BONAFIDE CERTIFICATE

Certified that this project report titled **"JAMMER-AWARE TRAFFIC ALLOCATION BASED ON POWER OPTIMIZATION IN WIRELESS SENSOR NETWORK"** is the bonafide work of **JAIPRIYA.S [Reg. No. 13MAE05]** who carried out the research under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of any other project or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Ms.S.UMAMAHESWARI

ASSOCIATE PROFESSOR

Department of ECE

Kumaraguru College of Technology

Coimbatore-641 049

SIGNATURE

Dr. RAJESWARI MARIAPPAN

HEAD OF THE DEPARTMENT

Department of ECE

Kumaraguru College of Technology

Coimbatore-641 049

The Candidate with university **Register No. 13MAE05** was examined by us in the project viva –voice examination held on .....

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

First I would like to express my praise and gratitude to the Lord, who has showered his grace and blessing enabling us to complete this project in an excellent manner. He has made all things in beautiful in his time.

I express my sincere thanks to our beloved Joint Correspondent, **Shri. Shankar Vanavarayar** for his kind support and for providing necessary facilities to carry out the project work.

I would like to express my sincere thanks to our beloved Principal **Dr.R.S.Kumar M.E., Ph.D.,** who encouraged us with his valuable thoughts.

I would like to express my sincere thanks and deep sense of gratitude to our HOD, **Dr. Rajeswari Mariappan M.E., Ph.D.,** for her valuable suggestions and encouragement which paved way for the successful completion of the project.

I am greatly privileged to express my deep sense of gratitude to the Project Coordinator **Ms.S.Sasikala M.E., (Ph.D)** , Associate Professor, for her continuous support throughout the course.

In particular, I wish to thank and express my everlasting gratitude to the Supervisor Ms**. S.Umamaheswari M.E., (Ph.D)**, Associate Professor for her expert counselling in each and every steps of project work and I wish to convey my deep sense of gratitude to all teaching and non-teaching staff members of ECE Department for their help and cooperation.

Finally, I thank my parents and my family members for giving us the moral support in all of my activities and my dear friends who helped us to endure my difficult times with their unfailing support and warm wishes.

ABSTRACT

A mobile ad hoc network is a collection of nodes with no pre-established infrastructure. As the network management functions are performed by the mobile nodes themselves, every node participating in the network is heavily burdened with transmissions and processing operations for the maintenance of the network, apart from its own intended ones for establishing / ansIring a call. Considering the limited processing ability, storage capacity and most importantly the available battery poIr of the nodes, it is required to minimize the transmission poIr and the amount of data transmitted, for efficient operation. One of the main design constraints in mobile Ad Hoc networks (MANETs) is that they are poIr constrained. Hence, every effort is to be channeled towards reducing poIr. A Secure Energy Saving Dynamic Smyce Routing in MANETs (SESDSR) has been proposed which will efficiently utilize the battery poIr of the mobile nodes in such a way that the network will get more life time and propose a secure routing the packet for reducing routing overhead and secure share the packet in MANETs. A novel rebroadcast delay to determine the rebroadcast order, and then I can obtain the more accurate additional coverage ratio by sensing neighbor coverage knowledge. The proposed system significantly decreases the number of retransmissions so as to reduce the routing overhead, and can also improve the routing performance. The simulation was carried out using the NS-2 network simulator.

CHAPTER I

1. INTRODUCTION

The explosion of wireless communication and mobile devices in recent years has opened the door of research on self-organizing networks that do not require a pre-established infrastructure. Ad hoc wireless networks are comparatively new paradigm in multi-hop wireless networking that is increasingly becoming popular and will become an essential part of the computing environment consisting of infrastructure and infrastructure less mobile networks. The credit for growth of ad hoc network goes to its self organizing and self configuring properties. All nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes.

Routing is one of the key issues in MANETs due to their highly dynamic and distributed nature. Ad hoc routing algorithms broadly can be categorized into pro-active and on-demand routing algorithm.

The on demand routing algorithms initiate to find out the suitable route when a route is requested. The proactive routing algorithm exchanges routing information periodically and generates the routing table in advance of route request. These protocols select the routes based on the metrics of minimum hop count. A mobile node which lies outside the transmission of its specific destination would need to relay its information flow through other mobile nodes. This implies that mobile nodes in Ad Hoc networks bear routing functionality so that they can act both as routers and hosts. In Mobile Ad Hoc networks the nodes are dynamically change their position.

An Ad Hoc network can be used in an area where infrastructures for mobile communication are not available probably due to high deployment costs or disaster destruction.

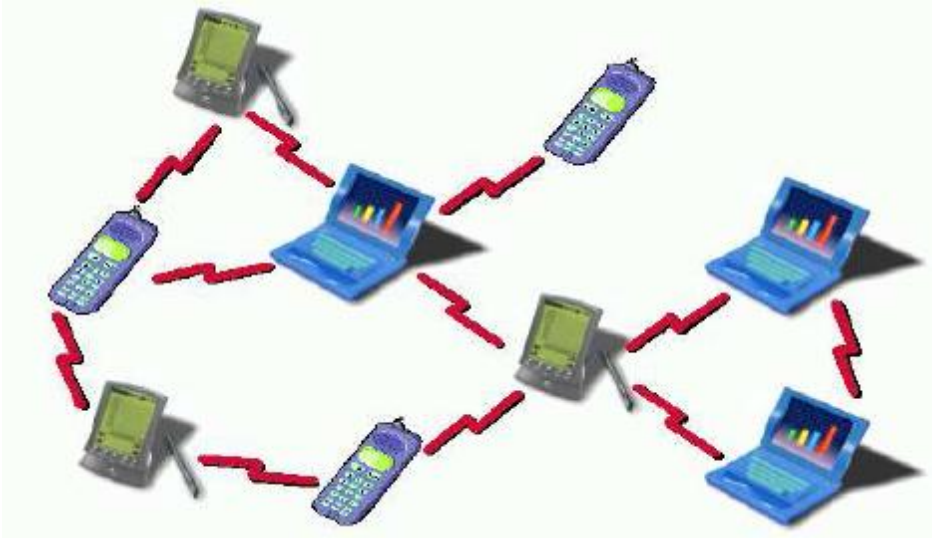

Fig. 1.1 Mobile Ad hoc Network

Figure 1 shows the structure of Mobile Ad hoc Network. The typical application of Ad Hoc networks includes battle field communication, emergency relief and extension of the coverage area of cellular networks. One of the main design constraints in mobile Ad Hoc networks (MANETs) is that they are power constrained. Hence, every effort is to be channeled towards reducing power. More precisely, network lifetime is a key design metric in MANETs. The typical MANET routing protocols (AODV, DSR and DSDV) are shortest routing protocols that is the least hops but do not consider the energy efficiency of the routes. Routing is one of the key issues in MANETs due to their highly dynamic and distributed nature. Ad hoc routing algorithms broadly can be categorized into proactive and on-demand routing algorithm.

1.1 TYPE OF ROUTING PROTOCOLS

Introduction to Routing Protocols Routing protocols between any pair of nodes within an ad hoc network can be difficult because the nodes can move randomly and can also join or leave the network. This means that an optimal route at a certain time may not work seconds later. Routing in a MANET depends on many other factors including topology, selection of routers and location of request initiator and specific underlying characteristics that could serve as a heuristic in finding the path quickly and efficiently. This makes the routing area perhaps the most active research area within the MANET domain. Especially over the last few years, numerous routing

protocols and algorithms have been proposed and their performance under various network environments and traffic conditions closely studied and compared.

- Table Driven Protocols
- On Demand Protocols
- Hybrid Protocols

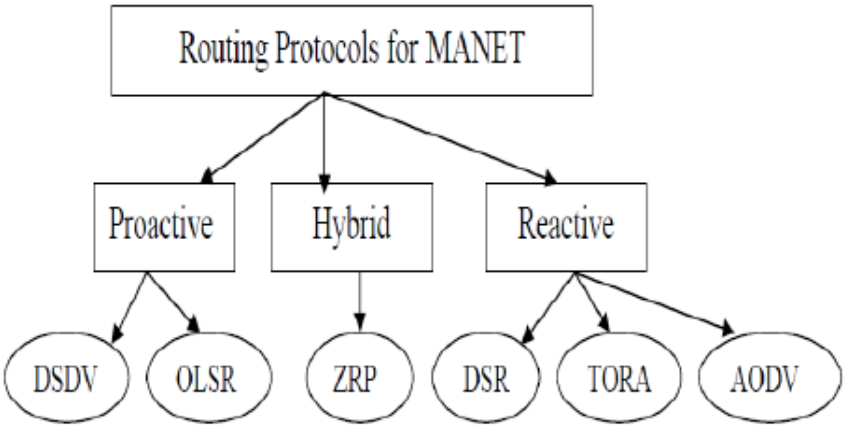

Fig. 1.2 Mobile Ad hoc Network Routing Protocols

1.1.1 Classification of Routing Protocols

a. Table Driven Routing Protocols: The Table Driven Routing Protocol, also known as Proactive Protocols, work out routes in the background independent of traffic demands. Each node uses routing information to store the location information of other nodes in the network and this information is then used to move data among different nodes in the network. These protocols keep a constant overview of the network and this can be a disadvantage as they may react to change in the network topology even if no traffic is affected by the topology modification which could create unnecessary overhead. Even in a network with little data traffic, Table Driven Protocols will use limited resources such as power and link bandwidth therefore they might not be considered an effective routing solution for Ad hoc Networks. Fisheye State Routing and DSDV are the examples of a Table Driven Protocol.

b. On Demand Routing Protocols: On Demand Routing Protocol, also known as Reactive Protocols establish routes between nodes only when they are required to route data packets.

There is no updating of every possible route in the network instead it focuses on routes that are being used or being set up. When a route is required by a source node to a destination for which it does not have route information, it starts a route discovery process which goes from one node to the other until it arrives at the destination or a node in between has a route to the destination. On Demand protocols are generally considered efficient when the route discovery is less frequent than the data transfer because the network traffic caused by the route discovery step is low compared to the total communication bandwidth. This makes On Demand Protocols more suited to large networks with light traffic and low mobility. Examples are: AODV and DSR.

c. Hybrid Routing Protocols: Hybrid routing protocol combine Table Based Routing Protocols with On Demand Routing Protocols. They use distance vectors for more precise metrics to establish the best paths to destination networks and report routing information only when there is a change in the topology of the network. Each node in the network has its own routing zone, the size of which is defined by a zone radius, which is defined by a metric such as the number of hops. Each node keeps a record of routing information for its own zone.

1.2 DYNAMIC SOURCE ROUTING

In the Dynamic Source Routing (DSR) each data packet to be transmitted carries the complete sequence of nodes by which the packets must pass to reach the target. This property is known as source routing, and requires the sender to know the complete route to the destination. The protocol is based on two basic processes: (a) the route discovery process and (b) the route maintenance process. The route discovery process is based on flooding and is used to dynamically discover new routes. The route maintenance process periodically detects and notifies networks topology changes.

In the route discovery procedure a node wishing to establish a route broadcasts a route request (RREQ). Each node receiving the RREQ appends its own address to the packet header and rebroadcasts it. The RREQ flooding terminates when it reaches either the destination or an intermediate node with a route to the destination. In this case a route reply (RREP) containing the series of accumulated addresses is sent back to the source. Upon receiving the RREP, the source node can start transmitting the data packets towards the destination using the route recorded in the RREP. Each node running the DSR protocol is equipped with a route cache

which maintains the routes that a node is aware about. DSR uses the cache intensively in order to reduce the overhead caused by the route discovery.

The major objective of the route maintenance procedure is to detect a broken link and find a new route to the destination. When a node along an established route detects a link disconnection due to the neighbour's movement, it informs the source using the route error (RERR) packet. The source then removes the broken link from its cache and attempts to find a new route to the intended destination.

1.3 ENERGY AWARE METRICS

The majority of energy efficient routing protocols for MANET try to reduce energy consumption by means of an energy efficient routing metric, used in routing table computation instead of the minimum-hop metric There are four possibilities to save power from the devices:

1) Minimal Energy Consumption per Packet The energy consumption is the sum of power consumed on every hop in the path from a packet. The power consumption on a hop is a function of the distance between the neighbor and the load of this hop. So it is interesting to choose a route where the distance between the nodes isn't too long and also it is interesting to take a shorter route so there aren't too many hopes on the route where the power level gets down.

2) Maximize Network Connectivity This metric tries to balance the load on all the nodes in the network. This assumes significance in environment where the network connectivity is to be ensured.

3) Minimum Variance in Node Power Levels This metric proposes to distribute the load among all nodes so that the power consumption remains uniform to all nodes. This problem is very complex when the rate and size of data packets vary. When every node has the same level in power, you can be sure that the network functions longer. Because when there is a node which has to switch off because of the power level the whole network is in danger and it can break down the connectivity between the nodes.

4) Minimize Maximum Node Cost This metric minimizes the maximum cost per nodes for a packet after routing an number of packets or after a specific period. So a node can be blocked for

routing to save battery power. This metrics saves the connectivity from every node. When a node has been used several times for route, it blocks itself to save the power.

Energy aware routing: The aim of energy-aware routing protocols is to reduce energy consumption in transmission of packets between source and a destination, to avoid routing of packets through nodes with low residual energy, to optimize flooding of routing information over the network and to avoid interference and medium collisions. A single node failure in sensor networks is usually unimportant because it does not lead to a loss of sensing and communication coverage whereas ad-hoc networks are oriented towards personal communication and the loss of connectivity to any node is significant.

CHAPTER II

2. LITERATURE SURVEY

Peterson R. L., Ziemer R. E., (1995) [20], Spread-spectrum communications technology was first described on paper by an actress and a musician! In 1941 Hollywood actress Hedy Lamarr and pianist George Antheil described a secure radio link to control torpedos. They received U.S. Patent #2.292.387. The technology was not taken seriously at that time by the U.S. Army and was forgotten until the 1980s, when it became active. Since then the technology has become increasingly popular for applications that involve radio links in hostile environments.

P. Bahl and V.N. Padmanabhan (2000) [2], The proliferation of mobile computing devices and local-area wireless networks has fostered a growing interest in location-aware systems and services. In this paper we present RADAR, a radio-frequency (RF) based system for locating and tracking users inside buildings. RADAR operates by recording and processing signal strength information at multiple base stations positioned to provide overlapping coverage in the area of interest. It combines empirical measurements with signal propagation modeling to determine user location and thereby enable location aware services and applications. We present experimental results that demonstrate the ability of RADAR to estimate user location with a high degree of accuracy.

Ståhlberg M. (2000) [24], A typical wireless sensor node has little protection against radio jamming. The situation becomes worse if energy-efficient jamming can be achieved by exploiting knowledge of the data link layer. Encrypting the packets may help to prevent the jammer from taking actions based on the content of the packets, but the temporal arrangement of the packets induced by the nature of the protocol might unravel patterns that the jammer can take advantage of, even when the packets are encrypted. By looking at the packet inter arrival times in three representative MAC protocols, S-MAC, LMAC, and B-MAC, we derive several jamming attacks that allow the jammer to jam S-MAC, LMAC, and B-MAC energy efficiently. The jamming attacks are based on realistic assumptions. The algorithms are described in detail and simulated. The effectiveness and efficiency of the attacks are examined. In addition, we validate our simulation model by comparing its results with measurements obtained from actual

implementation on our sensor node prototypes. We show that it takes little effort to implement such effective jammers, making them a realistic threat. Careful analysis of other protocols belonging to the respective categories of S-MAC, LMAC, and B-MAC reveals that those protocols are, to some extent, also susceptible to our attacks. The result of this investigation provides new insights into the security considerations of MAC protocols.

Wu S.L., Lin C.Y., Tseng (2002) [31], In a mobile ad-hoc networks (MANET), one essential issue is medium access control (MAC) which addresses how to utilize the radio spectrum efficiently and to resolve potential contention and collision among mobile hosts on using the medium. Existing work is dedicated to using multiple channels and power control to improve the performance of MANET. We investigate the possibility of bringing the concepts of power control and multi-channel medium access together in the MAC design problem in a MANET. Existing protocols only address one of these issues independently. The proposed protocol is characterized by the following features: it follows an "on-demand" style to assign channels to mobile hosts; the number of channels required is independent of the network topology and degree; it flexibly adapts to host mobility; no form of clock synchronization is required; and power control is used to exploit frequency reuse. Power control may also extend battery life and reduce signal interference, both of which are important in wireless communication. Through simulations, we demonstrate the advantage of our new protocol.

Hung W.C., Law K.L.E., Garcia A.L. (2002) [5], This paper proposes a medium access control (MAC) protocol for ad hoc wireless networks that utilizes multiple channels dynamically to improve performance. The IEEE 802.11 standard allows for the use of multiple channels available at the physical layer, but its MAC protocol is designed only for a single channel. A single-channel MAC protocol does not work well in a multi-channel environment, because of the multi-channel hidden terminal problem . Our proposed protocol enables hosts to utilize multiple channels by switching hannels dynamically, thus increasing network throughput. The protocol requires only one transceiver per host, but solves the multi-channel hidden terminal problem using temporal synchronization. Our scheme improves network throughput signifiantly, especially when the network is highly congested. The simulation results show that our protocol successfully exploits multiple hannels to achieve higher throughput than IEEE 802.11. Also, the performance of our protocol is comparable to another multi-hannel MAC protocol that requires

multiple transceivers per host. Since our protocol requires only one transceiver per host, it an be implemented with a hardware complexity comparable to IEEE 802.11.

A. Wood, J. Stankovic, and S. Son (2003) [25], Preventing denial-of-service attacks in wireless sensor networks is difficult primarily because of the limited resources available to network nodes and the ease with which attacks are perpetrated. Rather than jeopardize design requirements which call for simple, inexpensive, mass-producible devices, we propose a coping strategy that detects and maps jammed regions. We describe a mapping protocol for nodes that surround a jammer which allows network applications to reason about the region as an entity, rather than as a collection of broken links and congested nodes. This solution is enabled by a set of design principles: loose group semantics, eager eavesdropping, supremacy of local information, robustness to packet loss and failure, and early use of results. Performance results show that regions can be mapped in 1-5 seconds, fast enough for real-time response. With a moderately connected network, the protocol is robust to failure rates as high as 25 percent.

Noubir G., Lin G (2003) [17], In this paper we investigate the resiliency to jamming of data protocols, such as IP, over WLAN. We show that, on existing WLAN, an adversary can successfully jam data packets at a very low energy cost. Such attacks allow a set of adversary nodes disseminated over an area to prevent communication, partition an ad hoc network, or force packets to be routed over adversary chosen paths. The ratio of the jamming pulses duration to the transmission duration can be as low as 10--4. We investigate and analyze the performance of using various coding schemes to improve the robustness of wireless LANs for IP packets transmission. A concatenated code that is simple to decode and can maintain a low Frame Error Rate (FER) under a jamming effort ratio of 15%. We argue that LDPC codes will be very suitable to prevent this type of jamming. We investigate the theoretical limits by analyzing the performance derived from upper bounds on binary error-control codes. We also propose an efficient anti-jamming technique for IEEE802.11b.

Xu W., Wood T., Trappe W., (2004) [16], Wireless networks are built upon a shared medium that makes it easy for adversaries to launch denial of service (DoS) attacks. One form of denial of service is targeted at preventing sources from communicating. These attacks can be easily accomplished by an adversary by either bypassing MAC-layer protocols, or emitting a radio signal targeted at jamming a particular channel. In this paper we present two strategies that

may be employed by wireless devices to evade a MAC/PHY-layer jamming-style wireless denial of service 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. The second strategy, spatial retreats, is a form of spatial evasion whereby legitimate mobile devices move away from the locality of the DoS emitter. We study both of these strategies for three broad wireless communication scenarios: two-party radio communication, an infrastructured wireless network, and an ad hoc wireless network. We evaluate several of our proposed strategies and protocols through ns-2 simulations and experiments on the Berkeley mote platform.

Acharya M., Thuente D (2005) [1], Abstract It has been shown that reservation based MAC protocols such as 802.11b DCF are susceptible to Intelligent Jammingwherein,a protocol aware jammer,can bring down,the network throughput essentially to zero by using very limited energy, see [1]. We propose and analyze intelligent jamming,techniques based on "misbehaving" MAC level access timings. An additional intelligent jamming,technique based on fakeRTS reservations is proposed in [6] to efficiently disrupt any general reservation based wireless network. [6] also proposes a protocol modification as a counterattack to the above denial of service attack. We instantiate these attacks and counterattacks to an access point based wireless network using 802.11b DCF protocol and perform a simulation in OPNET to study its effect on 802.11b network throughput. Furthermore, we present additional ways to attack the proposed countermeasure,in terms of network congestion. In doing so, we compare the efficiency of these various intelligent jamming,attacks and their counterattacks. Using OPNET simulations, we discuss the relative merits and demerits of the various denial of service attacks.

Z. Xu, W. Trappe, Y. Zhang, and T. Wood (2005) [7], Wireless networks are built upon a shared medium that makes it easy for adversaries to launch jamming-style attacks. These attacks can be easily accomplished by an adversary emitting radio frequency signals that do not follow an underlying MAC protocol. Jamming attacks can severely interfere with the normal operation of wireless networks and, consequently, mechanisms are needed that can cope with jamming attacks. In this paper, we examine radio interference attacks from both sides of the issue: first, we study the problem of conducting radio interference attacks on wireless networks, and second we examine the critical issue of diagnosing the presence of jamming attacks. Specifically, we propose four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how

each method affects the ability of a wireless node to send and receive packets. We then discuss different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack. In particular, we observe that signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. Further, we observe that although by using packet delivery ratio we may differentiate between congested and jammed scenarios, we are nonetheless unable to conclude whether poor link utility is due to jamming or the mobility of nodes. The fact that no single measurement is sufficient for reliably classifying the presence of a jammer is an important observation, and necessitates the development of enhanced detection schemes that can remove ambiguity when detecting a jammer. To address this need, we propose two enhanced detection protocols that employ consistency checking. The first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. Throughout our discussions, we examine the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform.

Salem M., Sarhan A., Abu-Bakr M (2007) [21], Security is one of the most important issues to be considered in the Wireless Local Area Networks (WLANs). There are many weakness points of security in WLANs due its nature. Many security techniques were introduced to solve the available security bugs. However, there are still many bugs that were not solved yet such as Denial Of Service (DOS) attacks. In this paper, a new security technique is proposed that aims to detect the DOS attacks in WLANs and further prevent the detected attackers, in the future, from accessing the network. The proposed technique uses an intruders' database (IDB), which it creates and modifies each time an intruder is detected. This database will be used by the technique to inhibit intruders from bringing the network down by a DOS attack. The simulation results of the proposed technique measure the Probability of Denied Service (PDS) with respect to the number of attacks and the maximum number of connections that access point allows. These results show the effectiveness of this technique in securing the WLAN against the DOS attacks.

Mpitziopoulos A., Gavalas D., Pantziou G (2007) [13], Wireless sensor networks (WSNs) are used in many applications which often include the monitoring and recording of

sensitive information. Hence, their critical importance raises many security concerns. In the context of WSNs, jamming is the type of attack which interferes with the radio frequencies used by network nodes. In the event that an attacker uses a rather powerful jamming source, disruptions of WSNs proper function are likely to occur. As a result, the use of countermeasures against jamming in WSN environments is of immense importance. The main contribution of this article is the discussion of various defence methods against jamming that would allow a WSN to survive and work properly in a hostile jamming environment. Our focus is on frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS), two of the most effective countermeasures against jamming. We suggest the use of a specific FHSS technique in 5 GHz band with 55 frequency channels wherein the channel sequence is generated using a secret word, known only to the sink and the sensor nodes, as a seed. Each channel uses DSSS modulation with 16 bit Pseudo Noise (PN) code, which derives from the same secret word used for FHSS channel generation.

Li M., Koutsopoulos I., Poovendran R (2007) [8], We consider a scenario where a sophisticated jammer jams an area in a single-channel wireless sensor network. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by a monitoring node in the network, and a notification message is transferred out of the jamming region. The jammer is detected at a monitor node by employing an optimal detection test based on the percentage of incurred collisions. On the other hand, the network computes channel access probability in an effort to minimize the jamming detection plus notification time. In order for the jammer to optimize its benefit, it needs to know the network channel access probability and number of neighbors of the monitor node. Accordingly, the network needs to know the jamming probability of the jammer. We study the idealized case of perfect knowledge by both the jammer and the network about the strategy of one another, and the case where the jammer or the network lacks this knowledge. The latter is captured by formulating and solving optimization problems, the solutions of which constitute best responses of the attacker or the network to the worst-case strategy of each other. We also take into account potential energy constraints of the jammer and the network. We extend the problem to the case of multiple

observers and adaptable jamming transmission range and propose a intuitive heuristic jamming strategy for that case.

A.D. Wood, J.A. Stankovic, and G. Zhou, (2007) [26], Jamming is a very effective denial-of-service attack that renders most higher-layer security mechanisms moot - yet it is often ignored in WSN design. We show that an interrupt jamming attack is simple to perpetrate in software using a MICAz mote, is energy efficient and stealthy for the jammer, and completely disrupts communication. Solutions are needed to mitigate this insider threat even if more powerful attackers are not thwarted. We present DEEJAM, a novel MAC-layer protocol for defeating stealthy jammers with IEEE 802.15.4-based hardware, to address this problematic area. It layers four defensive mechanisms to hide communication from a jammer, evade its search, and reduce its impact. Given the difficulty of modeling the physical layer accurately in simulation, we evaluate DEEJAM instead on the MICAz mote. We show the performance of the protocol against successively more complex attacks: interrupt jamming, activity jamming, scan jamming, and pulse jamming. Results show that DEEJAM defeats the otherwise devastating interrupt jammer, and achieves a packet delivery ratio of 88% in the presence of a pulse jammer. To the best of our knowledge, this work is the first to confront multiple types of jamming on common WSN hardware with solutions that are shown empirically to enable continued communication despite an ongoing attack.

Navda V., Bohra A., Ganguly S (2007) [15], 802.11a, b, and g standards were designed for deployment in cooperative environments, and hence do not include mechanisms to protect from jamming attacks. In this paper, we explore how to protect 802.11 networks from jamming attacks by having the legitimate transmission hop among channels to hide the transmission from the jammer. Using a combination of mathematical analysis and prototype experimentation in an 802.11a environment, we explore how much throughput can be maintained in comparison to the maintainable throughput in a cooperative, jam-free environment. Our experimental and analytical results show that in today's conventional 802.11a networks, we can achieve up to 60 % of the original throughput. Our mathematical analysis allows us to extrapolate the throughput that can be maintained when the constraint on the number of orthogonal channels used for both legitimate communication and for jamming is relaxed.

Xu W., Trappe W., Zhang Y (2008) [23], Radio interference, whether intentional or otherwise, represents a serious threat to assuring the availability of sensor network services. As such, techniques that enhance the reliability of sensor communications in the presence of radio interference are critical. In this article, we propose to cope with this threat through a technique called channel surfing, whereby the sensor nodes in the network adapt their channel assignments to restore network connectivity in the presence of interference. We explore two different approaches to channel surfing: coordinated channel switching, in which the entire sensor network adjusts its channel; and spectral multiplexing, in which nodes in a jammed region switch channels and nodes on the boundary of a jammed region act as radio relays between different spectral zones. For coordinated channel switching, we examine an autonomous strategy where each node detects the loss of its neighbors in order to initiate channel switching. To cope with latency issues in the autonomous strategy, we propose a broadcast-assisted channel switching strategy to more rapidly coordinate channel switching. For spectral multiplexing, we have devised both synchronous and asynchronous strategies to facilitate the scheduling of nodes in order to improve network fidelity when sensor nodes operate on multiple channels. In designing these algorithms, we have taken a system-oriented approach that has focused on exploring actual implementation issues under realistic network settings. We have implemented these proposed methods on a testbed of 30 Mica2 sensor nodes, and the experimental results show that channel surfing, in its various forms, is an effective technique for repairing network connectivity in the presence of radio interference, while not introducing significant performance-overhead.

Zhang Z., Wu J., Deng J (2008) [32], In many Medium Access Control (MAC) schemes for wireless networks, an Acknowledgment (ACK) packet is transmitted from the data receiver to the data sender to announce the successful reception of the data packet. Such a protocol requirement may become a system weakness when malicious nodes attack these wireless networks. In this paper, we demonstrate the effects of such a Jamming ACK (JACK) attack to networks employing the popular Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme in IEEE 802.11 DCF. Our study shows that a JACK attacker can easily disrupt the traffic flow between two wireless nodes when it sends out JACK packets at the right time. The benefits of such a JACK attack include low energy consumption by the attacker, attack stealthiness, and great damage to the victim nodes. To mitigate the effects of JACK attacks, we propose in this paper an Extended Network Allocation Vector (ENAV) scheme. Our analysis and

simulations show that the ENAV scheme recovers a significant portion of the lost throughput and reduces the energy drainage of the attacked nodes to 40%.

Khattab S., Mosse D., Melhem R (2008) [6], Multi-radio (multi-interface, multi-channel) 802.11 and sensor networks have been proposed to increase network capacity and to reduce energy consumption, to name only a few of their applications. They are vulnerable, however, to jamming attacks, in which attackers block communication by radio interference or MAC-protocol violation. Two jamming countermeasures have been proposed, namely software-based channel hopping and error-correcting codes. In this paper, we introduce the problem of maximizing network goodput under jamming attacks through a combination of channel hopping and error-correction coding. We describe the solution space and investigate one point thereof, namely *reactive defense against scanning attack*. We develop a Markovian model of the reactive channel-hopping defense against the scanning jamming attack and validate it using simulation experiments. Our results suggest that an adaptive defense, based on our model, would improve the resiliency of multi-radio networks against jamming.

Soreanu P., Volkovich Z., Barzily Z (2008) [23], Wireless sensor networks (WSN) are practical implementations of distributed computing ad-hoc wireless networks. Typically empowered with scarce energy resources and limited computing power, they are mainly used for in situ data acquisition and monitoring of the deployment area. As such, they are susceptible to various forms of jamming, at the physical and data link layer. Of special interest are the moving jammers, which impose added strain on the WSN. We developed a detection protocol that takes into consideration the jammer's behavior and accordingly adopts new routes, in order to maximize the WSN life. We simulated our algorithm, which is an improvement of the well known LEACH energy- efficient routing protocol, vs. the original LEACH. We have found a significant improvement of the WSN lifetime, offering a proved improvement in the resilience of WSN against moving jamming attacks.

Bayraktaroglu E., King C., (2008) [3], In this paper, we study the performance of the IEEE 802.11 MAC protocol under a range of jammers that covers both channel-oblivious and channel-aware jamming. We study two channel-oblivious jammers: a periodic jammer that jams

deterministically at a specified rate, and a memoryless jammer whose signals arrive according to a Poisson process. We also develop new models for channel-aware jamming, including a reactive jammer that only jams non-colliding transmissions and an omniscient jammer that optimally adjusts its strategy according to current states of the participating nodes. Our study comprises of a theoretical analysis of the saturation throughput of 802.11 under jamming, an extensive simulation study, and a testbed to conduct real world experimentation of jamming IEEE 802.11 using GNU Radio and USRP platform. In our theoretical analysis, we use a discrete-time Markov chain analysis to derive formulae for the saturation throughput of IEEE 802.11 under memoryless, reactive and omniscient jamming. One of our key results is a characterization of optimal omniscient jamming that establishes a lower bound on the saturation throughput of 802.11 under arbitrary jammer attacks. We validate the theoretical analysis by means of Qualnet simulations. Finally, we measure the real-world performance of periodic and memoryless jammers using our GNU radio jammer prototype.

Nguyen H., Pongthawornkamol T (2009) [16], We consider the problem of identifying the insider-based attacks in the form of jammers in multi-channel wireless networks, where jammers have the inside knowledge of frequency hopping patterns and any protocols used in the wireless network. We propose a novel technique, called “alibi”, to identify the insider-based jammers in multi-channel wireless networks. Alibi is a form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime in question was committed. Starting from such a simple concept, we develop an alibi framework to cope with insider-based jamming attackers in various situations including single jammer, lossy channels, non-colluding jammers and colluding jammers. We evaluate the framework according to several properties such as accuracy, detection time & network performance in ns2 simulation and analysis. The overall results of these protocols show a promising research direction to deal with insider-based jamming attacks. unpublished.

Othman J.B., Hamieh A (2009) [18], Mobile ad hoc networks (MANETs) are dynamic mobile networks that can be formed in the absence of any pre-existing communication infrastructure. MANETs are vulnerable to jamming attack due to their salient characteristics. The objective of a jammer is to interfere with legitimate wireless communications, and to degrade the overall QoS of the network. In this paper, we propose a new method to react at jamming attacks.

The military has long dealt with jamming by using frequency-hopping spread spectrum communication. Unlike frequency hopping that takes place at the PHY layer, our purpose takes place at the MAC layer.

Reese K.W. Salem A (2009) [21], Ad-Hoc Sensory Networks present a cheap and efficient way to collect data through wireless transmissions between sensors. These transmissions create new problems that need to be overcome in order to insure that the data being collected is reliable. This paper surveys the latest research in Jamming Avoidance in Ad-Hoc Sensory Networks.

K. Pelechrinis, I. Koutsopoulos, I. Broustis (2009) [19], Jamming attacks have become prevalent during the last few years, due to the shared nature and the open access to the wireless medium. Finding the location of a jamming device is of great importance for restoring normal network operations. After detecting the malicious node we want to find its position, in order for further security actions to be taken. Our goal in this paper is the design and implementation of a simple, lightweight and generic localization algorithm. Our scheme is based on the principles of the gradient descent minimization algorithm. The key observation is that the Packet Delivery Ratio (PDR) has lower values as we move closer to the jammer. Hence, the use of a gradient-based scheme, operating on the discrete plane of the network topology, can help locate the jamming device. The contributions of our work are the following: (a) We demonstrate, through analysis and experimentation, the way that the jamming effects propagate through the network in terms of the observed PDR. (b) We design a distributed, lightweight jammer localization system which does not require any modifications to the driver/firmware of commercial NICs. (c) We implement and evaluate our localization system on our 802.11 indoor testbed. An attractive and important feature of our system is that it does not rely on special hardware.

H. Liu, Z. Liu, Y. Chen (2010)[10], Wireless communication is susceptible to radio interference and jamming attacks, which prevent the reception of communications. Most existing anti-jamming work does not consider the location information of radio interferers and jammers. However, this information can provide important insights for networks to manage its resource in different layers and to defend against radio interference. In this paper, the authors investigate issues associated with localizing jammers in wireless networks. In particular, they formulate the jamming effects using two jamming models: region-based and Signal-to-Noise-Ratio (SNR)-

based; and they categorize network nodes into three states based on the level of disturbance caused by the jammer. By exploiting the states of nodes, they propose to localize jammers in wireless networks using a virtual-force iterative approach.

Z. Liu, H. Liu, W. Xu (2010)[9], Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defense strategies. Thus, in this paper, we focus on developing mechanisms to localize a jammer. We first conduct jamming effect analysis to examine how a hearing range, e.g., the area from which a node can successfully receive and decode the packet, alters with the jammer's location and transmission power. Then, we show that the affected hearing range can be estimated purely by examining the network topology changes caused by jamming attacks. As such, we solve the jammer location estimation by constructing a least-squares problem, which exploits the changes of the hearing ranges. Compared with our previous iterative-search-based virtual force algorithm, our proposed hearing-range-based algorithm exhibits lower computational cost (i.e., one-step instead of iterative searches) and higher localization accuracy.

Nahrstedt K., Campbell R.H., Vaidya N.H (2010) [14], We consider the problem of identifying insider-based attacks in the form of jammers in multi-channel wireless networks, where jammers have the inside knowledge of frequency hopping patterns and any protocols used in the wireless network. We propose a novel technique, called "alibi", to identify the insider-based jammers in multi-channel wireless networks. Alibi is a form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime in question was committed. Starting from such simple concept, we develop an alibi framework to cope with insider-based jamming attackers in various situations including single/multiple jammer and lossy channels. We evaluate the framework according to several properties such as accuracy, detection time and network performance via TOSSIM simulation and analysis. The overall results of these protocols show a promising research direction to deal with insider-based jamming attacks.

Lee E.K., Oh S.Y., Gerla M (2010) [7], Jamming attacks have been recently studied as wireless security threats disrupting reliable RF communication in a wireless network. By emitting noise-like signals arbitrarily on the shared wireless medium, a jammer can easily disturb

the network. Countermeasures such as Frequency-Hopping Spread Spectrum enable nodes to avoid the jamming attacks by hopping over multiple channels. However, these solutions require pre-key establishment before data transmission, which in turns introduces several constraints. In order to solve the problem, this paper proposes a novel Quorum Rendezvous Channel Hopping (QRCH) scheme. Nodes are able to hop over random channels independently, bypassing the need for pre-key establishment. Furthermore, by using a quorum system, nodes are guaranteed to meet within a bounded time to exchange pending messages. The scheme also enables nodes to transmit packets to multiple receivers simultaneously. We validate the proposed scheme via extensive simulations and present its robustness and efficiency.

H. Liu, Z. Liu, Y. Chen, (2011) [11], Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defense strategies. In this paper, we focus on developing mechanisms to localize a jammer by exploiting neighbor changes. We first conduct jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free-space model. Then, we show that a node's affected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks and thus, we can perform the jammer location estimation by solving a least-squares (LSQ) problem that exploits the changes of communication range. Compared with our previous iterative-search-based virtual force algorithm, our LSQ-based algorithm exhibits lower computational cost (i.e., one step instead of iterative searches) and higher localization accuracy. Furthermore, we analyze the localization challenges in real systems by building the log-normal shadowing model empirically and devising an adaptive LSQ-based algorithm to address those challenges. The extensive evaluation shows that the adaptive LSQ-based algorithm can effectively estimate the location of the jammer even in a highly complex propagation environment.

T. Cheng, P. Li, and S. Zhu (2011) [4], Jamming attack is one of the most severe attacks in wireless sensor networks (WSNs). While existing countermeasures mainly focus on designing new communication mechanisms to survive under jamming, an alternative solution is to first localize the jammer(s) and then take necessary actions. In this work, we solve a multi-jammer localization problem, where multiple jammers launch collaborative jamming attacks. We

develop an x-rayed jammed-area localization (X-ray) algorithm which skeletonizes jammed areas and estimates the jammer locations based on bifurcation points on skeletons of jammed areas. Our extensive simulation results demonstrate that with one run of the algorithms, X-ray is efficient in localizing multiple jammers in WSN with small errors.

J. Yang, Y. Chen, and J. Cheng (2011)[30], Location estimation is a critical step for many location-aware applications. To obtain location information, localization methods employing received signal strength (RSS) are attestative since it can reuse the existing wireless infrastructure for localization. Among the large class of localization schemes, RSS-based lateration methods have the advantage of providing closed-form solutions for mathematical analysis as compared to heuristic-based localization approaches. However, the localization accuracy of RSS-based lateration methods are significantly affected by the unpredictable setup in indoor environments. To improve the applicability of RSS-based lateration methods in indoors, we propose two approaches, regression-based and correlation-based. The regression-based approach uses linear regression to discover a better fit of signal propagation model between RSS and the distance, while the correlation-based approach utilizes the correlation among RSS in local area to obtain more accurate signal propagation. Our results using both simulation as well as real experiments demonstrate that our improved methods outperform the original RSS-based lateration methods significantly.

Z. Liu, H. Liu, W. Xu, (2012) [9], Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defense strategies. In this paper, we focus on developing mechanisms to localize a jammer by exploiting neighbor changes. We first conduct jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free-space model. Then, we show that a node's affected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks and thus, we can perform the jammer location estimation by solving a least-squares (LSQ) problem that exploits the changes of communication range. Compared with our previous iterative-search-based virtual force algorithm, our LSQ-based algorithm exhibits lower computational cost (i.e., one step instead of iterative searches) and higher localization accuracy. Furthermore, we analyze the localization challenges in real systems by building the

log-normal shadowing model empirically and devising an adaptive LSQ-based algorithm to address those challenges. The extensive evaluation shows that the adaptive LSQ-based algorithm can effectively estimate the location of the jammer even in a highly complex propagation environment.

CHAPTER III

3. EXISTING SYSTEM

Jamming and radio interference are known threats and have attracted much attention. Traditionally, jamming is addressed through conventional PHY-layer communication techniques, e.g. spreading techniques. Countermeasures for coping with jamming in commodity wireless networks have been intensively investigated. Defense strategies include the use of error correcting codes to increase the likelihood of decoding corrupted packets, channel hopping to adapt the working channel to escape from jamming, and wormhole-based anti-jamming techniques. Range-based algorithms involve estimating distance to anchor points with known locations by utilizing the measurement of various physical properties, such as RSS.

3.1 Nodes' Hearing Ranges based jammer detection

Proposed a hearing-range-based localization scheme that also exploits the network topology changes caused by jamming attacks. In particular, to quantify the network topology changes, we introduced the concept of a node's hearing range, an area from which a node can successfully receive and decode the packet. We have discovered that a jammer may reduce the size of a node's hearing range, and the level of changes is determined by the relative location of the jammer and its jamming intensity. Therefore, instead of searching for the jammer's position iteratively, we can utilize the hearing range to localize the jammer in one round, which significantly reduces the computational cost yet achieves better localization performance than prior work.

3.2 Jammer detection based on Signal Strength

One seemingly natural measurement that can be employed to detect jamming is signal strength, or ambient energy. The rationale behind using this measurement is that the signal strength distribution may be affected by the presence of a jammer. In practice, since most commodity radio devices do not provide signal strength or noise level measurements that are calibrated (even across devices from the same manufacturer), it is necessary for each device to

employ its own empirically gathered statistics in order to make its decisions. Each device should sample the noise levels many times during a given time interval. By gathering enough noise level Measurements during a time period prior to jamming, network devices can build a statistical model describing normal energy levels in the network.

3.3 Jammer detection based on generic localization algorithm

Our goal is to exploit the inherent propagation characteristics of the wireless channel in order to expose the presence of jamming devices and localize them. The jamming attacker might be able to hide itself from all but the wireless channel's propagation characteristics. The attributes of the jamming signals (and in particular their spatial properties) can affect measurable attributes (such as the PDR) to varying degrees in different parts of the network, thereby revealing important information with regards to the location of the malicious device. significant performance improvement can be attained with the elimination of the local minima sensitivity. Thus, intelligent ways that can help avoid local-minima regions are needed. One possible way could be to gather all the information with regards to PDR (collected by each legitimate node) and try to fuse these data. A majority rule could subsequently be used in order to decide upon the location of jammer(s). However, since dense-deployment regions might contain most of the nodes, the majority of the votes might still point to a local minimum. Therefore, what is required is a way to increase the confidence of the users' decisions with regards to the location of the jammer. In particular, nodes need to be able to effectively distinguish between jamming interference and heavy, legitimate interference.

3.4 Neighbor Changes for Jammer Localization

Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defense strategies. In this paper, we focus on developing mechanisms to localize a jammer by exploiting neighbor changes. We first conduct jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free space model. Then, we show that a node's affected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks and thus, we can perform the jammer location estimation by solving a least-squares (LSQ) problem that exploits the

changes of communication range. Compared with our previous iterative-search-based virtual force algorithm, our LSQ based algorithm exhibits lower computational cost (i.e., one-step instead of iterative searches) and higher localization accuracy.

Furthermore, we analyze the localization challenges in real systems by building the log-normal shadowing model empirically and devising an adaptive LSQ-based algorithm to address those challenges.

3.5 Jammer detection based on virtual-force iterative approach

Wireless communication is susceptible to radio interference and jamming attacks, which prevent the reception of communications. Most existing anti-jamming work does not consider the location information of radio interferers and jammers. However, this information can provide important insights for networks to manage its resource in different layers and to defend against radio interference. In this paper, we investigate issues associated with localizing jammers in wireless networks. In particular, we formulate the jamming effects using two jamming models: region-based and signal-to-noise-ratio(SNR)- based; and we categorize network nodes into three states based on the level of disturbance caused by the jammer. By exploiting the states of nodes, we propose to localize jammers in wireless networks using a virtual-force iterative approach. The virtual-force iterative localization scheme is a range-free position estimation method that estimates the position of a jammer iteratively by utilizing the network topology. We have conducted experiments to validate our SNR-based jamming model and performed extensive simulation to evaluate our approach.

3.6 Jammer detection based RSS Techniques

Location estimation is a critical step for many location-aware applications. To obtain location information, localization methods employing received signal strength (RSS) are attestative since it can reuse the existing wireless infrastructure for localization. Among the large class of localization schemes, RSS-based lateration methods have the advantage of providing closed-form solutions for mathematical analysis as compared to heuristic-based localization approaches. However, the localization accuracy of RSS-based lateration methods are significantly affected by the unpredictable setup in indoor environments. To improve the applicability of RSS-based lateration methods in indoors, we propose two approaches,

regression-based and correlation-based. The regression-based approach uses linear regression to discover a better fit of signal propagation model between RSS and the distance, while the correlation-based approach utilizes the correlation among RSS in local area to obtain more accurate signal propagation.

3.7 Drawbacks

- Most jammers start to disturb network communication after network deployment
- No detailed prior knowledge about the jammers' transmission power is available.
- No detailed prior knowledge about the jammers' transmission power is available.
- Jamming and radio interference are known threats and have attracted much attention. Traditionally, jamming is addressed through conventional PHY-layer communication techniques, e.g. spreading techniques. Those PHY-layer techniques provide resilience to interference at the expense of advanced transceivers.

- Countermeasures for coping with jamming in commodity wireless networks have been intensively investigated. Defense strategies include the use of error correcting codes to increase the likelihood of decoding corrupted packets, channel hopping to adapt the working channel to escape from jamming, and wormhole-based anti-jamming techniques.

- Received signal strength (RSS) is an attractive approach because it can reuse the existing wireless infrastructure. Based on the localization methodology, the localization algorithms can be categorized into range-based and range-free.

- Range-based algorithms involve estimating distance to anchor points with known locations by utilizing the measurement of various physical properties, such as RSS.

- Localize the jamming by measuring packet delivery rate (PDR) and performing gradient decent search.

- Virtual force iterative localization algorithm (VFIL).

- Lease-squares-based algorithm that leverages the change of hearing range caused by jamming. Aforementioned algorithms can only localize one jammer and may fail to yield jammers' positions when multiple ones are present.

CHAPTER IV

4. PROPOSED SYSTEM

4.1 ENERGY SAVING DYNAMIC SOURCE ROUTING

In DSR algorithm, when a node receives a Route Request of which it is not on final recipient, before forwarding, it broadcasts to neighbouring nodes. It waits for a time interval pseudo random selected from uniform distribution of probabilities between 0 and constant "broadcast Jitter". The idea behind SESDSR is that this delay, instead of being random, should be inversely proportional to a level of energy residual of node in that moment. In this way the first RREQ that will come to node D(hypothetical destination) will be the one which was channeled through the best route from the overall energy point of view in the sense of the sum of energy levels of the intermediate nodes and maximum comparisons to all other possible paths from S(source) to D(destination).Consequently, the total delay between the sending of the RREQ by S and receiving by D is minimum. Despite these changes it is aimed at maintaining the connectivity between nodes not directly communicating. The SESDSR does not guarantee that S will always choose the best absolute path from the energy point of view in an element where it remains probabilistic algorithm. So, if there are two similar paths in terms of energy, despite RREQ arrivals to D before sending of the corresponding RREP containing the path better from the energy point of view is delayed more than another RREP containing path slightly less favourable.

In the traditional DSR algorithm, once a certain path is chosen for sending a stream of packets to a certain destination it tends to be used until one or more nodes that composing are no longer available (consume all their energy, moving outside the range of neighbouring nodes etc...). The difference in consumption changes from NIC to NIC but the otcl class "Energy Model" allows you to specify these values in phase of creation of nodes. Since a node consumes more energy in transmission and reception. The phenomenon may not be desirable. This is so because some of these nodes could have data to transmit and due to lack of energy would not be able to do so. It is desirable to maintain a balance in the energy consumption of nodes. The consequent loss connection which sooner or later leads to the division of the network into two or

more partitions not communicating. To end this, it is introduced a second enhancement for DSR in which the node accepts the packet depending on certain threshold percentage of initial energy. Think of this process as a sort of "survival instinct" of each node when it reaches a low level of energy.

4.1.1 Route Discovery: This mechanism is launched whenever a node wishes to send or contact a destination node which isn't in its transmission range therefore it must obtain a route to that node by launching the Route discovery mechanism. Figure shows the Route discovery mechanism. Normally the sender must first search this route in its route cache if there is no route it proceeds as follow: It creates a route request packets containing its address and the address of the destination node then it broadcast this packet to all its neighbors using flooding. Each neighbour when receiving this request consults its cache to find an eventual route to this destination to be returned back to the sender otherwise it rebroadcast the same route request to all its neighbours after adding its address to the header of the route request and learns from this request information to be added to its cache. If the node has already treated this route request it ignores the new received request by verifying its sequence number since each route request is identified by a unique sequence number. The same procedure is executed by each neighbouring node until the route request arrives to destination which adds its address at the end of the header and sends a route reply.

4.1.2 Route Reply: The Route reply mechanism. This procedure is executed by a node after receiving a route request destined to him thus this node executes the following actions:

4.1.3 Route Maintenance*:* When forwarding a packet each intermediate node is responsible for confirming that the packet is correctly received by the next node. Whenever this number of attempts was reached this node consider this link as broken than it deletes each route containing this link from its cache than it generates a route error packet to inform the source node and all intermediate nodes about this link failure in the same way each intermediate node deletes all routes containing this route until the route error packet arrives to its destination which chooses to launch a new route request or to find a new route in its route cache.

4.1.4 Route Cache: The route cache in DSR is used to maintain frequently used routes in order to avoid new route discovery mechanism which consumes lot of network resources in the way that each new discovered route is saved in the route cache of the corresponding node for future use, a node can also learns from route request to add new routes to its cache it also learns from route error packets to update its cache.

4.2 SECURE ROUTING

Encryption is the act of encoding text so that others cannot understand the content of the text. Encryption has long been the field of spies and diplomats, but recently it has moved into the public interest with the concern of the protection of electronic transmissions data and digitally stored data. Standard encryption techniques usually have two basic defects: A secure channel must be established at some point so that the sender may exchange the decrypting key with the receiver; and there is no assurance that sent a given message. Public key cryptography has rapidly grown in popularity (and controversy, see, for example, discussions of the Clipper chip on the archives given below) because it offers a very secure and reliable encryption method that addresses these concerns. In a traditional cryptosystem in order to make sure that nobody, except the intended recipient, decrypts the message, the people involved had to endeavor to keep the key secret. In public-key cryptography, it solves one of the most annoying problems of all prior cryptography i.e., the necessity of establishing a secure channel for the exchange of the key. In asymmetric cryptography, RSA is an algorithm for public-key cryptography. RSA is the first algorithm known to be appropriate for signing as well as encryption, and was one of the first great progresses in public key cryptography. RSA is broadly used in electronic commerce protocols, and is supposed to be secure given sufficiently long keys and the use of up-to-date implementations.

4.3 BLOCK DIAGRAM

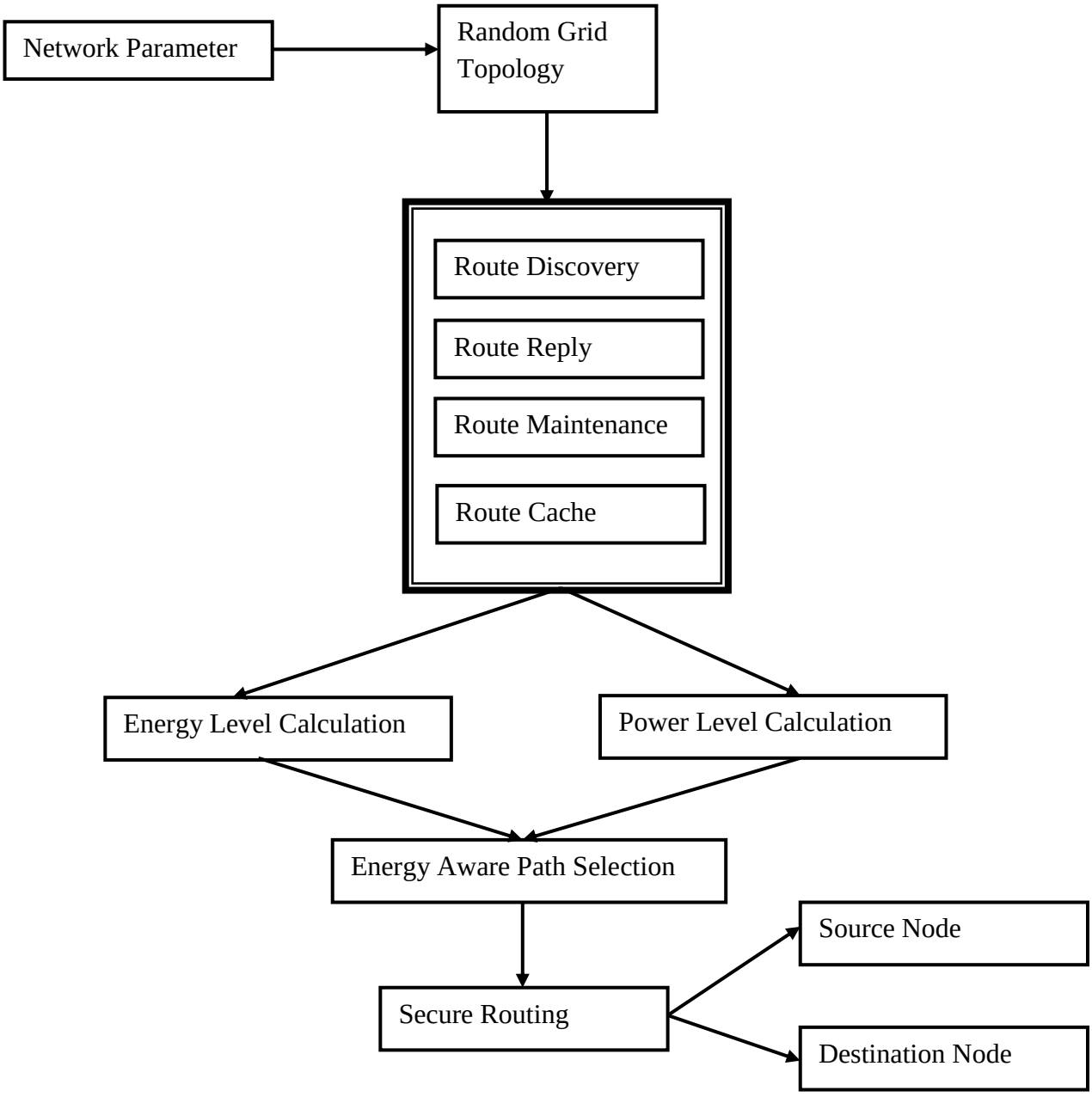

Fig 4.1 Block diagram of proposed system

4.4 WORKING

4.4.1 Energy Saving Dynamic Source Routing

Step 1: If the Source node S wants to send data to the destination node D, it will first send REQ message to all its neighbour nodes.

Step 2 When neighbour nodes receive REQ message they will check their Route_Cache, if this packet's ID is already in their Route_Cache then packet will be discarded.

Step 3 Otherwise, node will calculate its power by using: Pnew = Ptx - Pr + Pth + Pm + Pover and send this value as a reply to source node.

Step 4 Source node will calculate the mean value of all the values of Pnew of all the nodes and send a RREQ message to the node whose Pnew value is nearest to the mean value.

Step 5 When the node receives a RREQ message it will send REQ message to its own neighbours and this process will be continued till the destination node reaches.

Step 6 When destination node will receive the RREQ message it will send the RREP message back with the same route.

Step 7 RREP process is same as in traditional DSR.

4.4.2 Secure Routing

The RSA algorithm involves three basic steps i.e., key generation, encryption and decryption.

Step 1: Key Generation

RSA involves a public and a private key**.** The public key is known to everyone and is used for encryption of messages. Messages encrypted with the public key can only be decrypted using the private key of the user only i.e., confidential. The public and private keys for the RSA

algorithm can be generated in the following way: Choose two distinct prime numbers p and q. Note that the integers p and q should be chosen unvaryingly at random and should be of similar bit-length. Prime integers can be efficiently selected using a primality test.

1. Compute $n = pq$ where n is used as the modulus for both the public and private keys

2. Compute $\varphi(pq) = (p - 1)(q - 1)$ where φ is Euler's totient function.

3. Choose an integer e such that $1 < e < \varphi(pq)$, and e and $\varphi(pq)$ share no divisors other than 1 i.e. e and $\varphi(pq)$ are coprime.

- e is released as the public key exponent.
- e having a short bit-length and small Hamming weight results in more efficient encryption. However, small values of e (such as $e = 3$) have been shown to be less secure in some settings.

4. Determine d (using modular arithmetic) which satisfies the congruence relation.

$$de = 1(mod\varphi(pq) \qquad (1)$$

- Stated differently, $ed - 1$ can be evenly divided by the quotient $(p - 1)(q - 1)$

- This is often computed using the extended Euclidean algorithm.
- d is kept as the private key exponent

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the private (or decryption) exponent d which must be kept secret.

Step 2: Encryption

Destination node broadcasts its public key (n,e) to Source node and keeps the private key secret. Then source **S** wants to send message M to Destination D It first converts M into an integer $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme. It then computes the cipher text c corresponding to:

$$c = m^e \bmod n \qquad (2)$$

This can be done rapidly using the method of exponentiation by squaring. Source **S** then transmits *c* to Destination D.

Step 3: Decryption

Destination can decrypt ***M*** from *c* by using his private key exponent *d* by the following computation:

$$c^d = m(\text{mod } n) \qquad (3)$$

Given ***M***, Destination can recover the original message **M** by reversing the padding scheme.

Example of RSA Algorithm

Example of RSA with small numbers: *p* = 47, *q = 71*, compute *n = pq = 3337*

Compute phi = 46 * 70 = 3220

Let *e* be 79, compute d = *79-1 mod 3220 = 1019*

Public key is *n* and *e*, private key *d*, discard *p* and *q*.

Encrypt message *m = 688, 68879 mod 3337 = 1570 = c.*

Decrypt message c = *1570, 15701019 mod 3337 = 688 = m.*

Thus RSA is very practical algorithm in order to obtain the security aware AODV protocol as it uses both the public key as well as the private key.

CHAPTER V

5. NS2 SIMULATION TOOL

5.1 FRONT END NETWORK SIMULATOR (NS)

Network simulator 2 is used as the simulation tool in this project. NS was chosen as the simulator partly because of the range of features it provides and partly because it has an open source code that can be modified and extended. There are different versions of NS and the latest version is ns-2.1b9a while ns-2.1b10 is under development Network simulator (NS) is an object–oriented, discrete event simulator for networking research. NS provides substantial support for simulation of TCP, routing and multicast protocols over wired and wireless networks. The simulator is a result of an ongoing effort of research and developed. Even though there is a considerable confidence in NS, it is not a polished product yet and bugs are being discovered and corrected continuously.

NS is written in C++, with an OTcl1 interpreter as a command and configuration interface. The C++ part, which is fast to run but slower to change, is used for detailed protocol implementation. The OTcl part, on the other hand, which runs much slower but can be changed very fast quickly, is used for simulation configuration. One of the advantages of this split-language program approach is that it allows for fast generation of large scenarios. To simply use the simulator, it is sufficient to know OTcl. On the other hand, one disadvantage is that modifying and extending the simulator requires programming and debugging in both languages.

NS can simulate the following:

1. **Topology:** Wired, wireless
2. **Sheduling Algorithms:** RED, Drop Tail,
3. **Transport Protocols:** TCP, UDP
4. **Routing:** Static and dynamic routing
5. **Application:** FTP, HTTP, Telnet, Traffic generators

5.1.1 User's View Of Ns-2

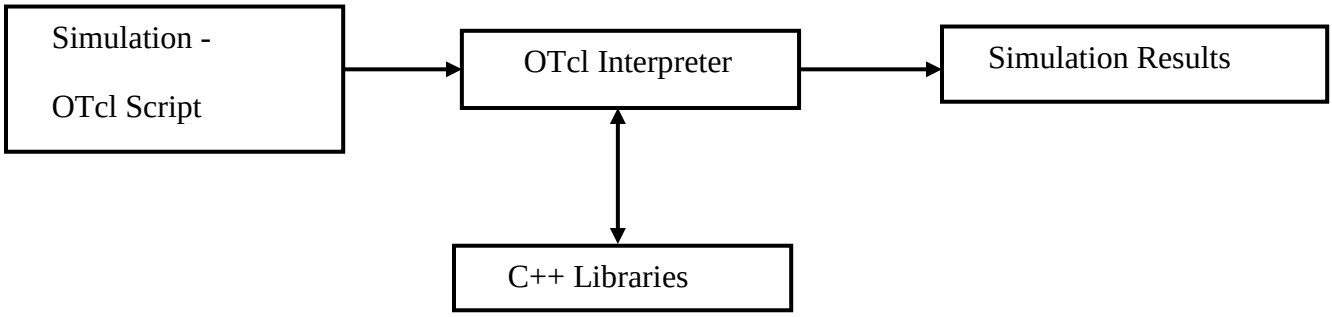

Figure 5.1 Block diagram of Architecture of NS-2

5.1.2 Network Components

This section talks about the NS components, mostly compound network components. Figure 5.1 shows a partial OTcl class hierarchy of NS, which will help understanding the basic network components.

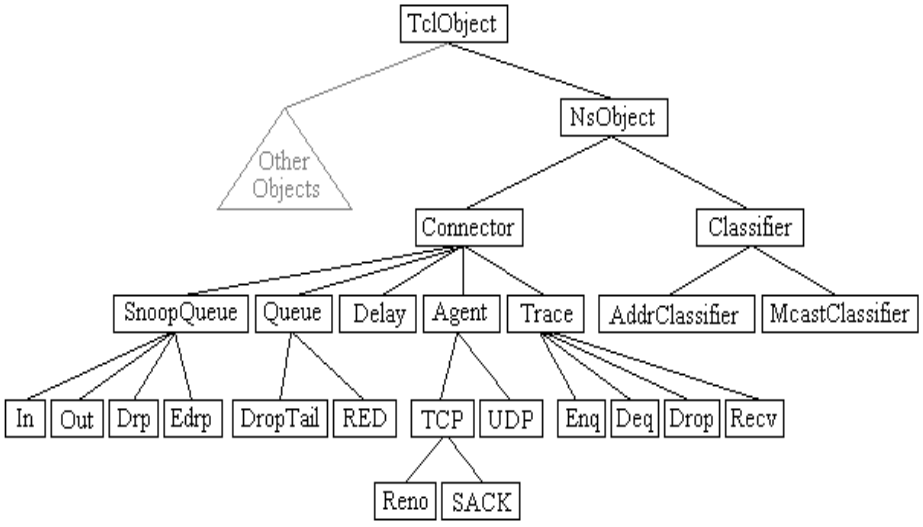

Figure 5.2 OTcl Class Hierarchy

The root of the hierarchy is the TclObject class that is the super class of all OTcl library objects (scheduler, network components, timers and the other objects including NAM

related ones). As an ancestor class of TclObject, NsObject class is the super class of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links. The basic network components are further divided into two subclasses, Connector and Classifier, based on the number of the possible output DATA paths. The basic network and objects that have only one output DATA path are under the Connector class, and switching objects that have possible multiple output DATA paths are under the Classifier class.

5.1.3 Class Tcl

The class Tcl encapsulates the actual instance of the OTcl interpreter and provides the methods to access and communicate with that interpreter, code. The class provides methods for the following operations:

1.obtain a reference to the Tel instance

2.invoke OTcl procedures through the interpreter

3.retrieve, or pass back results to the interpreter

4.report error situations and exit in an uniform manner

5.store and lookup "TclObjects"

6.acquire direct access to the interpreter.

5.1.3.1 Obtain a Reference to the class Tcl instance

A single instance of the class is declared in -tclcl/Tcl.cc as a static member variable. The statement required to access this instance is Tel& tel = Tcl::instance();

5.1.3.2 Invoking OTcl Procedures

There are four different methods to invoke an OTcl command through the instance, tcl. They differ essentially in their calling arguments. Each function passes a string to the interpreter that then evaluates the string in a global context. These methods will return to the caller if the interpreter returns TCL_OK. On the other hand, if the interpreter returns TCL_ERROR, the methods will call tkerror{}. The user can overload this procedure to selectively disregard certain types of errors.

1. **Passing Results to/from the Interpreter :** When the interpreter invokes a C++ method, it expects the result back in the private member variable, tcl-> result.
2. **Error Reporting and Exit:** This method provides a uniform way to report errors in the compiled code.

5.1.4 Command Methods: Definition And Invocation

For every TclObject that is created, ns establishes the instance procedure,cmd{}, as a hook to executing methods through the compiled shadow object. The procedure cmd{} invokes the method command() of the shadow object automatically, passing the arguments to cmd{} as an argument vector to the command() method. The user can invoke the cmd {} method in one of two ways, by explicitly invoking the procedure, specifying the desired operation as the first argument, or implicitly, as if there were an instance procedure of the same name as the desired operation. Most simulation scripts will use the latter form. Consider the distance computation in SRM is done by the compiled object. It is often used by the interpreted object. It is usually invoked as $srmObject distance? (agentAddress)If there is no instance procedure called distance? the interpreter will invoke the instance procedure unknown{}, defined in the base class TclObject. The unknown procedure then invokes $srmObject cmd distance? (agentAddress) to execute the operation through the compiled object's command() procedure. The user could explicitly invoke the operation directly. One reason for this might be to overload the operation by using an instance procedure of the same name.

The function is called with two arguments. The first argument (argc) indicates the number of arguments specified in the command line to the interpreter. The command line arguments vector (argv) consists of argv[0] contains the name of the method, "cmd" and argv[1] specifies the desired operation. If the user specified any arguments, then they are placed in argv[2...(argc - 1)]. The arguments are passed as strings. They must be converted to the appropriate data type.If the operation is successfully matched, the match should return the result of the operation, command () itself must return either TCL_OK or TCL_ERROR to indicate success or failure as its return code. If matched in this method, it must invoke its parent's command method, and return the corresponding result. This permits the user to conceive of operations as having the same inheritance properties as instance procedures or compiled methods. In the event that this command method is defined for a class with multipleinheritance, one of two implementations

can be chosen Either they can invoke one of the parent's command method, and return the result of that invocation. They can each of the parent's command methods in some sequence, and return the result of the first invocation that is successful. If none of them are successful, then they should return an error.

5.1.5 Mobile Networking In Ns

The wireless model essentially consists of the Mobile Node at the core with additional supporting features that allows simulations of multi-hop ad-hoc networks, wireless LANs etc. The Mobile Node object is a split object. The C++ class Mobile Node is derived from parent class Node. A Mobile Node thus is the basic Node object with added functionalities of a wireless and mobile node like ability to move within a given topology, ability to receive and transmit signals to and from a wireless channel etc. A major difference between them is that a mobile Node is not connected by means of Links to other nodes or mobile nodes.

Mobile Node is the basic nsNode object with added functionalities like movement, ability to transmit and receive on a channel that allows it to be used to create mobile, wireless simulation environments. The class Mobile Node is derived from the base class Node. The four ad-hoc routing protocols that are currently supported are, Dynamic Source Routing (DSR), Temporally ordered Routing Algorithm (TORA) and Adhoc On-demand Distance Vector (AODV).

The general structure for defining a mobile node in ns2 is described as follows:

$ns node-config -adhocRouting $opt (adhocRouting)

-IIType $opt (II)

-macType $opt (mac)

-ifqType $opt (ifq) -ifqLen $opt (ifqlen)

-antType $opt (ant)

-proplnstance [new $opt (prop) -phyType $opt (netif)

-channel [new $opt (chan)]

-topolnstance $topo

-wiredRouting OFF

-agent Trace ON

-router Trace OFF

-macTrace OFF

The above API configures for a mobile node with all the given values of ad hoc-routing protocol, network stack, channel, topography, propagation model, with wired routing turned on or off (required for wired-cum-wireless scenarios) and tracing turned on or off at different levels (router, mac, agent).

5.2 FEATURES

- Protocols: TCP, UDP, HTTP, Routing algorithms etc
- Traffic Models: CBR, VBR, Web etc
- Error Models: Uniform, bursty etc
- Radio propagation, Mobility models
- Energy Models
- Topology Generation tools
- Visualization tools
- Extensibility

CHAPTER VI

6. EXPERIMENTAL RESULT

The evaluate the performance of SESDSR mechanism compared against pure DSR, MDR and LEAR in a dense network scenario and a sparse network scenario. Here analyzed the energy consumption behavior of the four mechanisms. Here mainly concentrate on the node energy value, i.e., the time it takes for a node to stop working due to lack of battery capacity. To evaluate how the different layers affect the total energy consumption we also classify the total energy spent depending on the packet type (Application, Routing and MAC). Finally, we also study how security activities contribute to the total energy expenditure. For the purpose of investigating the effect of overhearing, we repeated all simulation by considering the energy cost due to the overhearing activities.

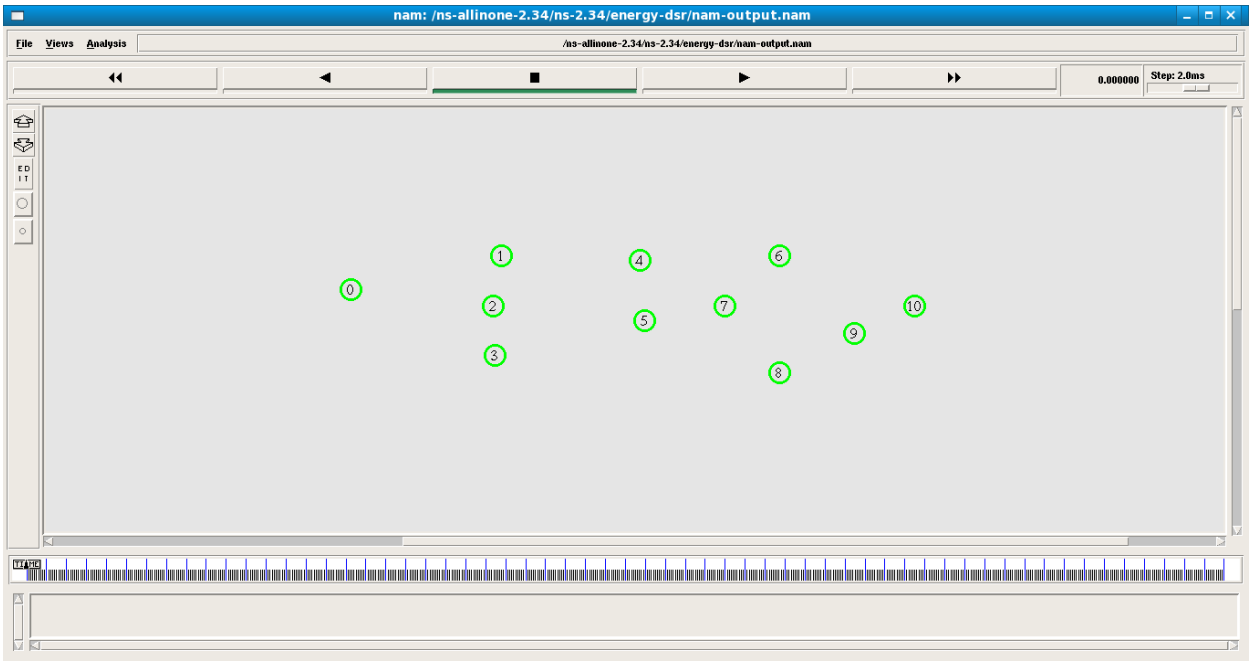

Fig 6.1 Node distribution

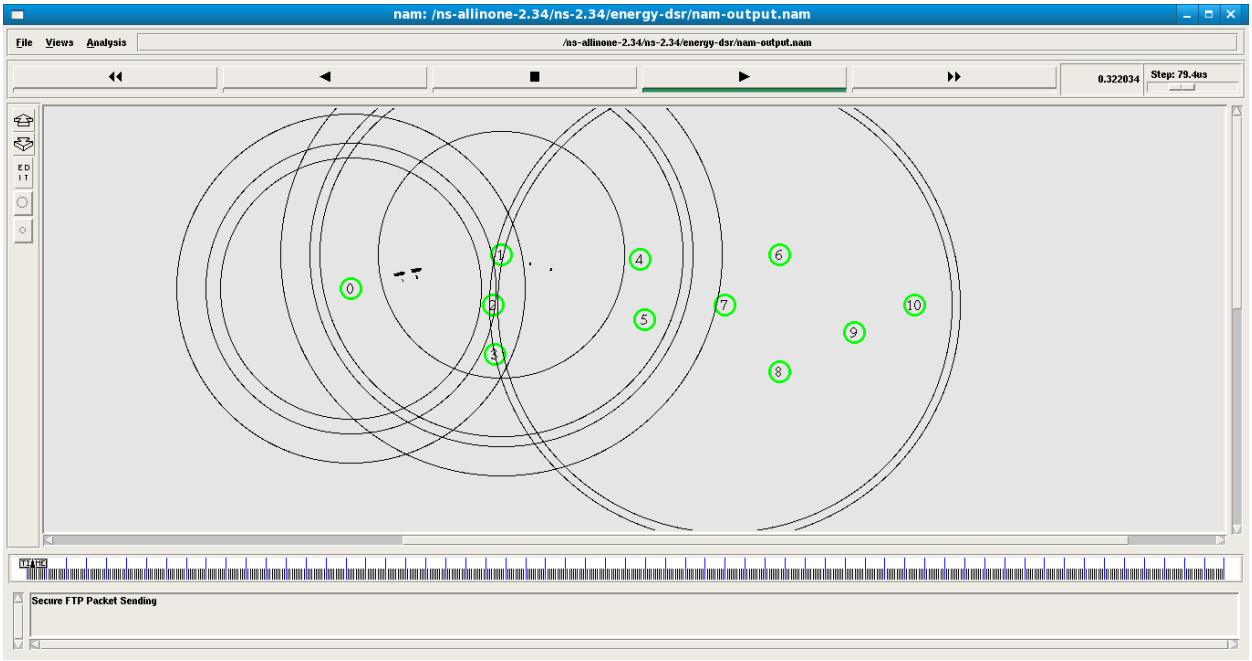

Fig 6.2 Route discovery

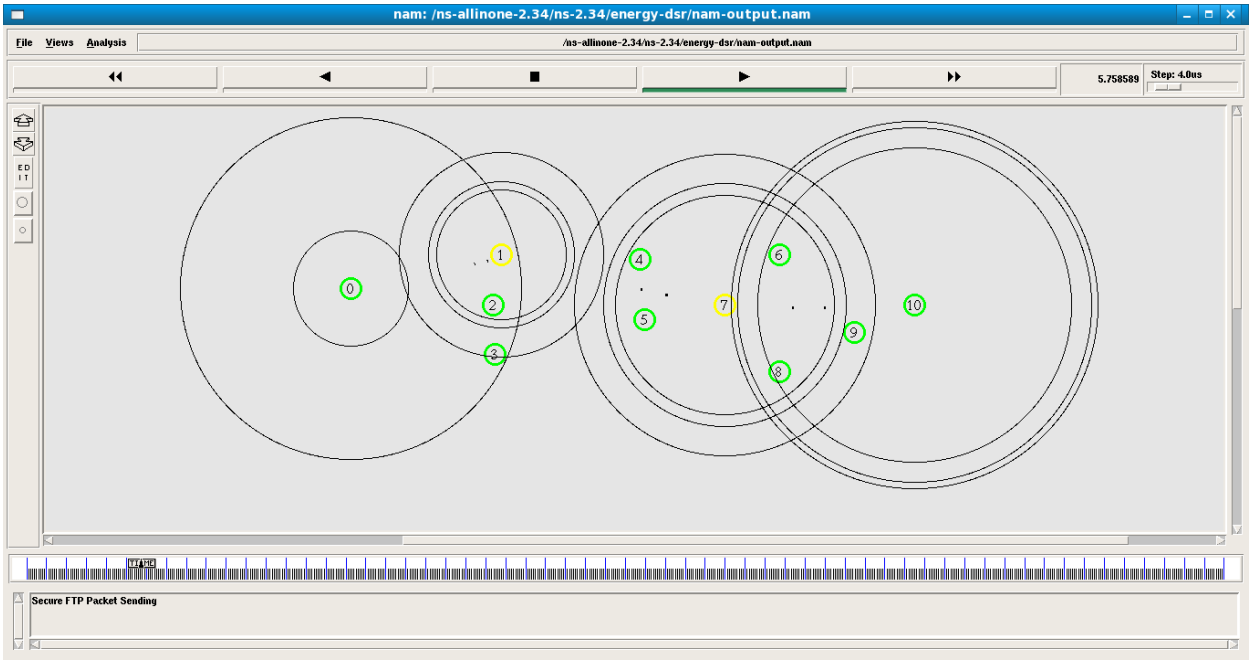

Fig 6.3 50% power loss in node 1 and 7

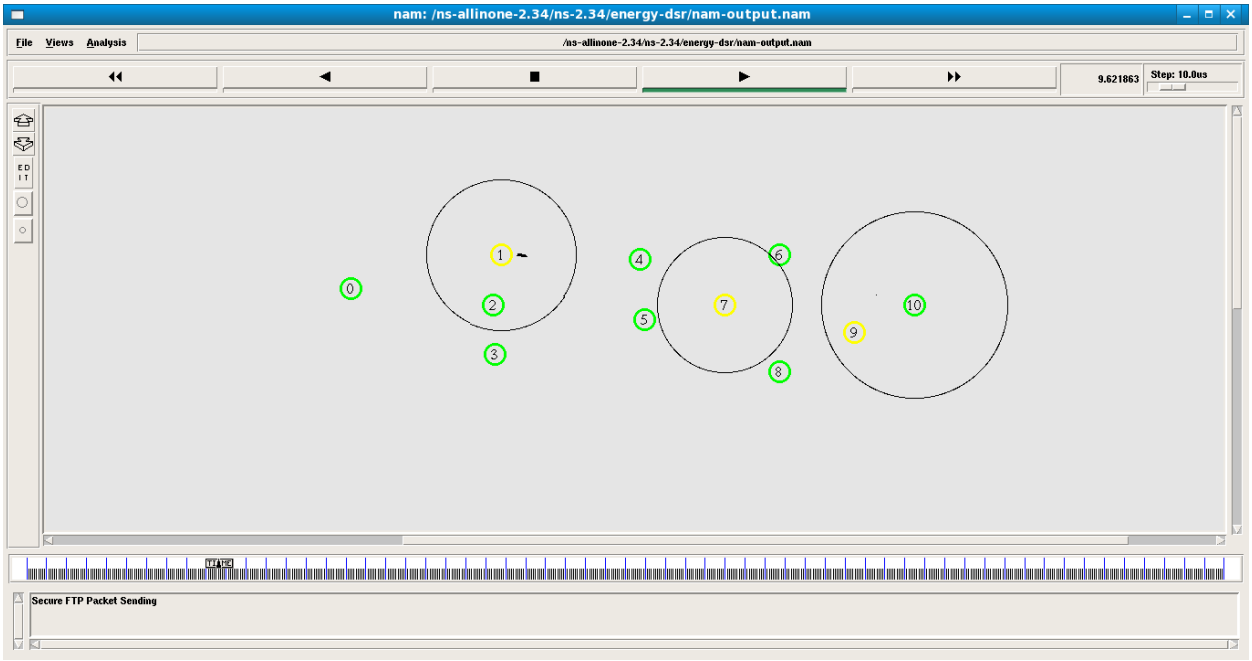

Fig 6.4 50% power loss in path 1,7,9

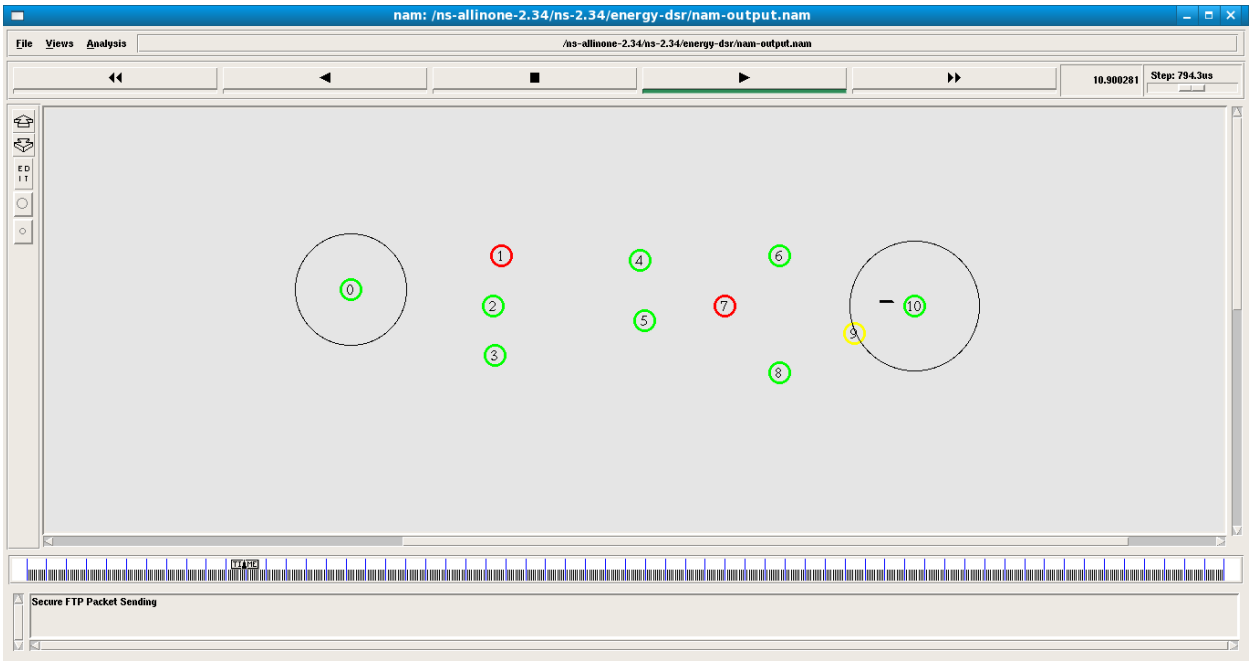

Fig 6.5 Maximum power loss at node 1 and 7

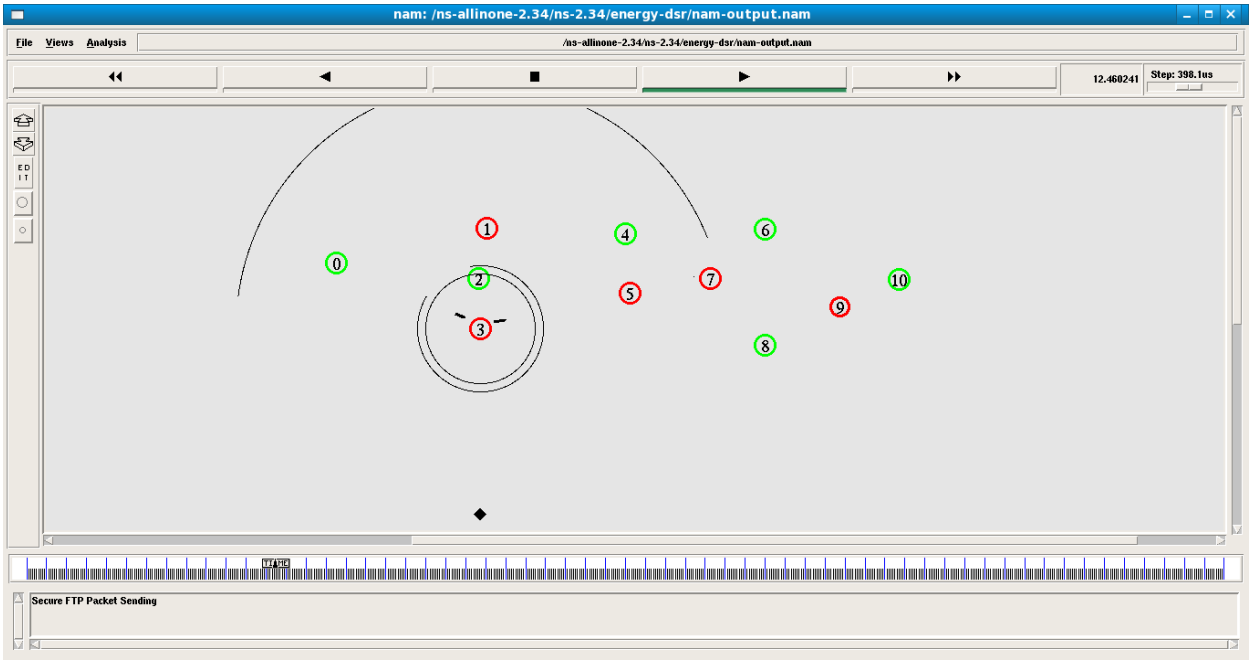

Fig 6.6 Energy aware traffic allocation

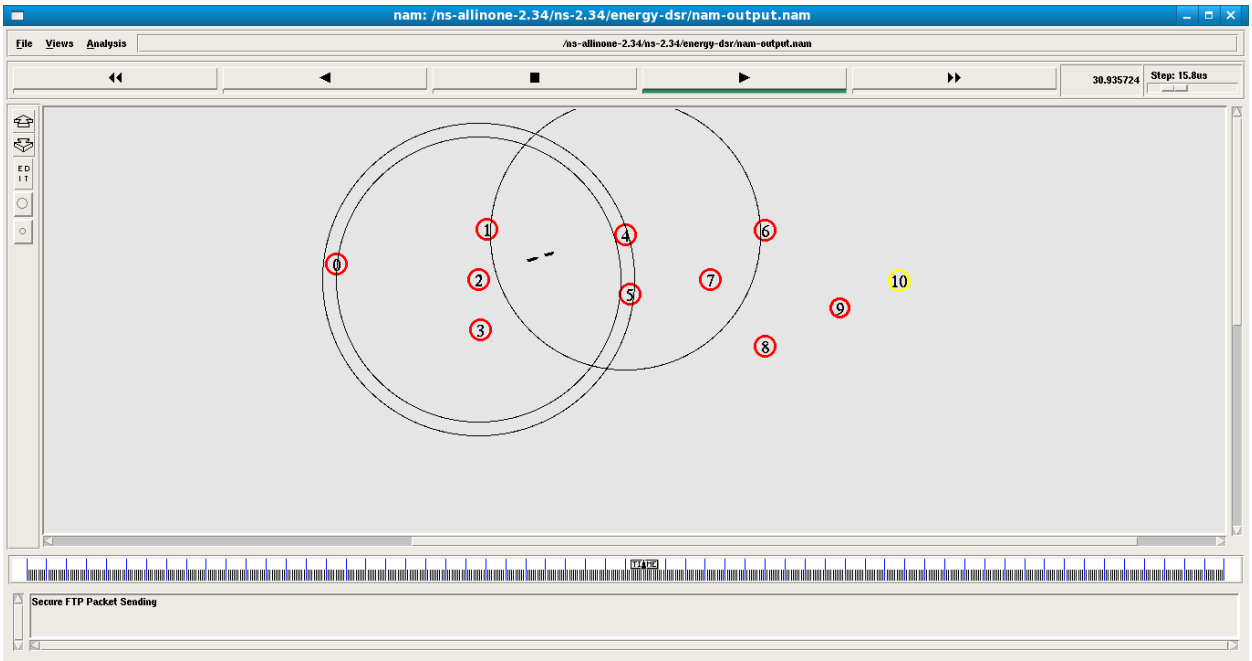

Fig 6.7 Total power loss at entire network

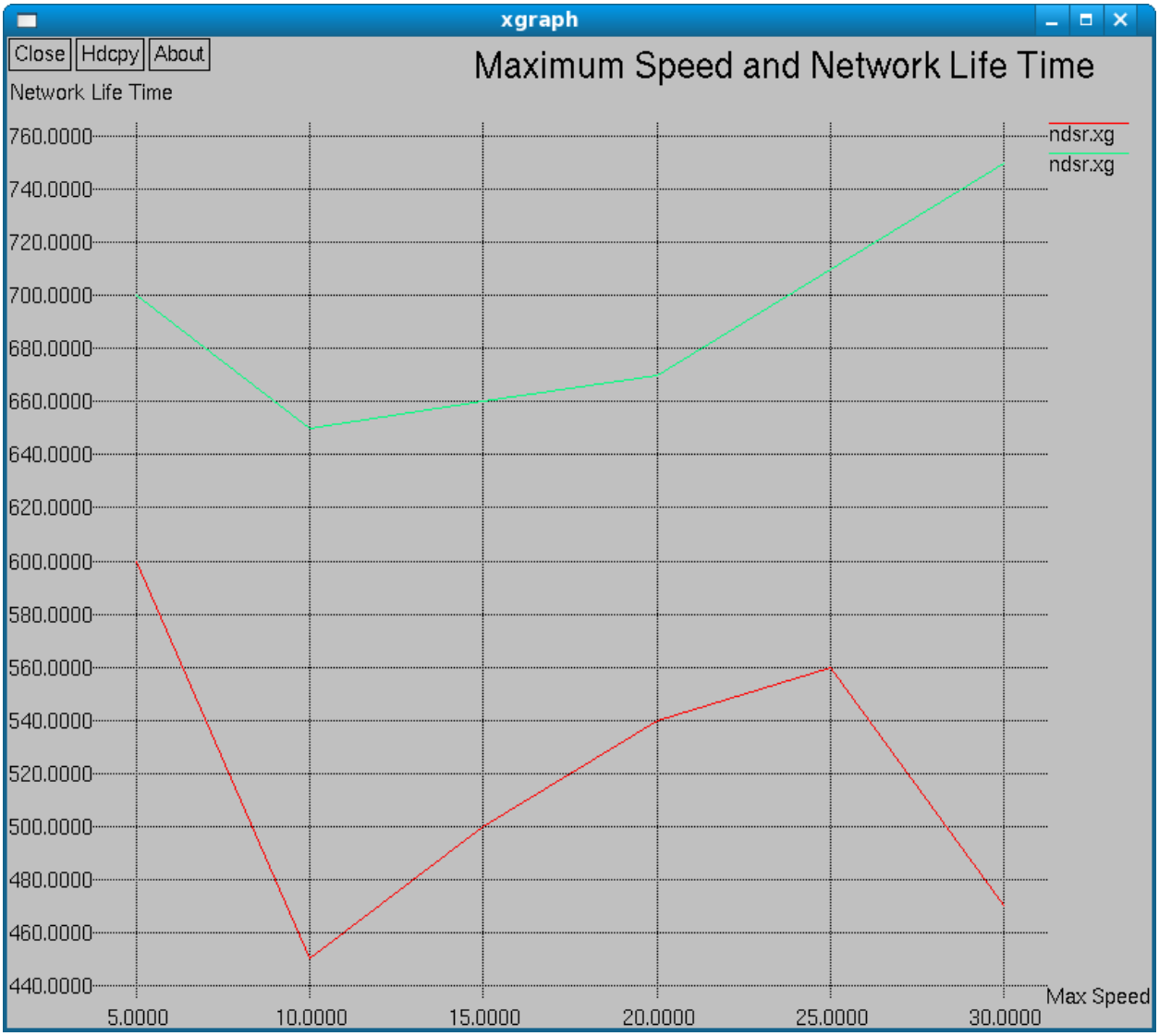

Fig 6.8 Maximum speed and Network life time

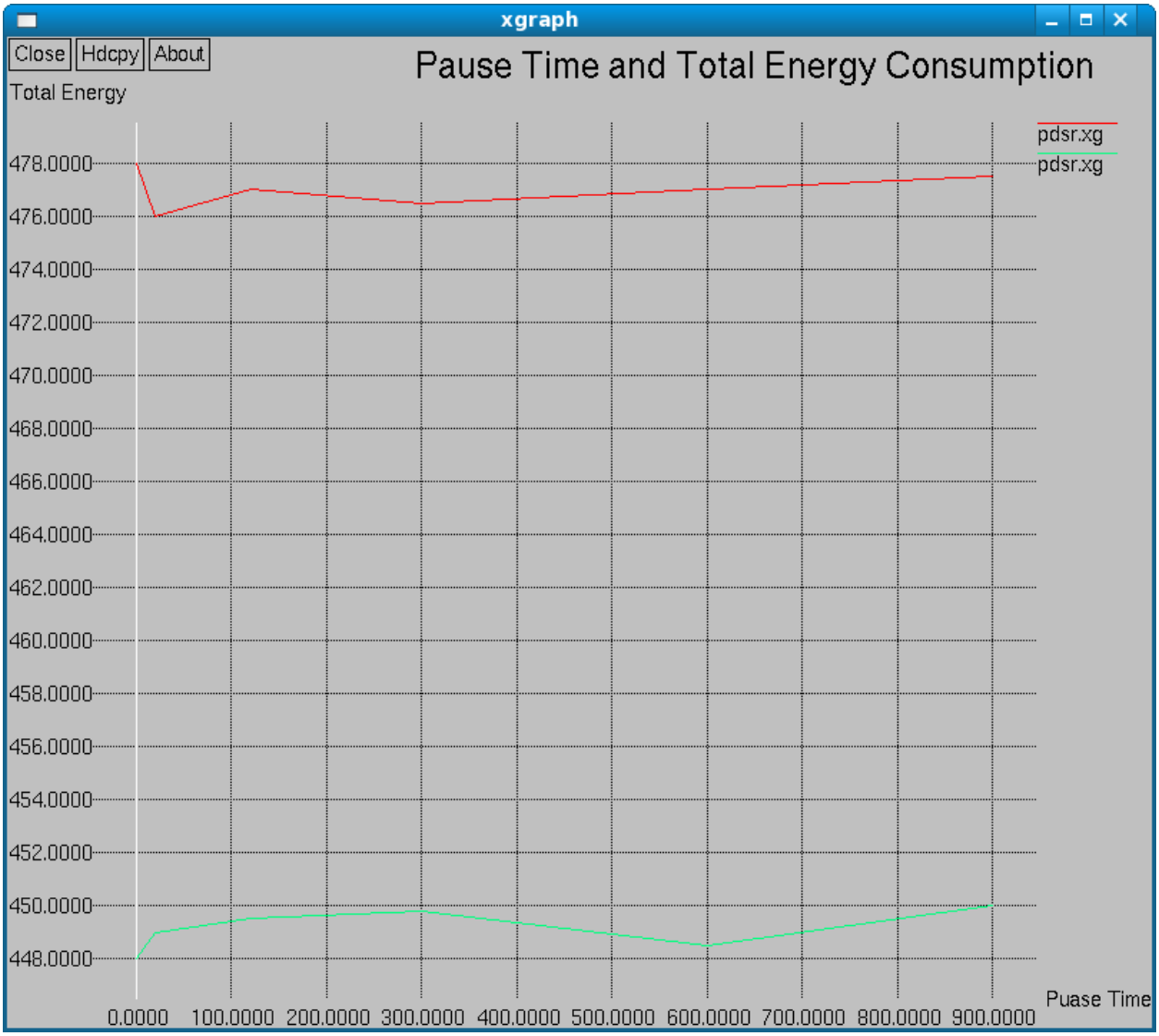

Fig 6.9 Pause time and Total energy consumption

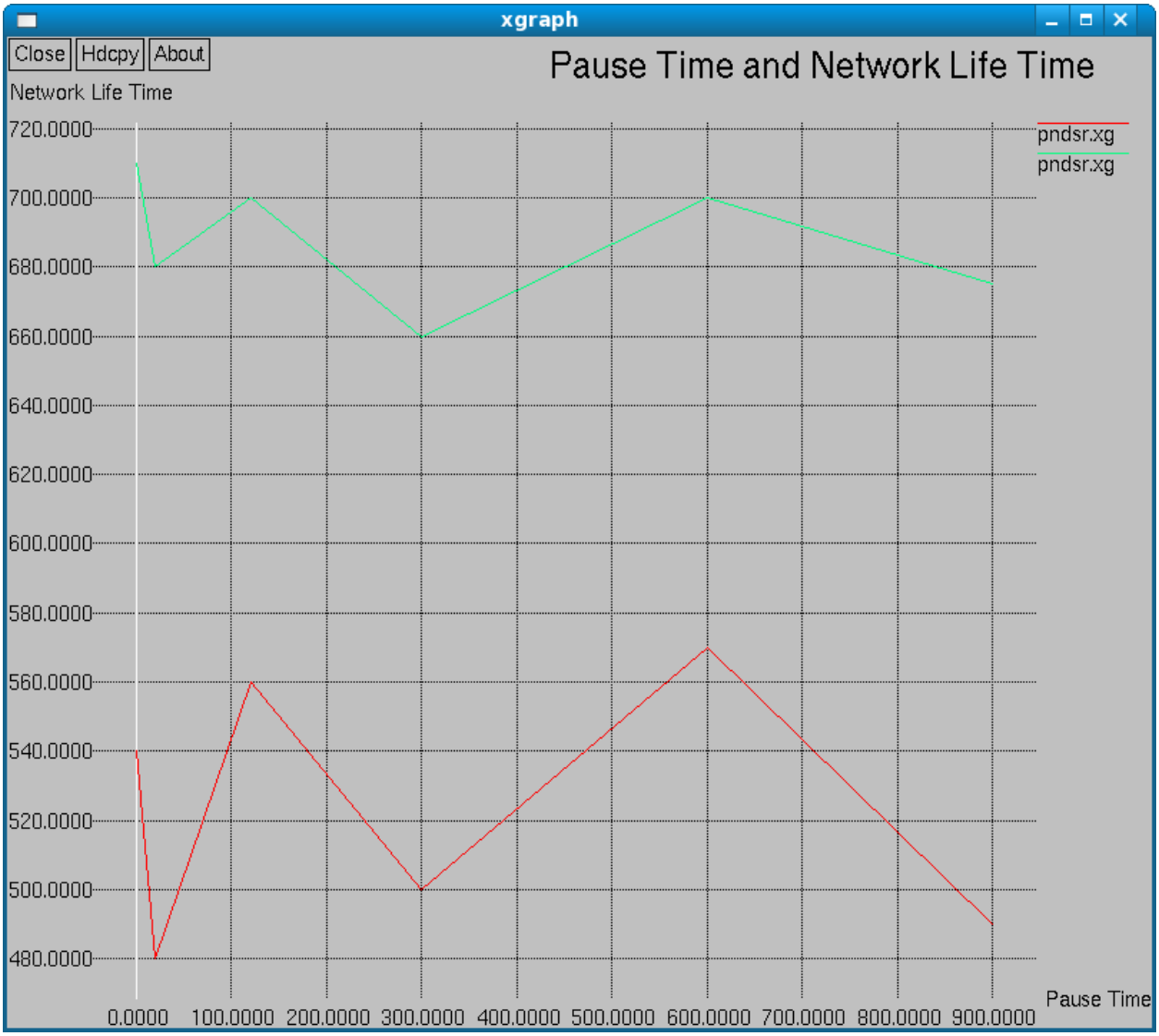

Fig 6.9 Pause time and Network life time

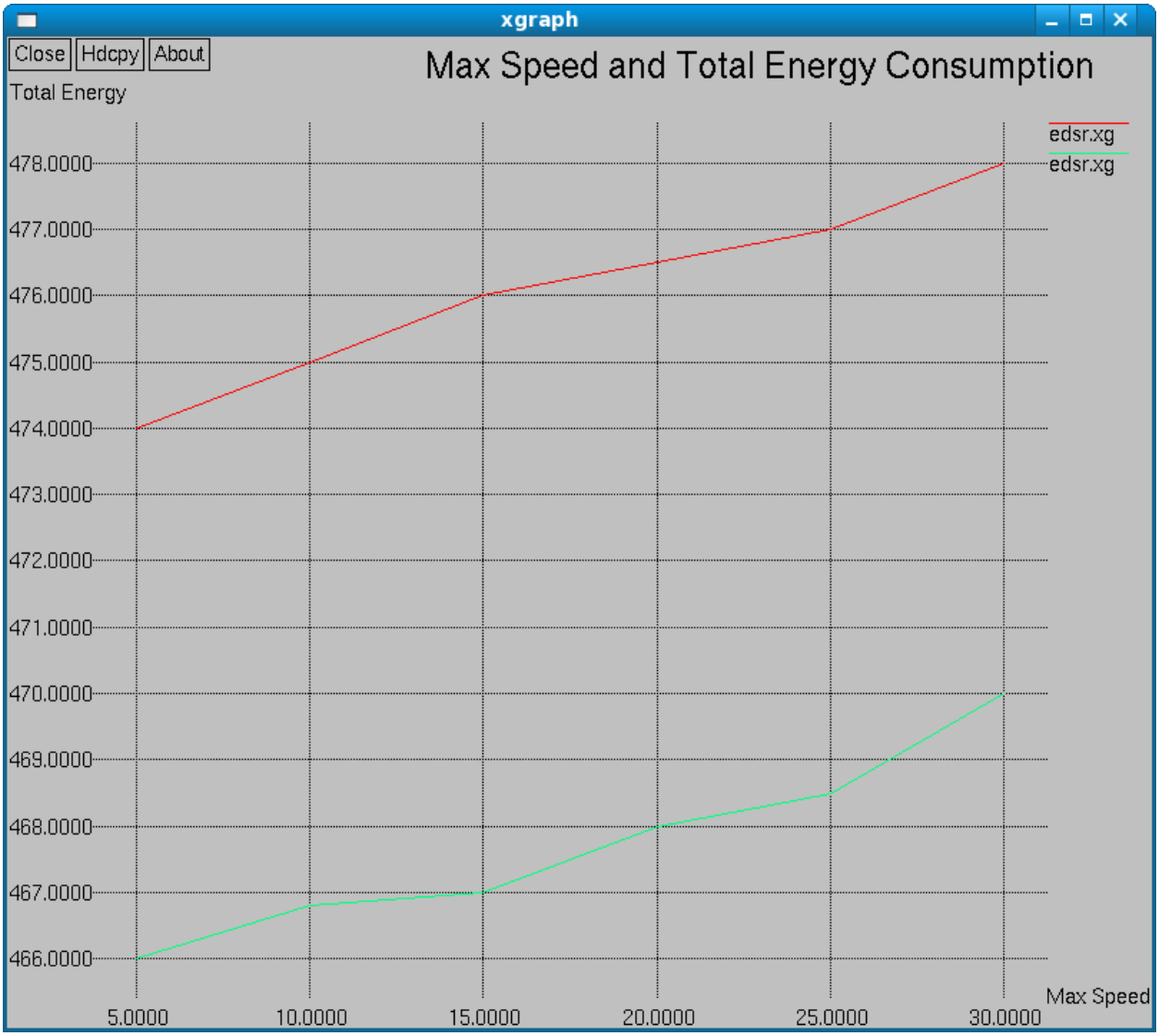

Fig 6.9 Maximum speed and Total energy consumption

CHAPTER VII

7. CONCLUSION

A novel energy aware multipath routing protocol has been proposed (SESDSR and DSR). It has been integrated with different energy metrics. The proposed protocol is mainly useful for enhancing the lifetime of MANET and secure routing source to destination regardless of the secure of data exchanged. It has been tested under conditions of different initial energies of nodes. At lower initial energies, it behaves considerably better as compared to higher energies of the concerned nodes. The performance of SESDSR is better than DSR as it induces less instability. However, if it set the values of initial energies of nodes asymmetrical the performance of proposed protocol degrades. The only parameter we find improvement in energy depletion of first node. It has shown that it is feasible to build such a protocol to run on real embedded platform while there are many improvements that can be made to our design and implementation. The protocol does not seem to behave effectively at higher energy of nodes. There is a limitation of the protocol that under different conditions of initial energy, even SESDSR seems to behave worse than traditional DSR. In order to maximize the lifetime of a node, the selection of optimal path is based entirely on the initial energy of the node. This point is considered valid in the proposed protocol to increase the overall lifetime of MANET.

REFERENCE

[1]. Acharya M., Thuente D., “Intelligent Jamming Attacks, Counterattacks and (Counter)2 Attacks in 802.11b Wireless Networks”, in Proceedings of the OPNETWORK Conference, Washington DC, USA, August 2005.

[2]. Bahl.P and Padmanabhan.V.N, “RADAR: An In-Building RFBased User Location and Tracking System,” Proc. IEEE INFOCOM, 2000.

[3]. Bayraktaroglu E., King C., Liu X., Noubir G., Rajaraman R., Thapa B., “On the Performance of IEEE 802.11 under Jamming,” in Proceedings of IEEE 27th Conference on Computer Communications (INFOCOM’08), Phoenix, Arizona, USA, April 13 - 19 2008.

[4]. Cheng.T, Li.P, and Zhu.S, “Multi-Jammer Localization in Wireless Sensor Networks,” Proc. Seventh Int’l Conf. Computational Intelligence and Security (CIS), 2011.Communications" Prentice Hall, 1st Edition, 1995. Defenses Against Wireless Denial of Service, " in Proceedings of the 2004 ACM workshop on Wireless security (WiSe), pg. 80 - 89, 2004.

[5]. Hung W.C., Law K.L.E., Garcia A.L., “A Dynamic Multi-Channel MAC for Ad Hoc LAN,” in Proceedings of 21st Biennial Symposium on Communications, Kingston, Ontario, June 2002. pp. 31-35.

[6]. Khattab S., Mosse D., Melhem R., "Modeling of the Channel-Hopping Anti-Increase 802.11 Resilience to Jamming Attacks", in proceedings of 26th IEEE International Conference on Computer Communications.

[7]. Lee E.K., Oh S.Y., Gerla M., "Randomized Channel Hopping Scheme for Anti-Jamming Communication", In proceedings of Wireless Days Conference, Venice, Italy, October. 2010.

[8]. Li M., Koutsopoulos I., Poovendran R., “Optimal Jamming Attacks and Network Defense” In IEEE International Conference on Computer Communications (INFOCOM), Anchorage, Alaska, USA, 6-12 May, 2007.

[9]. Liu. Z, Liu.H, Xu.W, and Chen.Y, “Wireless Jamming Localization by Exploiting Nodes’ Hearing Ranges,” Proc. IEEE Int’l Conf. Distributed Computing in Sensor Systems, 2010.

[10]. Liu.H, Liu.Z, Chen.Y, and W. Xu, “Determining the Position of a Jammer Using a Virtual-Force Iterative Approach,” Wireless Networks, vol. 17, pp. 531-547, 2010.

[11]. Liu.H, Liu.Z, Chen.Y, and Xu.W, “Localizing Multiple Jamming Attackers in Wireless Networks,” Proc. 31st Int’l Conf. Distributed Computing Systems (ICDCS), 2011.

[12]. Liu.Z, Liu.H, Xu.W, and Chen.Y, “Exploiting Jamming-Caused Neighbor Changes for Jammer Localization,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 3, pp. 547-555, Mar. 2012.

[13]. Mpitziopoulos A., Gavalas D., Pantziou G., "Defending Wireless Sensor Networks from Jamming Attacks", in proceedings of The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Athens,. Greece, 3–7 September, 2007.

[14]. Nahrstedt K., Campbell R.H., Vaidya N.H., "Identifying Insider-based Jammers in Multi-channel Wireless Networks", in proceedings of GLOBECOM'10. Miami, Florida, USA, 6-10 December, pp.1-6

[15]. Navda V., Bohra A., Ganguly S., Rubenstein D., "Using Channel Hopping to Networks” Journal of Computing Sciences in Colleges, Volume 24 Issue 3, January 2009.

[16]. Nguyen H., Pongthawornkamol T., Nahrstedt K., "Alibi: A Framework for Identifying Insider-based Jamming Attacks in Multi-channel Wireless Networks", in Joint Conference of the IEEE Computer and Communications Societies, Anchorage, Alaska, USA, 6-12 May 2007.

[17]. Noubir G., Lin G., “Low-power DoS Attacks in Data Wireless LANs and Countermeasures,” in proceedings of the Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing, Annapolis, MD, USA, June 1-3, 2003.

[18]. Othman J.B., Hamieh A., "Defending Method Against Jamming Attack in Wireless Ad Hoc Networks", The 5th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks (P2MNET 2009), Zürich, Switzerland; 20-23 October 2009.

[19]. Pelechrinis.k, Koutsopoulos.I, Broustis.I, and S.V. Krishnamurthy, “Lightweight Jammer Localization in Wireless Networks: System Design and Implementation,” Proc. IEEE GLOBECOM, 2009.

[20]. Peterson R. L., Ziemer R. E., Borth D. E., "Introduction to Spread-Spectrum proceedings of 16th ACM Conference on Computer and Communications Security (CCS), Hyatt Regency Chicago, IL, USA, November 9-13, 2009.

[21]. Reese K.W. Salem A., “A Survey on Jamming Avoidance in Adhoc Sensory Jamming Defense in Multi-Radio Wireless Networks", in proceedings of MobiQuitous 2008, Dublin, Ireland, July 21 - 25, 2008

[22]. Salem M., Sarhan A., Abu-Bakr M., “A DOS Attack Intrusion Detection and Inhibition Technique for Wireless Computer Networks”, ICGST- CNIR, Volume (7), Issue (I), July 2007.

[23]. Soreanu P., Volkovich Z., Barzily Z., “Energy-Efficient Predictive Jamming Holes Detection Protocol for Wireless Sensor Networks” in Proceedings of the 2008 Second International Conference on Sensor Technologies and Applications (SENSORCOMM '08), Cap Esterel, France, August 25-31, 2008

[24]. Ståhlberg M. , “Radio Jamming Attacks Against Two Popular Mobile Networks”, Seminar on Network Security. Mobile Security. Helsinki University of Technology, Fall 2000.

[25]. Wood.A, Stankovic.J, and Son.S, “JAM: A Jammed-Area Mapping Service for Sensor Networks,” Proc. 24th IEEE Int’l Real-Time Systems Symp., 2003.

[26]. Wood.A.D, Stankovic.J.A, and Zhou.G, “DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15. 4-based Wireless Networks", in proceedings of 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON '07), San Diego, CA, USA, 18-21 June 2007. pp: 60-69

[27]. Wu S.L., Lin C.Y., Tseng Y.C., Lin C.Y., Sheu J.P., “A Multi-Channel MAC protocol with Power Control for Multi-Hop Mobile Ad Hoc Networks,” The Computer J., vol. 45, no. 1, 2002. pp.: 101-110.

[28]. Xu W., Trappe W., Zhang Y., "Defending Wireless Sensor Networks from Radio Interference through Channel Adaptation," ACM Transactions on Sensor Networks (TOSN), Volume 4, Issue 4, August 2008.

[29]. Xu W., Wood T., Trappe W., Zhang Y., "Channel Surfing and Spatial Retreats: in proceedings of The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), Athens,. Greece, 3–7 September, 2007.

[30]. Xu.W, Trappe.W, Zhang.Y, and Wood.T, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” Proc. ACM MobiHoc, 2005.

[31]. Yang.J, Chen.Y, and Cheng.J, “Improving Localization Accuracy of RSS-Based Lateration Methods in Indoor Environments,” Ad Hoc and Sensor Wireless Networks, vol. 11, nos. 3/4, pp. 307-329, 2011.

[32]. Zhang Z., Wu J., Deng J., Qiu M., "Jamming ACK Attack to Wireless Networks and a Mitigation Approach," in Proc. of IEEE Global Telecommunications Conference - Wireless Networking Symposium (GLOBECOM '08), New Orleans, LA, USA, November 30-December 4, 2008, vol.ECP.950, pp. 1-5.

LIST OF PUBLICATIONS

1. Jaipriya.S and Umamaheswari.S, "A Framework for Detection of Jammers in Wireless Sensor Network" International conference on Electrical, Instrumentation and Communication Engineering – Recent Trends and Research issues (ICE^2 – RTRI 2015), Sri Krishna college of Technology, Coimbatore, Jan 3 2015.