs). As WSNs gain popularity, providing security and trustworthiness is an issue of critical importance. A Denial of Service (DoS) attack is characterized by an explicit attempt to prevent the legitimate use of a service. Jamming is one form of DoS attack, which prevents sources from communicating. WSNs are highly susceptible to jamming attacks due to high possibility of sensor capture and compromise, and their resource limitations. In WSN architecture, BS is a single point of failure, because it collects sensor readings and performs command and control tasks. So BSs are main targets of the jamming attack.

For mitigating the effects of BS jamming attacks, we propose a hybrid technique of defense, which combines 3 defense techniques. The first technique is BS replication, so that in a jamming condition, there may be some unjammed replicated BSs for providing service to the network. The second technique is the evasion of BS from jammed location to any unjammed location. The third technique is multipath routing to provide alternative paths for communication with the BS in case of jamming of one or more paths.

We have performed a simulative evaluation of our proposed technique to compare it with the scenarios of WSNs with no defense technique, single defense technique of BS replication and combination of two defense techniques of BS replication with evasion. A comparison of these techniques has been done with respect to legitimate traffic analysis, jamming traffic analysis and relative power consumption in WSNs. Results show that the proposed hybrid technique gives better results for all the above metrics.

In order to simulate the proposed technique, we used a discrete event simulator called QualNet 4.5. The code for simulating multipath routing protocol is written in C++. The simulation runs under the Windows platform on a Pentium Core 2 duo machine.

# TABLE OF CONTENTS

---

<b>CANDIDATE'S DECLARATION .....</b>	<b>i</b>
<b>ACKNOWLEDGEMENT.....</b>	<b>ii</b>
<b>ABSTRACT.....</b>	<b>iii</b>
<b>TABLE OF CONTENTS.....</b>	<b>iv</b>
<b>CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
1.1 Introduction .....	1
1.2 Statement of the problem .....	2
1.3 Motivation.....	2
1.4 Organization of the Thesis.....	3
<b>CHAPTER 2: INTRODUCTION TO WIRELESS SENSOR NETWORKS.....</b>	<b>5</b>
2.1 Advantages of Wireless Sensor Networks.....	6
2.2 Applications of Wireless Sensor Networks.....	7
2.3 Challenges in Wireless Sensor Networks.....	9
2.4 Sensor Node Architecture.....	11
2.5 Communication in Wireless Sensor Networks.....	13
2.6 Security Requirement in Wireless Sensor Networks.....	14
2.7 Routing Protocols.....	16
2.7.1 Introduction to DYMO Multipath Routing Protocol.....	17
<b>CHAPTER 3: JAMMING ATTACK IN WIRELESS SENSOR NETWORKS.....</b>	<b>19</b>
3.1 Introduction.....	19
3.2 Existing Techniques for defense against BS Jamming.....	20
3.3 Research Gaps Identified.....	22
<b>CHAPTER 4: HYBRID TECHNIQUE FOR DEFENSE.....</b>	<b>23</b>
4.1 Introduction.....	23

4.2	Assumptions.....	23
4.3	Defense Techniques used in the Hybrid Technique.....	24
4.3.1	BS Replication.....	24
4.3.2	BS Evasion.....	25
4.3.3	Multipath Routing.....	26
<b>CHAPTER 5: SYSTEM DESIGN AND IMPLEMENTATION.....</b>		<b>27</b>
5.1	QualNet Overview.....	27
5.2	System Design.....	31
5.2.1	System Components.....	31
5.2.2	Simulation Model.....	32
5.3	Implementation.....	32
5.3.1	Simulation Parameters.....	32
5.3.2	Simulation Scenarios.....	32
5.3.3	Performance Evaluation Metrics.....	34
5.3.4	Performance Evaluation.....	34
<b>CHAPTER 6: CONCLUSION.....</b>		<b>39</b>
6.1	Analysis of Results.....	39
6.2	Suggestions for Future Work.....	39
6.3	Contribution of the Work.....	40

## REFERENCES

## APPENDIX

### Simulation Screen Shots

# CHAPTER 1

## INTRODUCTION

---

### 1.1 Introduction

In recent years, advances in wireless communication and miniaturization have made a new technological vision possible: Wireless Sensor Networks (WSNs). Recent advances in wireless communications and Micro-Electro-Mechanical Systems (MEMS) have motivated the development of extremely small and low cost sensors [1]. They have the capability to sense some environmental attributes around them and transform them into an electric signal to reveal some properties about objects and/or events. Data sensed by these sensors is sent hop by hop to the sink node (i.e. Base Station) for processing, using low power transceivers. These sensors can be deployed at a cost much lower than traditional wired sensor systems. The development of WSNs was originally motivated by military applications such as battlefield monitoring [2]. However, wireless sensor networks are now used in many industrial and civilian application areas, including machine health monitoring, environment and habitat monitoring [3], indoor sensor networks with sensor enabled user interfaces [4], home automation and traffic control.

In WSN, sensor nodes have limited resources such as energy, computation power and storage. As the applications of WSNs increase, providing security and trustworthiness has become important. The broadcast nature of communication in WSN significantly increases the capability of an adversary to initiate Denial of Service (DoS) attacks. Jamming attacks are representative of energy consumption DoS attacks in WSN. Jamming is a well known DoS attack, which interferes with the radio frequencies used by sensor nodes for communication. In a WSN, the Base Station (BS) aggregates sensor readings and conducts command and control tasks. So it is a central point of failure and an attractive target for jamming attack, because its failure can render the whole WSN out-of-service [5].

We propose a hybrid technique of defense for mitigating BS jamming in WSNs. The hybrid technique is a combination of three existing defense techniques: BS replication, BS evasion from jammed location to any unjammed location and multipath routing. In this work, we enhance DYMO (Dynamic MANET On-demand) routing protocol [9] to support multiple path data delivery.

## **1.2 Statement of the Problem**

The aim of this dissertation is to propose a new hybrid technique for defense against BS jamming in wireless sensor networks, which increases Legitimate Traffic Throughput, decreases Jamming Traffic Throughput and increases Power Consumption Ratio.

## **1.3 Motivation**

Wireless sensor networks are often used in mission critical environments such as in military and healthcare applications. These environments have demanding security requirements that must be addressed at the initial phase of design in an attempt to focus on a spherical security strategy that will cover as many security problems as possible. The loss of confidentiality and integrity and the threat of DoS attacks are risks typically associated with wireless communications due to the nature of wireless networks where data is freely available in air.

A jamming attack is representative of an energy consumption DoS attack, which interferes with the radio frequencies used by sensor nodes for communication. Base Station (BS) is an attractive target for a jamming attack, because its failure can render the whole WSN out-of-service. Due to the importance of a BS in WSNs, defense against BS jamming is an issue of critical importance.

A number of defenses have been proposed to mitigate BS jamming in WSNs. In [6], a jamming attack can be evaded by moving to an unjammed location. BS replication with





secure multi-path routing has been proposed in [7]. The strategy of multiple destination BSs is analyzed to provide tolerance against individual BS attacks. For example, if an adversary discovers the location of a BS, it can isolate it from the rest of the network by simply jamming the communication medium in its neighborhood. This drawback can be reduced by accommodating multiple BSs that cooperate with one another to build a robust wireless sensor network. In [5], *Honeybees*, an energy-aware defense framework against BS jamming attack in WSNs is proposed. This framework combines BS replication and evasion techniques to mitigate the effect of jamming attacks.

We intend to use a combination of the above techniques to solve the problem of DoS of the BS during a jamming attack.

## **1.4 Organization of the Thesis**

This report comprises of six chapters including this chapter that introduces the topic and states the problem. The rest of the dissertation report is organized as follows.

Chapter 2 gives an introduction to wireless sensor network. It gives an overview of the advantages, applications, challenges, communication and security requirements in wireless sensor networks. It also gives introduction about different routing protocols in wireless sensor networks and DYMO multipath routing protocol.

Chapter 3 gives an overview of the jamming attack in wireless sensor networks, and also explains about existing techniques for defense against BS jamming and research gaps identified in some of these techniques.

Chapter 4 gives a detailed description of different defense techniques used in hybrid technique for defense against BS jamming in Wireless Sensor Networks. It gives a complete picture of the solution proposed.

Chapter 5 describes about system design and implementation details. It includes QualNet overview. System design details consist of system components and simulation model. The implementation details are also charted out in terms of the scenarios and parameters used. This chapter also evaluates the performance of the proposed hybrid technique on the basis of some performance metrics.

Chapter 6 concludes the work by giving an analysis of results and presents directions for future work. It also gives the contributions of the present work.

## CHAPTER 2

# INTRODUCTION TO WIRELESS SENSOR NETWORKS

---

A Wireless Sensor Network (WSN) consists of hundreds or thousands of low cost nodes which either have a fixed location or are randomly deployed to monitor the environment. Sensors usually communicate with each other using a multi hop approach. The flow of data ends at special nodes called Base Stations (sometimes referred to as sinks). A BS links the sensor network to another network (like a gateway) to disseminate the data sensed for further processing. BSs have enhanced capabilities over simple sensor nodes since they must do complex data processing; they have workstation/laptop class processors and enough memory, energy, storage and computational power to perform their tasks well. WSNs are known for their flexibility, cost effectiveness and ease in deployment; as a result they are being widely used for various monitoring systems, data collection and process control applications, etc [10].

Wireless Sensor Networks have the following characteristics [11, 12]:

1. *Self organizing capability*: WSNs are self organized, because the ad-hoc deployment of nodes requires the system to form connections and cope with the resultant nodal distribution.
2. *Short range broadcast communication and multihop routing*: The bandwidth of the wireless links connecting sensor nodes is often limited, hence constraining inter-sensor communication. Moreover, limitations on energy forces sensor nodes to have short transmission ranges. Therefore, it is likely that a path from a source to a destination consists of multiple wireless hops.
3. *Frequent change in topology due to node failures*: A highly dynamic topology is a distinguishing feature and challenge of a mobile WSN. Links between nodes fail due to movement within the network. This node mobility affects not only the source and/or destination, as in a conventional wireless network, but also intermediate nodes, due to the network's multihop nature. The resulting routes

- can be extremely volatile, making successful routing dependent on efficiently reacting to these topology changes.
4. *Dense deployment of nodes*: Technological advances in Micro-Electro-Mechanical Systems (MEMS) are envisaged to allow the dense deployment of nodes with sensing, communication and processing capabilities in large areas for monitoring purposes.
  5. *Broadcast communication paradigm*: Broadcast communication paradigm is prevalent used to facilitate data acquisition in WSNs.
  6. *Several orders of magnitude of nodes*: The number of sensor nodes can be several orders of magnitude higher than the nodes in an ad-hoc network.
  7. *Limited power, computational capability and memory*: In a WSN, nodes have limited power, computational capability and memory.
  8. *No global identification*: Sensor nodes may not have global identification because of the large amount of overhead and large number of sensors.
  9. *Location awareness*: It is an important issue, since most data collection is based on location; it is desirable that the nodes know their position whenever needed.

## 2.1 Advantages of Wireless Sensor Networks [12, 13]

- *Ease of Deployment*: Wireless sensors can be deployed (dropped from plane or placed in a factory) at the site of interest without any prior organization, thus reducing the installation cost and time and also increasing the flexibility of deployment. They are able to discover their locations and organize themselves as a wireless network.
- *Extended Range*: A network of smaller sensors can distribute over a wider range within an affordable cost range.
- *Fault Tolerant*: Failure of one node in a wireless sensor network does not affect network operation because other adjacent nodes are collecting similar data. At most the accuracy of data collected may be somewhat reduced.

- *Uniform Coverage:* mobile sensors can re-spread in an area to ensure uniform coverage, move closer to loaded nodes in order to prevent bottlenecks or increase bandwidth by carrying data to the base-station.

## 2.2 Applications of Wireless Sensor Networks [13]

There are many applications of WSNs in various fields. Some of the common applications are as follows:

### 1. General Engineering

- *Automotive telematics:* Cars, which comprise a network of dozens of sensors and actuators, are networked into a system of systems to improve the safety and efficiency of traffic.
- *Fingertrip accelerometer virtual keyboards:* These devices may replace the conventional input devices for PCs and musical instruments.
- *Sensing and maintenance in industrial plants:* Complex industrial robots equipped with many sensor nodes and connected to the main computer through wireless link, because a robot's movement may be subject to wear and tear of wired links.
- *Social studies:* Equipping human beings with sensor nodes permits interesting studies of human interaction and social behavior.
- *Tracking of goods in retail stores:* Tagging facilitates store and warehouse management.
- *Tracking of container and boxes:* Shipping companies are assisted in keeping track of their goods, atleast until they move out of range of other goods.

### 2. Agriculture and Environmental Monitoring

- *Precision agriculture:* Crop and livestock management and precise control of fertilizer concentrations are possible.

- *Geophysical monitoring:* Seismic activity can be detected at a much finer scale using a network of sensors equipped with accelerometers.
- *Planetary exploration:* Exploration and surveillance in inhospitable environments such as remote geographic regions or toxic locations can take place.
- *Habitat monitoring:* Used to measure humidity, pressure, temperature, infrared radiation, total solar radiation, photo synthetically active radiation etc.
- *Contaminant transport:* The assessment of exposure levels requires high spatial and temporal sampling rates, which can be provided by wireless sensor networks.
- *Disaster detection:* Forest fire and floods can be detected early and causes can be localized precisely by densely deployed sensor networks.

### 3. Civil Engineering

- *Monitoring of structures:* Sensor nodes can be placed in bridges to detect and warn of structural weakness and in water reservoirs to spot hazardous materials. The reaction of tall buildings to wind and earthquakes can be studied and material fatigue can be monitored closely.
- *Urban planning:* Urban planners can track groundwater patterns and how much carbon dioxide cities are expelling, enabling them to make better land use decisions.
- *Disaster recovery:* Buildings razed by an earthquake may be infiltrated with sensor robots to locate signs of life.

### 4. Military Applications

- *Asset monitoring and management:* Commanders can monitor the status and locations of troops, weapons and supplies to improve military commands, control, communications and computing.

- *Surveillance and battle space monitoring:* Vibration and magnetic sensor nodes can report vehicle and personnel movement, permitting close surveillance of opposing forces.
- *Protection:* Sensitive objects such as atomic plants, bridges, retaining walls, oil and gas pipelines, communication towers, ammunition depots and military headquarters can be protected by intelligent sensor fields able to discriminate between different classes of intruders. Biological and chemical attacks can be detected early or even prevented by a sensor network acting as a warning system.

#### 5. Health Monitoring and Surgery

- *Medical sensing:* Physiological data such as body temperature, blood pressure and pulse are sensed and automatically transmitted to a computer or physician, where it can be used for health status monitoring and medical exploration. Wireless sensing bandages may warn of infection. Tiny sensor nodes in the blood stream, possibly powered by a weak external electromagnetic field, can continuously analyze the blood and prevent coagulation and thrombosis.
- *Micro-surgery:* A swarm of MEMS based robots may collaborate to perform microscopic and minimally invasive surgery.

### 2.3 Challenges in Wireless Sensor Networks [12, 13]

Some of the major challenges in WSNs are listed as follows:

- *Ad-hoc deployment:* Sensor nodes are randomly deployed, which requires that the system be able to cope up with the resultant distribution and form connections between the nodes.
- *Computational capabilities:* Sensor nodes have limited computing power and therefore may not be able to run sophisticated network protocols leading to light-weight and simple versions of routing protocols.



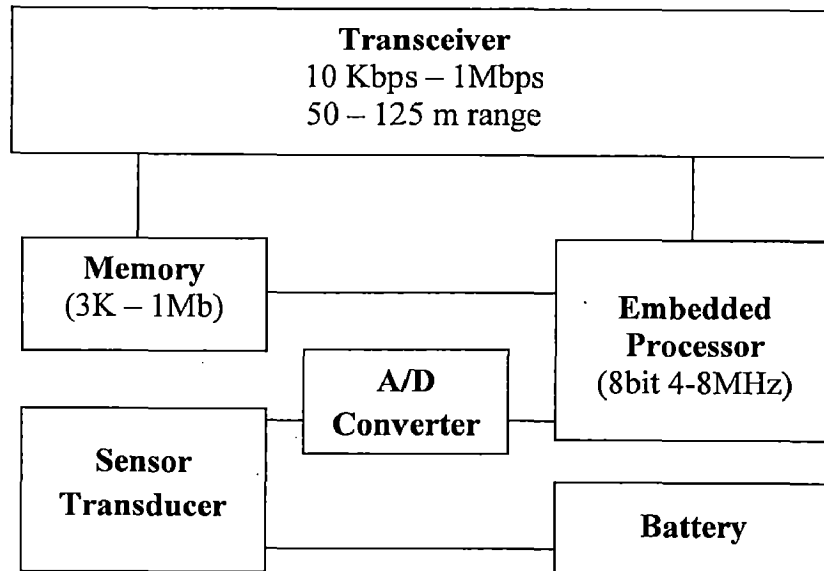
- *Energy consumption without losing accuracy:* Sensor nodes can use their limited energy supply carrying out computations and transmitting information. As such, energy conserving forms of communication and computation are crucial as the node lifetime shows a strong dependence on the battery lifetime.
- *Scalability:* The number of sensor nodes deployed in a sensing area may be of the order of hundreds, thousands, or more. Any routing scheme must be scalable enough to respond to events and capable of operating with such large number of sensor nodes. Most sensor nodes can remain in the sleep state until an event occurs, with data from only a few remaining sensor nodes providing a coarse quality.
- *Communication range:* The bandwidth of the wireless links connecting sensor nodes is often limited, thus constraining inter-sensor communication. Moreover, limitations on energy forces sensor nodes to have short transmission ranges. Therefore, it is likely that a path from a source to a destination consists of multiple wireless hops.
- *Transmission media:* In a wireless sensor network, nodes communicate through wireless links. Therefore, the traditional problems associated with a wireless channel (e.g. fading, higher error rate) also affect the operation of the sensor network. In general, bandwidth requirements of sensor applications will be low, in the order of 1-100 kbps.
- *Quality of Service (QoS):* In some applications (e.g. some military applications), data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore, bounded latency for data delivery is another condition for time constrained applications.
- *Control overhead:* When the number of retransmissions in a wireless medium increase due to collisions, latency and energy consumption also increases. Hence, control packet overhead increases linearly with the node density. As a result, tradeoffs between energy conservation, self-configuration and latency may exist.
- *Security:* This is an important issue which does not mean physical security, but implies that both authentication and encryption should be feasible. But, with

limited resources, implementation of any complex algorithm needs to be avoided. Thus, a tradeoff exists between the security level and energy consumption in a wireless sensor networks.

- *Application Specific:* WSNs are application specific, i.e. design requirements of a sensor network change with application. For example, the challenging problem of low-latency precision tactical surveillance is different from that required for a periodic weather monitoring task.
- *Data redundancy:* Data collected by many nearby sensor nodes is based on common phenomena, thus there is a high probability that the data has redundancy. Therefore, data aggregation and in-network processing are desirable to yield energy efficient data delivery before being sent to destinations.
- *Hardware constraints:* They should adapt to the environment of sensor networks and function correctly.
- *Distributed signal processing.* Most tasks require the combined effort of multiple network nodes, which requires protocols that provide coordination, efficient local exchange of information, and possibly, hierarchical operation.
- *Synchronization and localization.* The notion of time is critical. Coordinated sensing and actuating in the physical world require a sense of global time that must be paired with relative or absolute knowledge of nodes' locations.
- *Wireless reprogramming.* A deployed WSN may need to be reprogrammed or updated. So far, no networking protocols are available to carry out such a task reliably in a multihop network. The main difficulty is the acknowledgment of packets in such a joint multihop/multicast communication.

## 2.4 Sensor Node Architecture [12]

A wireless sensor node is composed basically of a power supply, computational module (processor and memory), transceiver and sensor unit as shown in Figure 2.1.



**Figure 2.1: Functional Block Diagram of a typical Sensor Node**

- *Power Supply:* The most widely used power supply in sensor nodes is the battery. The choice of the battery type is important since it can affect the lifetime of the sensor node.
- *Memory and Processor:* These form the computational module of the sensor node. They permit a sensor node to process local data. In the case of the processor, low power is a quality of a device that consumes low energy per clock. For example, the ATmega128L@4MHz processor consumes 16.5mW and its efficiency is 242MIPS/W, spending 4nJ/instruction.
- *Transceiver:* The transceiver connects the node to the network. The main types of transceivers are: radio frequency (RF), infrared and optical. An example of transceiver radio frequency is the TR1000 which has 916 MHz or 433MHz of frequency, with transmission rate of 50 Kbps and ranges from 30 to 90 meters. An optical transceiver using a laser module and a Corner Cube Reflector (CCR),

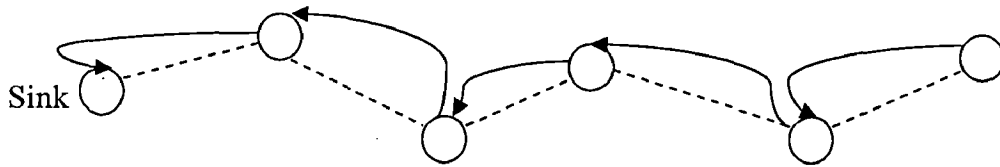
which has  $0.5 \times 0.5 \times 0.1 \text{ mm}^3$ , can transmit at a rate of the 10Kbps consuming  $1\mu$  Watt to 1 Km of range.

- *Sensor Unit*: Sensor unit can be composed of one or a group of sensors which are devices that produce electrical response to a change in physical conditions. Sensing devices have different design, manufacturing, modeling and signal processing. Thus many basic sensor transducers can convert many physical quantities such as pressure, light, humidity, luminosity, acceleration, mechanical stress, audio, video, temperature, angular rate, force, acoustic, ultrasonic, optoelectronic/photonic, ionizing radiation, viscosity, proximity, pH, gas, radiative, altitude, chemical, biological, microbalance, medical and so on into electrical signals. These generic transducers need to be interfaced and connected to other devices and such a custom made unit can be used for a specific application.
- *Software*: It is used to represent a set of programs and procedures, which becomes an autonomous system capable of performing the information processing, relaying or routing and management tasks. As previously seen, sensor nodes have strong hardware and software restrictions in terms of processing power, memory capacity, battery lifetime and communication throughput. These are typical characteristics of mobile and wireless devices and not of wired network elements. Thus, software designed for sensor nodes must consider those limitations, whereas an element for a wired network may have other restrictions such as performance and response time.

## **2.5 Communication in Wireless Sensor Networks [12, 14]**

In WSNs, nodes communicate using RF, so broadcast is the fundamental communication primitive. Various sensor nodes communicate with each other to collect the desired information and data, which is passed to the sink or data collection center. Sensor nodes

constitute a multi-hop network. Sensor nodes begin to establish routes by which information is passed to one or more sink nodes. The limited available energy and small form of the sensor nodes impose a limit on the radio transmission range and suggest small multi-hop transmission schemes as shown in Figure 2.2.



**Figure 2.2: Multihop Communication**

Communication is the major energy consumer in wireless networks, especially data transmission. The transmission power required for communication between nodes is dependent on distance. In the sensor applications developed so far, communication patterns within the network fall into the following categories:

- Node to base station communication, e.g. sensor readings, specific alerts.
- Base station to node communication, e.g. specific requests, key updating.
- Base stations to all nodes communication, e.g. routing beacons, queries or reprogramming of the entire network.

## 2.6 Security Requirements in Wireless Sensor Networks

Sensor networks are used in a number of domains that handle sensitive information. However it is obvious that due to the nature of wireless networks, data is freely available in air. The loss of confidentiality and integrity and the threat of DoS attacks are risks typically associated with wireless communications. Unauthorized users may gain access to agency systems and information, corrupt the agency's data, consume network bandwidth, degrade network performance and launch attacks that prevent authorized users from accessing the network, or use agency resources to launch attacks on other networks. There are many security challenges in WSN [15, 16]. Some of these are:

Confidentiality, Authentication, Freshness, Availability and Integrity etc. A brief description of these security challenges is given below.

- *Confidentiality:* Confidentiality is needed to ensure that sensitive information is well protected. The confidentiality objective is required in a sensor's environment to protect information traveling between sensor nodes of the network, since an attacker having the appropriate equipment may eavesdrop on the communication.
- *Authentication:* As in conventional systems, authentication techniques verify the identity of the participant in a communication. In the case of wireless sensor networks, it is essential for each sensor node and BS to have the ability to verify that the data received was really sent by a trusted sender and not by an attacker.
- *Freshness:* One of the many attacks launched against sensor networks is the message replay attack, where an adversary may capture messages exchanged between nodes and replay them later to cause confusion to the network. The data freshness objective ensures that messages are fresh, meaning that they obey a message ordering and have not been reused.
- *Availability:* Availability ensures that services and information can be accessed at the time when they are required. In sensor networks, there are many risks that could result in loss of availability, such as sensor node capturing and DoS attacks. Lack of availability may affect the operation of many critical real time applications like those in the healthcare sector that require a 24 × 7 operation that could even result in loss of life. Therefore, it is critical to ensure resilience to attacks targeting the availability of the system and find ways to fill in the gap created by the capturing, jamming or disablement of a specific node by assigning its duties to some other nodes in the network.
- *Integrity:* Moving on to the integrity objective, there is the danger that information could be altered when exchanged over insecure networks. Lack of integrity could result in many problems since the consequences of using inaccurate information could be disastrous, for example, for the healthcare sector,

where lives are endangered. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way.

## **2.7 Routing Protocols [26, 27]**

Routing in sensor networks is very challenging due to several characteristics that distinguish them from contemporary communication and wireless ad hoc networks. First of all, it is not possible to build a global addressing scheme for the deployment of sheer number of sensor nodes. Therefore, classical IP-based protocols cannot be applied to sensor networks. Second, in contrary to typical communication networks almost all applications of sensor networks require the flow of sensed data from multiple regions (sources) to a particular BS. Third, generated data traffic has significant redundancy in it since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by the routing protocols to improve energy and bandwidth utilization. Fourth, sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage and thus require careful resource management.

Due to such differences, many new algorithms have been proposed for the problem of routing data in sensor networks. These routing mechanisms have considered the characteristics of sensor nodes along with the application and architecture requirements.

Flooding and gossiping are two classical mechanisms to relay data in sensor networks without the need for any routing algorithms and topology maintenance. In flooding, each sensor, receiving a data packet, broadcasts it to all of its neighbors and this process continues until the packet arrives at the destination or the maximum number of hops for the packet is reached. On the other hand, gossiping is a slightly enhanced version of flooding where the receiving node sends the packet to a randomly selected neighbor, which picks another random neighbor to forward the packet to and so on.

SPIN [16] is the first protocol, which considers data negotiation between nodes in order to eliminate redundant data and save energy. The idea behind SPIN is to name the data using high-level descriptors or meta-data. Before transmission, metadata are exchanged among sensors via a data advertisement mechanism, which is the key feature of SPIN. Each node upon receiving new data, advertises it to its neighbors and interested neighbors, i.e. those who do not have the data, retrieve the data by sending a request message. SPIN's meta-data negotiation solves the classic problems of flooding such as redundant information passing, overlapping of sensing areas and resource blindness, thus achieving a lot of energy efficiency.

Minimum cost forwarding protocol aims at finding the minimum cost path in a large sensor network, which will also be simple and scalable. The protocol is not really flow-based; however since data flows over the minimum cost path and the resources on the nodes are updated after each flow. The cost function for the protocol captures the effect of delay, throughput and energy consumption from any node to the sink.

On-demand routing algorithms developed for MANET, such as AODV [23] could be applied for sensor networks. They might be too heavy to be directly employed, because they are developed inherently for dynamic mobile nodes in MANET. Considering the load balance for conserving the energy of sensor nodes, multipath routing protocols which have the advantage on sharing energy depletion between all sensor nodes have been proposed previously. In this research work, we are using multipath extension of DYMO (Dynamic MANET On-demand) routing protocol, which is based on [22].

### **2.7.1 Introduction to DYMO Multipath Routing Protocol**

Our multipath routing protocol is an extension of DYMO (Dynamic MANET On-demand) routing protocol, which is based on [22]. DYMO [9] is basically an enhancement of the AODV protocol [23]. In the multipath route discovery process, if several Route Replies arrive at the source through different neighbor nodes and different path identifiers, the DYMO agent marks these nodes as next hops in the destination entry of its route table,



which enables extending the path selection algorithm to make traffic dispersion. For traffic dispersion, multiple paths between a source-destination pair will be *link disjoint* routes, so that nodes can be common for two or more paths.

Multipath extension of DYMO routing protocol proposed in [22] introduces the advertised hop count to prevent loops and a header extension (the last hop field) to identify the path. Last hop is the destination neighbour. The path is identified with the pair next-hop/last-hop.

The following are the modifications made by [22] in DYMO routing protocol for extending it to a multipath routing protocol:

1. During the request phase, every intermediate node has to save the path to request the packet's originator in order to send the corresponding reply message to it. Therefore, every intermediate node registers all the paths with different last hops, though they may arrive through the same neighbour (next hop in the path register).
2. During the reply phase, when the destination node receives a Route Request, it sends the reply back through the neighbour node from which it received the packet; the last-hop value is the same as contained in the request packet. The first path used by each intermediate node with this last hop is the valid path and determines its next hop; the node removes the other paths with the same next hop although with a different last hop.
3. After the route discovery process, every node will have one or more routes for every possible destination.

Simulation results of [22] show that by introducing multipath routing, reduction in the throughput of both UDP and TCP connections is under 20%. It shows that multipath extension of the routing protocol decreases the throughput only by a little amount.

In the next chapter, we discuss different jamming attacks possible in WSN.

## CHAPTER 3

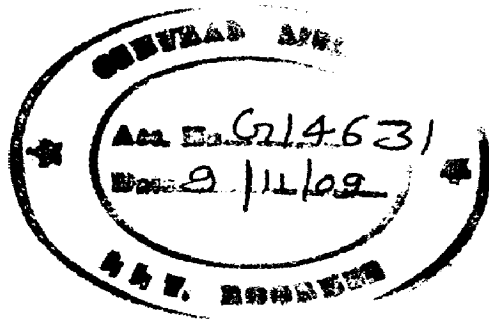
# JAMMING ATTACK IN WIRELESS SENSOR NETWORKS

### 3.1 Introduction

Jamming is the deliberate interference with radio reception to deny the target's use of a communication channel [17]. Jamming attacks are the representative of energy consumption DoS attacks in WSNs [18, 19]. The attacker deploys the jammers randomly to jam the area. Jammers can disturb communication between sensor nodes or launch radio frequencies to interfere with the open wireless environment. Although jammers are randomly deployed, the damage on the monitor systems is still marked. The loss of some crucial messages may destroy the entire system.

For single-frequency networks, jamming is simple and effective, rendering the jammed node unable to communicate or coordinate with others in the network. It can be launched in the link layer or the physical layer. Link layer jamming attacks focus on disturbing the communication between sensor nodes around the jammer [17]. Physical layer jamming attacks [11, 18] let radio frequencies interfere with the open wireless environment. Because sensor nodes have only a single channel, the jammer will take control of the channel. As a result, sensor nodes cannot transmit the sensing report to the BS. Therefore, both link layer jamming attacks and physical jamming attacks can be launched easily and are difficult to defend.

In WSNs, BSs act as gateways to the wired world, e.g. a satellite uplink connecting to terrestrial networks. The BS is responsible for aggregating sensor readings and conducting command and control tasks. So it is a central point of failure and is an attractive target for jamming attack, because its failure can render the whole wireless sensor network out-of-service during attacks [5]. Jamming attackers try to isolate the BS from the rest of the network by jamming the communication channel around it, so that it cannot provide service to the network.



### 3.2 Existing Techniques for defense against BS Jamming

A number of defense techniques have been proposed to mitigate BS jamming in WSNs. In [6], two strategies are given for use by wireless devices to evade a MAC/PHY-layer jamming-style wireless DoS attack. The first strategy, *channel surfing*, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. In particular, although changing the frequency of the carrier wave is easy to accomplish in the case of frequency hopping spread spectrum, changing channels at the link-layer is more involved as it requires synchronization between both parties, which necessitates additional time cost.

The second strategy, *spatial retreats*, is a form of spatial evasion whereby legitimate mobile devices move away from the locality of the DoS emitter. The basic idea of spatial retreat is that a mobile device will move to a new access point and reconnect to the network under it. In order to perform a spatial retreat for an infrastructure wireless network, it is assumed that each mobile device has an Emergency Access Point List assigned to it, and that it knows how to move in order to reach its Emergency Access Point. The Emergency Access Point can be assigned to each device by its current Access Point prior to the denial of service.

In [20], a novel and powerful jamming attack called *mobile jamming attack* is presented. A multi-dataflow topologies scheme is proposed in it, that can effectively mitigate the damage caused by the mobile jammer. An advantage of this scheme is that the BS can receive messages from the affected area continuously under the mobile jamming attack. It has the following properties:

1. It is lightweight and simple. Sensor nodes do not take much effort to defend the mobile jamming attack. In other words, each sensor node tries its best to save energy, when it is suffering attack.

2. BS receives report messages from the affected area continuously under the mobile jamming attack.
3. When the mobile jamming attack occurs, the affected sensor nodes do not need to re-route.

In [5], for mitigating BS jamming, replication of BSs as well as jamming evasion, by relocation to unjammed locations, have been proposed. In this paper, *Honeybees*, an energy-aware defense framework against BS jamming attack in WSNs is proposed. The honeybees framework efficiently integrates replication and evasion mechanisms, whereby replicated BSs change their physical locations, either proactively with a predetermined schedule, reactively in response to attack, or in a hybrid proactive-reactive fashion. From the simulation study, it is found that if the jamming attack is low to medium in strength, hybrid honeybees with moderate replication performs better than other strategies. Although hybrid honeybees degrade gracefully with strong attacks, massive replication outperforms other strategies for high number of attackers. We note that the reactive-uncoordinated scheme is robust to node compromise due to independent operation of mobile BSs. However, node compromise is a threat to proactive and coordinated strategies as it can reveal the pseudo-random seed and the schedule.

In [7, 8] strategies for securing the sensor network against a variety of threats that can lead to the failure of the BS are considered. In the first strategy, multipath routing to multiple destination BSs is analyzed as a strategy to provide tolerance against individual BS attacks and/or compromise. It also analyzes the extent to which the number of BSs enhances the resilience of the network. The second approach uses confusion of address and identification fields in packet headers via hashing functions. This approach is designed to disguise the location of the BS and thereby counter threats from a passive observer who would eavesdrop on packet headers, especially the source, destination and type fields, in order to infer and trace back the location of the BS. In the third approach, relocation of the BS in the network topology is studied as a means of enhancing resiliency and mitigating the scope of damage.

In [21], examination of radio interference attacks from both sides of the issue is done: first, the study of the problem of conducting radio interference attacks on wireless networks is done; and second, it examines the critical issue of diagnosing the presence of jamming attacks.

### 3.3 Research Gaps Identified

1. In [6], it is assumed that the adversary cannot pretend to be a valid member of the network. But it is possible that the adversary can be a valid member of the network. Spatial retreats primarily focuses on a simple scenario in which the adversary is assumed stationary, although it can be mobile. We have assumed that adversaries are mobile and they can be valid member of the network.
2. In mobile jamming attack counter measure [20], use of more than one topology will cause more overhead and lower connectivity in WSN. So we have assumed single topology in the network.
3. In honeybees framework [5], the resilience of replication degrades proportionally to the increasing number of attackers, particularly when the number exceeds that of base stations. Also the evasion overhead in terms of energy and time consumed in movement and network reconfiguration can amplify the attack effect because of reactive approach, if it is not controlled carefully.
4. In [7, 8], a technique of *multipath routing* to multiple replicated BSs is proposed as a strategy to provide tolerance against BS jamming attacks. But if the number of multipath increase, the communication cost also proportionally increase. So we have assumed some upper limit on number of paths from nodes to BSs.

## CHAPTER 4

# HYBRID TECHNIQUE FOR DEFENSE

---

### 4.1 Introduction

A jamming attack can be launched in the data-link layer or the physical layer. Link layer jamming attacks disturb the communication between sensor nodes around the jammer. Physical layer jamming attacks let the radio frequency interfere with the open wireless environment. In WSN architecture, BSs are the prime target for jamming attack because of their importance in aggregating sensor readings, and for playing a role in security protocols. We propose a hybrid technique of defense against BS jamming in WSNs. The main aim of the hybrid technique is to mitigate BS jamming in WSNs. The hybrid technique combines three defense techniques: BS replication, evasion of BS from jammed location to any unjammed location and multipath routing. A detailed description about these techniques is given in the following sections.

### 4.2 Assumptions

To facilitate our work, we make following assumptions:

1. All sensor nodes in the network are homogenous.
2. Sensor nodes communicate through wireless links over a single shared channel.
3. Links between two sensor nodes are bidirectional.
4. Transmission power is uniform across the network.
5. An attacker can compromise a sensor node and can obtain all its information.
6. Jammers can move, so that jammed locations can be changed by the mobile jammers.
7. Mobile jammers are uncoordinated and unsynchronized. They follow an off-line schedule to determine when, where and which jammers to move. So it may happen

that successfully jamming attackers have to move, while unsuccessful ones remain still.

8. Jammers continuously emit RF signals to fill the wireless channel, so that legitimate traffic may be blocked. A jammer can do this by either preventing sensor nodes to send sensor readings, or by preventing the reception of legitimate traffic at the BSs.
9. A jammer does not have information about the whole network, and it cannot jam the entire network.
10. Jammers can flood the BS with illegitimate packets, preventing it from receiving legitimate packets from sensor nodes.
11. Attackers cannot be captured.

### **4.3 Defense Techniques used in the Hybrid Technique**

Our proposed hybrid model of defense against BS jamming in WSNs combines following three defense techniques:

#### **4.3.1 BS Replication**

Our first defense technique is BS replication. According to this technique, there should be multiple replicated BS in WSN, so that in case of a jamming attack, if one or more BSs are not jammed, these can serve the whole WSN, and the WSN can continue delivering data for a longer time during attack. When jammed BSs become unjammed, they may request for the sensor readings (during jammed condition) from unjammed BSs, and update themselves.

Figure 4.1 shows a WSN which consists of 5 replicated BSs and 3 mobile jammers. Two jammers successfully jam two replicated BS. So three BSs are not jammed, and these can serve the whole WSN, so that WSN can provide its services for longer time duration.



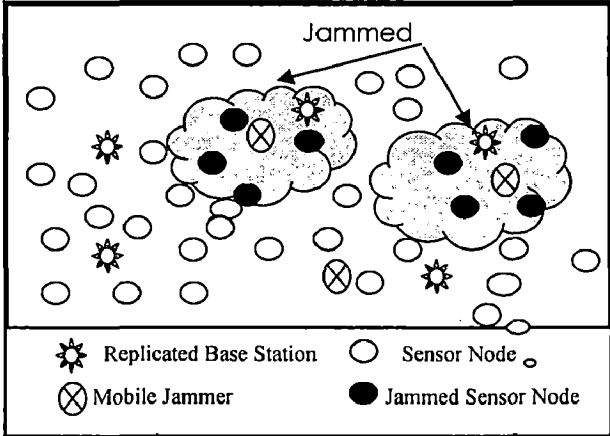


Figure 4.1 Base station replication

4.3.2 BS Evasion

Our second defense technique is BS evasion from jammed location to unjammed location in the network. According to this technique, the BS should be mobile, so that in case of a jamming attack, it can physically move to any unjammed location. In the hybrid model, replicated BSs change their physical locations *pro-actively* with a pre-determined off-line schedule, so that more than one BS cannot collide by reaching the same location at the same time.

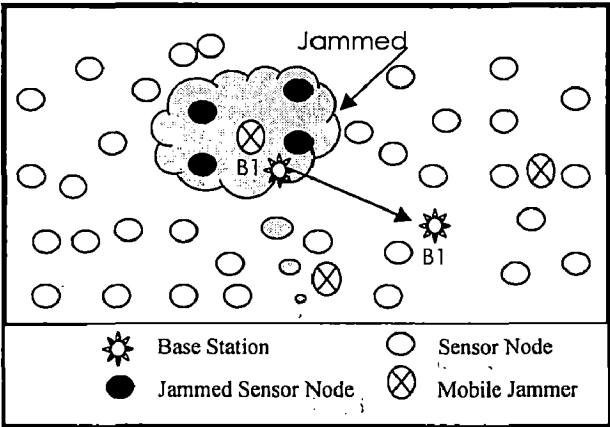


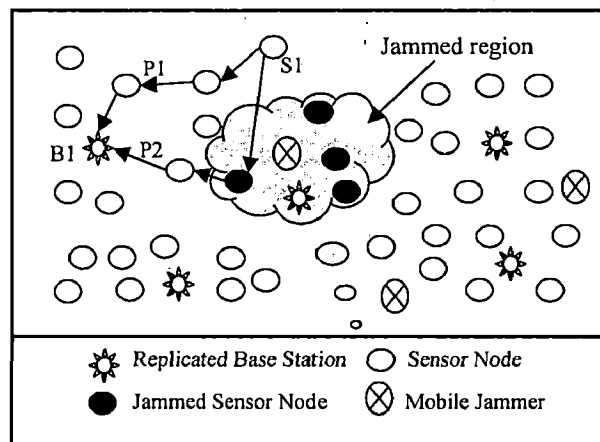
Figure 4.2 Base station evasion

Figure 4.2 shows a WSN consisting of a BS and 3 mobile jammers, one of which successfully jams a BS. Since the BS is mobile, it physically moves from the jammed

location to any unjammed location (shown in the Figure by arrow) and again starts communication with sensor nodes.

### 4.3.3 Multipath Routing

Our third defense technique is multipath routing. According to this technique, there should be multiple paths between sensor nodes and the BS, so that in case of a jamming attack, if atleast one path between the sensor nodes and BS is not jammed, the BS can get sensor readings through this path and the sensor network can continue working. Through multipath routing, traffic dispersion can be used to prevent eavesdropping, to do load balancing or to minimize energy consumption by nodes. Traffic dispersion means that for the same source-destination pair, communication simultaneously uses different paths (i.e. multiple paths) instead of a single one [22].



**Figure 4.3 Multipath routing**

Figure 4.3 shows a WSN consisting of 5 BSs and 3 mobile jammers. One of the mobile jammer successfully jams a BS. There are two paths from sensor node S1 to BS B1 (path P1 and path P2 shown in Figure 4.3). As one sensor node under path P2 is jammed, sensor readings are delivered by path P1. Thus there is no effect of jamming on unjammed BSs for reading the sensor information from unjammed sensor nodes.

## CHAPTER 5

### SYSTEM DESIGN AND IMPLEMENTATION

---

The aim of our simulation is to evaluate the communication performance of the proposed hybrid technique of defense against BS jamming in WSNs. Also, we present a simulation model of the proposed defense technique that provides us results on legitimate traffic throughput, jamming traffic throughput, and power consumption ratio. The simulation has been carried out in a discrete event simulator named QualNet [24].

#### 5.1 QualNet Overview [24]

QualNet is a commercial spin-off from the GloMoSim simulator, which was developed at the University of California, Los Angeles (UCLA) and is distributed by Scalable Network Technologies. The simulator itself is C++ based. All protocols are implemented in a series of C++ files, and called by the simulation kernel. One of the major selling points of QualNet is that it is very scalable. No efficiency is lost in running large simulations of many thousands of nodes with heavy traffic.

Whilst it is possible to run simulations completely from the command line, QualNet comes with a java based graphical user interface. A screenshot of this can be seen in Figure 5.1. This allows for easy, more intuitive setup of simulations as well as easy observation of results. During simulation runtime, it allows the user to observe the signals being transmitted and received at each node, which aids in the understanding of what is physically happening.

The three main programs used in QualNet are the simulator, the analyzer and the packet tracer. The simulator runs the given simulation, the analyzer displays the results and the packet tracer allows us to follow the path of a packet through the network. There is also a protocol developer in the GUI; however, it is much more powerful to develop protocols from C++ coding.

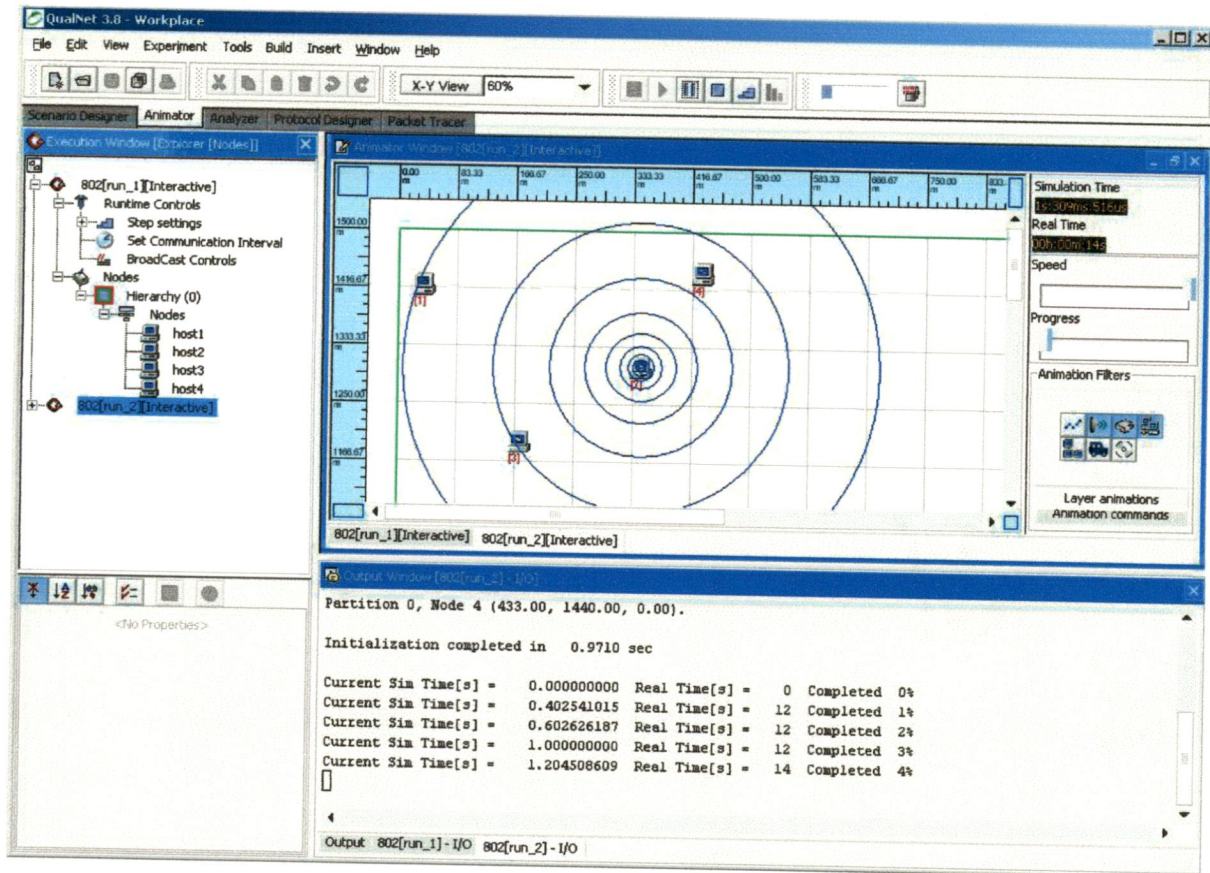
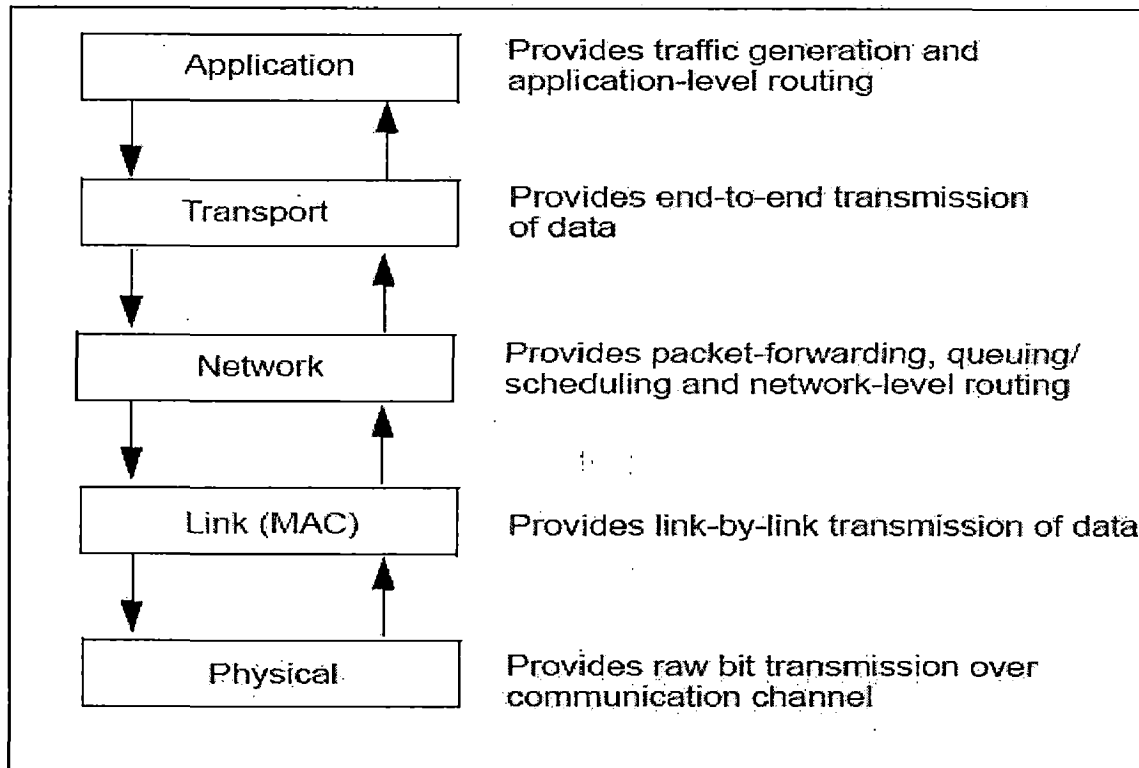


Figure 5.1: QualNet GUI Screenshot

## Operations of QualNet

QualNet bases its operation around the OSI protocol stack. At each layer in the stack, a different protocol can be implemented for a given simulation. The protocol stack used can be seen in Figure 5.2. Because of this modular approach, it makes it very easy to integrate existing protocols with ones we develop ourselves.

For any given simulation, we have a configuration file. This file specifies what protocol is to run at each layer and any parameters such protocols may require. QualNet provides a whole range of existing protocols. For example, at the application layer, models exist for Constant Bit Rate (CBR), File Transfer Protocol (FTP), HTTP and TELNET traffic. It also contains models for TCP and IP at the transport and network layers respectively.



**Figure 5.2: QualNet protocol stack**

A number of routing protocols are also available such as AODV, RIP, OSPF, DYMOM and Bellman-Ford to name but a few. At the MAC layer, there are implementations of the IEEE 802.3 protocol and the IEEE 802.11 (Wi-Fi) protocol.

A major strength of QualNet is the detail with which it models the physical channel. It is because of this that QualNet performs well in wireless scenarios. Detailed models exist for fading, path loss and shadowing. In addition to this, the antennas are very well modeled, providing omnidirectional, steered beam and switched beam antennae. Physical layer protocols exist for IEEE 802.11, IEEE 802.3 and an abstract physical layer. The modular design of QualNet allows combinations of all these protocols to produce a very powerful network simulator.

Whilst each protocol obviously performs different functions, there is a common ground to their operation. Firstly, the protocol undergoes initialization at each node it is to be run

at. Depending on the node, different states may be occupied at initialization. For example, a node running IEEE 802.16 as its MAC layer will have different states depending on whether it is a Base Station or a Subscriber Station.

After this step, the two other functions of importance are the event dispatcher and the event handler. The event dispatcher is responsible for starting any events such as sending packets or starting timers etc. The event handler is responsible for reacting to certain events. An event may constitute receipt of a packet, or a change of state. Whilst it is difficult to appreciate how a protocol may work at such a high level, it is important to think of any protocol being run as a state machine, which then implements an event dispatcher and an event handler.

At the end of the simulation, a finalization function is run, which allows us to print out statistics. It is useful to discuss the structure of a QualNet configuration file, which is the input to the program. Firstly, the network structure is specified. This involves telling the program the number of subnets, their addresses and the number of nodes in each one. Following this, the channel parameters should be specified. This involves the channel frequencies, propagation limits and propagation models.

The next step is to declare the physical layer model. Here, the transmit power, receiver sensitivity and all antenna parameters must be specified. Next the MAC layer should be specified, followed by the network layer and its routing protocol. The parameters here are specific to the protocol used. The application layer is one of the last things to be specified, and is contained in a separate \*.app file. In this file, the type of traffic being sent between two nodes is provided. Giving this config file as a parameter to the QualNet program allows us to run the simulation. The output is the statistics file, which gives us details of what has happened at each layer.

## 5.2 System Design

### 5.2.1 System Components

The system consists of the following components:

1. *Sensor nodes*: Sensor nodes are the heart of the network. They are in charge of collecting and processing data and routing this information back to BS. In other words, a sensor node senses data from the environment, performs simple computations and transmits this data wirelessly to BS either directly or in a multi-hop fashion through neighbours. In the network, there are two kinds of sensor nodes: those which are working properly and are not jammed, and other which are jammed by jammers through the communication channels around it and are not able to provide their services to the network.
2. *Base stations*: Base station is a distinguished component of the WSN with more computational, energy and communication resources. It is a radio receiver/transmitter that serves as the hub of the local wireless network, and may also be the gateway between a wired network and the wireless network. It typically consists of a low-power transmitter and wireless router. In a WSN, the BS aggregates sensor readings and conducts command and control tasks. In our network, these BSs are mobile, i.e. they can physically move from one location to another to mitigate jamming.
3. *Jammers*: Jammers are the attackers in WSNs, which try to jam the communication channels between sensor nodes and BS. Jammers can disturb the communication between sensor nodes or launch radio frequencies to interfere with the open wireless environment. These jammers can be more powerful than the sensor nodes in terms of memory, power capacity, etc.

### 5.2.2 Simulation Model

In the simulation model, we implemented different scenarios consisting of different defense techniques and different number of attackers. To maintain multipath routing between sensor nodes and BSs, a multipath extension of DYMO routing protocol has been implemented as given in [8]. This extension is done through the changes made in the DYMO protocol available in the QualNet simulator.

In our simulation model, BSs send request messages periodically to every sensor node asking them for reports. On getting these sensing reports, BSs perform computation on them and store them in their memory. This request-reply of the sensing report between BS and sensor node is implemented by HTTP protocol at the application layer.

Jammers continuously transmit noisy signals in the network, to interfere with the legitimate radio signals and jam the communication channel between sensor nodes and BSs. Jammers also continuously transmit messages to BSs to flood them, so that they are not able to accept sensor readings from the nodes. This traffic from jammers to BSs is created through CBR packets in QualNet.

## 5.3 Implementation

### 5.3.1 Simulation Parameters

Table 5.1 shows the different parameters and their values used in the simulation.

### 5.3.2 Simulation Scenarios

The simulation scenarios are as follows:

1. The first four scenarios consist of 1, 11, 12 and 16 replicated stationary BSs respectively and 8 jammers with single path DYMO routing protocol.



2. The next four scenarios consist of 1, 11, 12 and 16 replicated mobile BSs respectively and 8 jammers with single path DYMO routing protocol.
3. The next four scenarios consist of 1, 11, 12 and 16 replicated mobile BSs respectively and 8 jammers with multi-path DYMO routing protocol.
4. The next four scenarios consist of 1, 11, 12 and 16 replicated stationary BSs respectively and 12 jammers with single path DYMO routing protocol.
5. The next four scenarios consist of 1, 11, 12 and 16 replicated mobile BSs respectively and 12 jammers with single path DYMO routing protocol.
6. The next four scenarios consist of 1, 11, 12 and 16 replicated mobile BSs respectively and 12 jammers with multi-path DYMO routing protocol.

**Table 5.1: Simulation parameters**

Parameter	Value
Field size	1500m × 1500m
Number of nodes	80
Number of jammers	8 and 12
Node placement	Linear
Nominal radio range of BS	170m
MAC protocol	MACDOT11
PHY model	PHY802.11b
PHY802.11-DATA-RATE	2Mbps
Routing protocol	DYMO
IP-FRAGMENTATION-UNIT	2048
Simulation time	600S

### 5.3.3 Performance Evaluation Metrics

For all scenarios that have been simulated, the following metrics are used to measure the effectiveness of the proposed hybrid technique.

- **Legitimate Traffic Throughput:** Legitimate Traffic Throughput is the amount of sensing information sent in a particular time period by the sensor nodes to the BSs. This is measured in terms of bits/sec.
- **Jamming Traffic Throughput:** Jamming Traffic Throughput is the amount of data sent in a particular time period by the jammers to the BSs for jamming purpose. This is measured in terms of bits/sec.
- **Relative Power Consumption:** Relative power consumption is the ratio of attack power consumption to the power consumption of the WSN augmented with the defense.

$$\text{So } \text{RPC} = \frac{\text{Attack power consumption}}{\text{Defense power consumption}}$$

If the value of  $\text{RPC} > 1$ , it means the defenders will outlast attackers, otherwise attackers will be able to jam the whole WSN.

### 5.2.4 Performance Evaluation

We present the simulation results to observe the following:

- To compare the performance of different defense techniques against BS jamming in WSN.
- To prove the effectiveness of the proposed hybrid technique.

*Legitimate Traffic Throughput:*

Figures 5.3 and 5.4 show the legitimate traffic throughput of different scenarios with 8 and 12 jammers, respectively. In these graphs, we observe that as we increase the number of replicated BSs, the legitimate traffic throughput also increases proportionally with it.

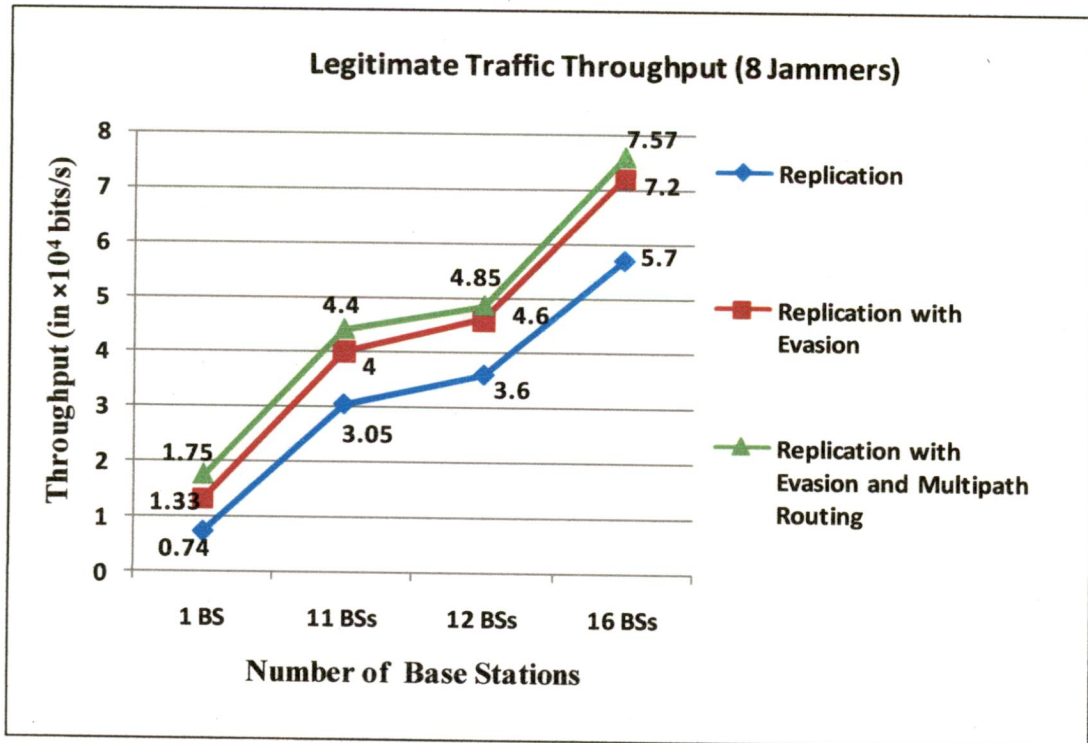


Figure 5.3: Legitimate Traffic Throughput (in  $\times 10^4$  bits/s) with 8 jammers

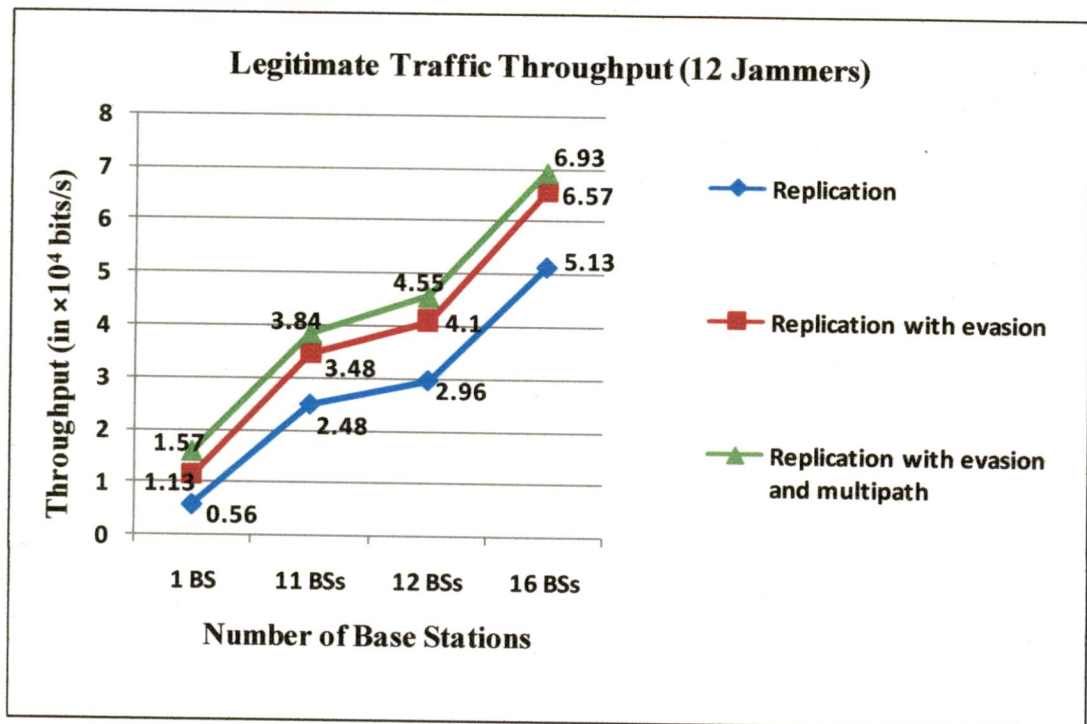
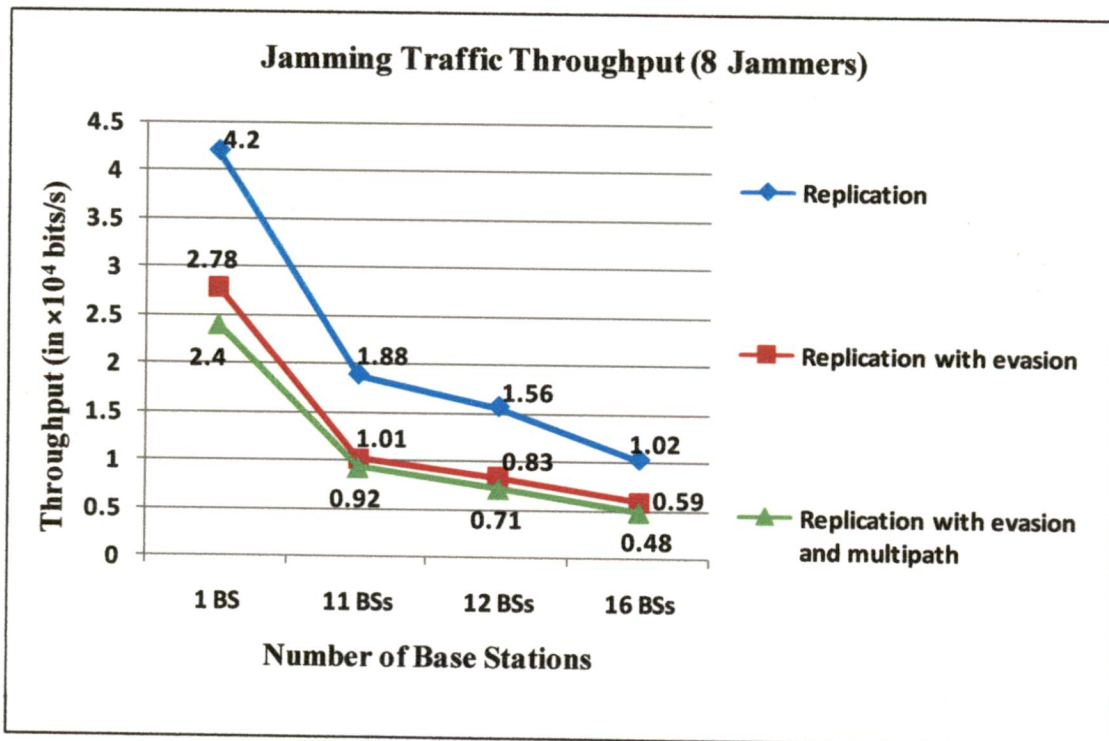


Figure 5.4: Legitimate Traffic Throughput (in  $\times 10^4$  bits/s) with 12 jammers

We also see that our technique gives better legitimate traffic throughput as compared to no defense technique, single defense technique of BS replication or a combination of BS replication with evasion defense techniques in WSN. Increase in the legitimate traffic throughput means that the effect of BS jamming is mitigated, because sensor nodes are able to send more information to BSs. It can be seen that legitimate traffic throughput decreases on increasing the number of attackers.

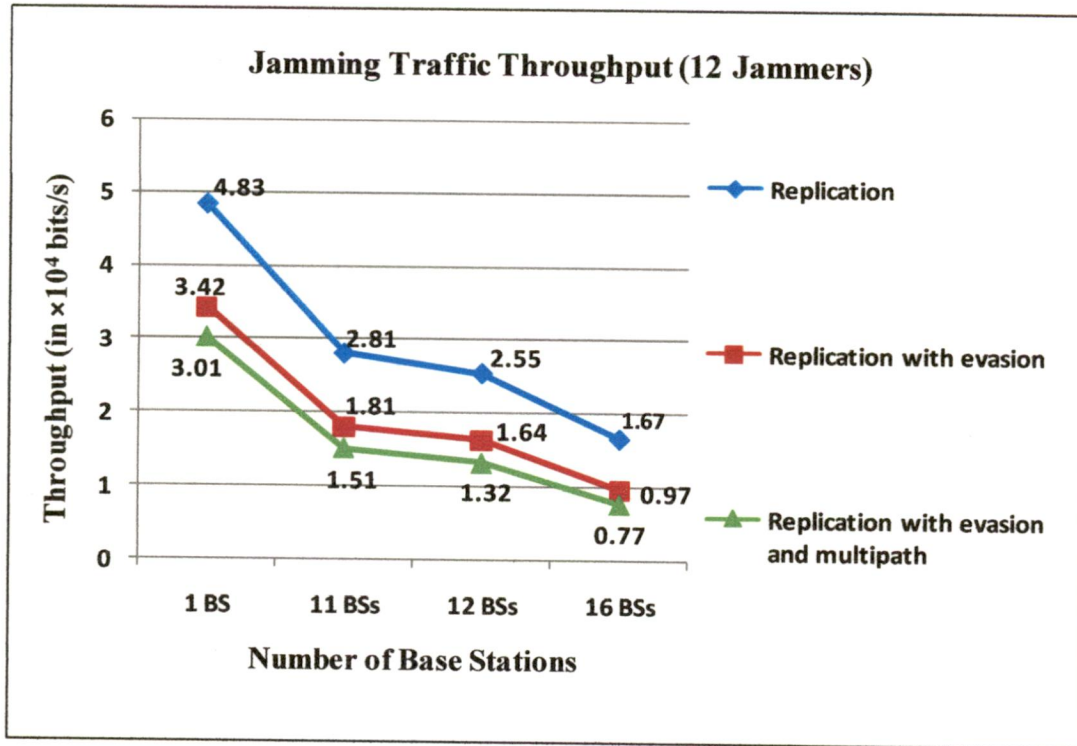
*Jamming Traffic Throughput:*



**Figure 5.5: Jamming Traffic Throughput (in  $\times 10^4$  bits/s) with 8 jammers**

Figures 5.5 and 5.6 show the jamming traffic throughput of different scenarios with 8 and 12 jammers respectively. We observe that as the replication of BS increases, the jamming traffic throughput decreases proportionally. We also see that our technique gives less jamming traffic throughput as compared to using no defense technique, single defense technique of BS replication, or a combination of BS replication with evasion defense techniques in WSN. Decrease in jamming traffic throughput means that average amount

of data sent in a particular time period by the jammers to the BSs for jamming it is reducing. It also shows that the effect of jamming is being mitigated and that jamming traffic throughput increases with increasing number of attackers.

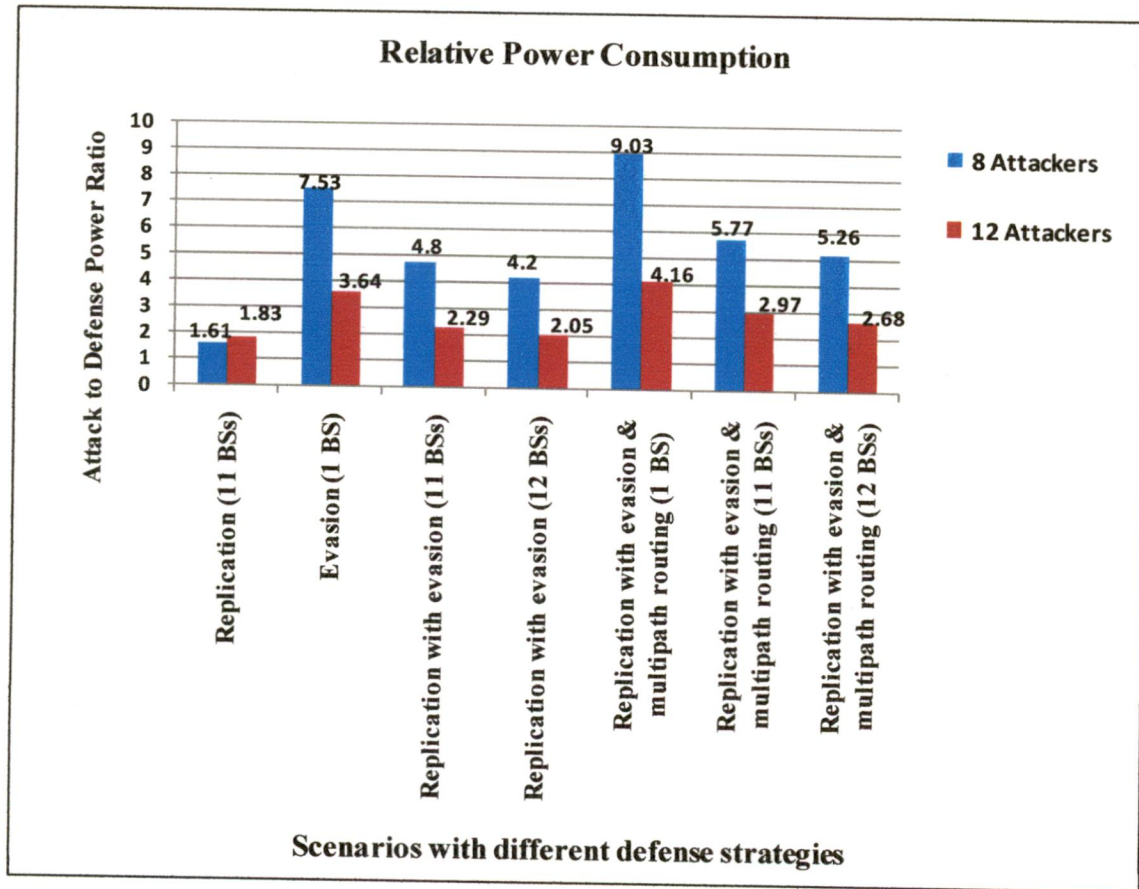


**Figure 5.6: Jamming Traffic Throughput (in  $\times 10^4$  bits/s) with 8 jammers**

#### *Relative Power Consumption:*

Figure 5.7 shows the relative power consumption of different scenarios. We observe that in replication with 11 BSs, attack to defense power ratio increase proportionally with the number of attackers, because the number of BSs is constant and BSs are stationary. In this case only the number of mobile attackers is increasing, and these attackers are moving for jamming the network, so their power consumption is increasing more than the BSs. Hence the relative power consumption is increasing.

In other scenarios of Figure 5.7, we observe that as the number of attackers is increasing, their attack to defense power ratio is decreasing. The reason is that BSs are mobile in



**Figure 5.7: Relative Power Consumption**

these scenarios, so they have to move more often from one location to another for mitigating the jamming attack, as the number of attackers is increasing. Hence the power consumption of the BSs is increasing more than the attackers as the number of attackers increased. Also relative power consumption is decreasing.

## CHAPTER 6

### CONCLUSION

---

#### 6.1 Analysis of Results

In this thesis, we have presented a hybrid technique of defense against BS jamming attack in WSNs. This hybrid technique combines 3 defense techniques, BS replication, BS evasion from jammed location to unjammed location, and multipath routing between sensor nodes and BSs. Simulation results indicate that Legitimate Traffic Throughput between sensor nodes and BSs increases, and Jamming Traffic Throughput created by the jammers decreases after the implementation of the hybrid technique.

Results also indicate that the hybrid model gives better Relative Power Consumption as compared to using no defense technique, single defense technique of BS replication or a combination of two defense techniques of BS replication with evasion. Results also show that as the number of attackers increases, legitimate traffic throughput decreases, and jamming traffic throughput increases. Also relative power consumption decreases. Hence the proposed hybrid technique is able to mitigate the effect of BS jamming more than any single defense technique separately or a combination of any two defense techniques.


Though there are overheads of increasing network setup cost, communication cost, extra power consumption and transportation cost, these overheads are acceptable and reasonable in comparison to the effects of BS jamming attacks.

#### 6.2 Suggestions for Future Work

The proposed hybrid technique can be augmented in many ways. Some suggestions for further work are as follows:

1. The controlled BS evasion based on reactive approach can be used for getting better results in our hybrid technique, because a reactive approach conserves BS power, so that it can give its service to the network for the longer time duration.
2. We can make the hybrid technique more efficient for defense against BS jamming by combining some more effective defense techniques in it.

### 6.3 Contribution of the Work

1. Sushil Kumar Jain, Kumkum Garg, "A Hybrid Model of Defense against Base Station Jamming Attack in Wireless Sensor Networks", accepted for publication in International Journal of Computer Science and Information Security, May 2009.  *withdrawn*
2. Sushil Kumar Jain, Kumkum Garg, "A Hybrid Model of Defense Techniques against Base Station Jamming Attack in Wireless Sensor Networks", In CICSyN'09, July 2009. (Under Press)



---

## References

---

- [1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A survey on sensor networks", *IEEE Communication Magazine*, vol. 40, no. 8, pp. 102-114, Aug. 2002.
- [2] U. A. F. ARGUS, "Advanced Remote Ground Unattended Sensor Systems", Department of Defense Argus, <http://www.globalsecurity.org/intell/systems/arguss.htm>
- [3] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless sensor networks for habitat monitoring", In *WSNA'02*, pp. 88-97, 2002.
- [4] James Carlson, Richard Han, Shandong Lao, Chaitanya Narayan, and Sagar Sanghani, "Rapid prototyping of mobile input devices using wireless sensor nodes", In *WMCSA'03*, Monterey, California, USA, pp. 21, October 2003.
- [5] Sherif Khattab, Daniel Mosse, and Rami Melhem, "Honeybees: Combining Replication and Evasion for mitigating Base station Jamming in Sensor Networks", *Parallel and Distributed Processing Symposium*, pp. 25-29, April 2006.
- [6] W. Xu, T. Wood, W. Trappe, and Y. Zhang. "Channel surfing and spatial retreats: defenses against wireless denial of service", In *Proceedings of the 2004 ACM workshop on Wireless security*, pp. 80-89, 2004.
- [7] J. Deng, R. Han, and S. Mishra. "Enhancing base station security in wireless sensor networks", *Technical Report CUCS 951-03*, Department of Computer Science, University of Colorado, Boulder, CO, 2002.
- [8] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies in wireless sensor networks", In *IEEE DSN*, pp. 637-646, 2004.

- [9] I. Chakeres, and C. Perkins, "Dynamic manet on-demand (dymo) routing", <http://www.ietf.org/internet-drafts/draft-ietf-manet-dymo-17.txt>, March 2009.
- [10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless Sensor Networks: A Survey", *IEEE Computer Networks*, vol. 38, no. 4, pp. 393-442, June 2007.
- [11] Song Han, Elizabeth Chang, Li Gao, and Tharam Dillon, "Taxonomy of Attacks on Wireless Sensor Networks", *Proceedings of the First European Conference on Computer Network Defense School of Computing*, University of Glamorgan, Wales, UK, pp. 97-105, 2005.
- [12] Carlos de Morais Cordeiro, Dharam Prakash Aggarwal, "AD HOC & SENSOR NETWORKS-Theory and Applications", *World Scientific Publishing Company*, ISBN-13: 9789812566812, May 2006.
- [13] M. Ilyas, I. Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems", *CRC press*, August 2004.
- [14] <http://homepages.dcc.ufmg.br/~linnyer>
- [15] Sabah, Adnan Majeed, Kyoung-Don Kang, Ke liu and Nael Abu-Ghazeleh, "An Application-Driven Perspective on Wireless Sensor Network Security", *In proceedings of the 2<sup>nd</sup> ACM international workshop on quality of service & security for wireless and mobile networks*, pp. 1-8, Oct. 2006.
- [16] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks", *In proceeding Wireless Networks*, vol. 8, no. 5, pp. 521-534, Sep. 2002.

- 
- [17] A.D. Wood and J.A. Stankovic, "A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks", *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*, CRC press, 2004.
- [18] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks", *IEEE Computer*, pp. 54–62, Oct. 2002.
- [19] Y. W. Law, P. Hartel, J. D. Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC", *Technical Paper*, Univ. of Twente, NL, 2005.
- [20] Hung-Min Sun, Shih-Pu Hsu, and Chien-Ming Chen, "Mobile Jamming Attack and its Countermeasure in Wireless Sensor Networks", *Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops*, vol. 1, pp 457-462, 2007.
- [21] W. Xu, W. Trappe, Y. Zhang, and T. Wood. "The feasibility of launching and detecting jamming attacks in wireless networks", In *ACM MobiHoc*, pp. 46-57, 2005.
- [22] Marga Nacher, Carlos T. Calafate, and Pietro Manzoni, "Multipath extensions to the DYMO routing protocol", *Mobile Wireless Communications Networks, 9th IFIP International Conference*, pp. 1–5, Sept. 2007.
- [23] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (aodv) routing", <http://www.ietf.org/rfc/rfc3561.txt>, July 2003.
- [24] *QualNet 4.0 User's Guide*, Scalable Network Technologies, Inc., Dec. 2006.
- [25] A. D. Wood, J. A. Stankovic, and S. H. Son, "JAM: A Jammed-Area mapping Service for Sensor Networks", In *RTSS*, pp. 286-297, 2003.

- [26] Kemal Akkaya, Mohamed Younis, "A survey on routing protocols for wireless sensor networks" in *Elsevier Ad Hoc Network Journal*, Vol. 3, pp. 325-349, 2005.
- [27] K.H.Kim and et. al., "A Resilient Multipath Routing Protocol for Wireless Sensor Networks," *ICN 2005, Lecture Notes in Computer Science*, vol. 3421, pp. 1122-1129, 2005.

# APPENDIX

## SIMULATION SCREEN SHOTS

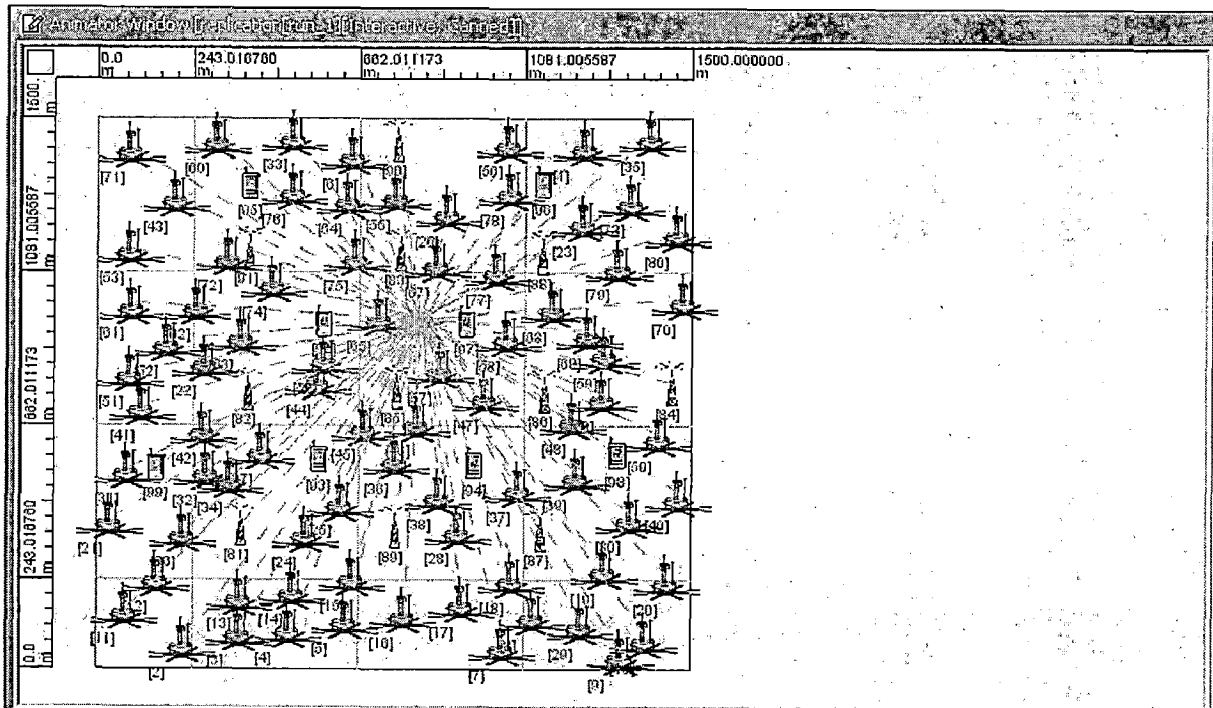
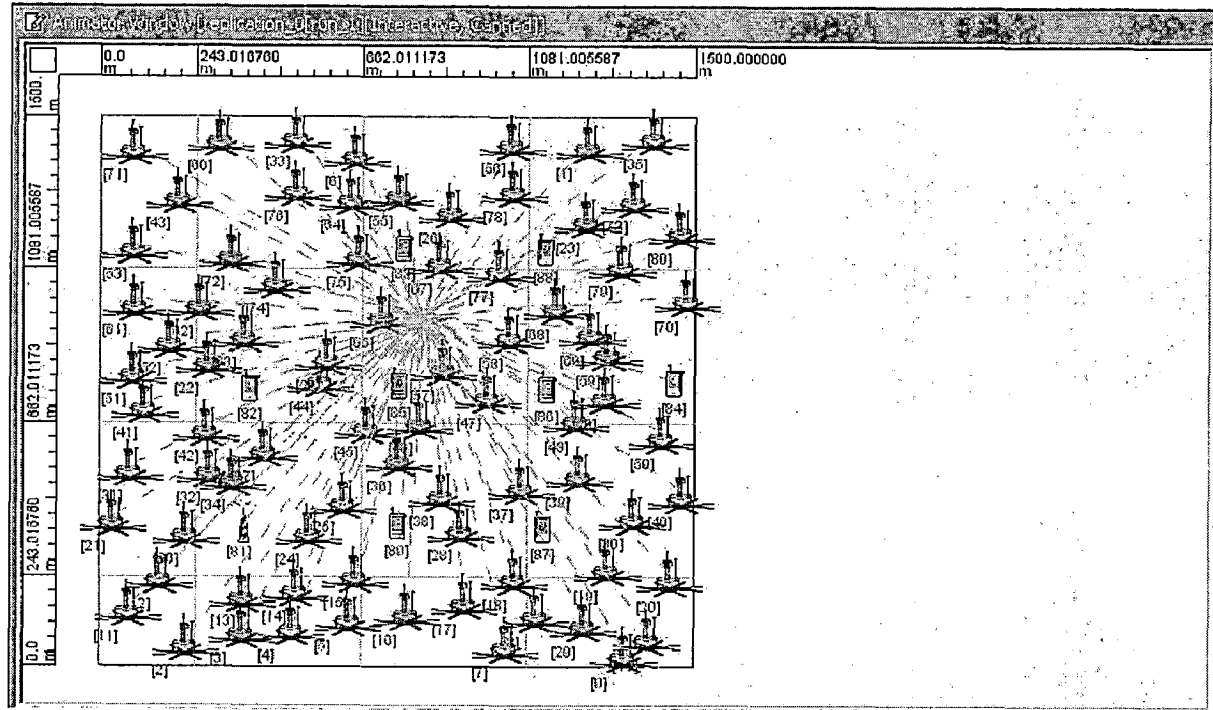
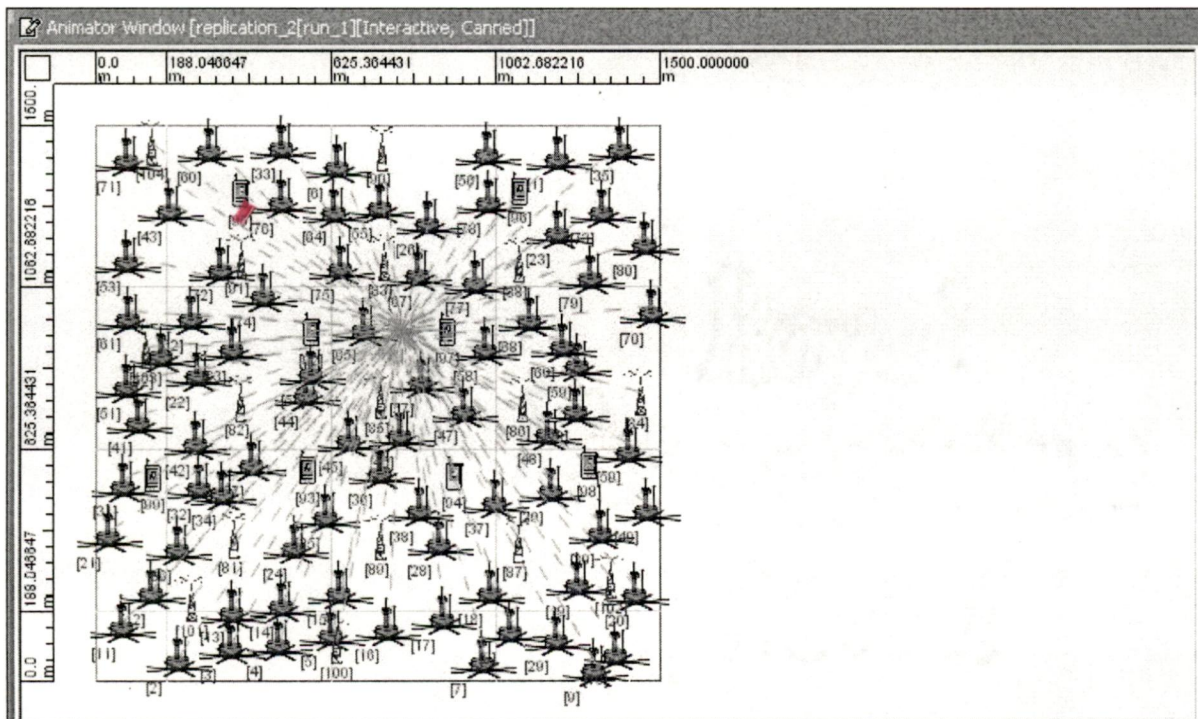
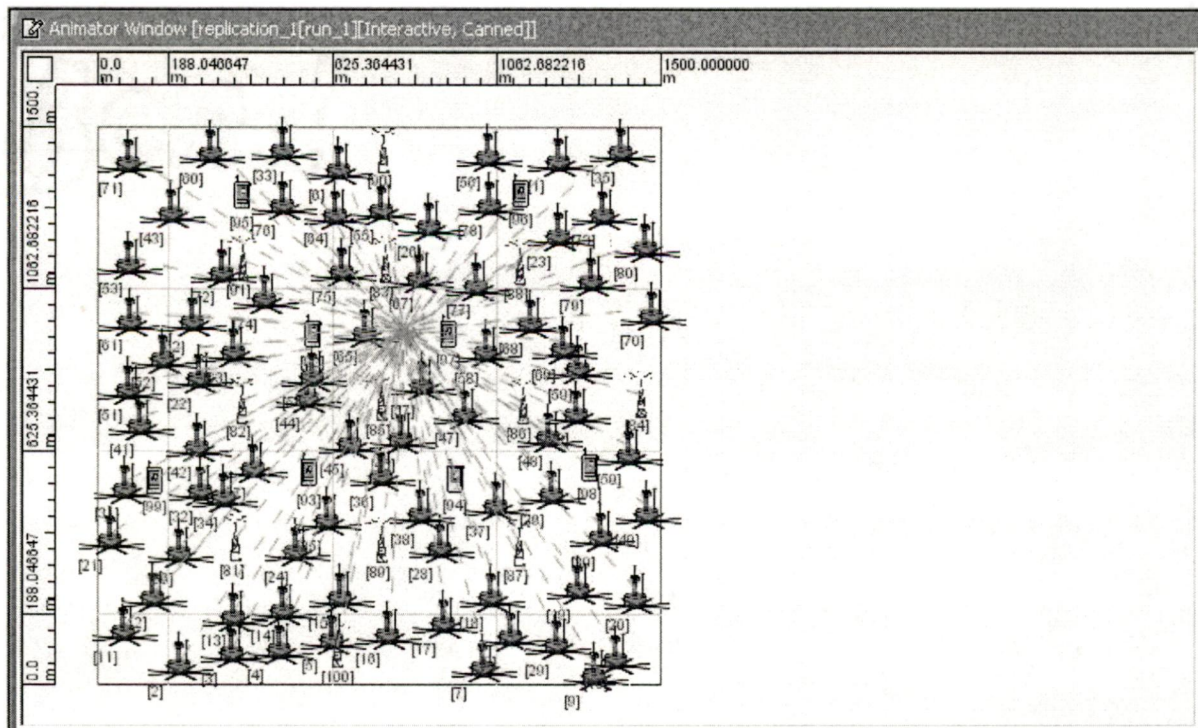
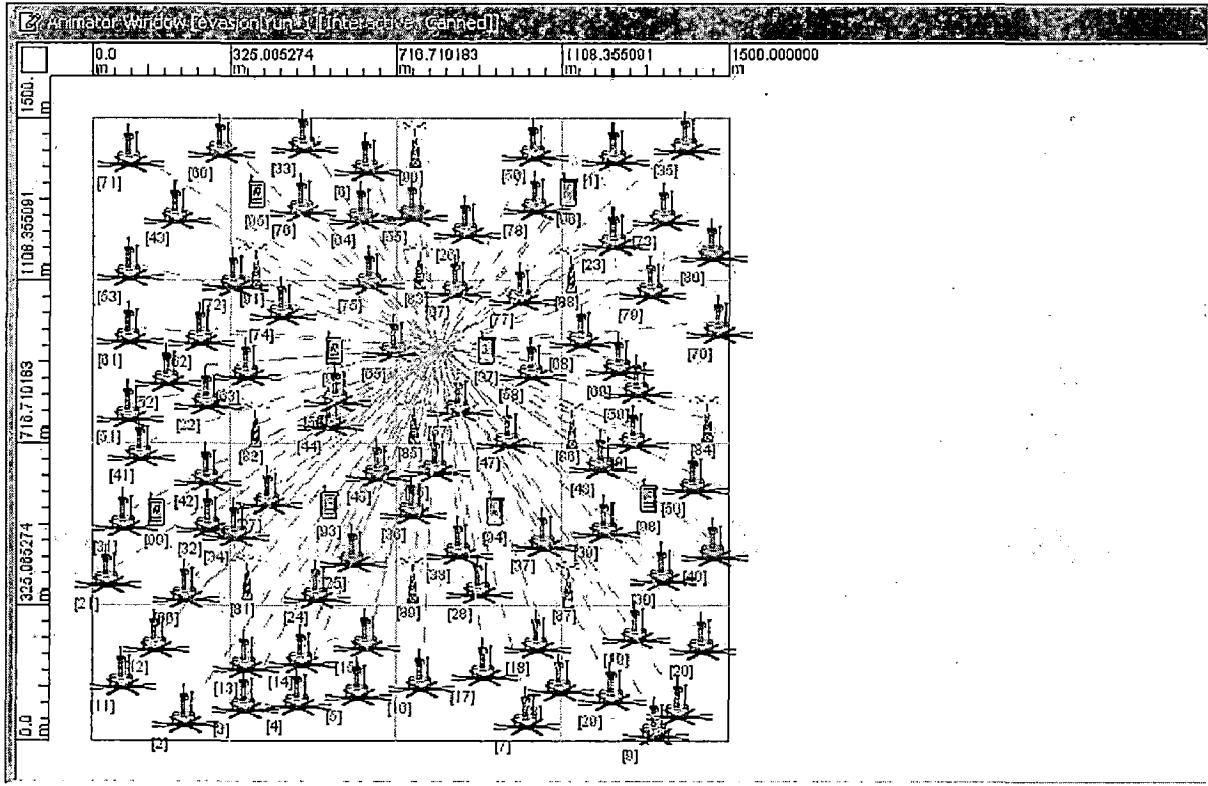
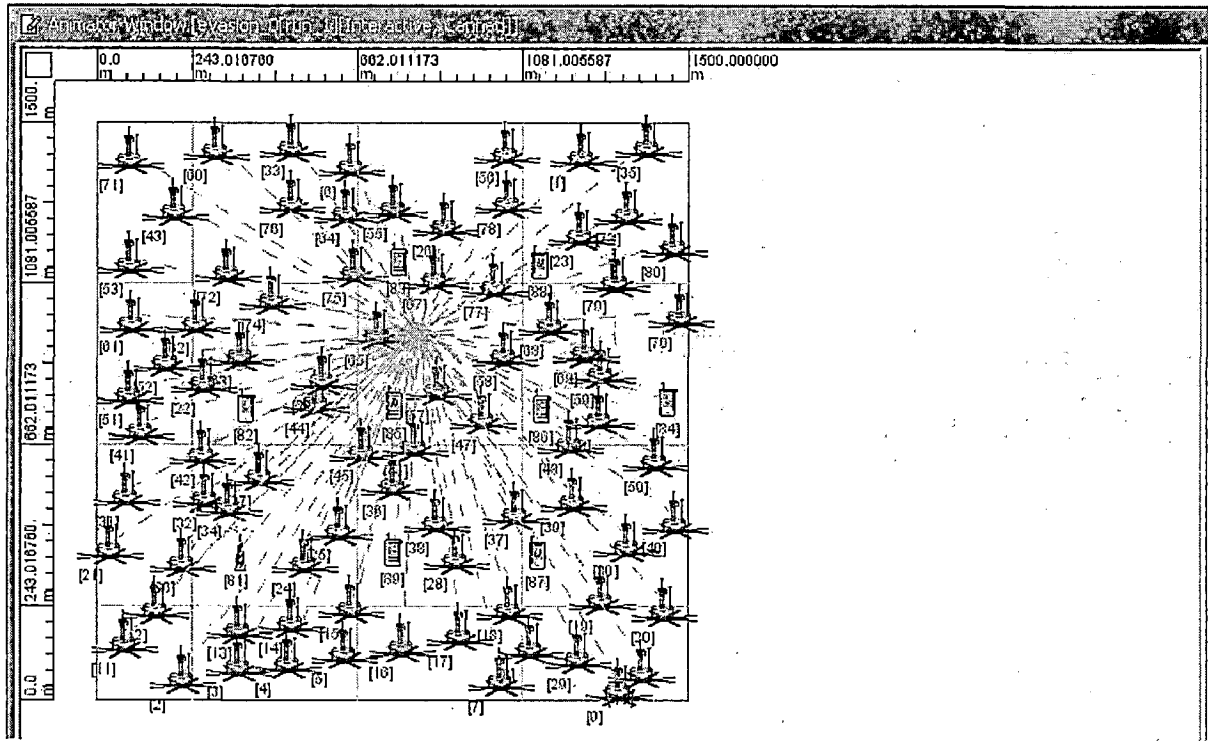


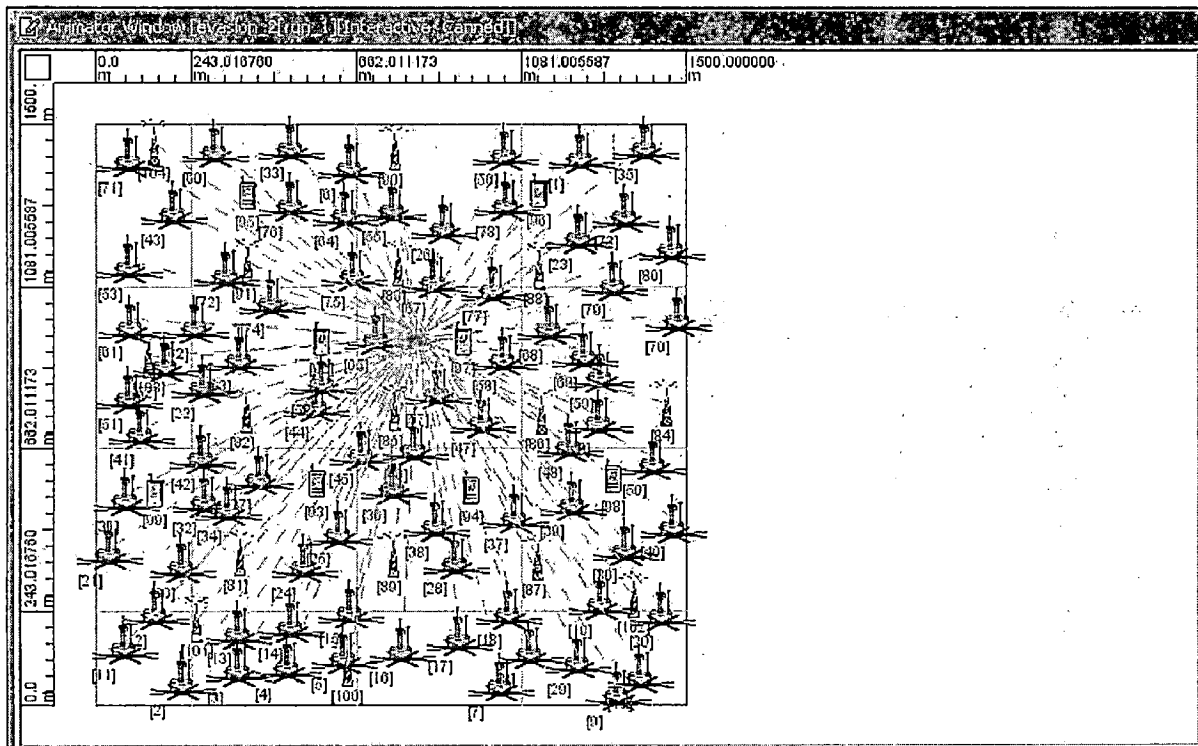
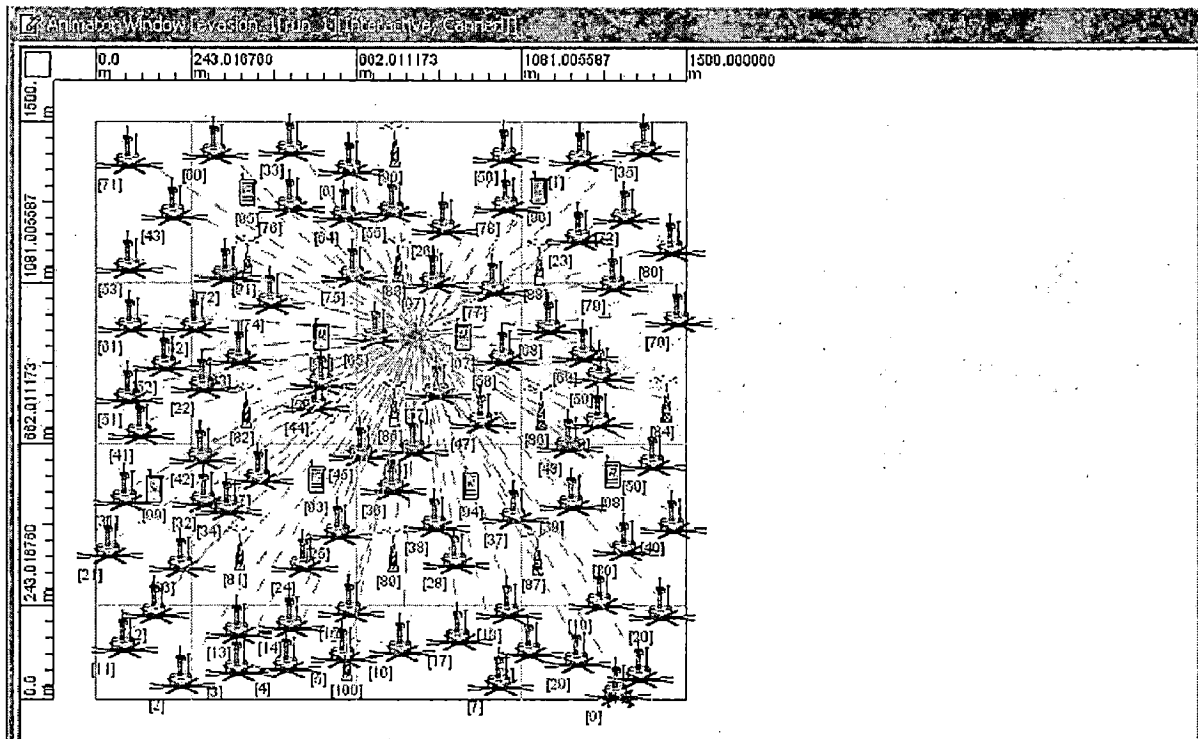
Figure 1 and 2: Simulation scenarios of 1 and 11 replicated stationary BSs respectively and 8 jammers with single path DYMO routing protocol



**Figure 3 and 4: Simulation scenarios of 12 and 16 replicated stationary BSs respectively and 8 jammers with single path DYMO routing protocol**



**Figure 5 and 6: Simulation scenarios of 1 and 11 replicated mobile BSs respectively and 8 jammers with single path DYMO routing protocol**



**Figure 7 and 8: Simulation scenarios of 12 and 16 replicated mobile BSs respectively and 8 jammers with single path DYMO routing protocol**



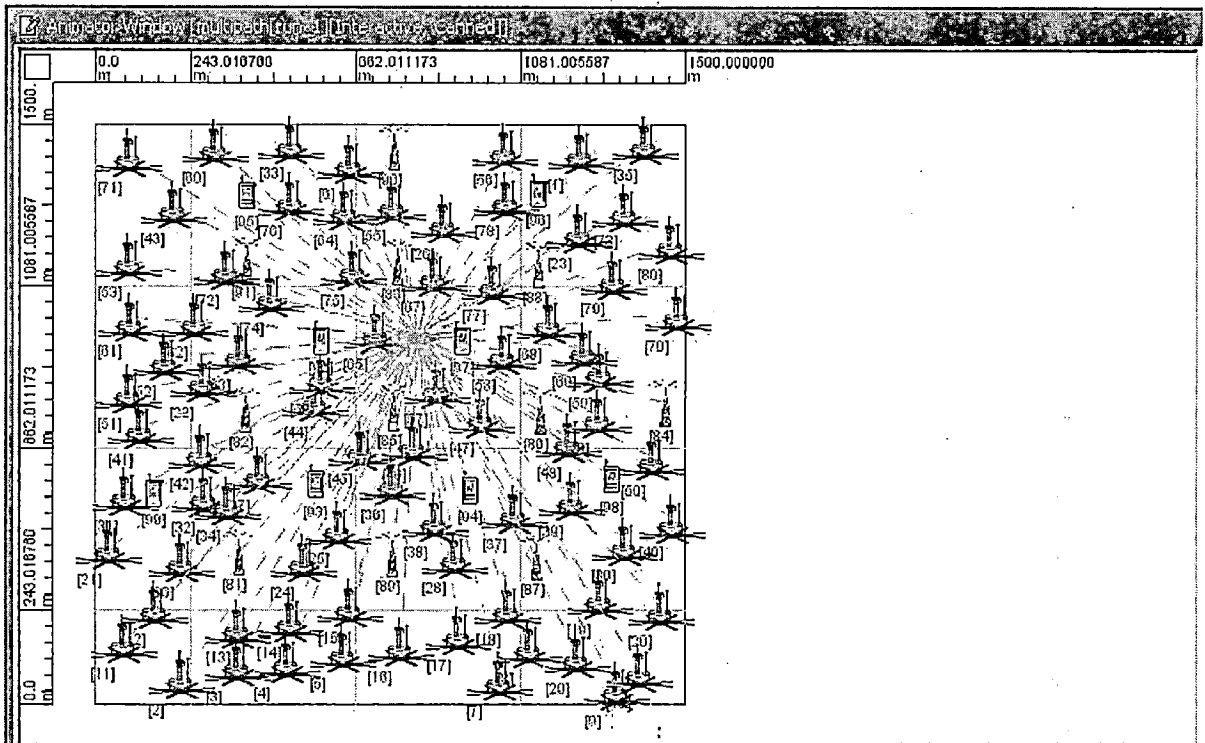
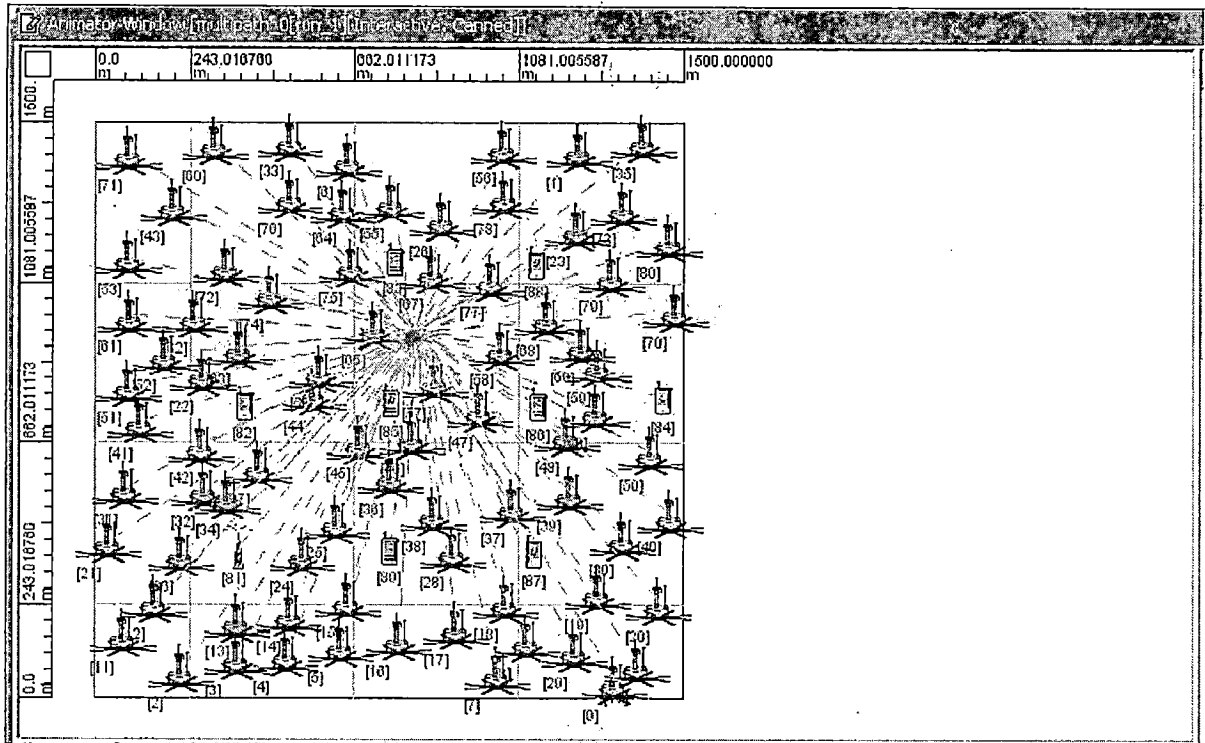
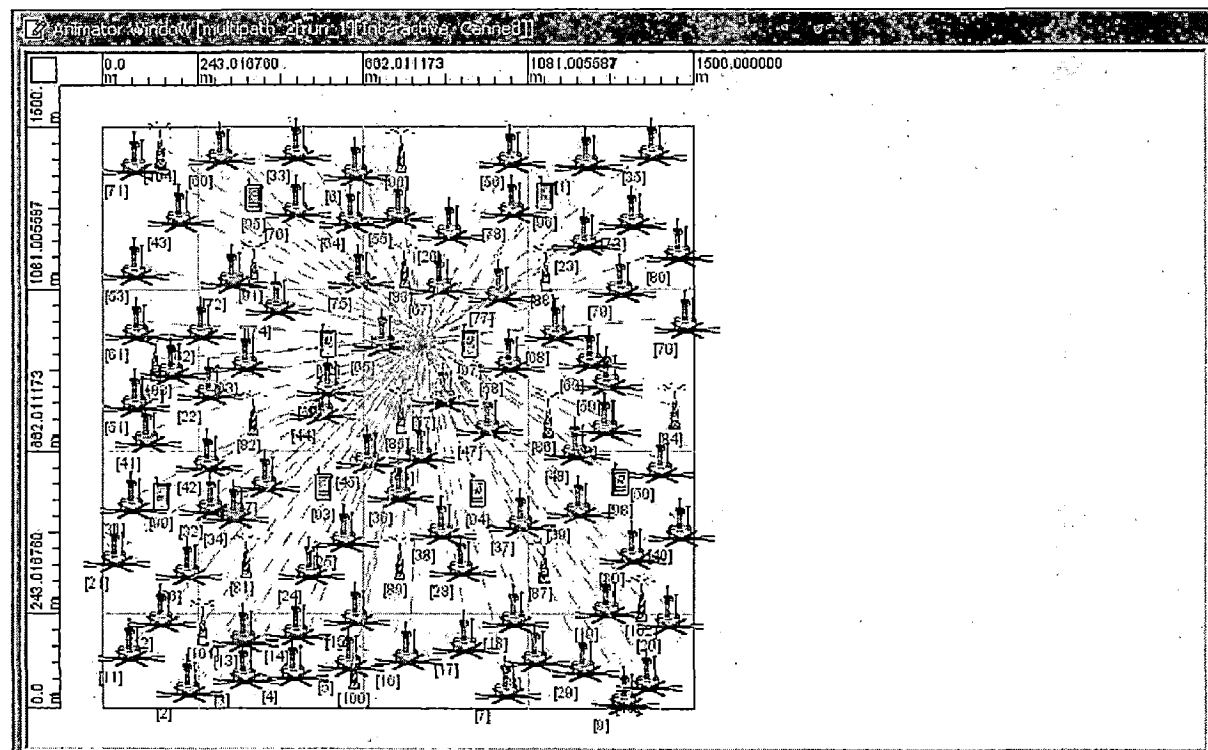
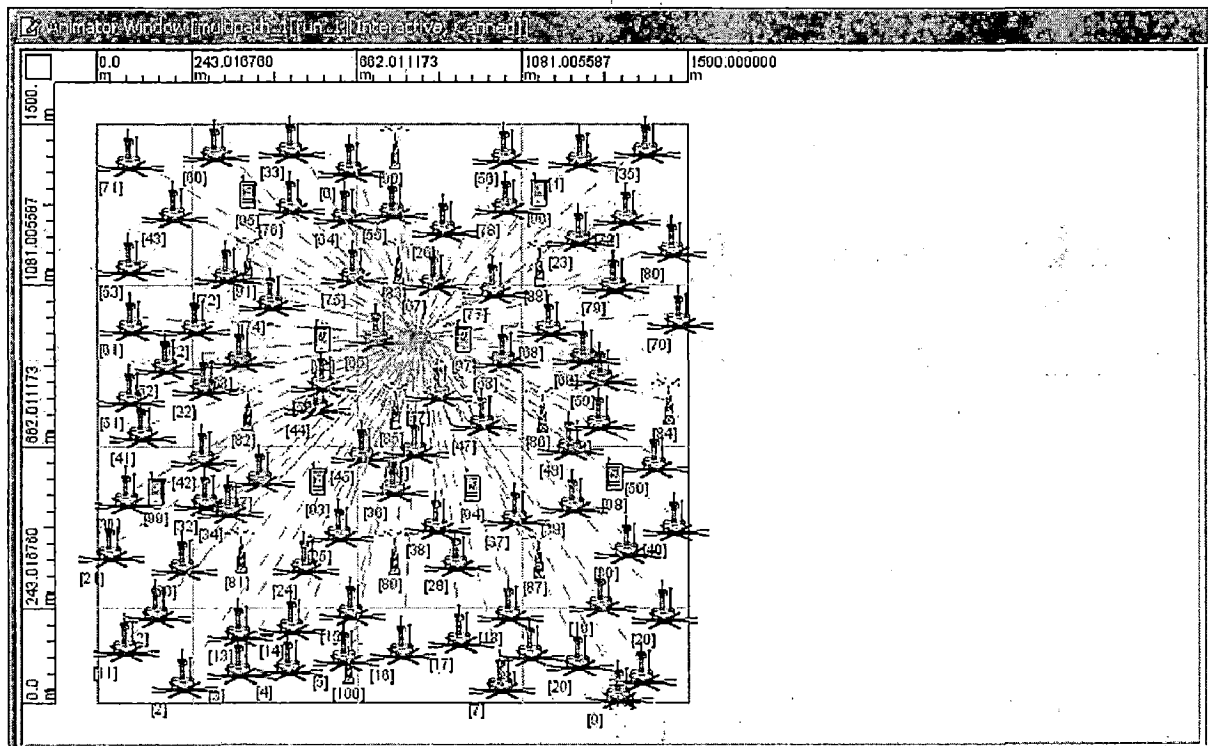


Figure 9 and 10: Simulation scenarios of 1 and 11 replicated mobile BSs respectively and 8 jammers with multi-path DYMO routing protocol



**Figure 11 and 12: Simulation scenarios of 12 and 16 replicated mobile BSs respectively and 8 jammers with multi-path DYMO routing protocol**

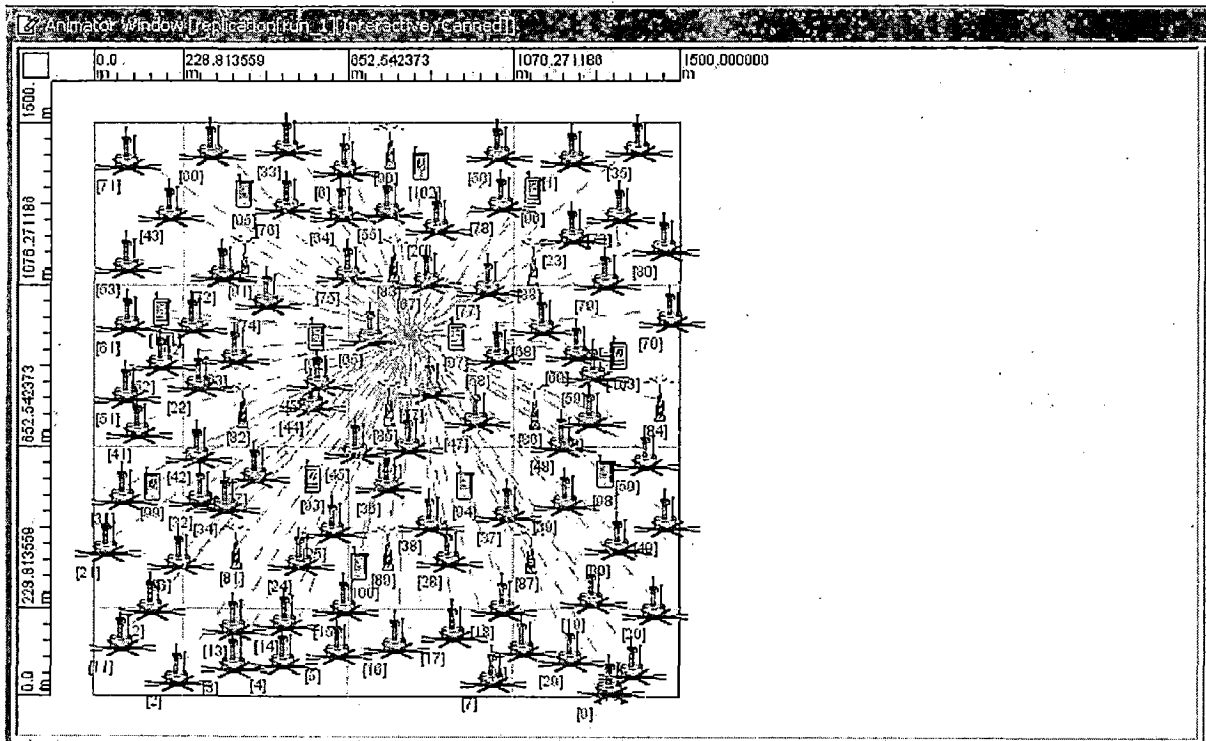
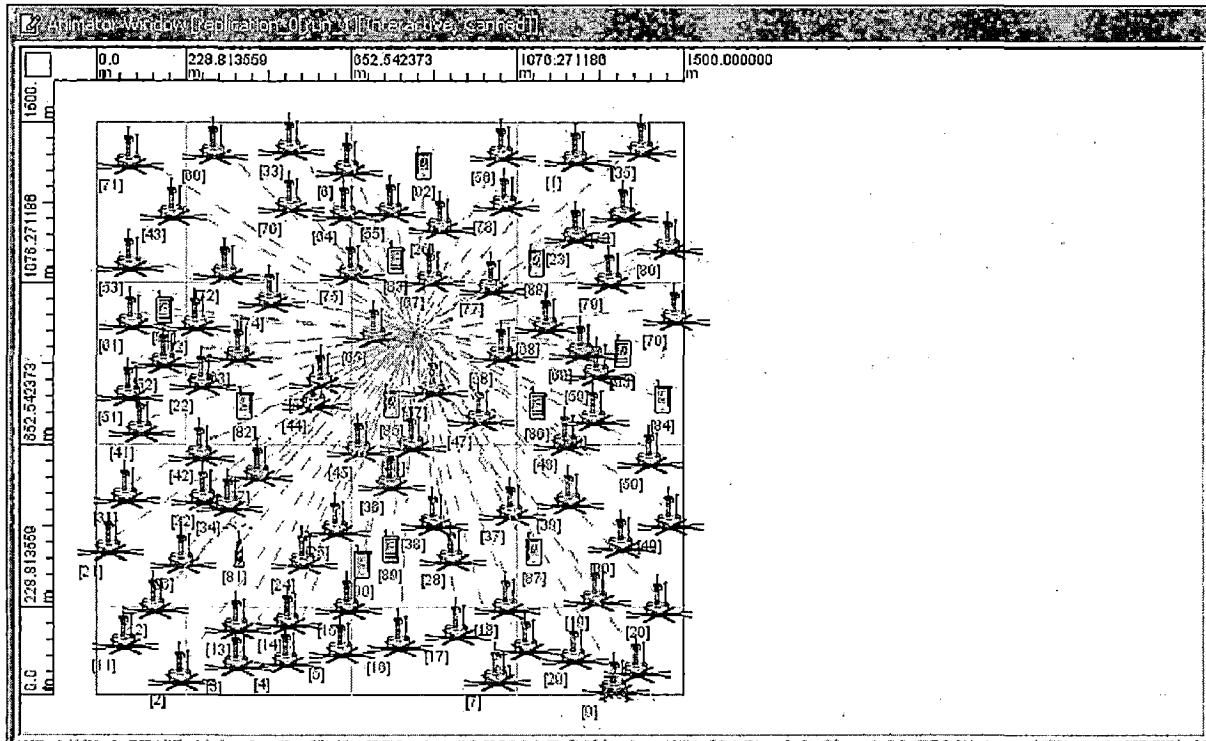
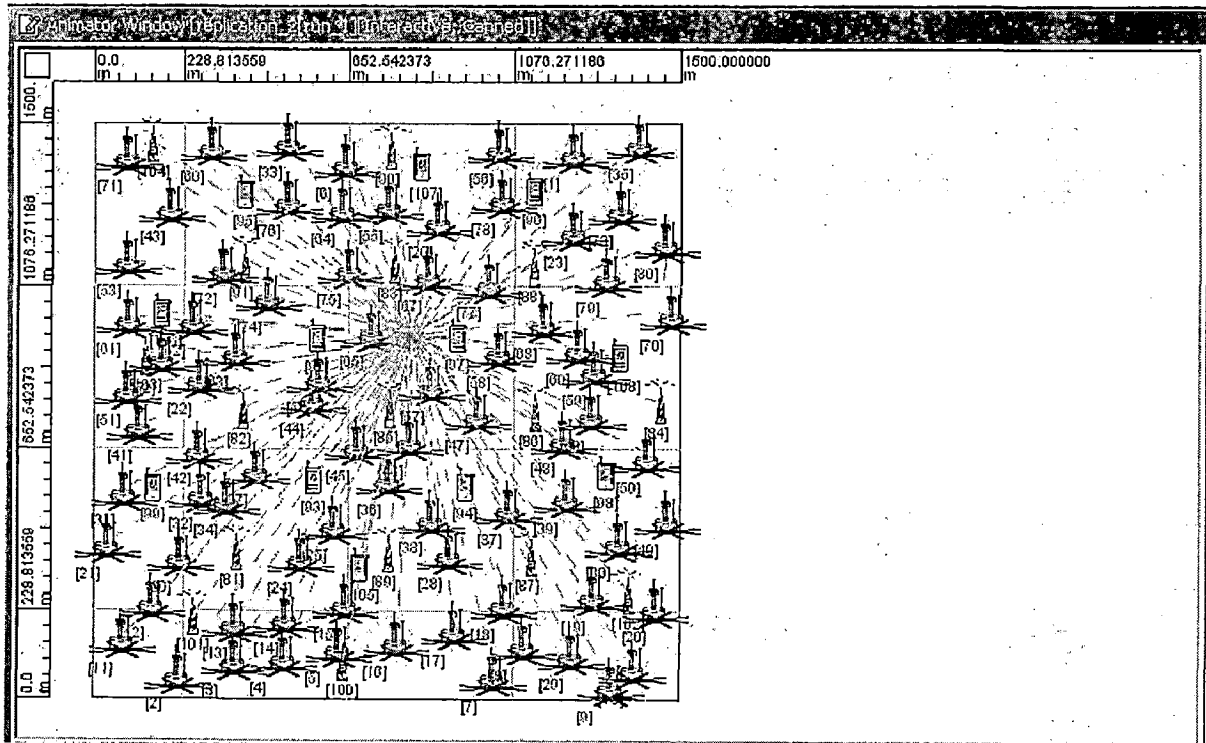
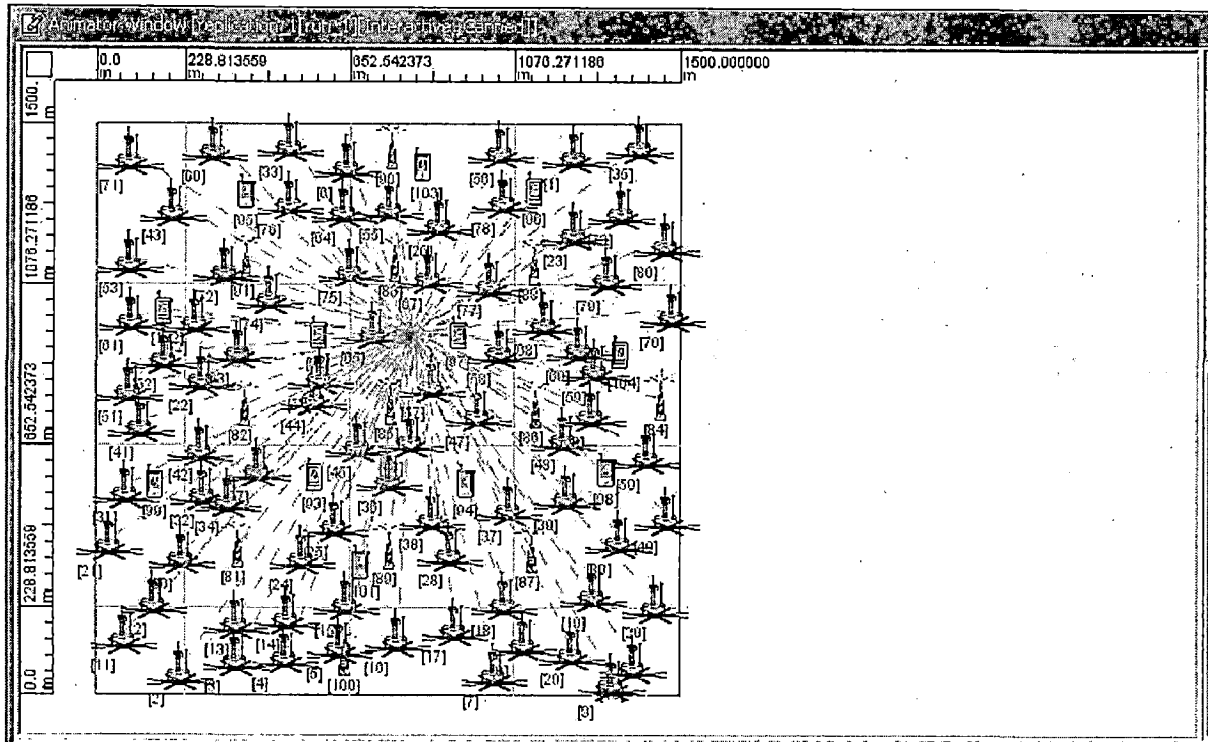
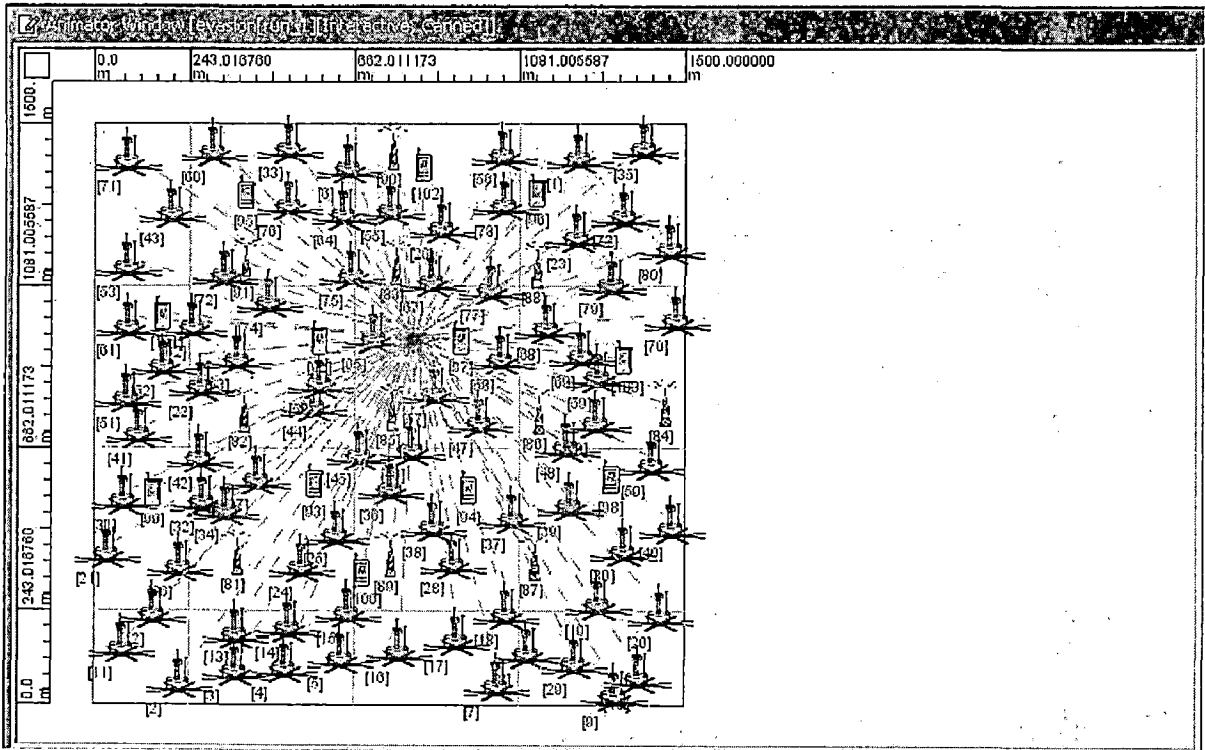
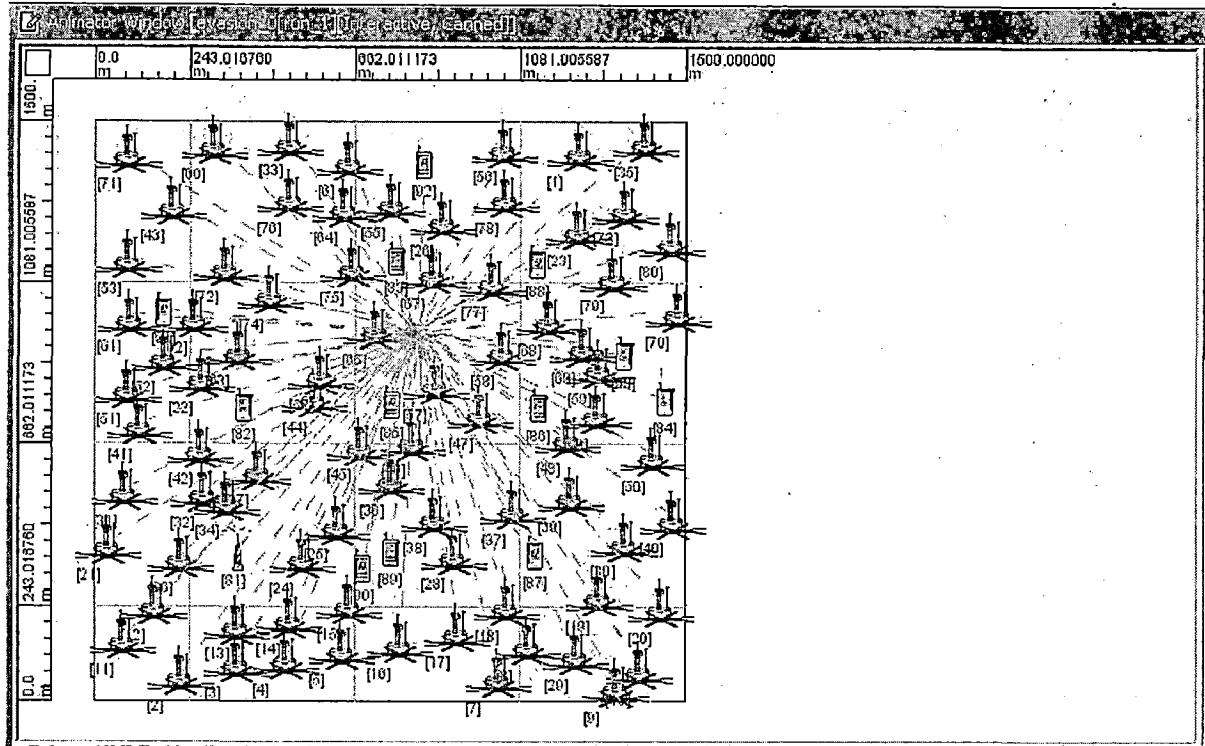


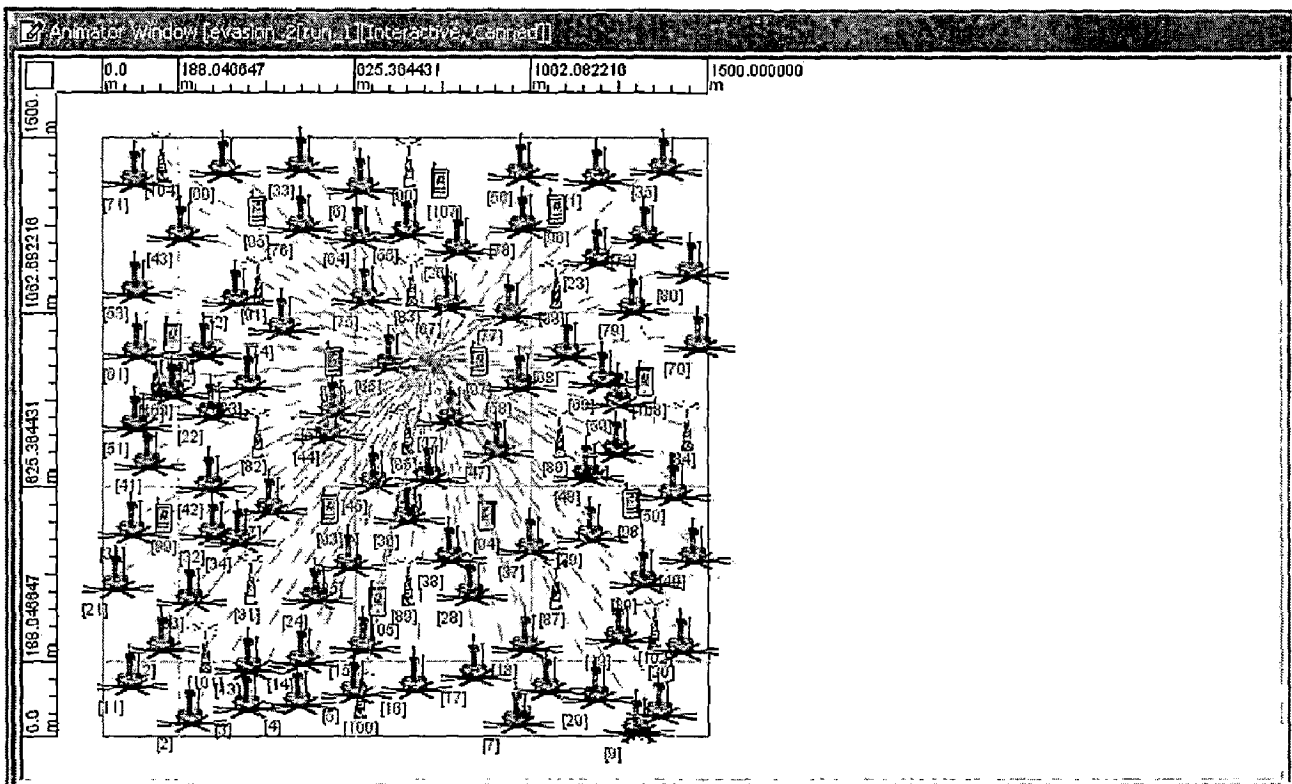
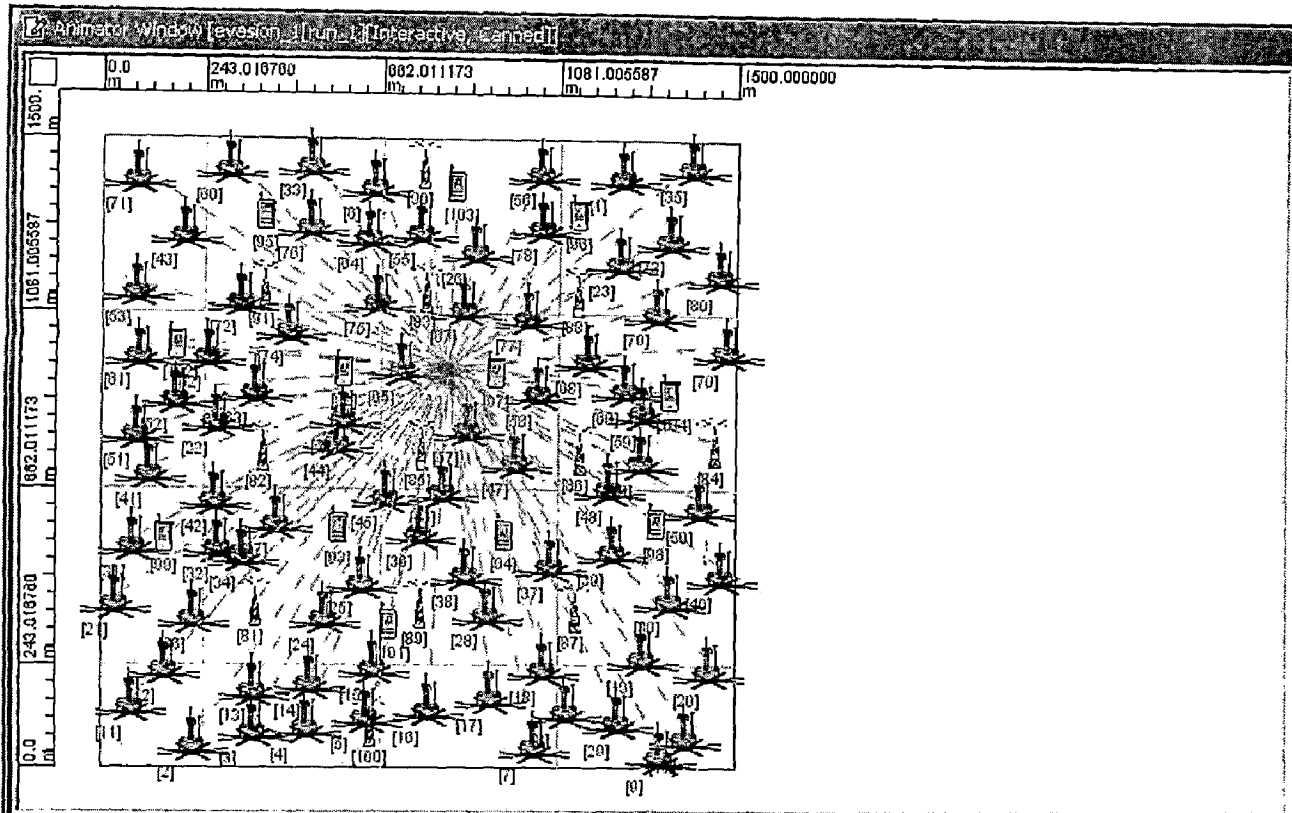
Figure 13 and 14: Simulation scenarios of 1 and 11 replicated stationary BSs respectively and 12 jammers with single path DYMO routing protocol



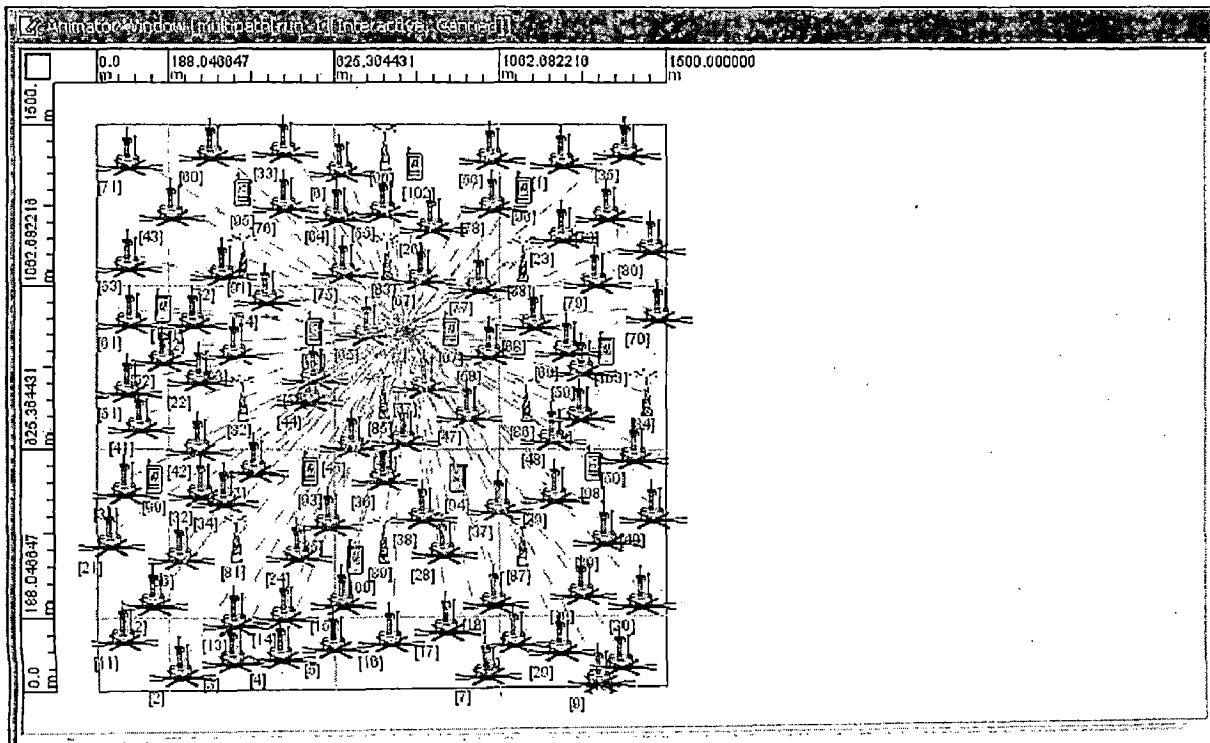
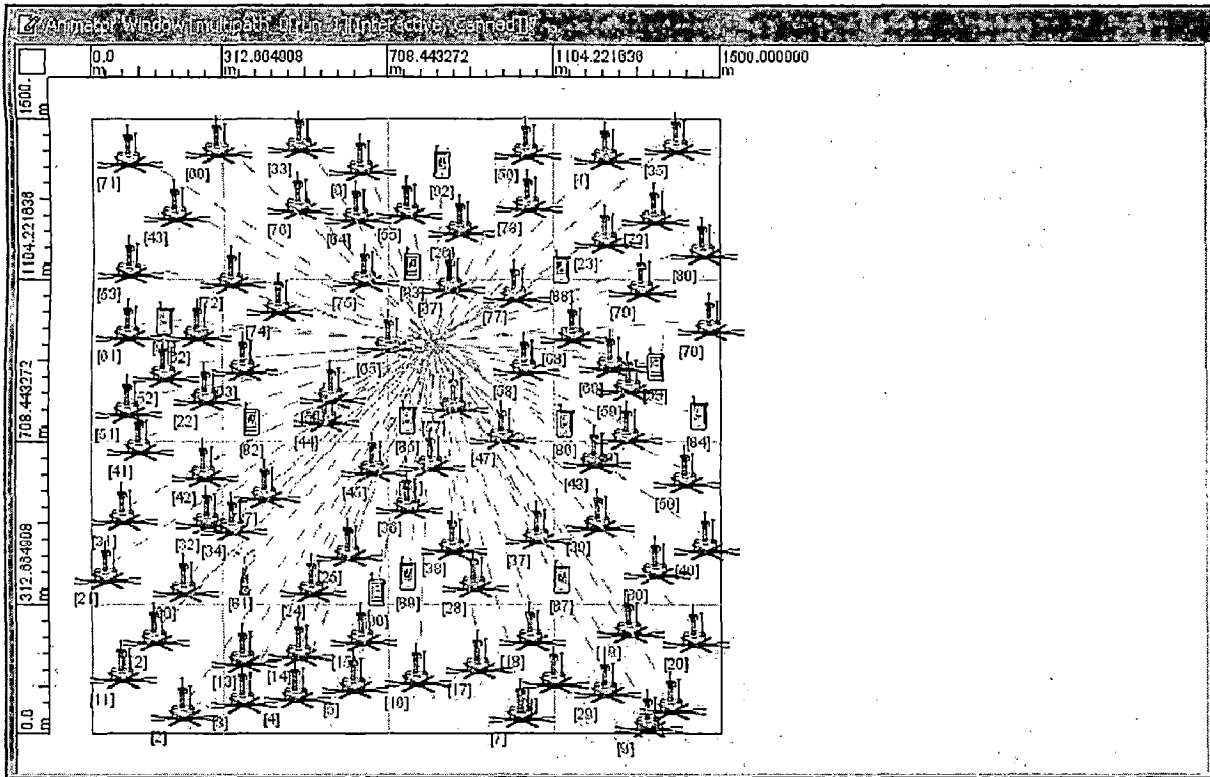
**Figure 15 and 16: Simulation scenarios of 12 and 16 replicated stationary BSs respectively and 12 jammers with single path DYMO routing protocol**



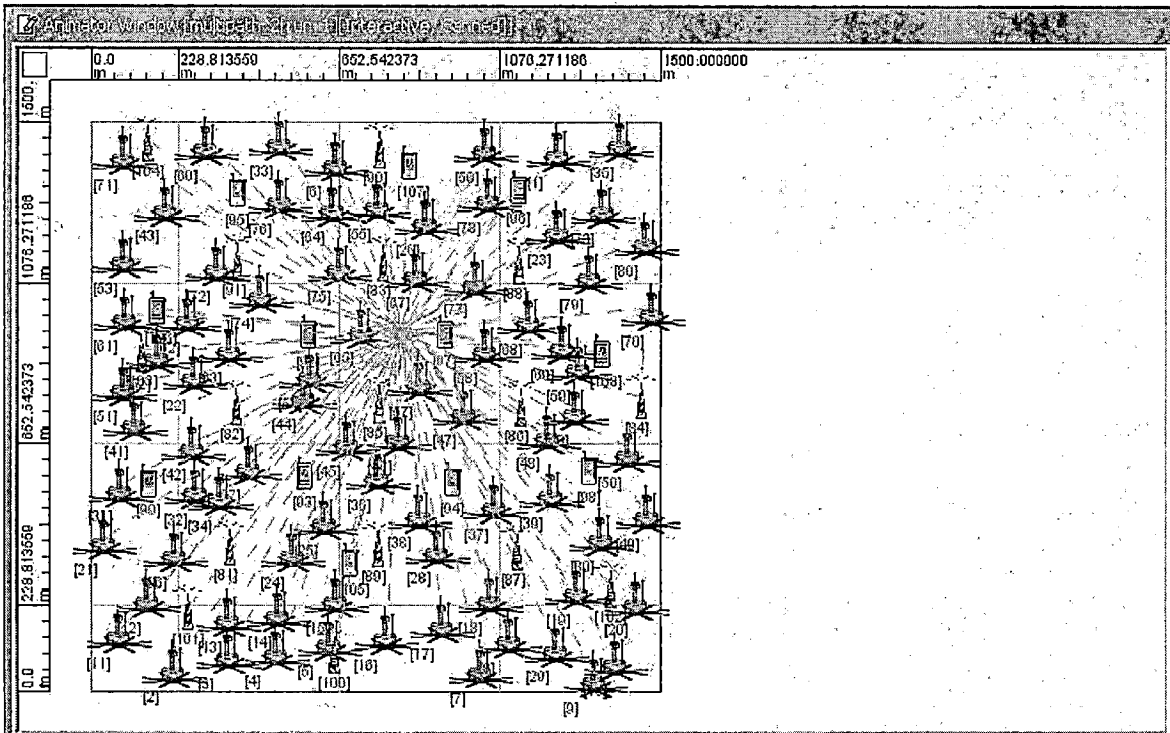
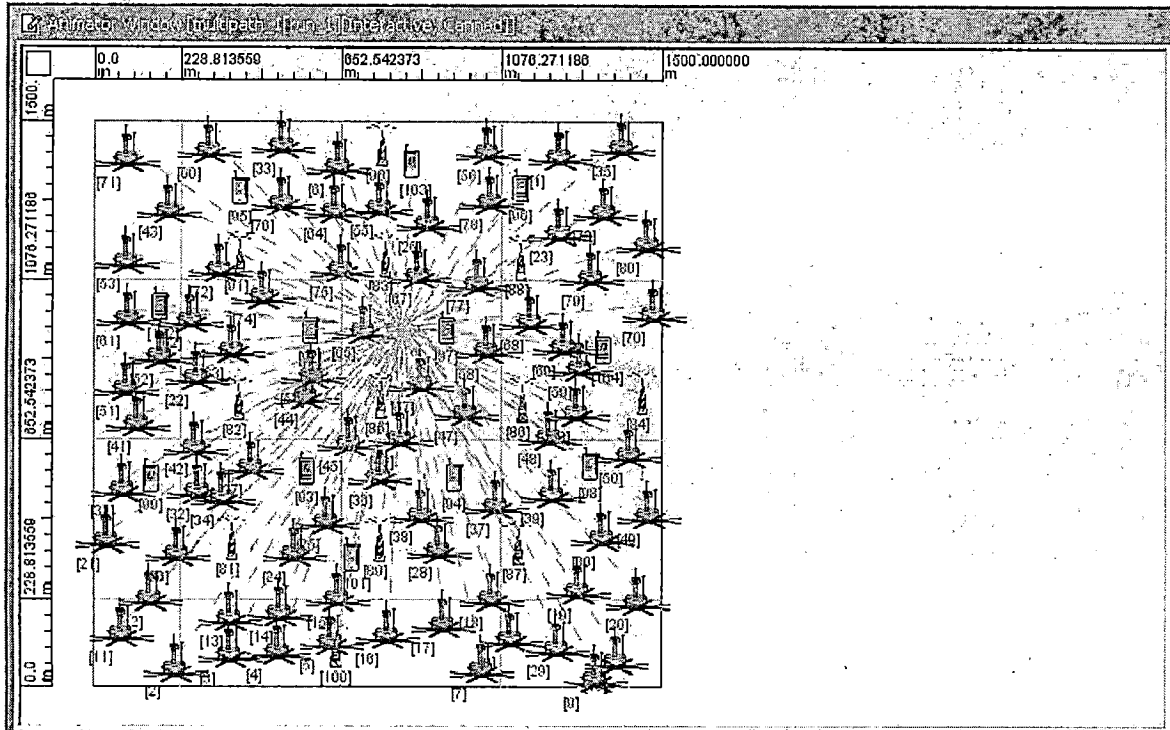
**Figure 17 and 18: Simulation scenarios of 1 and 11 replicated mobile BSs respectively and 12 jammers with single path DYMO routing protocol**



**Figure 19 and 20: Simulation scenarios of 12 and 16 replicated mobile BSs respectively and 12 jammers with single path DYMO routing**



**Figure 21 and 22: Simulation scenarios of 1 and 11 replicated mobile BSs respectively and 12 jammers with multi-path DYMO routing protocol**



**Figure 23 and 24: Simulation scenarios of 12 and 16 replicated mobile BSs respectively and 12 jammers with multi-path DYMO routing**