NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SIMULATION OF PHYSICAL AND MEDIA ACCESS CONTROL (MAC) FOR RESILIENT AND SCALABLE WIRELESS SENSOR NETWORKS

by

Daniel Chia Kim Boon

March 2006

Thesis Advisor:	Tri T. Ha
Thesis Co-Advisor:	Weilian Su

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Simulation of Physical and Media Access Control (MAC) for Resilient and Scalable Wireless Sensor Networks			**5. FUNDING NUMBERS**
6. AUTHOR(S) Daniel Kim Boon Chia			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

The resilience of wireless sensor networks is investigated. A key concept is that scale-free network principles can be adapted to artificially create resilient wireless sensor networks. As scale-free networks are known to be resilient to errors but vulnerable to attack, a strategy using "cold-start" diversity is proposed to reduce the vulnerability to attacks. The IEEE 802.15.4 MAC and ZigBee protocols are investigated for their ability to form resilient clusters. Our investigation reveals there exists deficiencies in these protocols and the possibility of self-directed and attack-directed denial-of-service is significant. Through insights gained, techniques are recommended to augment the protocols, increasing their resilience without major changes to the standard itself. Since both topological and protocol resilience properties are investigated, our results reveal important insights. Simulation of the physical and media access control layers using ns-2 is carried out to validate key concepts and approach.

14. SUBJECT TERMS Wireless Sensor Networks, Resilience, Scale-Free Networks, Ns-2, IEEE 802.15.4, ZigBee, denial-0f-service, topology resilience			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

SIMULATION OF PHYSICAL AND MEDIA ACCESS CONTROL (MAC) LAYER FOR SCALABLE WIRELESS SENSOR NETWORKS

Daniel Kim Boon Chia
Civilian, Ministry of Defense, Singapore
B.Eng, National University of Singapore, 1996
M.Eng, National University of Singapore, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2006

Author: Daniel, Kim Boon Chia

Approved by: Professor Tri T. Ha
Thesis Advisor

Professor Weilian Su
Co-Advisor

Professor Jeffrey B. Knorr
Chairman, Electrical and Computer Engineering Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The resilience of wireless sensor networks is investigated. A key concept is that scale-free network principles can be adapted to artificially create resilient wireless sensor networks. As scale-free networks are known to be resilient to errors but vulnerable to attack, a strategy using “cold-start” diversity is proposed to reduce the vulnerability to attacks. The IEEE 802.15.4 MAC and ZigBee protocols are investigated for their ability to form resilient clusters. Our investigation reveals there exists deficiencies in these protocols and the possibility of self-directed and attack-directed denial-of-service is significant. Through insights gained, techniques are recommended to augment the protocols, increasing their resilience without major changes to the standard itself. Since both topological and protocol resilience properties are investigated, our results reveal important insights. Simulation of the physical and media access control layers using NS-2 is carried out to validate key concepts and approach.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my gratitude to Prof. Tri Ha and Prof. Weilian Su for their professional advice, insights and careful guidance. Their care, patience and belief in me are deeply appreciated.

To my wife, Flora, and son, Zach, your sacrifice is my strength and optimism. This thesis is as much your work as it is mine.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Wireless Sensor Networks have great promise to revolutionize military deployment of sensor fields through their value proposition of low-cost, stealth, and the anticipation of an unprecedented scale of deployment. The academia and industry have focused R&D on the creation of protocols enabling mass wireless connectivity of sensor systems. Energy efficiency, throughput and latency of such systems are well studied and published. However, as wireless sensor networks are prototyped and tested under real-world conditions, there arises a general sense that greater resilience and autonomy are required for potential of wireless sensor networks to be fully realized.

There are very few studies conducted on resilience of wireless sensor networks. Resilience, when studied, is normally associated with the notion of performance of the network protocols under stress. Thus, resilience becomes a subset of protocol performance.

A contrary approach is adopted in this thesis – resilience is the key driver for performance. Another significant contribution is the investigation of creating artificial scale-free networks using the IEEE 802.15.4/ZigBee protocol, thus, directly extending the resilience properties of scale-free networks to wireless sensor networks in general. The investigation on resilience includes not only topological resilience but also IEEE 802.15.4/ZigBee protocol resilience.

Since the investigation combines resilience studies of topology and protocol, it can provide insights not gained previously. These insights enable us to understand and augment current protocol mechanisms and highlight techniques and strategies that are critical to more resilient operation of wireless sensor networks.

Our investigation leverages simulation of the media access control layer and the media dependent physical layer to understand the protocols and their significant properties. This thesis gives an outline of the approach, key concepts and results which in turn demonstrates the validity of our approach.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. MOTIVATION FOR DEVELOPMENT OF SENSOR NETWORKS

Sensor networks are extremely valuable to the military. They could be a swarming fleet of Predator UAVs carrying sensor payloads collecting information on the battlespace or it could be a fleet of swarming mini-submarines carrying acoustic sensors used to triangulate enemy submarines or mine fields through multilateration techniques.

The Global Positioning System (GPS) exemplifies the value proposition of sensor networks. GPS satellites are placed into the geosynchronous orbits. Their main function is to sense their own position in these orbits by interacting with a group of ground control stations to receive "ephemeris errors" correction data. They can then broadcast accurate position and clock/timing information to GPS terminals that simply extract position and timing data from the "GPS message". By fusing information from multiple satellites, the terminal in turn fixes its own position. GPS has been extremely successful in military applications. It was used during Operation Dessert Storm in 1991 to help the US forces navigate, position and mass in an unfamiliar territory regardless of day or night.

Almost a decade later, the application of GPS has widened. It is used in Joint Direct Attack Munitions (JDAMs) against the Iraqis in Operation Iraqi Freedom (OIF). JDAMs are guided using GPS. The positioning and massing of indirect fire using guided munitions on a large-scale replaced the navigation, positioning and massing of troops to a large extent, reducing the level of Coalition troops deployed.

Sensor networks have existed for over twenty years. However, sensor networks have constantly been difficult and expensive to deploy. The GPS constellation, for example, requires multi-billions of dollars to develop and deploy.

Even when sensor networks do not require multi-billions of dollars to develop and deploy, they are limited by the number of sensor nodes that can be deployed and linked, i.e., GPS and US Navy's Cooperative Engagement Capability.

Wireless Sensor Networks (WSN) extends the concept of sensor networks by driving four parameters of sensor networks to the extreme:

- Scale. Researchers anticipate WSNs to comprise of hundreds, thousands and even tens of thousands of sensor nodes connected through wireless media. The information that such a huge network of sensor nodes collect will be fused to give meaningful information of the environment.
- Size. WSNs are expected to have nodes with small form factors. It is anticipated that the sensors are so small that they can be embedded within the environment, machinery, transportation containers and even the human body etc.
- Function. The sensors are capable of sensing and discriminating different signatures, i.e., mechanical movements, heat, magnetic and acoustic signature in the environment. It is anticipated that nanoscale sensors with the ability to sense chemicals and biologic changes [49][50] will be prevalent.
- Cost. Unlike conventional sensor networks, which cost a tremendous amount of money to build and deploy, sensor networks have to be built and deployed at a small fraction of the costs. This is true as a result of economies of scale.

These highly cost-efficient, multi-function sensor networks will be extremely valuable to the military. A key challenge to realizing these capabilities is in connecting and interacting with the sensor nodes that are dispersed and embedded in the environment usually across a wide geographic expanse. A breakthrough could have a high impact on wide area surveillance. Thus, the development of un-manned ground sensors (UGS) has intensified.

B. UGS NETWORK CONCEPTS

Darpa has funded the development of sensor networks through the Sensor Information Technology (SensIT) Program [1]. The goal is to define, experiment and overcome the challenges of sensor networks. Initial experimentation and tests emphasized the use of UGS for the detection and tracking of (enemy) vehicles, accuracy

of the fusion and tracking (bearing) algorithms, comparison of different configurations of acoustic arrays, and the efficiency of the networking protocols.

A rudimentary experiment of sensor networks was completed during SITEX-01 using acoustic sensors lined along the roadside to detect and track vehicles. This is shown in Fig. 1.

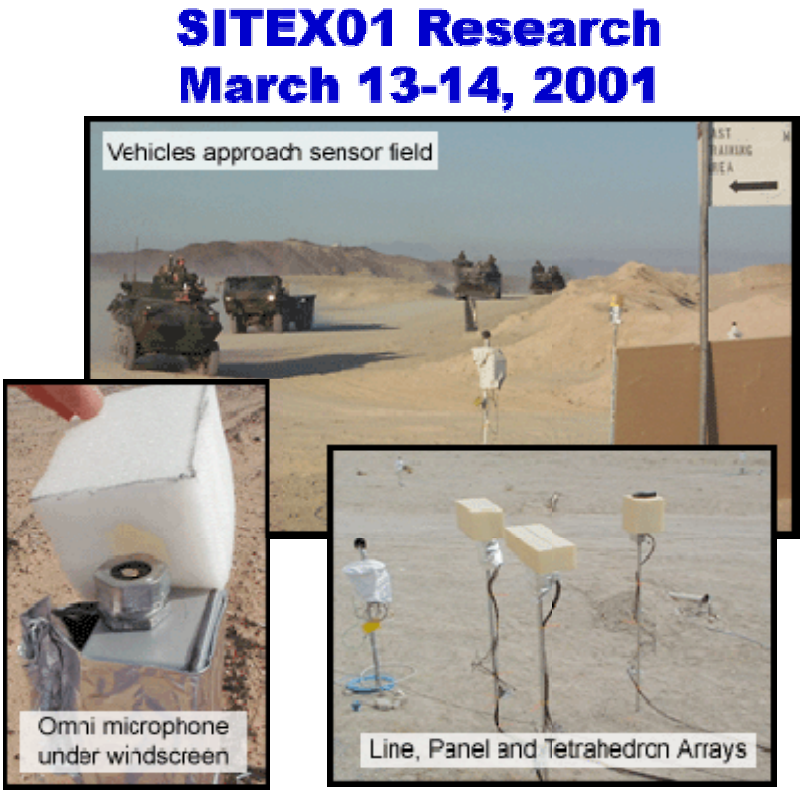


Figure 1. SensIT Experimentations During SITEX-01 (from [1]).

Acoustic networks are extremely promising. A recent study [2] using Mica2 sensor nodes demonstrates the possibility of achieving an error of 9 cm for a 2-dimensional outlay of sensor nodes.

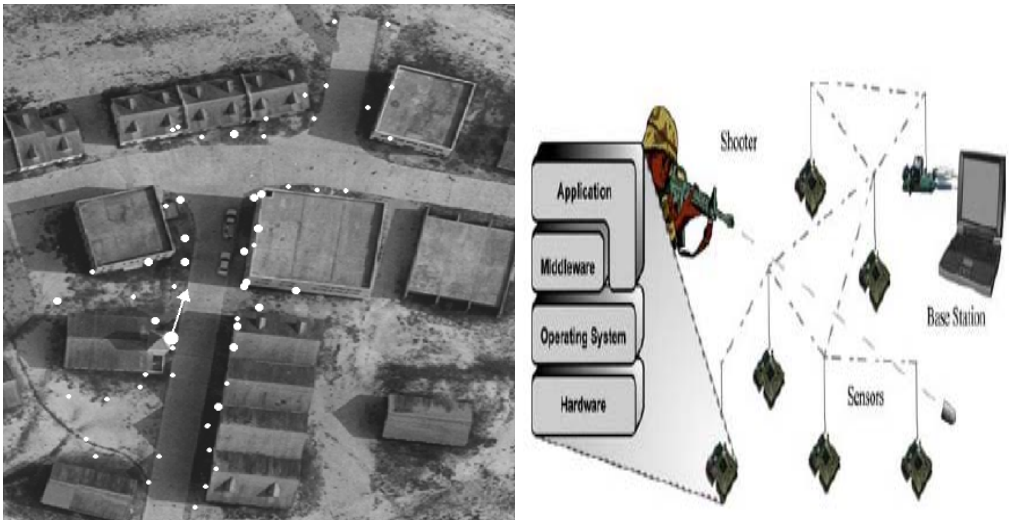


Figure 2. Countersniper System (from Fig.2 and 5 [38]).

The concept could be easily adapted to an urban countersniper system as shown in Fig.2. In this scenario, the sensor nodes i.e., acoustic sensors are pre-deployed along fixed infrastructure such as lamp posts, housing rooftops etc. The sensors are networked in a "sensor-to-shooter" system to detect and accurately locate snipers by linking to an armed vehicle in a military convoy on an ad hoc basis. The armed vehicle can then automatically target and prosecute the sniper using surveillance, acquisition and tracking information from the sensor network.

A third concept that the military is keen to experiment and investigate is an indoor three-dimensional localization system to enhance in-building, intra-team situation awareness of enemy agents for Special Operations Forces. Because of the narrow radiofrequency pulses (in the order of nanoseconds), ultra-wideband (UWB) technology is investigated for in-building localization. Using multiple transmitter and receivers, it is shown that it is possible to achieve an accuracy of 20cm even in a dense multipath environment [3].

This concept can be extended to encompass not only friendly positions, but also foes'[4]. This is illustrated in Fig.3. The sensors would have to be very small to remain unobtrusive and stealthy to avoid enemy detection. They would also have to be inexpensive to be disposable. The sensors could either be placed by hand or in the future, by robotics. The network of sensors would detect and track potential enemy agents and

interact seamlessly with the soldiers' communications systems, providing the soldiers with timely information on the enemies' whereabouts.

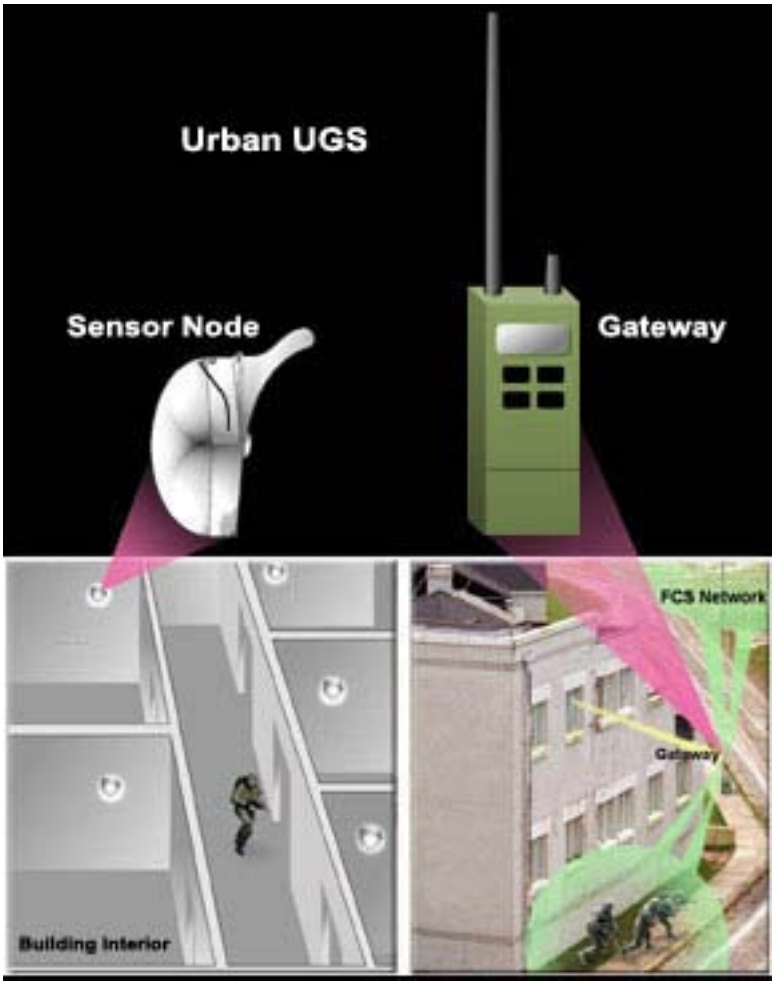


Figure 3. Urban Un-manned Ground Sensors (U-UGS) (from [4]).

In all three concepts, sensor networks have the potential to provide the warfighters with timely information about the enemy's locations and thus, enable the warfighters to decipher the enemy's intent, plan an appropriate course of action and respond in a timely fashion to eliminate the threats.

Military sensor networks encompass far-ranging concepts and are not limited to the three mentioned above. The environment is usually complex, and the deployment is equally difficult. In the next section, the challenges are outlined.

C. SENSOR NETWORK CHALLENGES

An excellent survey on sensor networks and some of its challenges are given in references [11], [12], [16] and [24]. According to Lewis [11], an understanding of the challenges of sensor-based communication networks can be achieved through five dimensions: network topology, network protocols, network structure and hierarchy, power management and the standards.

A more detailed framework is provided by Romer and Mattern [16] which frames the challenges of sensor networks from the perspective of the "design space". The "design space" is composed of twelve considerations:

- Deployment (*Classes: random vs. manual; one-time vs. iterative)*
- Mobility (*Classes: immobile vs. partly vs. all; occasional vs. continuous active vs. passive)*
- Cost, Size, Resources and Energy (*Classes: brick vs. matchbox vs. grain vs. dust)*
- Heterogeneity (*Classes: homogeneous vs. heterogeneous)*
- Communication Modality (*Classes: radio vs lasers vs sound)*
- Infrastructure (*infrastructure vs. ad hoc)*
- Network Topology (*Classes: single-hop vs. star vs. networked stars vs. tree vs. graph)*
- Coverage (*Classes: sparse vs. dense vs. redundant)*
- Connectivity (*Classes: connected vs. intermittent vs. sporadic)*
- Network Size
- Lifetime
- Quality of Service requirements

Although resilience is an important factor, it is missing from the "design space". Tilak et al., [76] defined five performance metrics of sensor networks: energy efficiency/system lifetime, latency, accuracy, fault-tolerance and scalability.

A review of Table 1 in [24] reveals the following:

- The size of current sensor networks deployed is usually a few tens of nodes. An exception is an oceanic sensor network comprising of 1300 nodes (possibly buoys).
- Sensor networks deployed can be either homogenous or heterogeneous and a large percentage of these sensor networks are infrastructure assisted i.e., satellites, cellular etc.
- The lifetime requirements can vary widely, ranging from days to years.
- Two of the fifteen applications specified require real-time communications.
- Four of the fifteen applications require dependability and often temper-resistance.

Even though Tilek et al listed fault-tolerance as one of five important factors for wireless sensor networks, the notion of fault-tolerance is geared towards hardware fault-tolerance. In the literature surveyed, there has been very little work done on the resilience of wireless sensor networks from a topological perspective.

Through literature survey, it is found that a lot of emphasis on wireless sensor networks is focused on the design of appropriate network protocols. The protocols enable wireless sensor networks to self-heal and self-form. More importantly, the research focus has been on improving the energy efficiency of the protocols to extend the lifetime of sensor networks.

The challenges of network protocol design are outlined in reference [12]. Further considerations are given below.

1. Physical Layer

The challenge is for the radio device to transmit in an energy efficient manner to prevent rapid draining of the batteries of the wireless sensor node [17] [20]. In many aspects, this is an extension of current work in cellular communications devices, where

the lifetime and hence energy efficiency and power management are crucial. However, since wireless sensor nodes are required to operate for prolonged periods unattended, the radio has to be as energy efficient as possible. This means that the hardware must be designed differently.

Enz et al [32] give a good account of their work in designing a low-power sensor wireless network known as “WiseNET”. The salient objectives of the hardware project are typical of sensor nodes in general and are given below:

- Keep the power consumption within the 1 milliwatt range while the transceiver is in the receive mode
- Achieve node operational lifetime of several years with the sensor node operating off a single 1.5V AA alkaline battery. Furthermore, the sensor node must operate off a voltage of 0.9 volts corresponding to the end-of-life battery voltage
- Use of a 0.18 micron standard digital CMOS process for the fabrication for the “system-on-a-chip” (SOC) sensor node with no precision analog components such as resistors and capacitors, or special RF technology such as isolated substrate
- Minimize external component count and costs of overall SoC design

The parameters of WiseNET are given in Fig.4. It provides a good rule-of-thumb on what is currently technically feasible.

WiseNET radio parameters

Operating frequency	433 MHz (ISM) and 868 MHz (SRD)
Channel separation	600 kHz (primary), 200 kHz (secondary)
Propagation range	~2 km outdoors — ~10 m indoors
Data rate/modulation	<100 Kbps with FSK (Δf = 25 kHz) <4 Kbps with 00K
Power consumption in Rx mode	1.8 mW
Power consumption in Tx mode	31.5 mW
Wake-up time	800 µs
Rx to Tx and Tx to Rx turnaround time	400 µs

Main measured results for the Rx and Tx blocks.

Supply voltage	V_{DD} = 0.9 V — 1.5 V (Rx and Tx)
Sleep current	3.5 µA
Receiver (Rx) (measured at V_{DD} = 1 V and at 25 °C)	
Sensitivity	–105 dBm @ BER = 10^{-3} and 25 Kbps
PLL phase noise	–120 dBc/Hz @ 600 kHz offset
Supply current	I_{Rx} = 2 mA
Transmitter (Tx) (measured at V_{DD} = 1 V and at 25 °C)	
Output power	10 dBm
Efficiency @ 10 dBm	30%
Supply current @ 10 dBm	I_{Tx} = 24 mA (PA-preamp)

Figure 4. WiseNET Radio Parameters (from Table 1 [32]).

In addition to the hardware design, consideration must be given to the modulation format as this also impacts the energy efficiency. In [26], it is shown that an M-ary modulation format is the most energy-efficient provided that the radio startup time is low. This, in turn, increases the complexity of the radio. The trade-off is therefore between circuitry simplicity (and hence lower cost) and better energy-efficiency.

In recent experimentations, Zhang et al. [25] conceded that one of the most difficult parameters to predict in any environment was the range of the transmission device. They tested the sensor nodes in New Jersey to a range of 1 km. However, in actual deployments in Kenya, where the sensor nodes are deployed around the necks of a pack of Zebras, they experienced a wide variation in range, from 100m to 1.2 km. They attributed this difficulty to physical layer (and real-world) challenges:

- Antenna’s ground plane design
- Deployment of sensors too close to the ground (caused by Zebras grazing near to the ground)
- Robustness of the hardware

Since it is possible that the physical layer design may result in completely unpredictable performance in the real-world, the wireless sensor protocols have to be designed to compensate for this inadequacy and adapt as much as possible to environmental conditions. This adaptation can be in the form of dynamically changing the modulation format to suit the transmission range, i.e., changing the code rate. With energy as a constraint, this means a trade-off between range and data rates.

2. Medium Access Control (MAC) Layer

Zhang et al. [25] has shown in their experimentations the value of a wireless sensor network that can track Zebras. In many cases, wireless sensor networks derive their value from being able to adapt to mobility of sensor nodes, changes in their environment or mobility of the targets they are used to sense and track, or simply adapt and react to sensor topology due to node failures.

In these adaptations, the wireless sensor network must manage association and disassociation rapidly to achieve a coherent and consistent network topology for addressing and routing. Furthermore, the MAC is the critical function for maintaining a virtual link between pairs of nodes in the wireless world. Without establishing and maintaining this point-to-point links, none of the end-to-end functions of a network can be achieved. Real-world experiences validate the importance of the MAC layer [21].

Similar to the physical layer, the MAC layer has to be energy efficient. The challenges of the MAC layer design is further elaborated in a subsequent chapter.

3. Network Layer

The challenge for the network layer is to design protocols that can create minimum energy paths for end-to-end routing. This has an impact on latency, throughput and congestion as minimum energy paths may not coincide with minimum hop paths.

The research done in this area is certainly extensive. An excellent summary of such protocols are given in Table 1 of reference [13] and Fig. 8 of reference [14]. Kemal et al. [13] classified these protocols into six categories: data-centric, hierarchical, location-based, QoS (Quality of Service), network-flow and data aggregation. From [13], it is possible to make the following observations:

- Cluster-based (hierarchical) algorithms such as LEACH [27] are promising and attempt to optimize both energy and latency.
- Data-centric protocols such as SPIN [28] and Directed Diffusion [29] attempt to avoid the overheads and heterogeneity, i.e., creating / electing a cluster-head, of cluster-based protocols
- It is worth noting that Jamal [33] compared the energy-efficiency of LEACH, SPIN and Directed Diffusion, and concluded that LEACH is the most efficient.
- Location-based or geographical based routing protocols are able to exploit location data to determine the optimum path. They have a relative advantage in ease of scalability. Recent advances [19] have attempted to correct the “planarization” problems of location-based routing protocols.
- Current focus on research at the network layer emphasized energy-efficiency. Protocols such as SAR [30] and SPEED [31] attempt to provide “soft” Quality of Service. Nevertheless, very little work is done for real-time applications which require Quality of Service i.e., military applications requiring video surveillance sensors etc. (A good survey of QoS support for wireless sensor networks is given in reference [15].)
- As in many cases, the simulations and analyses are conducted for static source and sink nodes. Work has yet to be extended to extensive mobility of source and sinks which may be significantly beneficial to real-world deployments [25].

D. RESILIENCE TOPOLOGY

A lot of work has already been done in providing the core networking capabilities for enabling wireless sensor networks. The approaches to overcoming some of the challenges of wireless sensor networks are mentioned above. However, the big issue of resilience has not been readily discussed by the community although empirical evidence hints at its importance [21][22].

Resilience was a big issue 30 years ago when the Internet was first conceived. This can be attributed to the work of Paul Baran [7].

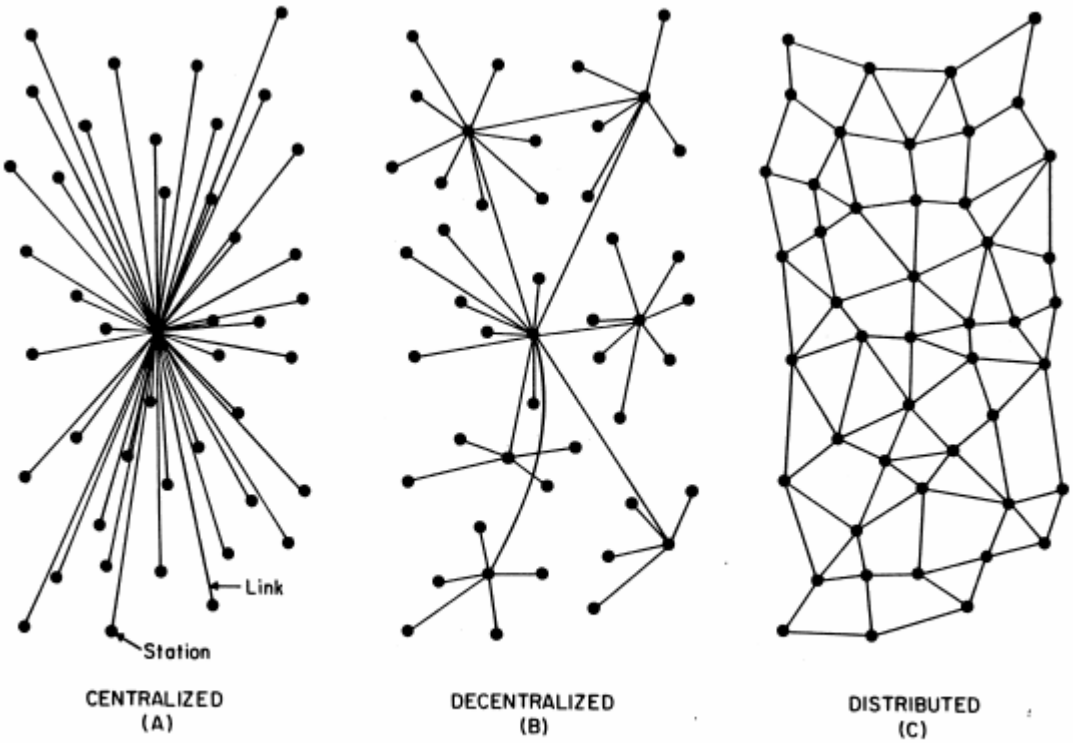


FIG. 1 — Centralized, Decentralized and Distributed Networks

Figure 5. Topologies (from Fig.1 [7])

Baran analyzed the different topologies for their resilience. The topologies are classified into centralized, decentralized and distributed as shown above. The centralized topology is depicted as a “star” or “hub-spoke” structure. The “stars” or “hubs” can in turn be connected to form extended networks. This is the larger “decentralized” structure. Finally, there is the distributed structure which is a “random” network.

Baran analyzed the topologies for their redundancy level and resilience to destruction and this gives the survivability of the network [7]. It is expected that the distributed networks have the highest level of survivability.

Many of the simulations conducted in the literature to investigate the strength of different protocol designs for wireless sensor networks are based on random networks. Furthermore, there is a focus on homogenous networks – all nodes in the networks have similar capabilities. Thus, it may be possible to extend Baran's work to this class of sensor networks.

However, sensor networks are anticipated ***not*** to be fully random or distributed according to the definition of Baran. The military, for example, operates in extremely complex environment. In both urban and forested environments, the military cannot assume line-of-sight operations for adjacent nodes, either due to terrain masking / shadowing, blockage or a lack of RF power to complete the link budget. Under these scenarios, wireless sensor networks do not normally operate in a complete "meshed" topology.

Wireless sensor networks also do not necessarily have to be homogenous [8], [9], [10]. One class of wireless sensor network relies on infrastructure assistance [10]. Leveraging infrastructure provides range extension and direct connectivity to critical core information infrastructure, thus enabling rapid information fusion and dissemination necessary for concerted information awareness and decision-making.

Thus, a problem of Baran's work is that it does not easily extend to non-distributed, non-homogenous networks. An example of a non-distributed, non-homogenous network could be a typical "reporting" wireless sensor network whose structure is given below. In Fig.6, the sensor nodes are dispersed and report either periodically or through event triggers to a central administration console where the information is fused and analyzed. This structure resembles a "tree" topology rather than random distributed network.

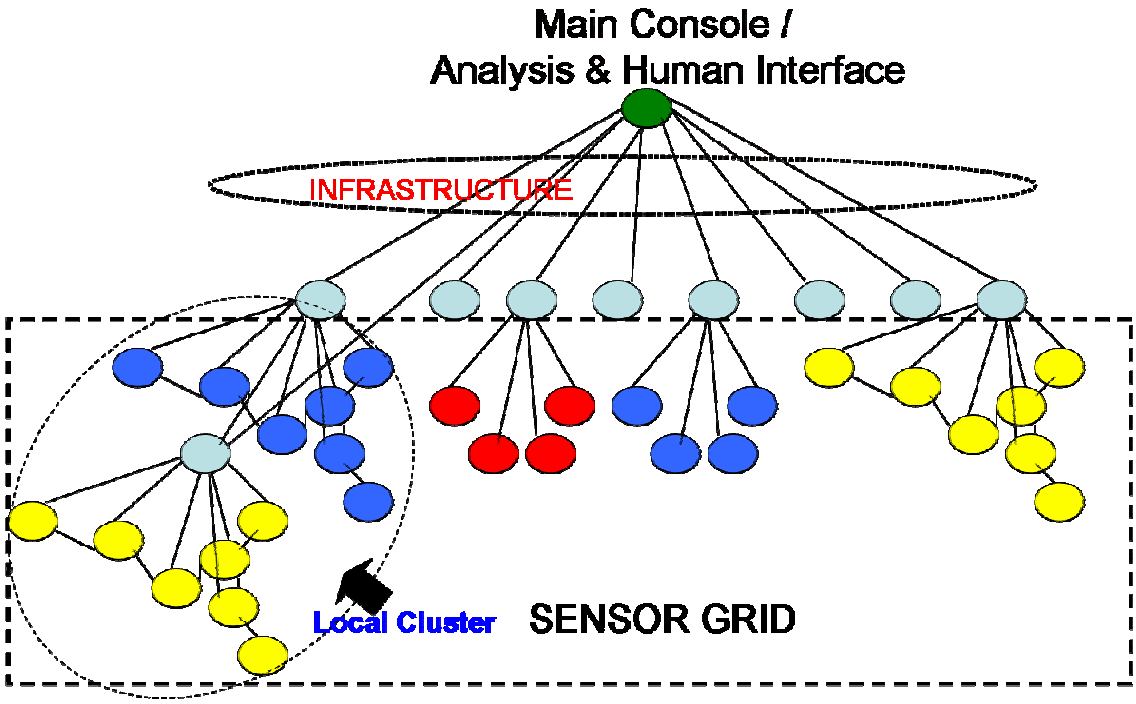


Figure 6. Example Sensor Grid.

Besides the extensibility issue of Baran's model, scale-free networks (SFN) have emerged as a form of network structure with important resilience properties [64]-[68], [70]-[72]. Scale-free networks have topology with centrally connected "hubs".

While investigating the topological structures in 1988, physicist Albert-Laszlo Barabasi and his colleagues from the University of Notre Dame discovered that the World Wide Web did not correspond to a "random" connectivity as was anticipated. Rather, it resembled what they termed a scale-free network. A visual depiction of scale-free networks is shown in Fig.7 where the "Wikipedia" server plays the central role of such a distinct "hub".

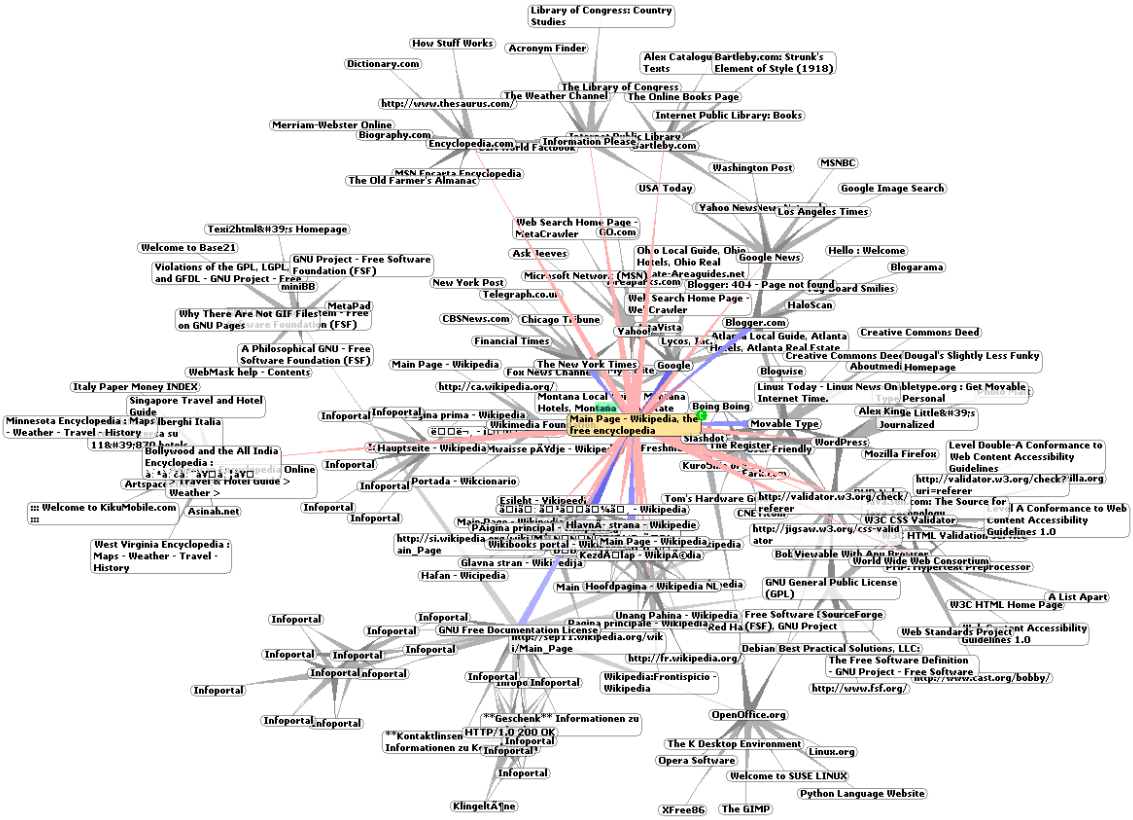


Figure 7. A Typical World Wide Web Connectivity.

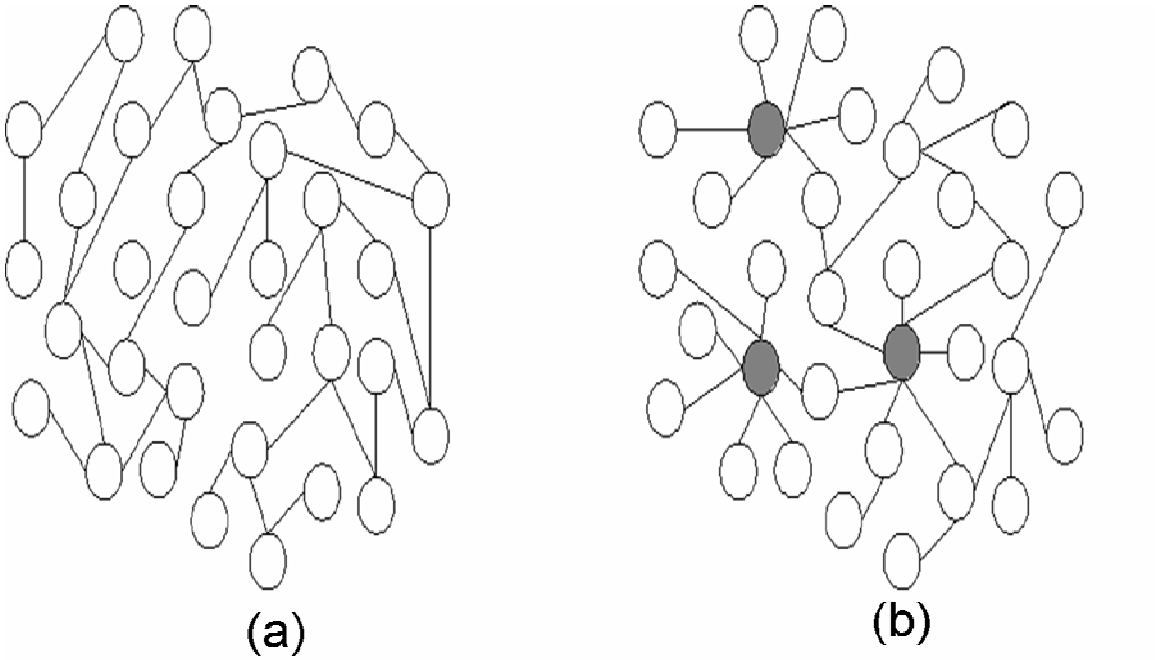


Figure 8. Comparison of Random and Scale-Free Networks. (a) Random, (b) Scale-free.

In Fig.8, a comparison of random and scale-free network is given. More specifically, scale-free networks exhibit power law degree distribution, i.e., $P(k) \sim k^{-\gamma}$ where *p(k)* gives the connectivity distribution of nodes in a network and *k* the number of edges that a node possess. The degree exponent γ is not universal and depends on the topology. Values of γ are mostly in the range $2 < \gamma \leq 3$.

One reason for the formation of such topologies given is due to "preferential attachment". This behaviour results in a few nodes in a network having a large number of connecting edges while a large number of nodes have few connecting edges. This is reflected by the power law degree distribution. Thus, scale-free networks do not resemble Baran's distributed networks or random networks in general. Scale-free networks can have different structures. These are illustrated in the Fig.9. Fig.9a illustrates metabolic network of a eukaryote organism, Emericella Nidulans. Fig 9b illustrates the Internet at the "Autonomous System" (AS) level while Fig.9c illustrates the metabolic network for archaea. Fig.9d illustrates the World Wide Web ("WWW"). Thus, scale-free networks are found in nature as well as man-made topologies.

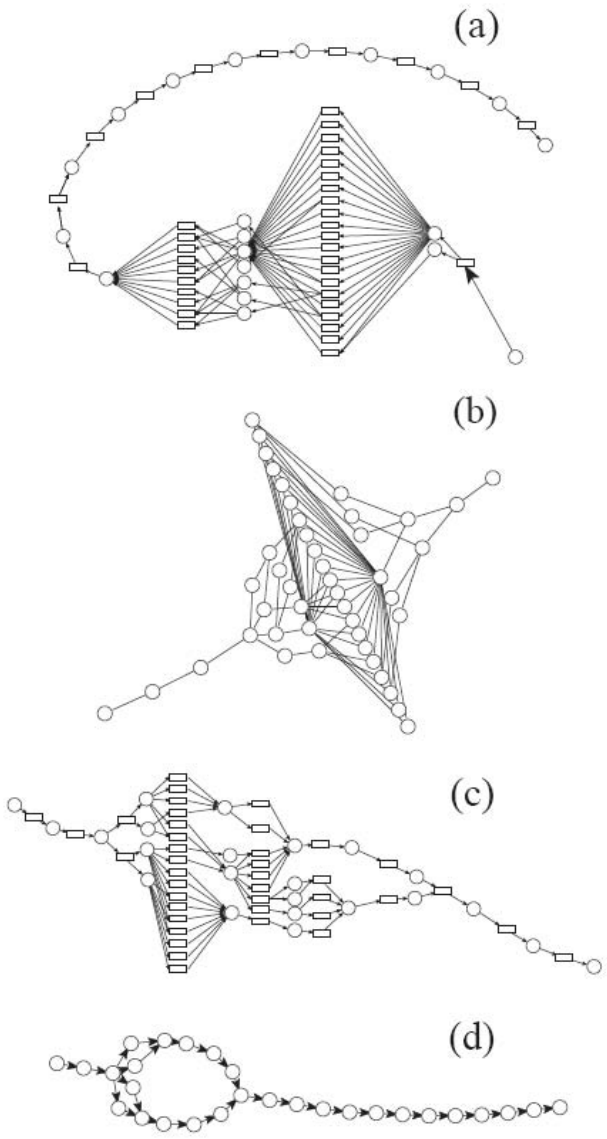


Figure 9. Different structures of scale-free networks (from Fig.4 [66]). (a) Metabolic network of a eukaryote organism, “Emericella Nidulans”, (b) Internet at the “Autonomous System” (AS) level, (c) Metabolic network for archaea, and (d) World Wide Web (“WWW”)

Scale-free networks have been analyzed [64]-[68], [71] and two main properties with respect to network resilience are:

- Robust against random removal of nodes, also known as “resilience to errors”

- Vulnerable to attacks, such as removal of specific nodes, i.e., those with large number of connecting edges

Another important property of this resilience is given by Adilson et al [73]. Adilson et al shows that the resilience of scale-free networks can be attributed to short-range links rather than long-range links. They explained that the short-range links have greater importance because of its higher traffic loading.

This gives insights that impact a design of robust wireless sensor networks:

- Point to point link quality is critical, especially in wireless networks where the link fluctuation can be substantial
- A network is vulnerable to errors on those links with high traffic loading. Thus, the protocols which are responsible for point-to-point communications should be robust at high traffic loading.

In addition, many scale-free networks exhibit small average distances between two nodes and also a high degree of clustering, although scale-free networks constructed using the Barabasi-Albert model do not necessarily result in high-degree clustering. The presence of such “small-world” phenomenon means that scale-free networks could indeed have the most resilient as well as efficient topologies that is currently known.

Since scale-free networks are inherently resilient and efficient, wireless sensor networks generated using scale-free topologies should be resilient as well as efficient. Furthermore, scale-free networks, as opposed to Baran’s distributed topology, is non-distributed and heterogeneous in nature.

This discussion of scale-free networks is important for wireless sensor networks from these considerations:

- It allows us to design artificial topologies modeled after scale-free networks to achieve both resilience and efficiency
- Design of a suitable artificial topology for wireless sensor network should consider the inherent vulnerability to attacks of specific links and cluster nodes

- A primary concern is the resilience of links with high traffic loads. Thus, wireless sensor networks should be enabled by protocols that maintains point-to-point links efficiently even under high loads

E. SCOPE OF INVESTIGATION

In general, the resilience of wireless sensor networks can be predicted based on two models: Baran's distributed, regular topology and scale-free networks. Baran's analysis on resilience can potentially be applied to wireless sensor networks with random topologies. However, it is a contention that many practical wireless sensor networks need not be random or distributed.

Furthermore, analysis and results on scale-free networks have recently emerged that demonstrate the resilience of scale-free networks compared to random, distributed networks. Thus, resilience can be incorporated into wireless sensors by creating artificial topologies that mimic scale-free networks.

The models for generating scale-free networks are not a focus of this thesis, since much work has been done in this area including notable works of Barabasi and Albert [70][71], Klemm and Eguiluz [72]. The purpose of this thesis is to investigate the protocol building blocks, with particular focus on the media access control (MAC) layer that enables the design and deployment of artificial scale-free wireless sensor networks.

The approach is as follows:

- Survey media access control protocols and identify a suitable MAC as a basic module to enable robust links for the formation of scale-free networks. The MAC selected should be flexible to incorporate an algorithm for "preferential attachment".
- Although scale-free networks are resilient to errors, they are vulnerable to attacks on key nodes. Thus, the proposed solution is to incorporate an appropriate redundancy scheme that operates seamlessly with the selected MAC. This concept is illustrated in Fig.10. In Fig.10, a secondary cluster head is used to backup the primary clusterhead in case it fails due to

physical or electronic attacks. A possible implementation of this scheme is shown in Fig.11 where a network of micro-sensors deployed and embedded possibly in a building structure communicates with an infrastructure through a clusterhead. The infrastructure comprise of both fixed, i.e., cellular as well as mobile, i.e., a fleet of micro- or nano-UAVs. In case the primary clusterhead fails or is attacked, a secondary clusterhead is immediately initialized to restore the connectivity of the sensor network with the communications infrastructure.

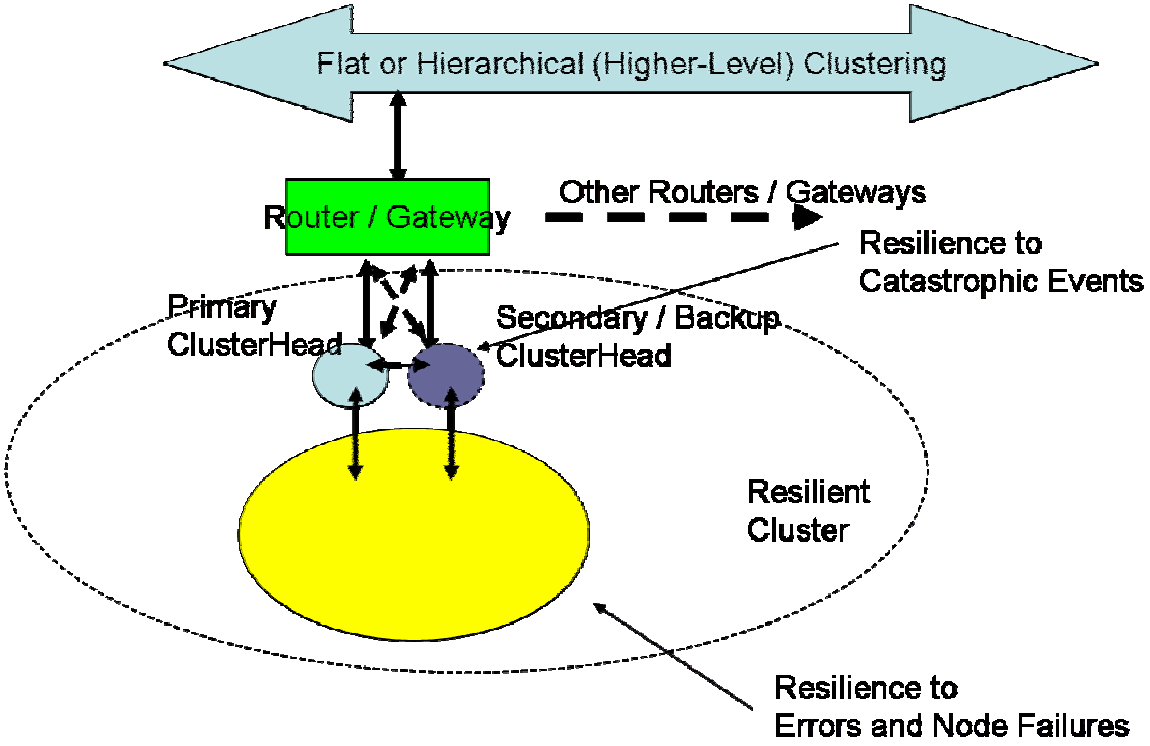


Figure 10. Proposed redundant and resilient wireless sensor network architecture.

- The selected MAC shall also be subjected to simulations to understand its efficiency and error resilience characteristics.

Our focus in this thesis differs from conventional research in wireless sensor networks from the following perspective:

- Emphasize resilience as the key to achieving high performance in wireless sensor networks that could meet complex and challenging requirements, especially those encountered by the military
- Combine a theory of scale-free networks with the protocol mechanisms of wireless sensor networks
- Understanding generic aspects of MAC protocols that enable scale-free networks, thus creating the widest possibility to complement current research by incorporating this work into a wide variety of wireless sensor MACs that are currently developed.

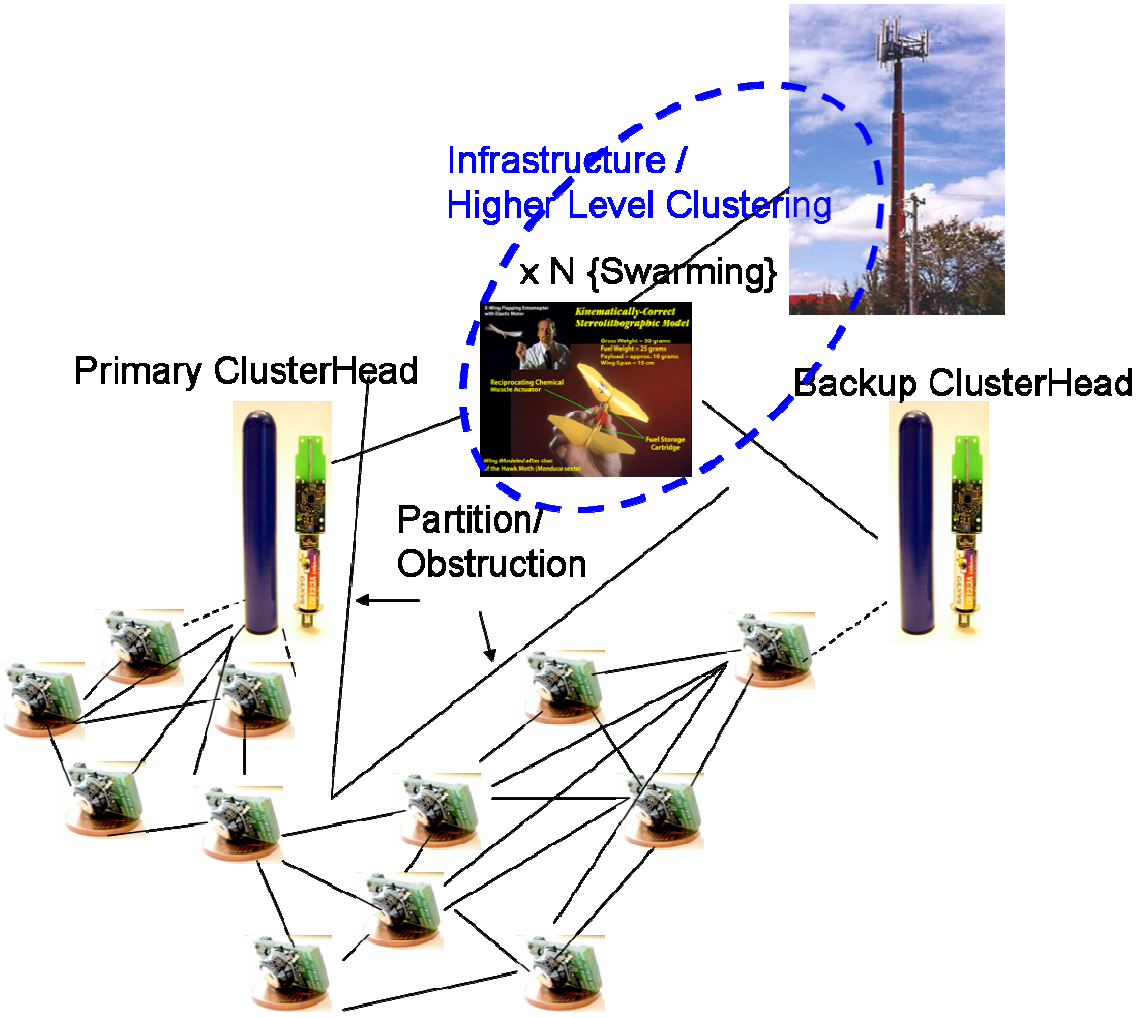


Figure 11. An example of a redundant and resilient wireless sensor network.

THIS PAGE INTENTIONALLY LEFT BLANK

II. MEDIA ACCESS CONTROL (MAC)

A. CHALLENGES OF MAC LAYER

In this chapter, the main emphasis shall be to survey some contemporary MACs and identify the key mechanisms that are relevant to wireless sensor networks. Using this understanding of the mechanisms, an appropriate MAC is selected as a possible basic building block of scale-free wireless sensor networks.

The concept of scale free networks and "small-world" phenomenon are introduced in Chapter I. In this chapter, results of experiments from real-world deployments and simulations of wireless sensor networks reinforce the notion that "small-world" phenomenon indeed contributes to the resilience and efficiency of sensor networks.

1. Performance of Wireless Sensor Network Experiments in Open Space

Turau et al. [34] deployed a real-world sensor network in the heathlands of Northern Germany. The goal of the experiment was to gain insight into the real-world problems of sensor networks, in particular, problems related to the radio links and the quality of those links as affecting multi-hop packet delivery performance.

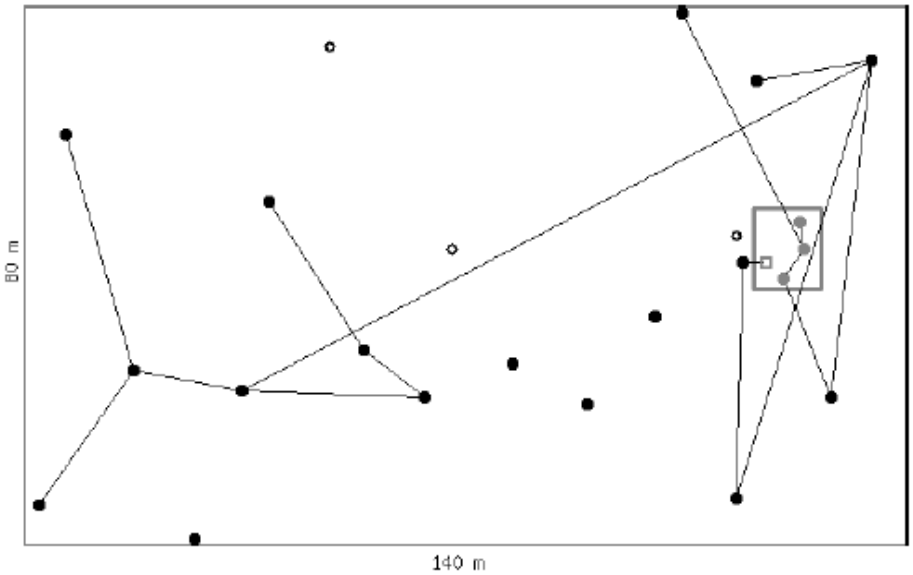


Figure 12. Heathland Deployment Topology (from Fig.3 [34]).

There were approximately 24 nodes and they were deployed as shown in Fig.12. A key result of those experiments was the exponential decay in the success of packet delivery as the hop count of the packet increases. This is shown in Fig.13.

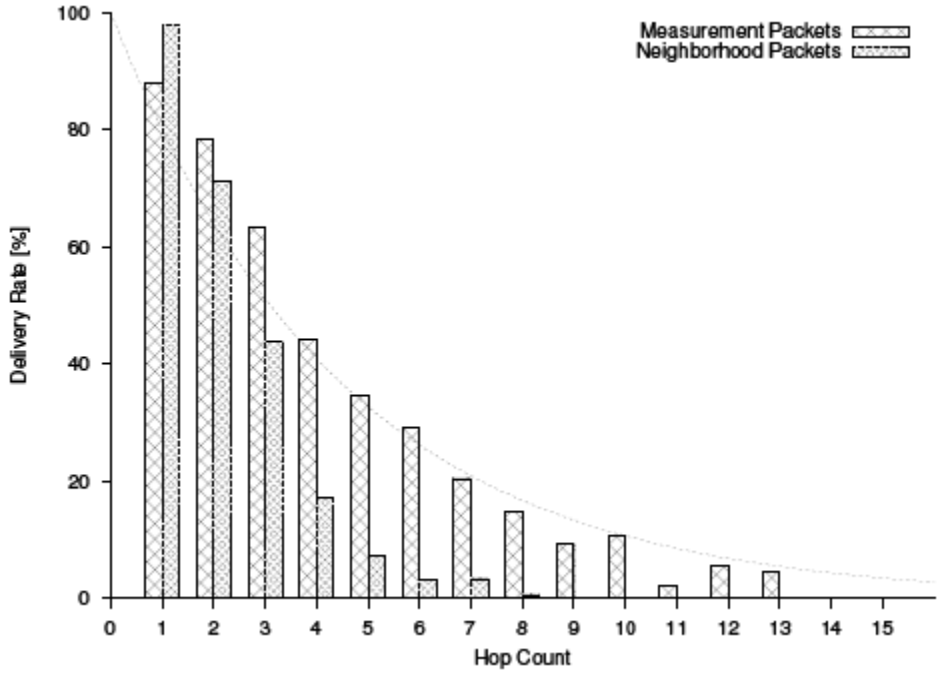


Figure 13. Relationship between Delivery Rate and Hop Count (from Fig.8 [34]).

Ideally, the network should have a 100% delivery rate. Unfortunately, in a wireless sensor network, because of energy restrictions, imperfection of the medium etc, the delivery rate will be much less than 100% in most cases. It is sensible to specify a delivery rate of at least 50-60%. In this case, the hop count of the packet should be restricted to three or less. This translates to a network with an end-to-end hop count of less than or equal to three. This relates directly to the cluster dimensions that are specified in Chapter I.

2. Performance in Urban Environment

It is interesting to note that in a separate experiment using sensor nodes in a building context, Schmid et al. [35] produced similar results to Turau et al. The topology and some results of that experiment are shown in Fig.14 and 15, respectively.

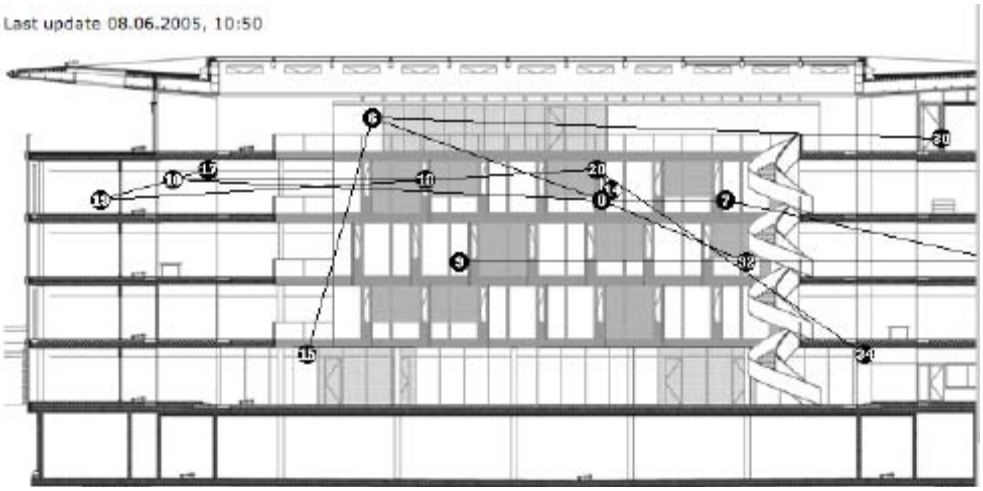


Figure 14. Topology of SensorScope (from Fig.2 [35]).

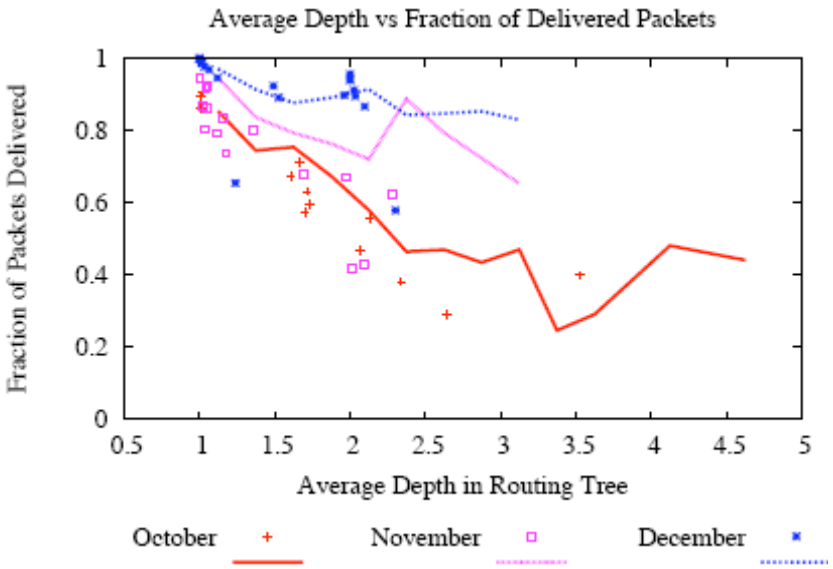


Figure 15. Relationship of Delivery Rate and Hop Count (from Fig.4 [35]).

In this experiment, 20 sensor nodes were deployed. They were all static and the batteries were changed whenever the voltage level falls below a certain threshold. It is evident from Fig.15 that an average hop count of three supports a packet delivery rate of at least 50-60%.

3. Insights and Implications from Limited Real-World Experiments

Although the above real-world experiments have limitations, they provide excellent sources of insight:

- Turau et al. [34] collected packet delivery rates in networks for up to 13-15 hop counts. The objective of extending the hop count is to test the routing algorithm. In general, the routing protocol is responsible for end-to-end routing of packets and has a large impact on multi-hop transmission delivery of packets. Routing protocols are responsible for how well networks scale to large number of nodes and perform at those scales.
- The MAC, on the other hand, is highly skewed towards the performance of hop-to-hop transmission and relaying of packets at the link level. It has a smaller scope of influence, i.e., 2 to 3 hops. Thus, the MAC performance is crucial to the performance of wireless sensor networks at the local cluster level. The routing protocols will have a larger role and are more critical at the system level.
- It is interesting that a low hop-count is required to support a fairly stable network. This result holds despite the fact that the two different experiments were conducted with different sensor platforms and protocols in very different RF propagation settings. Thus, the resilience of a wireless sensor networks is better built around the concept of “clusters”. This emphasizes the importance of “Small-world” phenomenon.

Before a discussion of energy-efficiency for MAC, which follows, it is non-trivial to note that insights from the experiments have implications:

- A resilient wireless sensor network that scales to large number of nodes is more likely to exhibit “small-world” phenomenon.
- From a cost perspective, it also makes sense to build the hierarchy for the wireless sensor network by leveraging existing infrastructure, i.e., cellular, satellite systems etc. An interesting and challenging aspect of future wireless sensor networks will be the investigation of multimode, multiband transceivers that can leverage the existing infrastructure in an energy-efficient manner, i.e., adapting protocols for extremely low-duty cycle transmission / reception.

B. ENERGY CONSUMPTION IN WIRELESS SENSOR NETWORKS

1. MAC Energy Consumption

In [41], Mustafa et al derived equations for the energy consumption of the MAC corresponding to the IEEE 802.11 standard. They derived and calculated the average energy consumed per Megabyte of information sent and received on an IEEE 802.11 network by modeling the state machine of a saturated IEEE 802.11 network using Markov chains for both the basic access and RTS/CTS modes. The energy consumed for basic access and RTS/CTS operations are given in Fig.16.

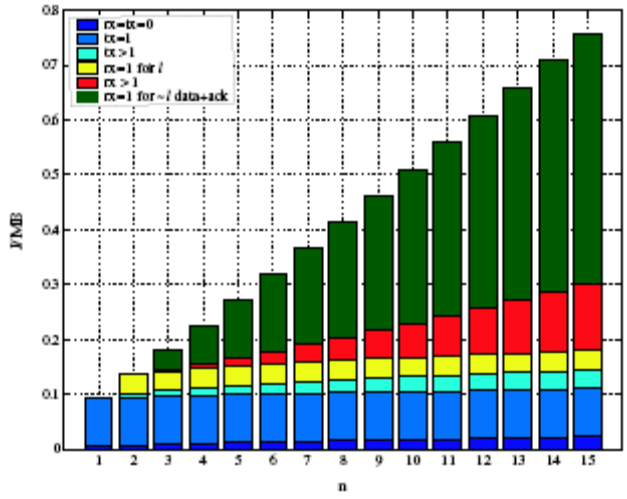


Figure 16. Energy Consumed per Megabyte of Information (J/MB) v.s. Network Size (n) for IEEE 802.11 Basic Access (from Fig.7 [41]).

There are several interesting observations from Fig. 16 based on the calculations of [41] (Note: Energy consumed is normalized to maximum total network energy consumption.):

- The successful transmission ('tx = 1') comprise 10 percent of the energy consumed and is constant regardless of the network size, n.
- The successful reception ('rx=1 for ~*l*') comprise approximately five percent of the energy consumed and is constant regardless of the network size, n.
- Failure to transmit because of backoff ('tx>1') wastes very little energy.
- Overhearing ('rx>1 for ~*l* data+ack'), the phenomenon where the receiver is turned on to listen on the channel even when the packet is not destined for it, wastes the most energy. This is almost 60 percent for network size of 15 terminals.
- Reception of collided packets ('rx>1') is the second most wasteful mechanism of the MAC in terms of energy consumption. This is responsible for approximately 15 percent for network size of 15 terminals.
- An interesting observation follows: an 'ideal' MAC should at least be six to seven times more energy-efficient compared to the IEEE 802.11 MAC operating in the CSMA/CA or basic access mode.

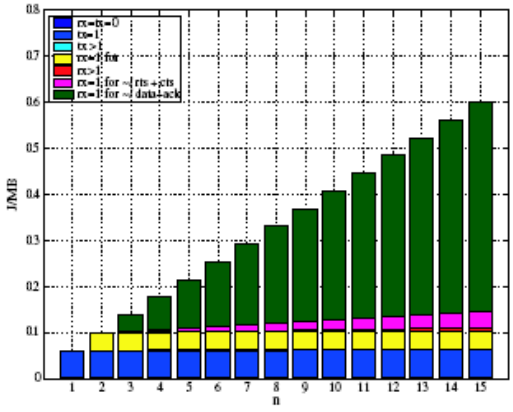


Figure 17. Energy Consumed per Megabyte of Information (J/MB) v.s. Network Size (n) for IEEE 802.11 RTS/CTS Mode (from Fig.8 [41]).

There are several interesting observations from Fig.17, based on the calculations of [41] (Note: Energy consumed is normalized to maximum total network energy consumption.):

- The overall energy consumed using the RTS/CTS mode is lower when compared to the basic access (CSMA/CA) mode.
- The successful transmission ('tx = 1') is again constant regardless of the network size, $_n$. For a network size of 15, the energy consumed is approximately 10 percent, similar to the basic access mode.
- The successful reception ('rx=1 for ~*l*') comprise approximately five percent of the energy consumed for network size of 15 and is constant regardless of the network size, $_n$.
- There is no energy wastage due to re-transmissions.
- Overhearing ('rx>1 for ~*l* data+ack'), the phenomenon where the receiver is turned on to listen on the channel even when the packet is not destined for it, wastes the most energy. This is almost 75 percent for network size of 15 terminals.
- Overhearing ('rx>1 for RTS/CTS') due to the RTS/CTS packets adds another 10 percent of energy wastage for a network size of 15 terminals.
- Collision of packets ('rx>1') is greatly reduced with the RTS/CTS mechanism and only slightly increase the energy wastage when the network size is substantial, i.e., network size of 15.
- An interesting observation follows: an 'ideal' MAC should at least be four times more energy-efficient compared to the IEEE 802.11 MAC operating in the RTS/CTS mode.

From both Fig.16 and 17, it is observed that the energy consumption and hence wastage (because the useful energy corresponding to perfect transmission and reception is constant regardless of network size) grows linearly with network size. This observation

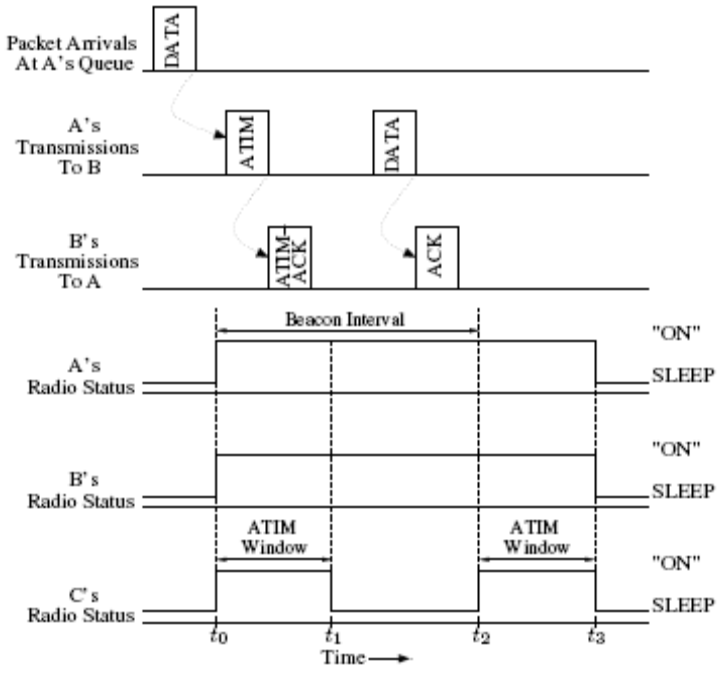
has implications: the size of a localized cluster matters in terms of energy efficiency and should preferably be small to medium sized.

An obvious conclusion that can be drawn is that ‘overhearing’ or ‘idle listening’ should be eliminated in order to minimize the energy wastage. This is also the direction taken for most MACs that will be discussed subsequently in this chapter.

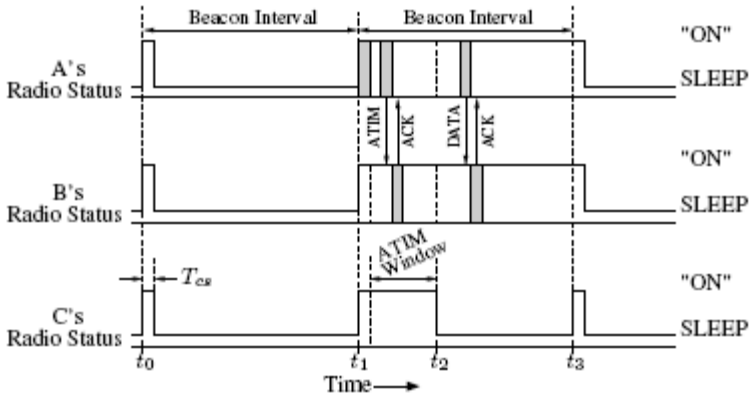
2. Impact of Carrier Sense

In an attempt to improve the energy-efficiency of IEEE 802.11 networks, Matthew et al. [43] indicated three possible approaches to augment the IEEE 802.11 Power Save Mechanism (PSM). The three key approaches are:

- Using carrier sense to determine if a node should listen on a channel for traffic advertisements. This is an attempt to reduce “overhearing” discussed in the previous section. The authors called this technique, “CS-ATIM” (Carrier Sense – Ad Hoc Traffic Indication Message). A modification to IEEE 802.11 PSM is shown in Fig.18. The scheme uses a beacon to synchronize all nodes and the “ATIM” message to indicate the traffic on the channel.



(a)



(b)

Figure 18. (a) IEEE 802.11 PSM mode (b) Proposed CS-ATIM augmention (from Fig.1 and 2 [43]).

- Dynamically resizing the ATIM window used by IEEE 802.11 PSM so that a node, not a recipient of a packet, should go to "sleep" much earlier than specified IEEE 802.11. This saves more energy. This technique is known as "D-ATIM" (D, for Dynamic). The augmentations are shown in Fig.19.

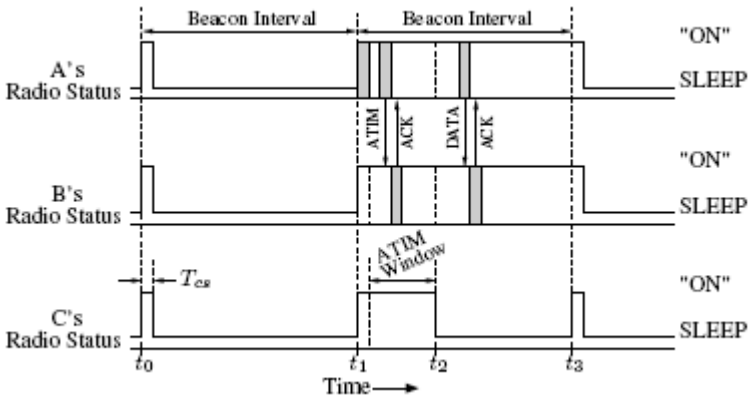


Figure 19. D-ATIM Augmention (from Fig.3 [43])

- The last technique is known as "per link beacon intervals" ("PLBI"). This technique is used to augment both "CS-ATIM" and "D-ATIM". "PLBI" addresses the problem that if many nodes send "ATIMs", a node in the

vicinity of those nodes would fair no better in terms of energy-efficiency than the IEEE 802.11 PSM mode as the node would have to be always "on" to listen to the "ATIMs". The proposal is to have each pair of node schedule their "wake-up" or "beacons" independent of the IEEE 802.11 PSM beacon. In the ideal scenario, where the schedules converge, every node will wake up accurately and specifically to send or receive data. In this scenario, the "PLBI"-based network converges to an optimal, energy-efficient operation.

The three approaches represent the three key ideas commonly used to reduce energy wastage due to "overhearing". They are:

- Using Carrier Sense (CS) or preamble sampling (a variation) to determine if a node should stay awake on a channel
- Using "adaptive listening" to minimize the amount of time a node "eavesdrop" on a communication, wasting unnecessary energy.
- Using distributed scheduling on a pair-wise basis to create an effective "conversation" cycle based on prevalent traffic conditions of the load

The second and third approaches are often bundled with carrier sense, highlighting the importance of carrier sense as a mechanism to reduce energy wastage. This can also be confirmed by scrutinizing Fig.4 [43] which shows that the performance of "CS-ATIM" is very close to the ideal or optimal IEEE 802.11 PSM performance.

The reader should also bear in mind that "optimality" here refers ***only*** to energy-efficiency. Intuitively, the latency increases as the energy consumed is decreased by using very low duty cycles. This can refer to low duration of the "on" radio state compared to the "off" radio state. For "CS-ATIM" scenarios, the beacons can be made to have very low frequency if a low-duty cycle is required.

It should also be mentioned that carrier sense techniques have its limitations [42] with respect to network throughput. Jamieson et al. [42] found through an experiment of 60 sensor nodes that:

- Carrier sense improves the link delivery rate under moderate loads because it improves re-transmission success rates.
- It has negligible effect for light loads.
- Throughput suffers at high loads because the nodes spend too much time performing carrier sense.

Thus, applying carrier sense and a combination of other energy reduction techniques, i.e., low-duty cycling, adaptive listening etc, result in a trade-off amongst three parameters: energy, throughput and latency. Intuitively, this means that the product of the three parameters of energy, throughput and latency results in a constant performance envelope; the energy-efficiency cannot be improved dramatically without severe degradation to throughput and latency and vice versa. Since a simple MAC cannot encompass all performance points within the envelope, the MAC must be designed and adapted to the scenarios as efficiently as possible to optimize performance.

3. Synchronous vs Asynchronous Wakeup Mechanisms

The IEEE 802.11 PSM is essentially a synchronous wakeup mechanism: it relies on all nodes having synchronized times. Thus, the IEEE 802.11 PSM is essentially a simple mechanism to reduce energy wastage over one-hop. Although Matthew et al [43] addresses the issue of extending the “D-ATIM” technique to a multiple hop environment using a “busy tone”, i.e., out-of-band, control channel, they have not tackled the issue of clock synchronization.

Thus, Rong et al. [44] proposes an asynchronous wakeup mechanism based on a randomly chosen wakeup pattern that is orthogonal for each node. Their proposed scheme has the potential to eliminate the need for system wide clock synchronization which could be very complex.

From the view of practical implementation, the technique of Rong et al. is more complicated. This is because different nodes in a network do not have to startup at the

same time and even if they do, subsequent clock drifts could degrade substantially the orthogonality of the schedules resulting in collisions or worse, non-communications equivalent to self denial-of-service.

C. MAC(S)

Since the IEEE 802.11 PSM standard and its augmentations have yet to be scalable to multiple hop environments, researchers in the field of sensor network communications have largely abandoned the use of IEEE 802.11 MAC and have instead chosen to design new MACs from scratch. This section studies some of these MACs.

1. S-MAC

S-MAC [45] is a low duty-cycle MAC using RTS/CTS scheme similar to the IEEE 802.11 wireless LAN standard. The main features of S-MAC are:

- A coordinated sleep-wake-listen-sleep cycle for all neighboring nodes. Each node maintains a table of the schedules for each neighboring nodes. This schedule is built up through the exchange of "SYNC" packets which reveal when the sender node wishes to sleep and wake. Essentially, every node can choose its own sleep and wake schedule, although the authors of S-MAC prefer that neighboring nodes are synchronized.
- Since the coordinated sleep-wake-listen-sleep cycle introduces substantially latency, S-MAC scheme proposes a technique called "adaptive listening". Adaptive listening enables intervening nodes in a chain of relaying hops to wake up at the end of the transmission of the preceding hop. In this way, the latency introduced by sleeping accumulated in the entire end-to-end path is greatly reduced. Each intervening node knows of the preceding neighbor's end of transmission because it has the schedule of its preceding neighbor and the sleep-wake cycle is fixed.
- Collisions are avoided through RTS/CTS mechanism. In addition, the RTS/CTS mechanism is also responsible for reducing "overhearing".

When a neighboring node, not participating in the conversation of two adjacent nodes, hears an RTS or CTS exchange not intended for itself, it goes immediately to sleep. (However, this has implications as mentioned in reference [46].)

In essence, S-MAC trades-off throughput and latency for energy-efficiency using a fixed sleep-listen cycle for each node with a low-duty cycle. The periodic listen-sleeping strategy is ideal for light loads. It is also shown in reference [51] that "adaptive listening" effectively reduces the latency incurred through accumulated sleep time across the path of communications.

Some problems of S-MAC are reported in reference [46]. One of the more critical impairment is that the scheme used to avoid overhearing using RTS/CTS actually increases the collision of packets and reduces the overall throughput. The authors [52] recommended not enabling "overhearing avoidance" as a solution. However, as RTS/CTS is also used to avoid collisions in S-MAC, this solution does not appear promising.

It should be mentioned that S-MAC is a complete protocol. This means that S-MAC is implemented and studied using Mica motes. The experiments in [45] are conducted using 11 nodes or less. The implementation has since been rewritten for ns-2 (simulation software) by Padma Haldar. Bugs are continued to be rectified and the S-MAC source is updated with newer releases of ns-2.

2. T-MAC

T-MAC [46] stands for "Timeout-MAC". Like S-MAC, T-MAC is a contention-based scheme. It attempts to improve over the original S-MAC (without "adaptive listening") by reducing the amount of time a node must be up listening even though it does not participate in a communication, i.e., "idle-listening" or "overhearing". In the original S-MAC, as the listen/sleep cycle is fixed, the listen duration is constant even though there is no real communication. T-MAC tackles this problem by using a "time-out" scheme to adapt the "listen" duration according to the traffic on the network. Thus, it

claims to be able to save up to 96 percent of the energy compared to the earlier version of S-MAC and use the channel for as little as 2.5 percent of the time (an extremely low duty cycle) for low loads.

The significance of T-MAC is its adaptive duty cycle. However, this has several problems including the "early sleep problem" mentioned by the authors [46]. The techniques in T-MAC and the "adaptive listening" protocol in the new version of S-MAC (discussed in the previous section) shares many similarities. From the literature, it is not clear if the new version of S-MAC, by adopting the same technique to reduce latency and duty-cycle, shares the same problems as indicated by the authors [46] for T-MAC.

3. B-MAC

B-MAC [47] was developed by Joseph Polastre who has since co-founded Moteiv, a company dedicated to the implementation of wireless sensor networks.

The philosophy of B-MAC is different from both S-MAC and T-MAC in the sense that it recognizes the inherent trade-offs amongst the parameters of energy, throughput and latency. Unlike S-MAC which uses energy-efficiency as its main criteria for design, B-MAC is a re-configurable MAC which enables an engineer to shape and optimize the energy-throughput-latency design space according to the applications and scenarios.

Its main features include using low overhead preamble sampling for clear channel assessment and packet backoff for lower power operations and collision avoidance, and link layer acknowledge for reliability. It does not have RTS/CTS scheme but it exposes a set of interfaces for such algorithms to operate on top of the B-MAC protocol.

It is also interesting to note that because of the lower overheads, B-MAC is capable of higher throughputs compared to S-MAC by approximately 4.5 times [47]. Since B-MAC is a minimalist protocol, it is possible to develope highly efficient bulk message transfer protocol over B-MAC that surpass the throughput, latency and energy-eficiency of S-MAC.

The central theme of “reconfiguration” underpinning B-MAC is an interesting concept. B-MAC demonstrates that for a rich platform like wireless sensor networks “reconfiguration” is a critical feature.

4. Etiquette Protocol

The Etiquette Protocol is devised by Goel et al. [48]. The main feature of the Etiquette Protocol is that instead of fixed listen / sleep cycles, typified by S-MAC, it enables sender and receiver pairs to schedule their own communications. A parameter – “maximum office hour period” – enables a designer to choose the desired operating point in the latency-energy tradeoff space. A larger value of this parameter increases the latency but reduce the energy consumption of the node.

The scheme operates on top of an RTS-CTS protocol and has important parameters configurable based on the applications and scenarios. As a result, it is capable of much lower duty-cycle operation compared to S-MAC [48].

5. IEEE 802.15.4

This shall be discussed in greater depth in the next chapter.

D. CHOICE OF MAC

The MACs discussed above share many similarities in their mechanisms. Essentially, these mechanisms are designed to enable a trade-off amongst the three parameters of throughput, latency and energy. Thus, no matter which MAC is chosen, a gain in performance of one dimension means a loss in another. A choice would depend on the specific circumstances of deployment scenarios and applications.

B-MAC differs from the other MACs by its greater adaptability. Adaptability is an important attribute if different scenarios and applications are to be accommodated. In many ways, adaptability complements resilience.

It will be discussed in the next chapter that the combination of IEEE 802.15.4 (physical and MAC layer) and ZigBee Alliance standard (network protocol) is the most promising for wireless sensor networks. Like B-MAC, it is well-layered and provides a

combination of link management mechanisms that can be enabled selectively depending on the user configuration. This means that it places adaptability tools at the hands of the user.

It also has a comprehensive specification addressing basic deployment requirements such as network configuration, management and security services to guarantee data confidentiality and integrity [54] [55].

In addition, a thorough study of the IEEE 802.15.4 standard reveals that it has the flexibility to incorporate scale-free network generation algorithms.

From the perspective of adoption, the ZigBee and IEEE 802.15.4 standard is rapidly adopted and commercialized, leading to mature rapid prototyping products. This creates ease of measurements using real wireless sensor nodes for concept validation.

Thus, the investigation on resilient and autonomous wireless sensor networks in this thesis shall be conducted using the ZigBee and IEEE 802.15.4 standard. The details of these standards are given in the next chapter.

III. IEEE 802.15.4 ZIGBEE PROTOCOL

A. ZIGBEE AND IEEE 802.15.4

The ZigBee technology was initially designed for low-rate, low power consumption wireless networking protocols for automation and remote wireless applications. Although IEEE 802.15.4 was established later, ZigBee and IEEE 802.15.4 soon form an alliance – ZigBee became the commercial name for the IEEE 802.15.4 standard.

There is another distinction: whereas IEEE 802.15.4 continues to specify the lower physical and Media Access Control (MAC) layers (as is IEEE 802.11), the ZigBee alliance provides Layer 3 and above specifications, i.e., networking, management protocols, etc.

The general IEEE 802.15.4 specifications are given in Fig.20.

IEEE 802.15.4 PHY PARAMETERS		
Parameter	***2.4 GHz PHY***	***868/915 MHz PHY***
Sensitivity @ 1% PER (dBm)	–85	–92
Receiver maximum input level (dBm)	–20	
Adjacent channel rejection (dB)	0	
Alternate channel rejection (dB)	30	
Output power (lowest maximum) (dBm)	–3	
Transmit modulation accuracy (%)	EVM < 35 for 1000 chips	
Number of channels	16	1/10
Channel spacing (MHz)	5	single-channel/2
Transmission rates data rate (kb/s) symbol rate (ksymbol/s) chip rate (kchip/s)	 250 62.5 2000	 20/40 20/40 300/600
Chip modulation	O-QPSK with half-sine pulse shaping (MSK)	BPSK with raised cosine pulse shaping
RX-TX and TX-RX turnaround time	12 symbols	

Figure 20. IEEE 802.15.4 Specifications (from Table I [75]).

ZigBee is basically different from Bluetooth. These are some targets for ZigBee:

- Operate for 6 months to 2 years with 2 AA sized batteries
- Operational range of ZigBee is 10-75m compared to 10m of Bluetooth
- Data rates are 250 kbps at 2.4 GHz, 40 kbps at 915 MHz and 20 kbps at 868 MHz. Bluetooth is 1 Mbps typically at 2.4 GHz.
- Enables 254 operational nodes in a network whereas the basic configuration of Bluetooth is the “scatternet” with 8 nodes operated in master-slave mode.
- Enables fast network synchronization, i.e., sleep to wake in 15 msec as compared to 3 seconds of Bluetooth.
- Simple protocol for handling small data packets compared to voice, images and file transfers in Bluetooth “scatternets”.

B. IEEE 802.15.4 – GENERAL DESCRIPTION

The IEEE 802.15.4 system comprises the full-functioning device (FFD) and the reduced-function device (RFD). The 802.15.4 network shall include a FFD operating as the network co-coordinator. (In the literature, this is normally referred to as the “PAN” coordinator.)

The network can be configured in 3 basic modes: star, peer-to-peer or meshed, and cluster-tree topology. These configurations are shown in Fig.21 and 22.

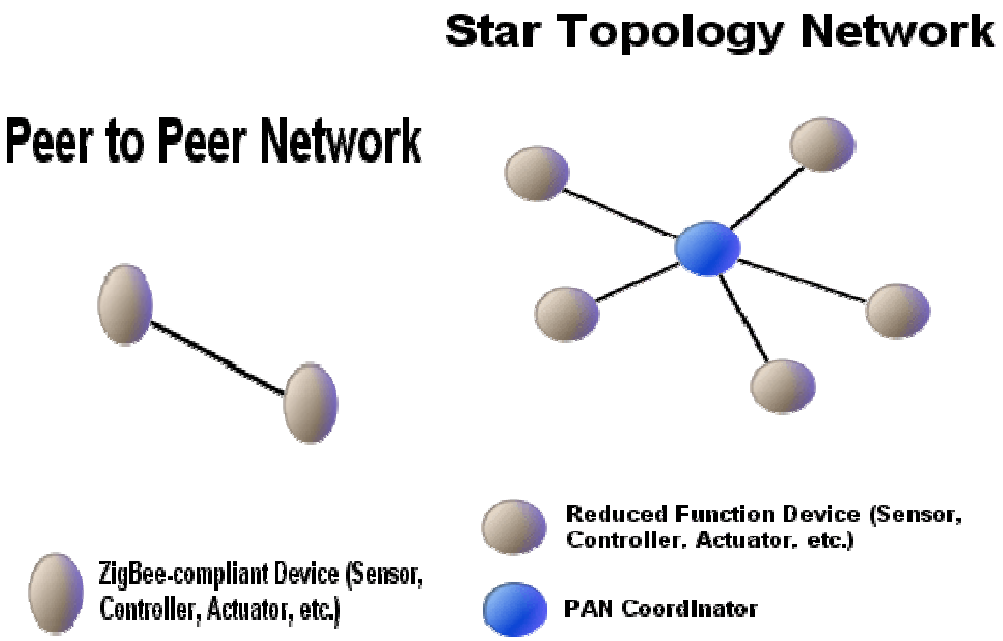


Figure 21. Star or Peer-to-Peer based Networks (from [74]).

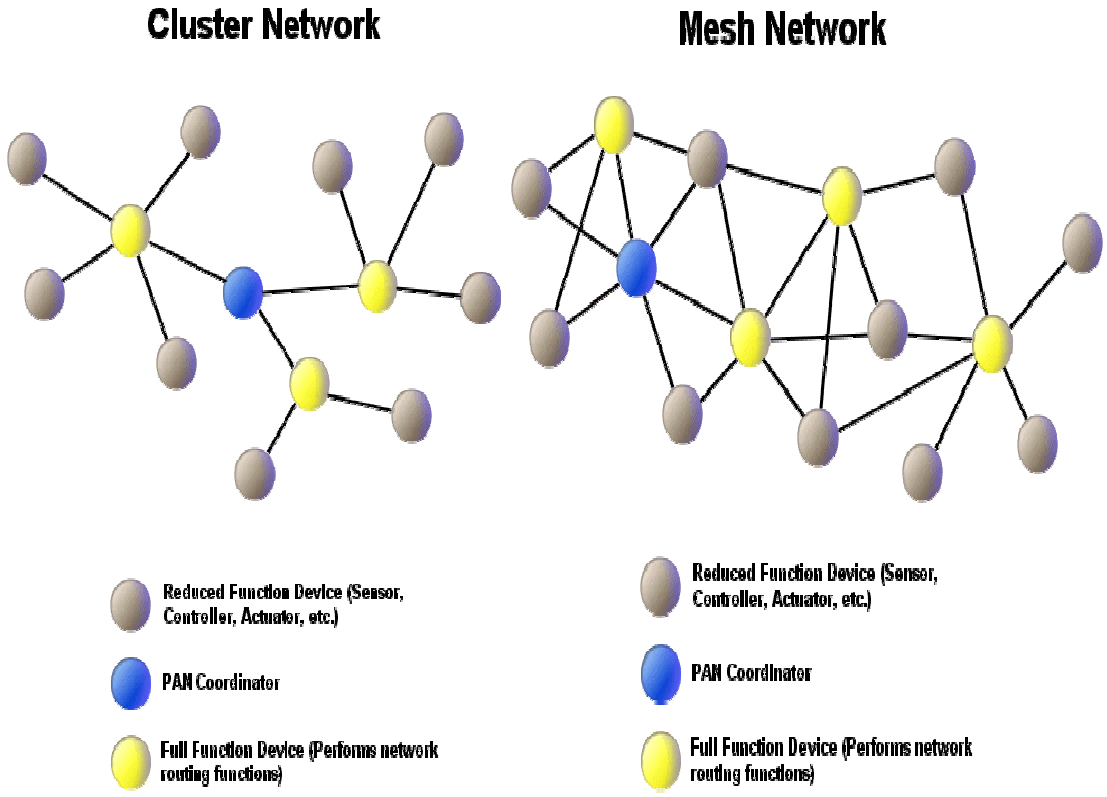


Figure 22. Cluster-based or Meshed Networks (from [74]).

In the “Star-Topology” network, the RFDs connect to each other via a central coordinator – a FFD acting as a PAN coordinator. The topology is suitable for direct connection of sensors to a coordinator or gateway.

In the “cluster” network, multiple “star-topology” networks are connected via a FFD acting as a PAN coordinator. In this configuration the intermediate FFDs (colored yellow) acts as routers for autonomous relaying of information. RFDs connect to FFDs only. The “cluster” configuration adds an additional layer of intermediate “routing” FFDs. This “clustering” configuration enables the network to scale up the number of nodes and extend the reach of the network. This network configuration is suitable for the creation of a hierarchical distribution of nodes. It is also suitable in networks where the data dissemination follows a hierarchical order.

The “meshed” network is a superset of the “cluster” network in that RFDs can connect directly with both FFDs and RFDs. In the “cluster” network, the RFDs connect with a single FFD.

In general, the ability of the IEEE 802.15.4 networks to route and forward information is limited by the presence and availability of the FFDs. These FFDs evidently consumes more power and may require special power supply compared to the RFDs.

The IEEE 802.15.4 device architecture is given in Fig. 23. The architecture is very similar to the IEEE 802.11 and Ethernet specification. It has a physical layer and a datalink layer comprising of Media Access Control (MAC) and the Logical Link Control (LLC) layers.

The difference is the presence of the “Service Specific Convergence Sublayer” (SSCS) which provides the necessary signals and handshakes to enable the different network topologies mentioned. It also abstracts these functions from the LLC.

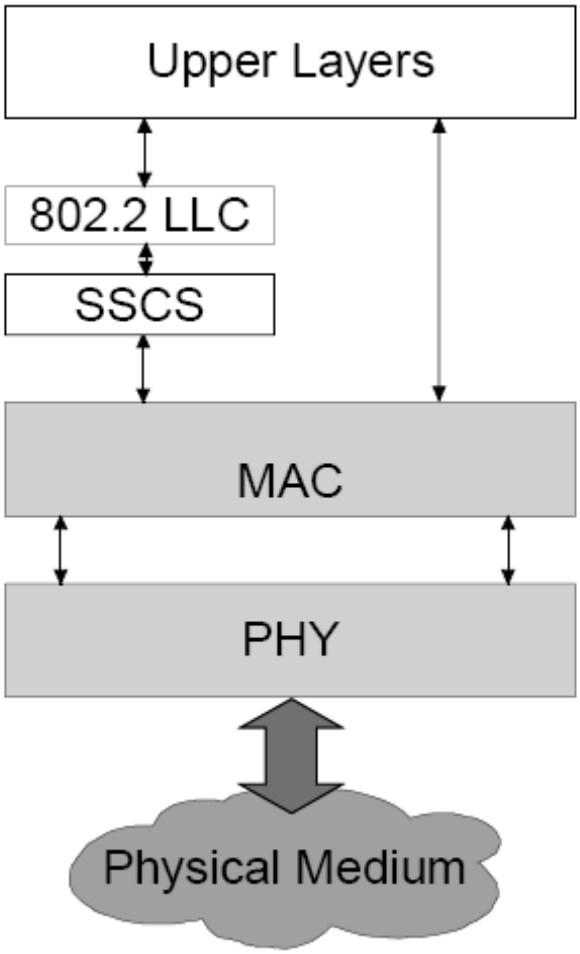


Figure 23. IEEE 802.15.4 Protocol Stack (from Fig.3 [55]).

C. IEEE 802.15.4 PHYSICAL LAYER

1. General Description

The physical layer provides activation and deactivation of the radio transceiver, and transmitting and receiving packets. In addition, to improve efficiency, the physical layer has the following features: energy detection (ED), link quality indication (LQI), channel selection, clear channel assessment (CCA).

The data signal is spread using Direct Sequence Spread Spectrum (DSSS) at the chip rate given in Fig.24. The spread signal is then modulated based on one of two modulation formats: BPSK and O-QPSK (MSK).

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

Figure 24. Modulation Formats (Table 1 [55]).

The receiver sensitivities are -85dBm for 2.4 GHz and -92dBm for 868/915 MHz. The sensitivity gain of 7dB derives from the lower rate at the higher frequency.

2. Receiver Energy Detection (ED)

The receiver energy detection (ED) is used by the channel selection algorithm in the network or application layer. It estimates the received signal power within the bandwidth of the channel. There is no attempt to decode signals on the channel. The ED time is equal to 8 symbol periods. The ED values span at least 40dB in the received signal.

3. Link Quality Indication

The LQI measurement gives an indication of the strength and/or quality of a received packet. The measurement may be implemented using receiver ED, a signal-to-noise estimation or a hybrid of such methods. The LQI result is used by the network or application layer.

4. Clear Channel Assessment (CCA)

The clear channel assessment uses one of three techniques:

a. Energy above threshold. CCA reports a busy medium upon detecting any energy above an ED threshold.

b. Carrier sense only. CCA reports a busy medium upon the detection of a signal with the modulation and spreading characteristics of IEEE 802.15.4. This signal may be above or below the ED threshold.

c. Carrier sense with energy above threshold. CCA reports a busy medium only upon the detection of an IEEE 802.15.4 signal with energy above the ED threshold.

5. Physical Protocol Data Unit (PPDU)

The PPDU structure is shown below. It consists of the following:

a. SHR. This allows a receiving device to synchronize and lock into the bit stream.

b. PHR. This contains the frame length information.

c. Payload. This carries the MAC sublayer frame.

Octets: 4	1	1		variable
Preamble	SFD	Frame length (7 bits)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

Figure 25. Physical Protocol Data Unit (PPDU) Structure (from Fig.16 [55]).

D. IEEE 802.15.4 MEDIA ACCESS CONTROLLER

1. Superframe Structure and CSMA-CA

The MAC sublayer provides beacon management, channel access, GTS management, frame validation, acknowledged frame delivery, association and disassociation functions. The MAC layer can support a superframe format shown in Fig. 26.

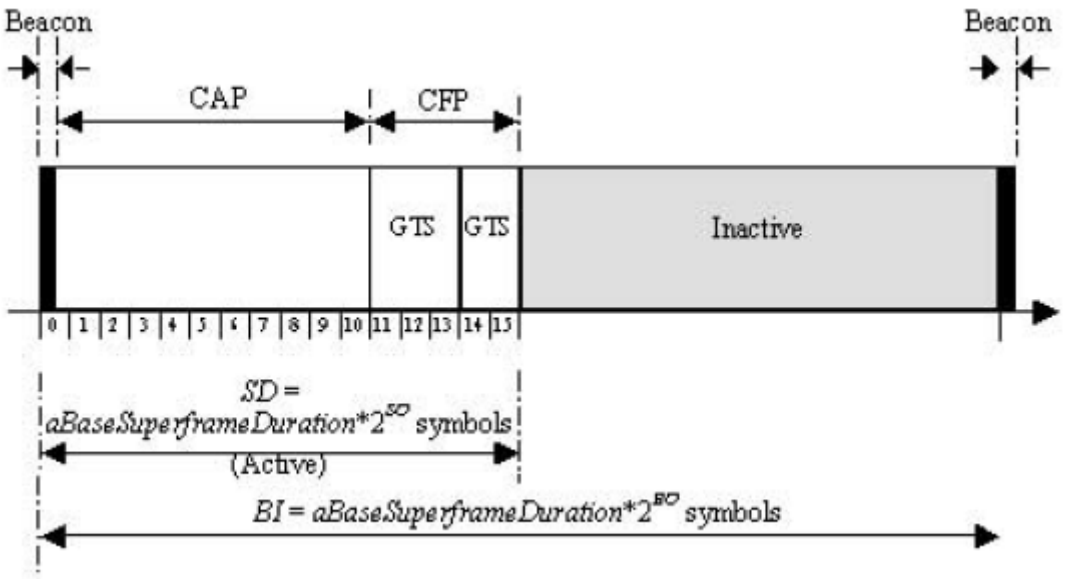


Figure 26. Superframe Structure (from Fig.59 [55]).

The superframe is delimited by the network beacons. The superframe can have both active and inactive portions. The network beacons are used by the coordinators (FFDs) to synchronize with the attached devices, network identification and to describe the superframe format. The active portion of the superframe comprise of two segments: the contention access period (CAP) and contention free period (CFP). The contention access period is self-explanatory. The CFP comprise guaranteed time slots (GTSs) for devices which require guaranteed bandwidth.

The duration of the active and inactive parts of the superframe are described by the values of "macBeaconOrder" *(BO)* and "macSuperFrameOrder" *(SO)*. Both BO and SO are indices that describe the length of the superframe and the active parts of the superframe respectively.

The beacon interval (BI) is equivalent to a length of aBaseSuperFrameDuration*2^{BO} symbols, where BO ranges from 0 to 14. The superframe duration (SD) is equivalent to a length of aBaseSuperFrameDuration*2^{SO} symbols, where SO ranges from 0 to 14.

The active part of each superframe is divided into “aNumSuperFrameSlots” equally spaced slots of duration aBaseSlotDuration*2^{SO} and is composed of three parts: a beacon, a CAP and CFP. (Therefore, aBaseSuperFrameDuration= aNumSuperFrameSlots* aBaseSlotDuration.)

The CAP shall be at least “aMinCAPLength” symbols. (This is relaxed if additional space is required to momentarily accommodate an increase in the **beacon** frame length to perform GTS maintenance. All frames shall use **slotted CSMA-CA** to access the channel during the CAP with the exception of acknowledgement frames and its subsequent data frames following a data request command.

A transmission during the CAP must be completed at least one IFS (“Inter-frame Separation”) duration before the end of the CAP. (IFS time is the amount of time necessary to process the received packet by the physical layer.) Otherwise, the transmission is deferred to the CAP of the next superframe. The CFP starts on a slot boundary immediately following the CAP and extends to the end of the active portion of the superframe.

As illustrated in Fig.27, frames up to a length given by “aMaxSIFSFrameSize” shall be followed by a SIFS (“Short-IFS”); frames of greater length shall be followed by a LIFS (“Long-IFS”).

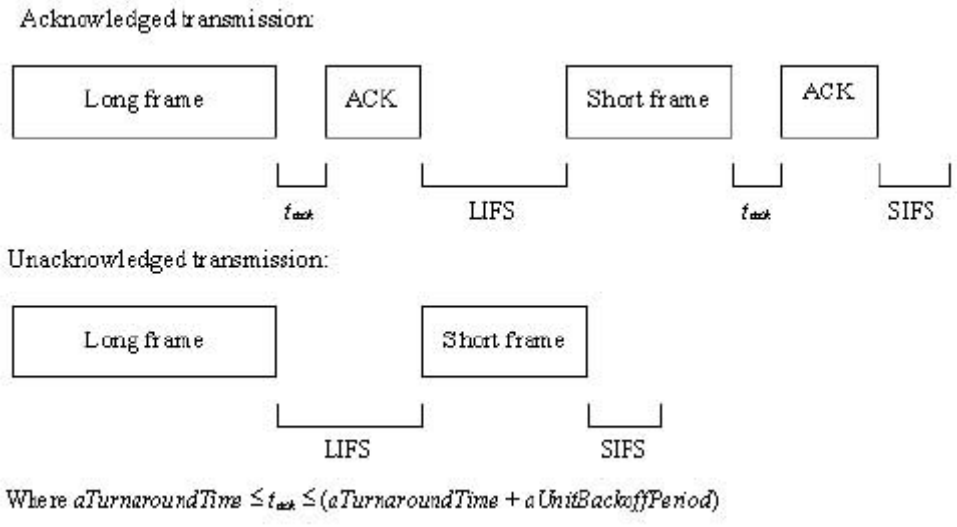


Figure 27. Interframe Separation (IFS) Concept Illustration (from Fig 60 [55]).

If the PAN does not use the superframe, i.e., operate in **non-beaconed mode**, both "macBeaconOrder" and "macSuperFrameOrder" shall be set to 15. In this kind of network, all transmissions except the acknowledgement frame shall use **unslotted CSMA-CA** to access channel. In this mode, there shall be no GTSs. (The interested reader is referred to Fig.61 of [55] for the CSMA-CA algorithm flow-chart.)

In the slotted CSMA-CA mode, the devices are synchronized on their backoff periods whereas, in unslotted CSMA-CA, devices do not need to be synchronized on their back-off periods.

IEEE 802.15.4 also offers a "battery life extension" (BLE) mode. This is illustrated in Fig.28. Note that the co-ordinator can turn off its receiver "macBattLifeExtPeriods" backoff periods after the interframe spacing (IFS) period of the beacon frame when there is no signal on the channel. This is illustrated by the arrow in Fig.28. Thus, it is able to reduce power consumption in the receive mode. If, as illustrated in Fig.28, "Device 1" transmits a frame that exceeds this turn-off point, the co-ordinator will continue to listen and receive the frame.

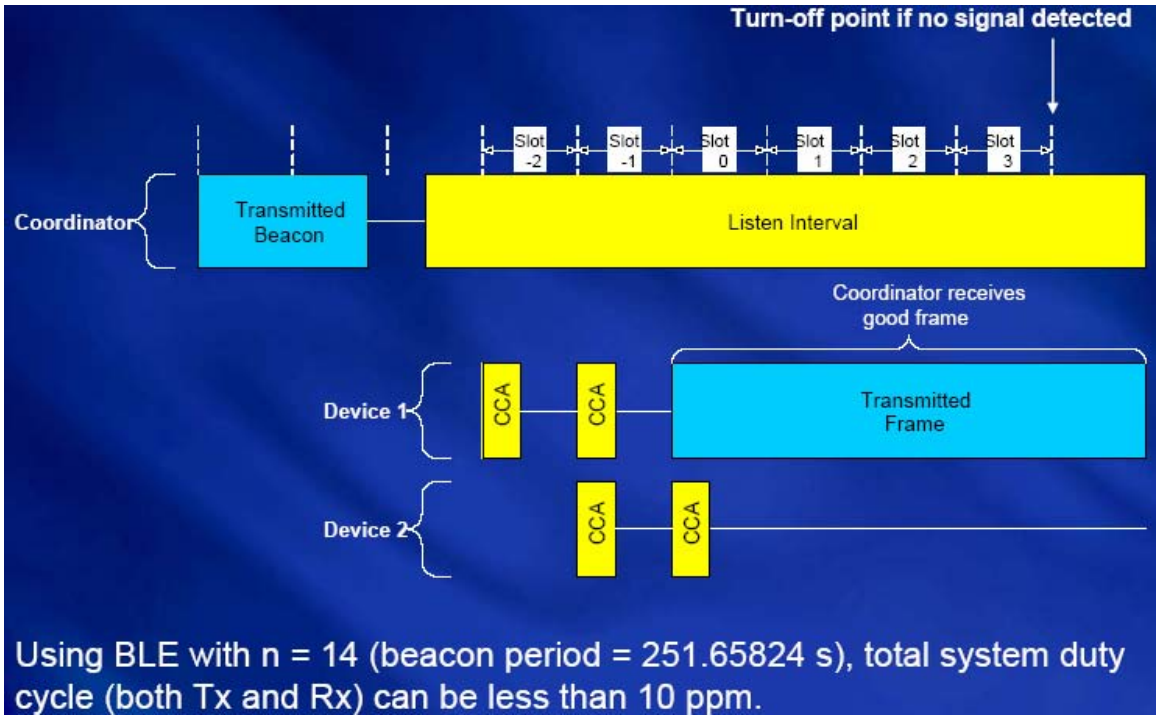


Figure 28. Battery Life Extension Mode (from [56]).

2. Data Transmission Modes

There are three types of data transmission modes: coordinator to device, device to coordinator and peer-to-peer.

When the coordinator wishes to send the device information, the coordinator would store the information and indicates that the message is pending in the beacon. In an un-beaconed network, the coordinator would store the message and wait for the device to poll the coordinator information. This polling is defined by a fixed interval that is pre-defined.

When a device wishes to send data to the coordinator, it has to synchronize with the superframe structure using the beacon from the coordinator and then transmitting the information at the right time using slotted CSMA-CA. In a non-beaconed network, the device just sends information using the unslotted CSMA-CA.

In peer-to-peer mode, the nodes can communicate directly with each other either through unslotted CSMA-CA or through node synchronization first before transmission to save power.

The data frame and acknowledgement frame are shown in Fig.29 and 30 respectively. The data frame comprise of the MAC header (MHR) followed by the data payload and a MAC footer (MFR). The MHR comprise of the frame control, sequence number and addressing fields while the MFR contains a 16-bit frame check sequence (FCS). The acknowledgement frame is essentially same as the data frame without the payload.

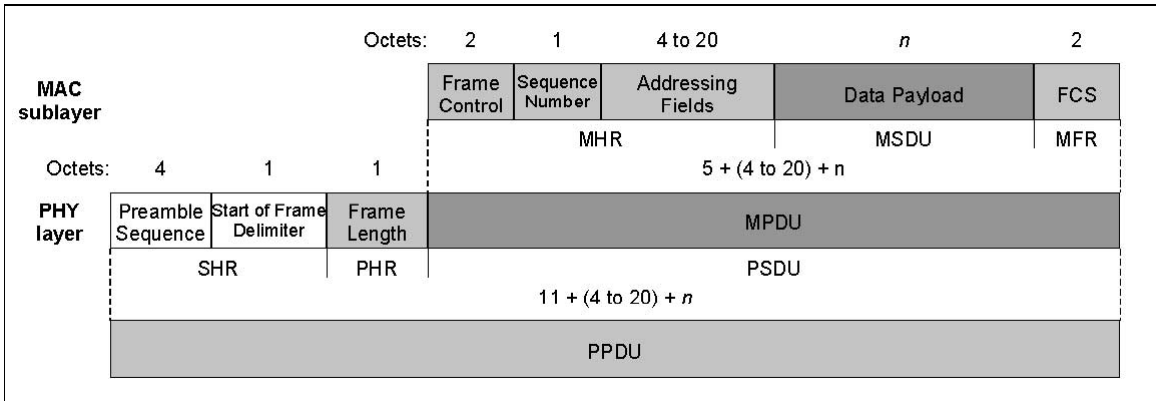


Figure 29. Data Frame (from Fig.11 [55]).

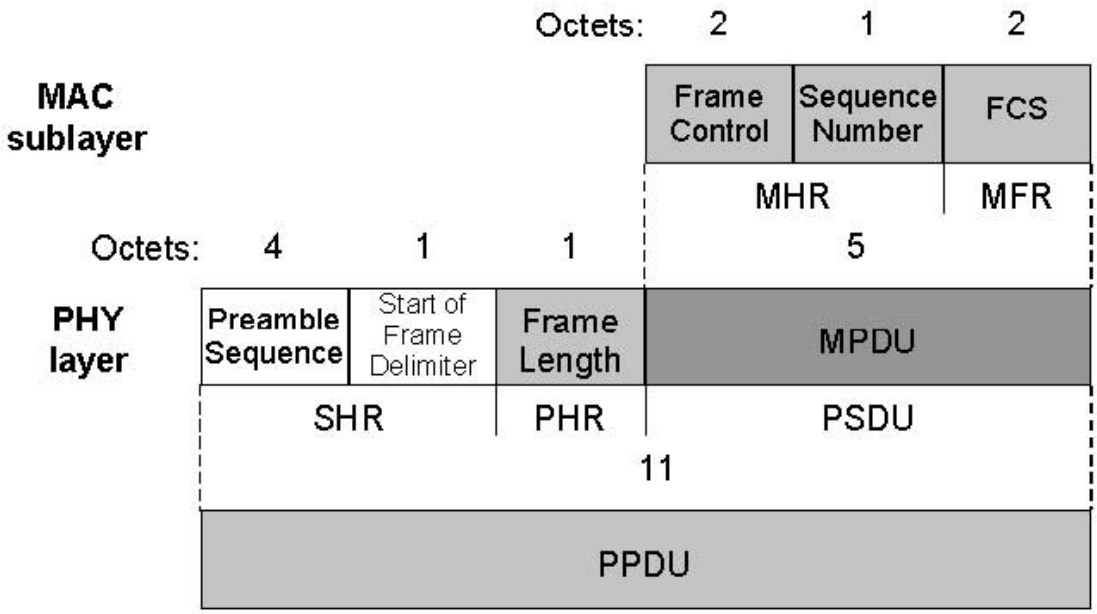


Figure 30. Acknowledgement Frame (from Fig.12 [55]).

3. Association and Disassociation

An FFD may transmit beacon frames shown in Fig.31. These frames enable RFDs to perform device discovery. An FFD that is not the network coordinator shall commence beaconing only when it has successfully associated with a network.

The association process commences when it has completed either an active channel scan or a passive channel scan. It is this scanning process that enables a device to locate any possible coordinator. It is possible that multiple coordinators are active. *From the channel scan, the device selects one of the multiple area networks to associate with. IEEE 802.15.4 leaves the selection algorithm open for implementation. (This flexibility can be very important because it means there is no restriction to any one node having preferential affiliation. This can result in nodes with very large number of links connecting to it. This is, afterall, a central tenet of scale-free networks. Thus, the flexibility leaves open the possibility for creating scale-free networks by appropriate node affiliation algorithms.)*

It should be reminded that during an active scan, *the MAC sublayer just listens to the beacon frames given in Fig.31 and discards everything else*. *If the beacon frames are intentionally or non-intentionally jammed, the device will continue to wait for the beacon*

frames and discard any data frames that it receives. This could pose a ***a self-inflicted denial-of-service*** *problem .*

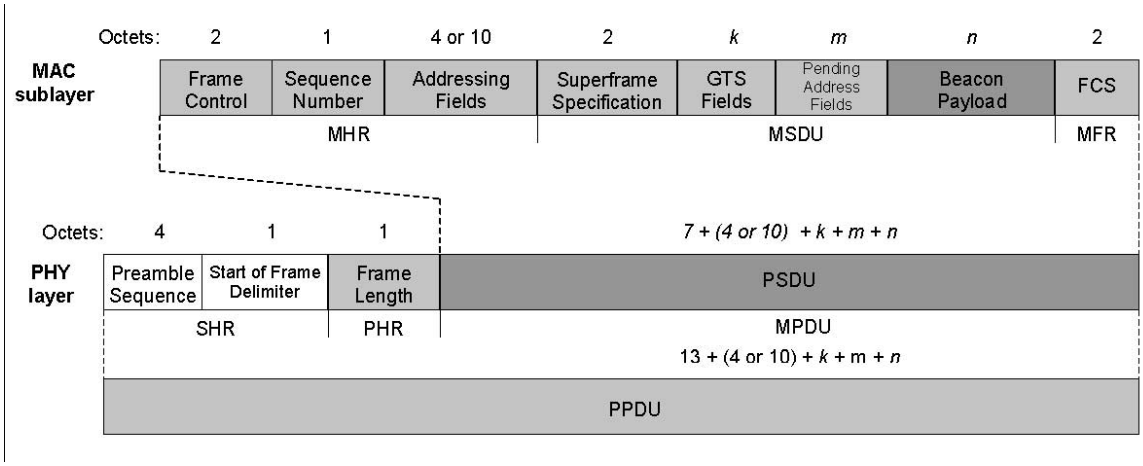


Figure 31. Beacon Frames (from Fig. 10 [55]).

4. Synchronization and Orphaning

One problem encountered in IEEE 802.15.4 network is **orphaned device**. When the higher layers receive repeated communication failures, i.e., failure to reach the coordinator after "aMaxFrameRetries" attempts at sending data, while attempting data transmission, it may conclude that it has been orphaned. Once a device concludes it is orphaned, it can either perform the association procedure or perform the orphaned device realignment procedure.

For the orphaned device alignment procedure, an orphan scan is performed. During the orphan scan, for each logical channel over a specified set of logical channels, the device sends an orphan notification command. The device then enables its receiver for at most "aResponseWaitTime" symbols. During this time, if the device successfully receives a coordinator realignment command, the device shall terminate the orphan scan procedure.

When a coordinator receives the orphan notification command, it scans its device list for the device sending the command. If a record of the device exists, it sends a coordinator realignment command to the orphaned device. Otherwise, it ignores the packet.

Again, during the orphan scan, the MAC sublayer discards all frames except those that are beacon frames, similar to the active and passive scan. This, too, can be a source of self-inflicted denial-of-service .

5. GTS Management

A GTS shall be allocated dynamically by the coordinator based on the GTS request (from a device) and the capacity available in the superframe. The GTS is allocated on a first-come-first-serve basis. Each GTS shall be de-allocated when the GTS is no longer required. A GTS can be de-allocated at any time by the coordinator or by the device that requested the GTSs. A device that is allocated GTS may simultaneously operate in the CAP.

The GTSs can be "transmit" or "receive" GTSs. For each allocated GTS, a device shall store its starting slot, length and direction. If a receive GTS is allocated, the device shall enable its receiver for the duration of the GTS. Similarly, a coordinator enables its receiver for the duration of the GTS if a device has been allocated a transmit GTS.

The coordinator can detect that a device has stopped using a transmit GTS if a data frame is not received for at least 2*n superframes. For receive GTSs, the coordinator shall determine that the device is no longer using its GTS if no acknowledgement frame is received within 2*n superframes. The value of n is equal to $2^{8\text{-macBeaconOrder}}$ if "macBeaconOrder" (BO) is in the range 0 to 8 and 1 if BO ranges from 9 to 14.

E. ZIGBEE ROUTING PROTOCOL

ZigBee routing algorithm is a competition between two routing protocols: the Internet Engineering Task Force (IETF) Ad hoc On Demand Distance Vector (AODV) and Motorola's Cluster-Tree algorithm.

The AODV has been well documented. AODV belongs to a class of ad hoc routing protocol that is reactive. Reactive protocols generate lower overheads and probably have lower energy consumption than proactive protocols. However, proactive protocols are able to adapt to changes in the topology, i.e., due to mobility. Since sensor networks are dominantly employed in static configurations with at most few moving nodes, the use of AODV is logical.

The Tree-Cluster Protocol is interesting from several perspectives. First, a sensor network normally has multiple sensors reporting to a gateway or "action" node; thus the protocol is clearly suitable in these scenarios where the sensor information is aggregated at the node. Second, the Tree-Cluster Protocol creates a hierarchy of nodes with each level corresponding approximately to the depth/distance of the network. Intuitively, the depth/distance together with the traffic on the network determines the latency and throughput. Thus, by configuring the hierarchy depth and breadth, a simple methodology exists to adapt the network to achieve specific Quality of Service (QoS). For a comprehensive introduction to 802.15.4 and ZigBee networking specifics, reference [63] should be interesting and helpful.

1. Using AODV as the Default Protocol of Choice

In the current investigation, AODV is the default routing protocol. The reason for this is threefold:

- AODV protocol source code for NS-2 simulation tool is readily available
- Facilitate comparison of different MACs in the future for benchmarking purpose
- Being a source of intense research for almost a decade, AODV is a mature and well-understood protocol

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SIMULATION & ANALYSIS

A. EXPERIMENT SETUP

Scale-free networks (SFNs) have inherent resilience to errors but are extremely vulnerable to catastrophic events such as the destruction or failure of a clusterhead since in SFNs the node connectivity to clusterheads can be extremely dense. In order to reap the full benefit of SFNs, it is proposed in Chapter I to reduce this vulnerability through a redundancy scheme provided by a pseudo-"dual-home" technique. In this concept, which is illustrated in Fig.32, a secondary cluster head is used to backup the primary clusterhead in case it fails due to physical or electronic attacks. The clusterheads are also separated by distance improving the diversity against attacks.

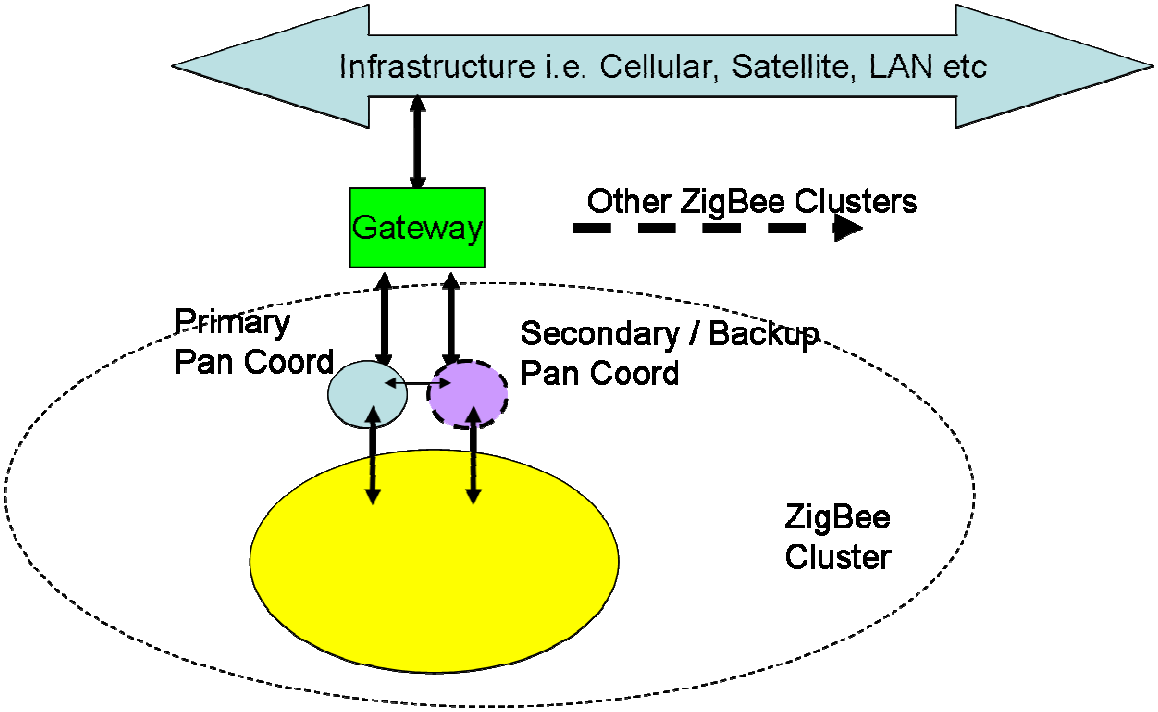


Figure 32. Resilient Wireless Sensor Network Architecture based on Scale-Free Network (SFN) Principles.

One reason the backup clusterhead should be operating in an off state when the network is operating in a normal mode and not as a "hot standby" is because this would substantially reduce the energy efficiency of the network. If the backup clusterhead is set to receive mode only, this means that the transceiver corresponding to that node would be

actively “overlistening” and this could deplete the energy resources available to that node. This could potentially happen even before the node is required to act as backup, thus, defeating the purpose of introduction of a backup clusterhead. This is also why, perhaps, “dual-homed” techniques have not been actively discussed or investigated in the literature as far as wireless sensor network technologies are concerned. In the following subsections, details are given on the experiment setup, the simulation tool used and the process, and a discussion of the analysis and results.

1. Initialization Time

Thus, a primary concern of this study is the initialization time of the cluster. The initialization time gives the amount of time that a network of nodes takes to form the network. If the initialization time is too long, important events in a sensor network may be missed and may impact the accuracy of higher level fusion algorithms and applications.

Evidently, the initialization time is also dependent on cluster size and depth. A larger cluster is expected to take a longer time to synchronize and achieve coherent topological mapping. Thus, the initialization time pertaining to two different cluster topology, i.e., different size and depth, will be studied. The two different topologies are given in Fig.33 (Star Topology) and 34 (Tree Topology).

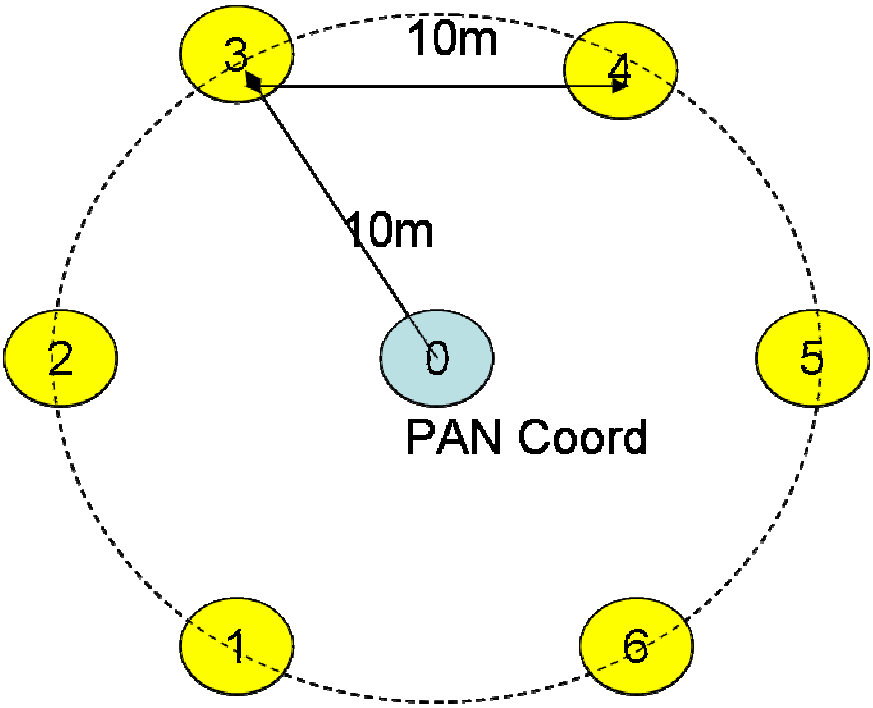


Figure 33. Star Topology, Single Level (Depth of One from PAN Coordinator).

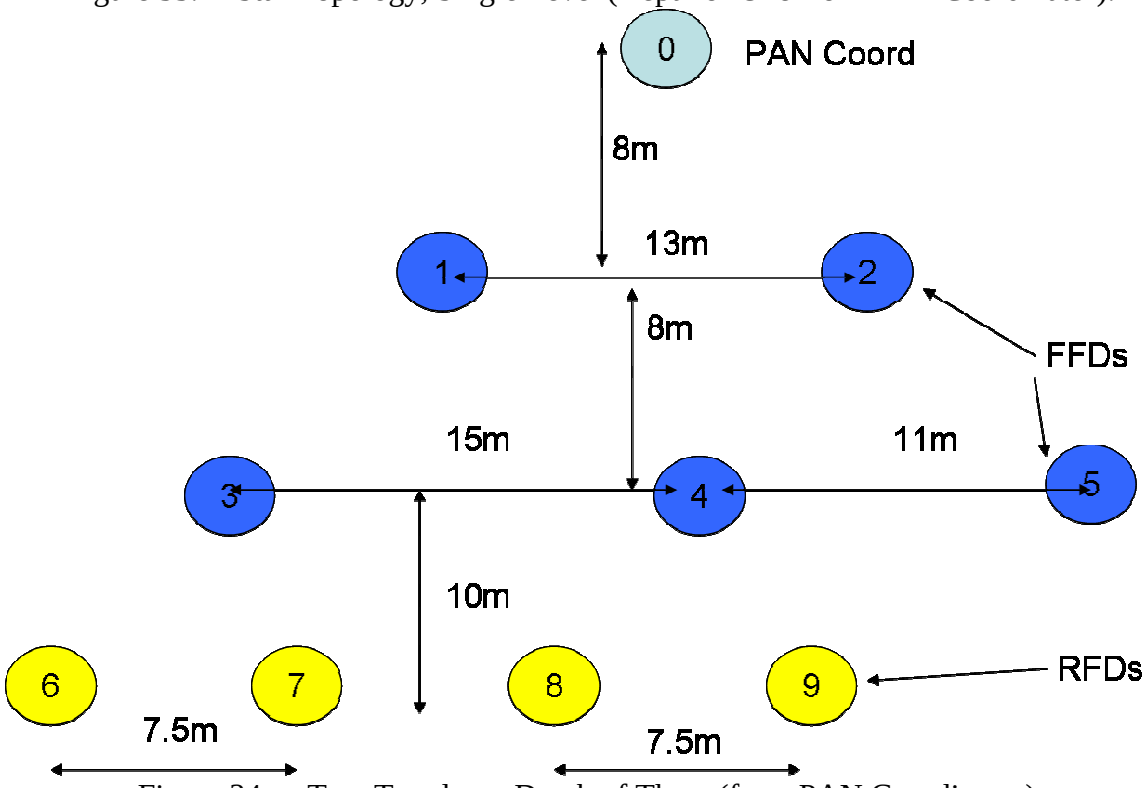


Figure 34. Tree Topology, Depth of Three (from PAN Coordinator).

2. Coordination Efficiency vs Energy Efficiency

MACs designed for wireless sensor networks derive their ability to conserve energy mainly from three sources as discussed in Chapter II: a) reducing “overhearing”, b) improving collision avoidance and c) through a scheduling mechanism which cycles the nodes in a network efficiently through coordinated periods of “sleep-wake”.

Measure c) essentially creates a distributed low-duty cycle network where energy efficiency is balanced against communication efficiency of throughput and latency. However, the efficiency is also predicated on scheduling efficiency. If the scheduling collapses, the network will collapse. Thus, all distributed networks, intuitively, designed this way, has vulnerability: the efficiency and error resilience of its scheduling / coordination mechanisms. In the case of IEEE 802.15.4, this mechanism is the beaconing coordination.

The error resilience of the beacon coordination will be tested against the two topologies above. The tree structure is expected to be more demanding as the beacons have to be distributed across the network compared to the star structure where the beacon can be simply broadcast across single hop.

3. Protocol Mechanisms and Vulnerability to Attacks

Scale-free networks (SFNs) have inherent resilience to errors. However, the resilience to errors from the protocol perspective must be studied. If the MAC protocol is resilient, it will add to the strength of the topological resilience. If the MAC protocol is vulnerable, then the simulations will serve to investigate those mechanisms which render the protocol vulnerable. From this assessment, measures could be proposed to “harden” the MAC protocol, if it is not already so.

B. SIMULATION

1. Simulation Tool

The network simulation is conducted using NS-2 with the Cygwin version [59]. The selection of NS-2 is based on the following reasons:

- Extensive research on network protocols has been conducted using ns-2.

- NS-2 has undergone continuous update. Bugs are reported and rectified on a continuous basis.
- NS-2 continues to maintain an active mailing list for use and problem assistance.

The IEEE 802.15.4 simulations are conducted on NS-2 using the codes contributed by Zheng et al [60]. The code has been readily distributed in the latest version of NS-2.28.

2. Simulation Process

The topology, superframe duration, beacon intervals, traffic source / destination / types and simulation durations are applied through developing a TCL file according to the NS-2 specifications for wireless nodes [62]. The NS-2 simulator interprets this TCL file for running the simulations.

The essential configurations in the TCL file are as follows:

- Propagation Model – The 2 ray ground model is used instead of the free space model. This is anticipated to better model the propagation effects arising from the antennas close to the ground, i.e., ground based sensor motes.
- Queue – The queue for each individual node is set to “drop tail” which means that packets will be dropped when the buffer is overwhelmed.
- MAC – This is set to point to the 802.15.4 MAC supplied by NS-2. The commands for 802.15.4 presented in the help manual provided in the “WPAN” folder in NS-2 are used to configure the operations of the 802.15.4 MAC.
- Routing – This is set to point to AODV as mentioned in the previous chapter.
- NS-2 Animation Program (NAM) – NAM is disabled and not used although this may be useful for debugging.
- Earliest Traffic Generation Times – The earliest traffic commence times are selected to be after complete network synchronization. The synchronization times differ for different IEEE 802.15.4 superframe parameters and topology.
- Types of Traffic – Three types of traffic are used for the star and tree topology mentioned above. They are constant bit rate (CBR), Poisson distributed, and stream-based (file transfer protocol).

The NS-2 trace files (type '.tr') are then analysed using Tracegraph version 2.0. Tracegraph essentially parses the NS-2 trace files and collate the measurements, aggregating these results for graphing.

C. ANALYSIS

1. Initialization Time

The superframe duration is given by $15.36*2^{BO}$ milliseconds where BO is the beacon order of the IEEE 802.15.4 MAC. The active portion is given by $15.36*2^{SO}$ milliseconds. The duty cycle of the individual node is approximately given by $\frac{2^{SO}}{16*2^{BO}}$. The duty cycle for various superframe structure configurations investigated is given in the table below.

SO	BO	Duty Cycle	Superframe Duration (msec)
3	3	6.25%	122.08
3	5	1.56%	491.52
4	4	6.25%	245.76

Table 1. Superframe configurations.

In the TCL program, the PAN coordinator is identified and a command is issued within the program for the selected node to commence broadcasting beacons. For the "star" network, "node 0" is the default PAN coordinator. The rest of the nodes affiliates with "node 0" using the association protocols for 802.15.4. The simulation is conducted using poisson distributed traffic with frame acknowledgement turned on. The TCL program confirms this through the following output when the simulation commences:

```
$ ns wpan_star.tcl -traffic poisson
num_nodes is set 7
INITIALIZE THE LIST xListHead

Traffic: poisson
Acknowledgement for data: on
```

Next the simulation begins. As mentioned, the TCL program controls when the node starts its operations. In this case, the nodes are turned on sequentially starting with "node 0" which has been designated the PAN coordinator. "Node 0", upon initialization, quickly performs an active channel scan. Each channel in its list, i.e., channel 11, 12 and 13, is scanned for $15.36*(2^{BO}+1)$ milliseconds which corresponds approximately to one superframe length. When it does not hear any beacons on the channels scanned, it begins to transmit its own beacons and set itself up as a PAN coordinator using channel 11. This is shown by the TCL program output as follows:

```
Starting Simulation...
--- startPANCoord [0] ---
[0.000000](node 0) performing active channel scan
[0.000000](node 0) scanning channel 11
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 35.9
SORTING LISTS ...DONE!
[0.141440](node 0) scanning channel 12
[0.280640](node 0) scanning channel 13
[0.420800](node 0) begin to transmit beacons
[0.421568](node 0) successfully started a new PAN (beacon enabled) [channel:11]
[PAN_ID:0]
```

The next device, "node 1", is initialized in sequence. It scans the channels to accumulate a list of PAN coordinators. It would then select a PAN coordinator to affiliate from this list. As shown below, it attempts to associate with "node 0". A series of requests, acknowledgements and responses ensue. This culminates in "node 1" synchronizing with coordinator once the association request is granted by the PAN coordinator. This is shown by the TCL program output as follows:

```
--- startDevice [1] ---
[0.500000](node 1) performing active channel scan ...
[0.500000](node 1) scanning channel 11
[0.762400](node 1) scanning channel 12
[1.024480](node 1) scanning channel 13
[1.287200](node 1) sending association request to [channel:11] [PAN_ID:0] [Coord
Addr:0] ...
[1.289248](node 1) sending association request command ...
[1.290784](node 1) ack for association request command received
--- startDevice [2] ---
[1.500000](node 2) performing active channel scan ...
[1.500000](node 2) scanning channel 11
[1.762400](node 2) scanning channel 12
[1.782304](node 1) sending data request command ...
```

```
[1.783584](node 1) ack for data request command received
[1.786048](node 1) association response command received
[1.786048](node 1) association successful (beacon enabled) [channel:11] [PAN_ID:
0] [CoordAddr:0]
[1.786048](node 1) begin to synchronize with the coordinator

……..// deleted for brevity
```

Each of the node undergoes the same initialization process as “node 1” above. This culminates with “node 6”. Upon successful synchronization of “node 6” with the co-ordinator, the network is established and the traffic is generated and sent across the network. This is illustrated by the “Transmitting data….” comment in the output. The TCL program output is shown as follows:

```
--- startDevice [6] ---
[5.500000](node 6) performing active channel scan ...
……..// delete for brevity

 [6.786048](node 6) association successful (beacon enabled) [channel:11] [PAN_ID:
0] [CoordAddr:0]
[6.786048](node 6) begin to synchronize with the coordinator

Transmitting data ...

NS EXITING...
```

It is interesting to note that the network formation process of a simple 7 node network requires approximately 56 frames to complete in a network with low duty cycle nodes. The initialization times of both the star and tree cluster topology are investigated and measured. The network formation time corresponding to the “cold” startup time of the network is given in Table 2.

Star Topology (7 nodes)	Sync Time (sec)	Tree Topology (10 nodes)	Sync Time (sec)
BO=3, SO=3	6.78	BO=3, SO=3	10.86
BO=4, SO=4	7.52	BO=4, SO=4	12.43
BO=5, SO=3	12.99	BO=5, SO=3	27.28

Table 2. Network Formation Time.

From the above table, it is observed that the network formation time differs for the two topologies. This is expected as the tree topology has more nodes. Nevertheless, for a beacon order of three, the increase in time is not significant. Even for a beacon order of four, the synchronization time is not significant.

For a beacon order of five, the synchronization time of the tree topology doubles when compared to the star topology. This increase is only approximately 50 percent for the lower beacon order of three.

Several insights can be drawn from these observations:

- ***The "cold start" time of 802.15.4 network is quite small. Thus, when the primary clusterhead is disabled, it is possible for the network to re-affiliate with the secondary clusterhead in an extremely short time even when the secondary clusterhead is initially in the "off" state.***

- The tree topology is more sensitive to an increase in the beacon order (and hence, greater latency and waiting time) than the star topology in its synchronization process. This is because for a larger superframe duration, the initialization and synchronization of the higher level FFDs with the PAN coordinator takes a longer time. During this time, the lower level ZigBee devices cannot affiliate to any coordinators – there is simply nothing to affiliate with. The RFDs or leaf nodes are simply wasting energy transmitting affiliation requests. The star topology does not suffer from this constraint – every device is in clear line-of-sight with a PAN coordinator and can constantly contend for the channel to affiliate with the PAN coordinator. ***Thus, a large number of nodes affiliating with a coordinator is not a concern – the synchronization delay merely scales linearly. The primary concern is with depth and placement of the coordinators. If the depth of the topology is large, the delay to re-affiliation is significant. This suggests that a star topology may be more resilient compared to a layered architecture.***

- It also makes sense to keep the beacon order small in large networks. This is because if different clusters fail sequentially, and the data fusion from

those clusters are not independent (for reasons of accuracy), the network re-affiliation time corresponding to the sum of the “cold start” time of the individual clusters could be magnified corresponding to larger beacon order values.

2. Network Self-Inflicted Denial-of-Service

As mentioned in Chapter III, it is possible to identify three sources of self-inflicted denial-of-service! These are mainly the active, passive and orphan scans. During these scans, the device ignores all frames except for beacon frames. Secondly, the duration of this scan can be considerable because the device has to scan through all the channels. There are a total of 27 channels set aside for 802.15.4 operations: 16 channels are available in the 2450 MHz band, 10 in the 915 MHz band and one in the 868 MHz band. In each band, the device scans for $15.36*(2^{BO}+1)$ * (number of channels in band) milliseconds. It is assumed that during this time, the device will be capable of locating the coordinator beacons. However, this also assumes a quasi-steady state where the FFDs in the network are fairly stable and similarly, the beacons are also fairly stable.

Through simulations, it is found that for high traffic intensity, i.e., 10 packets per second, ftp-type traffic and for the 10-node tree-cluster topology, the FFDs could themselves lose synchronization and/or are orphaned. This problem propagates through the network resulting in instability. The snippet below shows this problem. For reasons of space, only a snapshot is shown.

```
[115.697408](node 4) synchronization loss
[115.697408](node 4) orphan-scanning channel 11
[116.190336](node 4) orphan-scanning channel 12
[116.363776](node 9) synchronization loss
[116.363776](node 9) orphan-scanning channel 11
[116.363776](node 8) synchronization loss
[116.363776](node 8) orphan-scanning channel 11
[116.685184](node 4) orphan-scanning channel 13
[116.858304](node 9) orphan-scanning channel 12
[116.858304](node 8) orphan-scanning channel 12
[117.180352](node 4) coordinator relocation failed.
[117.352192](node 9) orphan-scanning channel 13
[117.353920](node 8) orphan-scanning channel 13
[117.357952](node 9) coordinator relocation successful, begin to re-synchronize
with the coordinator
```

[117.364992](node 8) coordinator relocation successful, begin to re-synchronize with the coordinator

Scale-free networks have properties that make them resilient to errors but extremely vulnerable to catastrophic events. It is shown here that the ***802.15.4 MAC could self-inflict denial-of-service resulting in another source of vulnerability that could paralyse the network. This cannot be solved by our introduction of clusterhead diversity and adopting a "cold-start" strategy.***

While a source of concern, it should be noted that this problem exists only at high traffic intensity and occurs very rarely for lower traffic loads. (This is because at high traffic intensity, there is a higher probability of nodes losing synchronization with the PAN coordinator.) Thus, several insights can be drawn:

- Network resilience depends on the traffic load
- Traffic load should be carefully selected not to exceed a point where the network experiences excessive or recurrent active, passive or orphan scanning

3. Vulnerability to Intentional / Non-intentional Interference

Following from the discussion above, it should be noted that the 802.15.4 access network is extremely vulnerable to both intentional and non-intentional interference of the PAN coordinator which connects the access network to the other clusters either with or without an infrastructure.

The reason for this vulnerability follows from the previous section: the active, orphan scanning conducted privy to association and synchronization can create an opportunity for the whole network to lock up. If the PAN coordinator experiences intentional or un-intentional interference, thus preventing it from listening to beacon requests, the FFDs and RFDs would be locked into a cycle of constant re-association and synchronization with the PAN coordinator.

For passive scan, the nodes do not make an initial beacon request. The passive scan is a receive-only operation and is more robust. However, when it has selected a coordinator to affiliate, it needs to go through the same process of association. The

exchange of messages that ensue makes the system vulnerable. Nevertheless, the system is now free to receive frames other than the beacon frames.

Thus, to reduce the vulnerability of the system to simple, directed attacks on the network, it is recommended that passive scans be used.

4. Error Resilience and Sleep-Wake Cycles

Two factors contribute to resilience of errors: network topology and traffic handling capabilities of the protocol. In Chapter I, a discussion of scale-free networks and their properties are given. By constructing the wireless sensor networks to resemble scale-free networks, the wireless sensor networks inherit similar error resilience.

The traffic handling capability of the physical and MAC layer also contribute to error resilience. In Chapter II, an insight is that the performance of all current MACs for wireless sensor networks is a trade-off amongst the three parameters of energy, latency and throughput. 802.15.4 leverages the beacon mechanism to coordinate and synchronize the network. The beacon mechanism in effect schedules uniform wakeup for all the nodes. When data is transmitted, only specific destination nodes need to remain awake. Other nodes not participating in the conversation may shut down [69]. This shut down mechanism for the nodes prevents “overhearing” which wastes energy.

The beacon mechanism does not save energy directly. It does so indirectly. Its main purpose is to coordinate the sleep-wake cycle for the network so that any two communicating pair of nodes is available for communications. When the sleep-wake cycles are synchronized and efficient, the nodes saves energy by going to sleep while creating an illusion to an information-sending node or higher level application that a persistent link exists when in fact, there is none. Thus, it would be interesting to examine if this illusion is efficiently maintained by 802.15.4.

Besides the efficiency of maintaining this sleep-wake cycle, other factors can affect the link performance. Even though a link physically exists, i.e., there is line-of-sight between two nodes, no meaningful communications can exist if the two nodes, communicating using a shared medium, cannot gain access to the medium for reasons such as inefficient CSMA-CA, congestion, RF interference, RF shadowing etc.

To determine the overall efficiency of 802.15.4 in creating the illusion of a link to higher level applications, the delay and dropped packets are measured for each topology with respect to deterministic traffic, i.e., Constant Bit Rate (CBR) applications and File Transfer Protocol (FTP). The results are indicative rather than exhaustive. Nevertheless, meaningful insights can be drawn. The traffic sources and data transmission directions are shown for the star and tree topology in Fig.35 and 36 respectively. (The physical layout of the nodes is given by Fig.33 and 34 for the star and tree topology respectively.)

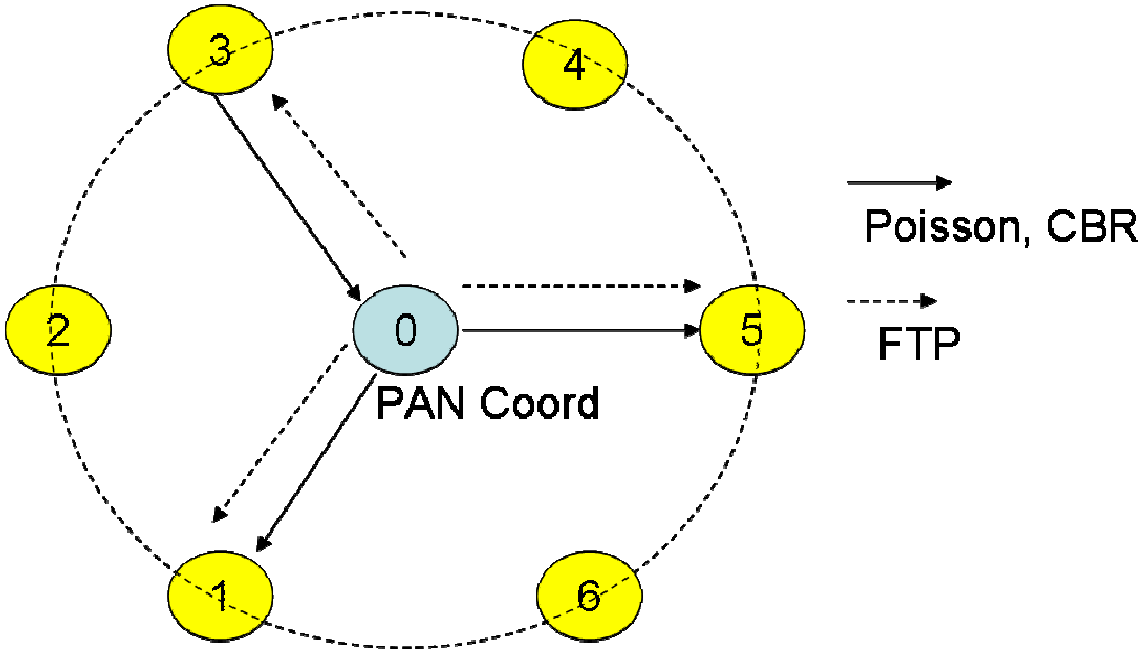


Figure 35. Star Topology Traffic Sources.

Compared to the star topology, the tree topology has a depth of three. There are two nodes single hop from the PAN coordinator, three nodes two hops away and four nodes three hops away. Given this setup, it is reasonable to introduce multi-hops traffic flow. There are two traffic flows across two hops and two traffic flows with single hop. As it takes more bandwidth to transmit data from end-to-end across two hops compared to one hop, i.e., roughly twice bandwidth, the traffic rate will be halved for the tree-topology simulation compared to the star topology simulations. This provides a more equitable comparison with the single-hop star topology scenario.

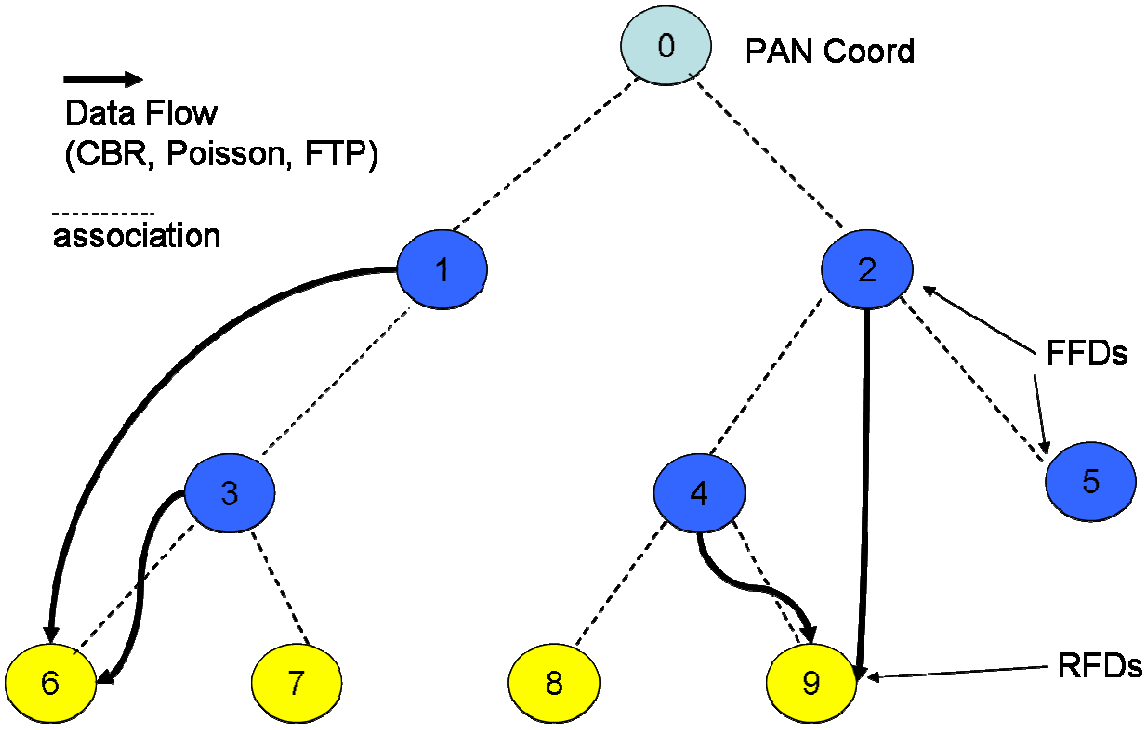


Figure 36. Tree-Cluster Topology Traffic Sources.

a. Star-Topology, BO=3, SO=3, 3 CBR Traffic Sources, Packet Size=70 bytes, 100 ppm (packets per minute)

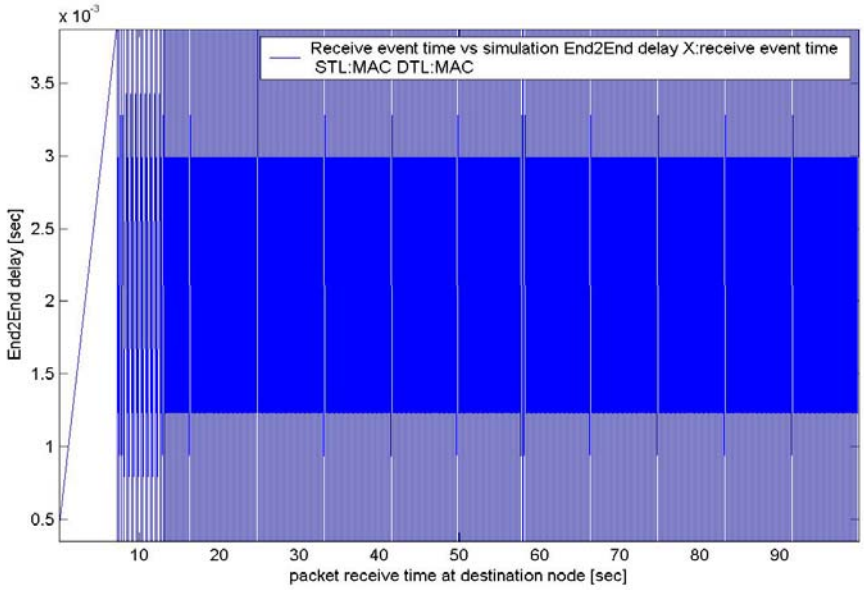


Figure 37. Delay.

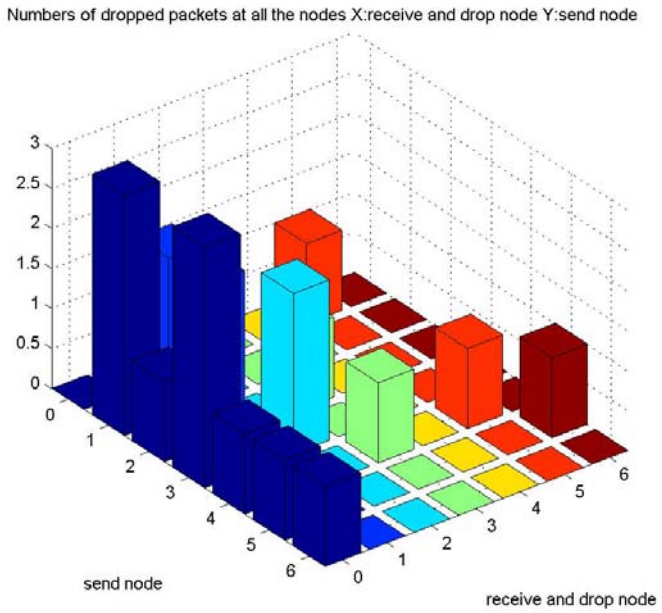


Figure 38. Dropped Packets.

Fig.37 illustrates the delivery latency of packets with respect to the simulation time (measured from the start of simulation). It shows that the delivery latency of packets never exceeds 4 milliseconds (sent within 1 frame).

Fig.38 illustrates the number of dropped packets with respect to any transmit/receive pair of nodes within the network. The total sent packets is ~5500 packets in this simulation and the total dropped packets given by Fig.38 are ~22 packets. This corresponds to a packet drop rate of 0.4 percent. It shows that the IEEE 802.15.4 protocol does not experience any difficulty with this traffic intensity and it can be considered a "light" traffic.

b. Star-Topology, BO=3, SO=3, 3 CBR Traffic Sources, Packet Size=70 bytes, 600 ppm (packets per minute)

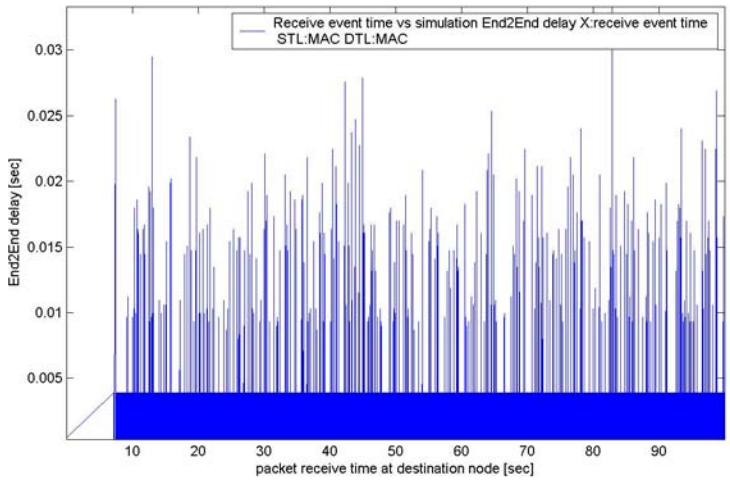


Figure 39. Delay.

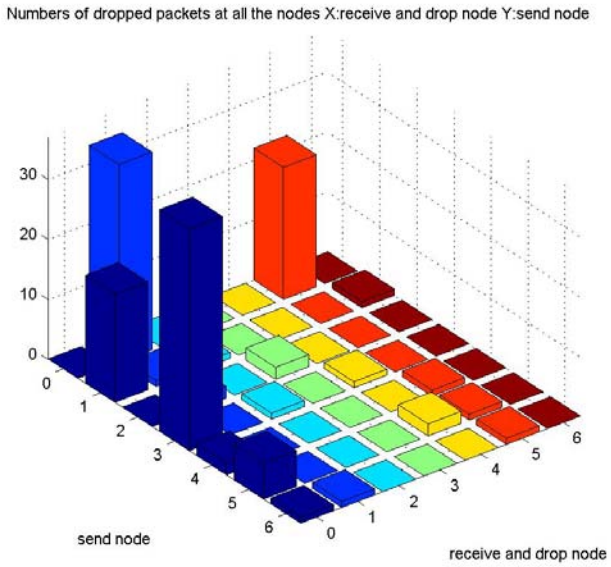


Figure 40. Dropped Packets.

In this scenario, the traffic intensity is increased from 100 packets per minute to 600 packets per minute. Fig.39 illustrates the delivery latency of packets with respect to the simulation time (measured from the start of simulation). It shows that the

delivery latency of packets never exceeds 30 milliseconds (sent within 1 frame). It also depicts a number of large peaks demonstrating a larger time delay variation.

Fig.40 illustrates the number of dropped packets with respect to any transmit/receive pair of nodes within the network. The total sent packets is ~10,000 packets in this simulation and the total dropped packets given by Fig.40 are ~130 packets. This corresponds to a packet drop rate of 1.3 percent. Again, IEEE 802.16.4 performs well. In the next scenario, the FTP traffic is used to investigate the effects of persistent flows.

c. Star-Topology, BO=3, SO=3, 3 FTP Traffic Sources

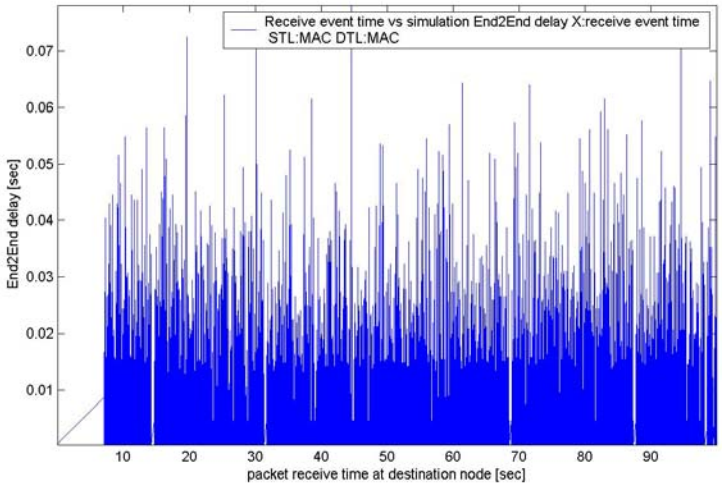


Figure 41. Delay.

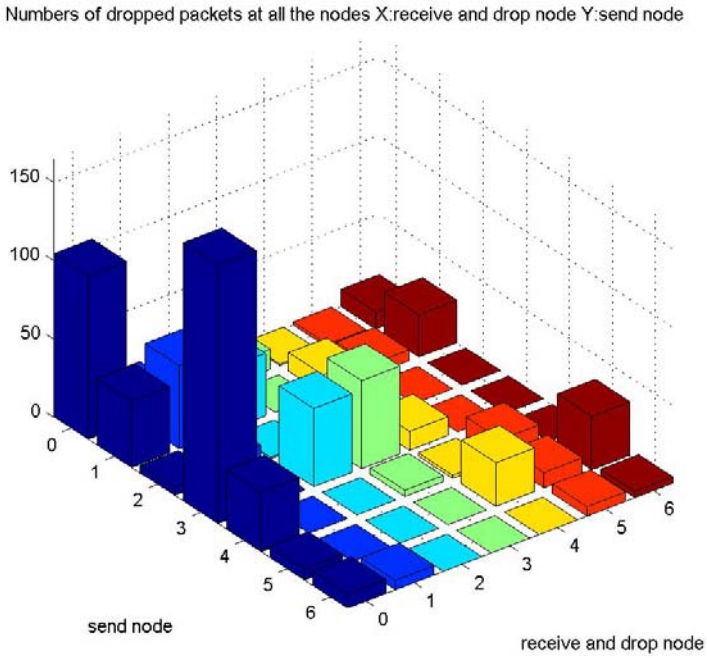


Figure 42. Dropped Packets.

Fig.41 illustrates the delivery latency of packets with respect to the simulation time (measured from the start of simulation). It shows that the delivery latency of packets never exceeds 70 milliseconds (sent within 1 frame). It also has a considerable amount of peaks, demonstrating large time delay variation.

Fig.42 illustrates the number of dropped packets with respect to any transmit/receive pair of nodes within the network. The total sent packets is ~30,000 packets in this simulation and the total dropped packets given by Fig.42 are ~800 packets. This corresponds to a packet drop rate of 2.6 percent.

For all the scenarios considered for the star topology, both latency and packet drop rates have been consistently low, regardless of CBR or FTP type applications. This could be attributed to its simple structure, no relaying and ease of synchronization. Next, the tree topology is simulated. This is a more complicated structure compared to the star topology. Similarly, we want to examine the latency and packet drop rates to investigate the ability of the IEEE 802.15.4 protocol to handle complex topologies.

d. Tree-Topology, BO=3, SO=3, 4 CBR Traffic Sources, Packet Size=70 bytes, 300 ppm (packets per minute)

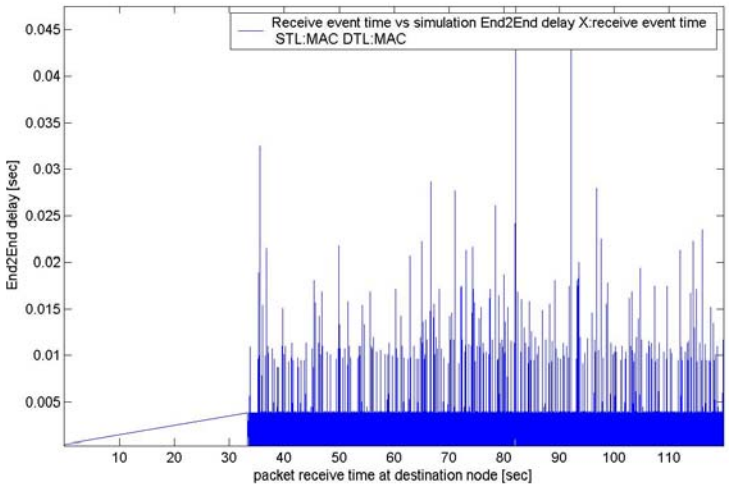


Figure 43. Delay.

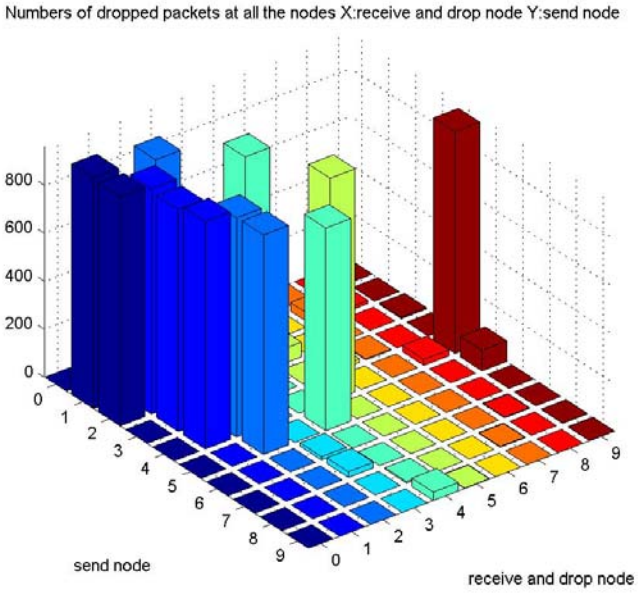


Figure 44. Dropped Packets.

Fig.43 illustrates the delivery latency of packets with respect to the simulation time (measured from the start of simulation). It shows that the delivery latency of packets never exceeds 50 milliseconds (sent within 1 frame) although there are considerable amount of peaks, demonstrating large time delay variation.

Fig.44 illustrates the number of dropped packets with respect to any transmit/receive pair of nodes within the network. The total sent packets is ~13,000 packets in this simulation and the total dropped packets given by Fig.42 are ~11,000 packets. This corresponds to a packet drop rate of ~85 percent. This is significantly higher than the packet drop rates corresponding to the star-topology for CBR traffic given by Fig.40.

e. Tree-Topology, BO=3, SO=3, 4 FTP Traffic Source

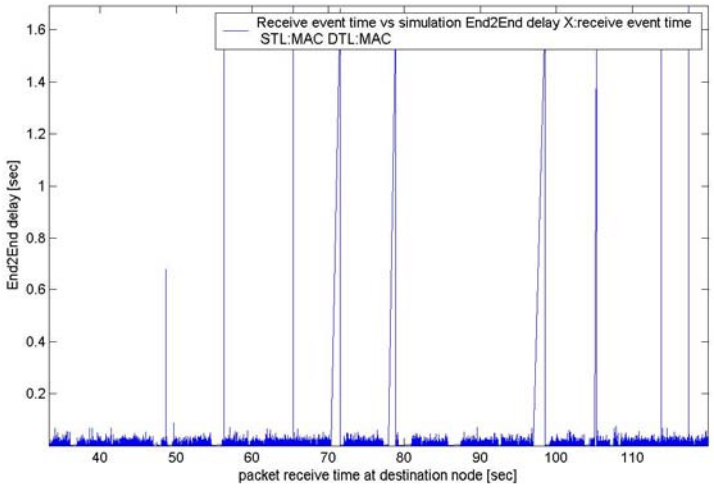


Figure 45. Delay.

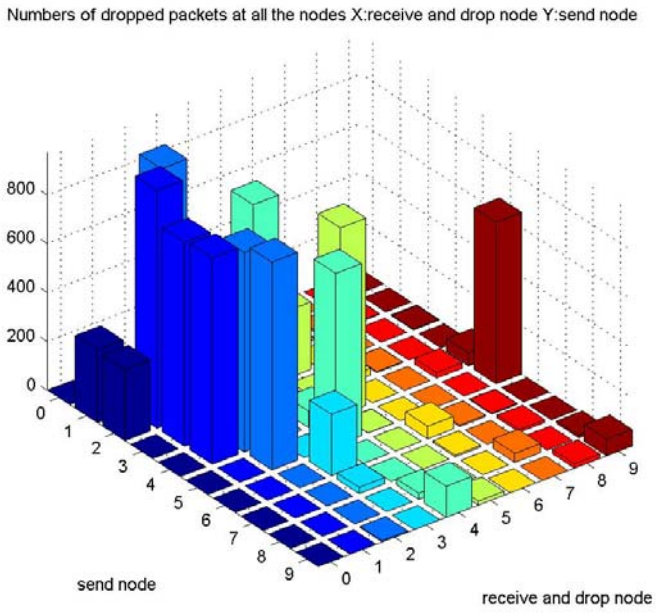


Figure 46. Dropped Packets.

Fig.45 illustrates the delivery latency of packets with respect to the simulation time (measured from the start of simulation). It shows that the delivery latency of packets never exceeds 1.7 seconds. It also has few very large peaks demonstrating large time delay variation.

Fig.46 illustrates the number of dropped packets with respect to any transmit/receive pair of nodes within the network. The total sent packets is ~35,000 packets in this simulation and the total dropped packets given by Fig.42 are ~10,000 packets. This corresponds to a packet drop rate of 28.6 percent. This is also significantly higher than the packet drop rates for the star-topology with FTP traffic flows given by Fig.42.

f. Observations

From the above simulation results, the tree topology cluster exhibit more dropped packets (at the receive node) than the star topology cluster. The dropping is done at the receiving end. Since this packet is dropped at the receiving end, it is concluded that the problem is not one of channel access, i.e., CSMA-CA. Rather, the problem, as

mentioned could be due to some inefficiencies with maintaining the sleep-wake cycle. To confirm, NS-2 output during simulation is checked. The output for the ftp case is given as follows:

```
[64.712704](node 4) coordinator relocation successful, begin to re-synchronize w
ith the coordinator
[64.878464](node 9) orphan-scanning channel 12
[64.880064](node 8) orphan-scanning channel 12
[65.372352](node 9) orphan-scanning channel 13
[65.374912](node 8) orphan-scanning channel 13
[65.379392](node 9) coordinator relocation successful, begin to re-synchronize w
ith the coordinator
[65.868160](node 8) coordinator relocation failed --> try to reassociate ...
--- startDevice [8] ---
[65.868160](node 8) performing active channel scan ...
[65.868160](node 8) scanning channel 11
[66.131840](node 8) scanning channel 12
[66.299648](node 4) synchronization loss
[66.299648](node 4) orphan-scanning channel 11
[66.394240](node 8) scanning channel 13
<!>[66.656960](node 8) no coordinator found for association.
[66.794176](node 4) orphan-scanning channel 12
[66.966016](node 9) synchronization loss
[66.966016](node 9) orphan-scanning channel 11
[67.288704](node 4) orphan-scanning channel 13
[67.461184](node 9) orphan-scanning channel 12
[67.783552](node 4) coordinator relocation failed.
[67.954432](node 9) orphan-scanning channel 13
[67.959872](node 9) coordinator relocation successful, begin to re-synchronize w
ith the coordinator
[69.389248](node 5) synchronization loss
[69.389248](node 5) orphan-scanning channel 11
[69.863168](node 4) synchronization loss
[69.863168](node 4) orphan-scanning channel 11
[69.884416](node 5) orphan-scanning channel 12
[70.354688](node 3) synchronization loss
[70.354688](node 3) orphan-scanning channel 11
[70.357056](node 4) orphan-scanning channel 12
[70.379584](node 5) orphan-scanning channel 13
[70.386944](node 5) coordinator relocation successful, begin to re-synchronize w
ith the coordinator
```

……(recurs for the whole session)…..

From the output, there is an indication of recurrent orphaning and re-synchronization process. Thus, the star topology is indeed more error resilient compared to the tree topology cluster. ***The error resilience comes from managing the sleep-wake cycle more efficiently across single hop rather than multiple hops.***

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

From Chapter III, the "clustering" mechanisms of IEEE 802.15.4 are investigated. It is found that it is possible to create high clustering coefficient networks through the design of an appropriate algorithm for the selection of the coordinators. This is because the IEEE 802.15.4 standard defers the task of coordinator selection policy to implementation. Thus, scale-free networks can be artificially created using the IEEE 802.15.4 MAC. The models to generate scale-free networks are well documented and the algorithm could be adapted from the works of Barabasi et al [70][71] and Klemm et al [72]. The efficiency of these algorithms artificially adapted to wireless sensor networks shall be pursued in future work.

Given the initialization and synchronization times from the simulation, the "cold-start" diversity strategy pursued to reduce the vulnerability of scale-free networks to attack is deemed feasible. In our investigation, a dual-diversity scheme is proposed. Nevertheless, an implementation of this diversity scheme can be extended to n-diversity protection if resources permit. The simulated results shall still be applicable in this case.

Both the star and tree topology provides reasonable synchronization / initialization times. The star is specifically chosen to represent a dispersed network of uniform single hop from the PAN so the depth for synchronization is essentially unity. The tree structure presents a more complex synchronization and the complexity increases with depth. In our simulation, the maximum depth of synchronization is three. Our simulated results indicate that as the depth increases, the synchronization time will increase.

The depth, as a proxy of structure complexity, indicates that synchronization time will be fairly well-behaved and appears to scale linearly. However, the depth of the network should be managed from the perspective of its inherent vulnerability to synchronization loss, coordination (beacon distribution) inefficiency and self-inflicted denial-of-service. This vulnerability is further compounded by the fact that prolonged

self-inflicted denial-of-service could be created with opportune injection of traffic by an attacker or fluctuation of the link quality through environmental constraints such as RF shadowing etc.

In order to reduce the vulnerability, the following measures are proposed:

- Use only passive scanning. An implementation should consider the effects of not using orphan scanning and leverage as far as possible the ability afforded by passive scanning.
- Limit the depth of the cluster structure. A high clustering coefficient network does not limit the depth of the cluster structure. However, the depth of the cluster structure, due to the performance of the MAC, increases the possibility of compounding inefficiencies in the coordination of the beacon distribution leading to an abrupt collapse in an otherwise stable structure.
- Mandate the use of integrity and authentication mechanisms. This shall serve to limit the possibility of a hostile injection of traffic which could again stress the efficiencies of beacon coordination and distribution.
- Have sufficient link budget to ensure that link fluctuations do not adversely affect the ability of the network to distribute coordination beacons.

Since it is possible to achieve the above by a careful configuration of the IEEE 802.15.4 MAC, it is concluded that a resilient scale-free network can be artificially created using the IEEE 802.15.4 MAC.

In conclusion, an approach for artificially creating resilient scale-free wireless sensor networks based on the IEEE 802.15.4 / ZigBee industrial standards has been outlined in this thesis. Our investigation conducted with the support of simulation tools validates this approach. This thesis has made the following contributions:

- Adapting the concept of scale-free networks as the fundamental basis to create resilient wireless sensor networks

- Propose and demonstrate that a “cold-start” strategy can be applied to leverage diversity in reducing the vulnerability to intentional attacks on critical nodes, i.e., PAN coordinator
- Identifying and proposing mechanisms to reduce the inherent vulnerability of the IEEE 802.15.4 MAC and increase its resilience.

The following future work is also recommended:

- Adapt the models of Barabasi et al [70][71] and Klemm et al [72]. The efficiency of these algorithms artificially adapted to wireless sensor networks should be pursued.
- Extend the simulation to encompass heterogeneity by including the possibility of an interface with an infrastructure network and/or three-dimensional space to understand urban deployments.
- Investigate the optimum depth of the cluster for the IEEE 802.15.4 MAC.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] "Sensor Information Technology," http://www.sainc.com/sensit/, last accessed on Jan 2006.

[2] Lewis David Girod, "A self-calibrating system of distributed acoustic arrays," thesis, 2005.

[3] Amr Eltaher and Thomas Kaiser, "A Novel Approach based on UWB Beamforming for Indoor Positioning in None-Line-of-Sight Environments," RadioTec Oct 26-27, 2005, Berlin, Germany.

[4] "Future Combat Systems Unattended Ground Sensors," https://peoiewswebinfo.monmouth.army.mil/portal_sites/IEWS_Public/rus/FCSUGS.htm last accessed on Jan 2006.

[5] M.Hurley, "Tactical Microsatellite Experiment," http://www.nrl.navy.mil/content.php?P=04REVIEW207, last accessed on Jan 2006.

[6] Paul Sereiko, "Wireless Mesh Sensor Networks Enable Building Owners, Managers, and Contractors to Easily Monitor HVAC Performance Issues," http://www.automatedbuildings.com/news/jun04/articles/sensicast/Sereiko.htm, last accessed on Jan 2006.

[7] Paul Baran, "On Distributed Communications: I. Introduction to Distributed Communications Networks," Rand Publication, http://www.rand.org/pubs/research_memoranda/RM3420/index.html, last accessed on Jan 2006.

[8] Mark Pacelle, "Selecting the Right Wireless Mesh Topology," http://www.wirelessnetdesignline.com/showArticle.jhtml?articleID=57701681, last accessed on Jan 2006.

[9] Yong Ma and James H. Aylor, "System Lifetime Optimization for Heterogeneous Sensor Networks with a Hub-Spoke Topology", IEEE Transactions On Mobile Computing, Vol. 3, No. 3, Jul-Sept 2004.

[10] Jonas Neander, Mikael Nolin and Mats Bj¨orkman, “Using Existing Infrastructure as Proxy Support for Sensor Networks”, Work-in-Progress Session of the 16th Euromicro Conference on Real-Time Systems, Catania, Italy 2004

[11] F.L.Lewis, “Wireless Sensor Networks”, Smart Environments: Technologies, Protocols, and Applications ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.

[12] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazine, pp. 102-114, Aug 2002.

[13] Kemal Akkaya and Mohamed Younis, “A Survey on Routing Protocols for Wireless Sensor Networks”, Elsevier Ad Hoc Network Journal, Vol. 3/3 pp. 325-349, 2005

[14] Jamal N. Al-Karaki and Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, IEEE Wireless Communications, Vol 11/6 pp.6-28, Dec 2004

[15] DaZhi Chen and Pramod K. Varshney, “QoS Support in Wireless Sensor Networks: A Survey”, Proceedings of the International Conference on Wireless Networks, ICWN '04, Las Vegas, Nevada, USA, Volume 1, pp.227-233, Jun 21-24, 2004

[16] Holger Karl and Andreas Willig, “A Short Survey of Wireless Sensor Networks”, TKN Technical Report TKN-03-018, Berlin, Oct 2003.

[17] Andre Barosso, Jonathan Benson, Tina Murphy, Utz Roedig, Cormac Sreenan, John Barton, Stephen Bellis, Brendan O’Flynn, and Kieran Delaney, “Demo Abstract: The DSYS25 Sensor Platform”, Sensys’04, Nov 3-5, 2004, Baltimore, Maryland, USA, pp. 314.

[18] L.F.W. van Hoesel and P.J.M. Havinga, “Poster Abstract: A TDMA-based MAC Protocol for WSNs”, Sensys’04, Nov 3-5, 2004, Baltimore, Maryland, USA, pp. 303-304.

[19] Young-Jin Kim, Ramesh Govinda, Brad Karp and Scott Shenker, “Poster Abstract: Practical and Robust Geographic Routing in Wireless Networks”, Sensys’04, Nov 3-5, 2004, Baltimore, Maryland, USA, pp. 295-296.

[20] Jan Beutel, Matthias Dyer, Martin Hinz, Lennart Meier and Matthias Ringwald, “Poster Abstract: Next-generation Prototyping of Sensor Networks”, Sensys’04, Nov 3-5, 2004, Baltimore, Maryland, USA, pp. 291-292.

[21] Sivaram Cheekiralla, “Poster Abstract: Wireless Sensor Network-based Tunnel Monitoring”, Proceedings of Workshop on Real-World Wireless Sensor Network (REALWSN’05), Jun 20-21 2005, http://www.sics.se/realwsn05/papers/cheekiralla05wireless.pdf, last accessed on Jan 2006.

[22] Jane Tateson, et al., “Real World Issues in Deploying a Wireless Sensor Network for Oceanography”, Proceedings of Workshop on Real-World Wireless Sensor Network (REALWSN’05), Jun 20-21 2005, http://www.sics.se/realwsn05/papers/tateson05realworld.pdf, last accessed on Jan 2006.

[23] Johan Lonn, Jonas Olsson and Shaofang Gong, “Zigbee-ready modules for Sensor Ntwork”, Proceedings of Workshop on Real-World Wireless Sensor Network (REALWSN’05), Jun 20-21 2005, http://www.sics.se/realwsn05/papers/lonn05zigbee.pdf, last accessed on Jan 2006.

[24] Kay Romer and Friedemann Mattern, “The Design Space of Wireless Sensor Networks”, IEEE Wireless Communications, pp. 54-61, Dec 2004.

[25] Pei Zhang, Christopher M. Sadler, Stephen A. Lyon and Magarat Martonosi, “Hardware Design Experiences in ZebraNet”, Sensys’04, November 3–5, 2004, Baltimore, Maryland, USA.

[26] Eugene Shih, SeongHwan Cho, Nathan Ickes, Rex Min, Amit Sinha, Alice Wang and Anantha Chandrakasan, “Physical Layer Driven Protocol and Algorithm Design for EnergyEfficient Wireless Sensor Networks”, ACM SIGMOBILE 7/01 Rome, Italy

[27] W.Heinzelman, A.Chandrakasan and H. Balakrishnan, “Energy-efficient communication protocol for wireless sensor networks,” Proceedings of the Hawaii International Conference System Sciences, Hawaii, Jan 2000.

[28] W. Heinzelman, J. Kulik and H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks”, Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’99), Seattle, WA, Aug 1999

[29] C. Intanagonwiwat, R. Govindan and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom’00), Boston, MA, Aug 2000.

[30] K. Sohrabi et al., “Protocols for self-organization of a wireless sensor network,” IEEE Personal Communications, Vol.7/5, pp. 16-27, Oct 2000.

[31] T. He et al., “SPEED: A stateless protocol for real-time communication in sensor networks,” Proceedings of International Conference on Distributed Computing Systems, Providence, RI, May 2003.

[32] Christian C. Enz, Amre El-Hoiydi, Jean-Dominique Decotignie and Vincent Peiris, “WiseNET: An Ultralow-Power Wireless Sensor Network Solution,” IEEE Computer, pp. 62-70, Aug 2004.

[33] Jamal N. Al-Karaki and Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks,” IEEE Wireless Communications, pp.6-28, Dec 2004.

[34] V. Turau et al., “The Heathland Experiment: Results and Experiences,” Proceedings of the REALWSN'05 Workshop on Real-World Wireless Sensor Networks. Stockholm, Sweden, Jun 2005

[35] Thomas Schmid, Henri Dubois-Ferriere and Martin Vetterli, “SensorScope: Experiences with a Wireless Building Monitoring Sensor Network,” Proceedings of the REALWSN'05 Workshop on Real-World Wireless Sensor Networks. Stockholm, Sweden, Jun 2005

[36] Anis KOUBAA and Mario Alves, “A Two-Tiered Architecture for Real-Time Communications in Large-Scale Wireless Sensor Networks: Research and Challenges,” Proceedings of 17th Euromicro Conference on Real-Time Systems (ECRTS'05), WiP Session, Palma de Mallorca (Spain), 5-7 Jul, 2005.

[37] Jussi Haapola, Zach Shelby, Carlos Pomalaza-Raez and Petri Mahonen, “Cross-Layer Energy Analysis of Multi-hop Wireless Sensor Networks,” Proceedings of 2nd European Workshop on Sensor Networks (EWSN) 2005, Istanbul, Jan-Feb 2005.

[38] Gyula Simon et al., “Sensor Network-Based Countersniper System,” Sensys’04, Nov 3-5 2004, Baltimore, Maryland, USA.

[39] Jerry Zhao and Ramesh Govindan, “Understanding Packet Delivery Performance in Dense Wireless Sensor Networks,” Sensys’03, Nov 5-7, 2003, Los Angeles, California, USA.

[40] Y. Yao and G. B. Giannakis, “Energy-Efficient Scheduling for Wireless Sensor Networks,” IEEE Transactions on Communications, Vol.53, No.8, pp.1333-1342, Aug. 2005.

[41] Mustafa Ergen and Pravin Varaiya, “Energy Consumption (J/MB) in 802.11 Networks,” http://paleale.eecs.berkeley.edu/~varaiya/comm.html, last accessed on Jan 2006.

[42] Kyle Jamieson, Bret Hull, Allen Miu and Hari Balakrishnan, “Understanding the Real-World Performance of Carrier Sense,” Proceedings of the ACM SIGCOMM Workshop on Experimental Approaches to Wireless Network Design and Analysis (E-WIND), pp. 52–57, Philadelphia, PA, 2005.

[43] Matthew J. Miller and Nitin H. Vaidya, “Improving Power Save Protocols Using Carrier Sensing and Busy-Tones for Dynamic Advertisement Windows,” The 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2005), Nov 2005.

[44] Rong Zheng, Jennifer C. Hou and Lui Sha, “Asynchronous Wakeup for Ad Hoc Networks,” Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, Annapolis, Maryland, USA, pp.35-45, 2003.

[45] Wei Ye, John Heidemann and Deborah Estrin, “Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks,” IEEE/ACM Transactions on Networking, Vol.12, No.3, pp.493-506, Jun 2004.

[46] Tijs van Dam and Koen Langendoen, “An Adaptive Energy-Efficient MAC Protocol for Wireless Sensor Networks,” Sensys’03, Nov 5-7 2003, Los Angeles, California, USA.

[47] Joseph Polastre, Jason Hill and David Culler, “Versatile Low Power Media Access for Wireless Sensor Networks,” Sensys’04, Baltimore, Maryland USA, pp.95-107, Nov 3-5 2004.

[48] Samir Goel and Tomasz Imielinski, “Etiquette Protocol for Ultra Low Power Operations in Sensor Networks,” Technical Report DCS-TR-552 (Revision), Department of Computer Science, Rutgers University, NJ, Oct 2004.

[49] Mike Southworth and David Godso, “Chem-Biosensor Platform Leverages PC/104”, COTS Journal, pp. 74-76, Mar 2003.

[50] Mary Rose Burnham et al., ”Membrane/Ion-Channel Biosensor”, Presentation given at the Cornell Multidisciplinary Sensor Network Workshop, 11th Oct 2005, http://wisl.ece.cornell.edu/workshops/2005_10_11/, last accessed on Jan 2006.

[51] J. Palet et al., “Analysis of IPv6 Multihoming Scenarios”, IETF Internet Draft, Jul 2004.

[52] Paolo Crucitti et al., “Efficiency of Scale-Free Networks: Error and Attack Tolerance,” Elsevier Physica A: Statistical Mechanics and Its Applications, Vol.320, pp.622-642, 2003.

[53] Jan Matlis, “Scale Free Networks,” http://www.computerworld.com/networkingtopics/networking/story/0,10801,75539,00.html, last accessed on Jan 2006.

[54] ZigBee Specification: "ZigBee Document 053474r06", Version 1.0, 27th Jun 2005

[55] IEEE Std 802.15.4-2003: "Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", IEEE Computer Society, 1 Oct 2003

[56] Ed Callaway, "Low Power Consumption Features of the IEEE 802.15.4/ZigBee LR-WPAN Standard," Presentation at Sensys'03, 6th Nov 2003.

[57] Ian Marsden, "Using ZigBee for Location Logging in Mobile Networks," Presentation at Wireless Networking in M2M Applications Congress, Duesseldorf, Germany, 21-22 Jun 2005

[58] Zachary Smith, "Network Layer Technical Overview," Presentation at ZigBee Alliance Open House Presentation, San Francisco, 2nd Mar 2005, http://www.zigbee.org/en/events/OpenHousePresentations_2005-03-02.asp, last accessed on Jan Dec 2005.

[59] "ns-2," http://www.isi.edu/nsnam/ns/, last accessed on Nov 2005.

[60] Jianliang Zheng and Myung J. Lee, "Will IEEE 802.15.4 Make Ubiquitous Networking a Reality?: A Discussion on a Potential Low Power, Low Bit Rate Standard," IEEE Communications Magazine, pp.2-8, Jun 2004.

[61] "Tracegraph," http://www.tracegraph.com/, last accessed on Jan 2006.

[62] "ns-2 manual," http://www.isi.edu/nsnam/ns/doc/index.html, last accessed on Jan 2006.

[63] "Understanding 802.15.4 and ZigBee Networking," http://www.daintree.net, last accessed on Jan 2006.

[64] Victor M. Eguiluz and Konstantin Klemm, "Epidemic threshold in structured scale-free networks," Physical Review Letters, Vol.89, 2002

[65] R. Pastor-Satorras and A. Vespignani, "Epidemics and immunization in scale-free networks," Handbook of Graphs and Networks: From the Genome to the Internet, Wiley-VCH, Berlin, pp. 113-132, 2002.

[66] K.I. Goh, E.S. Oh, H. Jeong, B. Kahng and D. Kim, "Classification of scale free networks," Proceedings of National Academy of Science, USA, Vol.99, No.20, pp. 12583-8, 1 Oct 2003.

[67] Paolo Crucitti et al., "Efficiency of Scale-Free Networks: Error and Attack Tolerance," *Physica A: Statistical Mechanics and its Applications*, Elsevier, 2003.

[68] Romualdo Pastor-Satorras and Alessandro Vespignani, "Epidemic spreading in scale-free networks," Physical Review Letters, 86(14), pp. 3200—3203, 2 Apr, 2001.

[69] Joseph Polastre, Robert Szewczyk and David Culler, "Telos: Enabling Ultra-Low Power Wireless Research," www.moteiv.com, last accessed on Jan 2006.

[70] Barabási, A.-L. and Albert, R. "Emergence of scaling in random networks," Science, Vol.286, pp. 509–512, 1999.

[71] Albert, R., Jeong, H. and Barabási, A.-L, "Error and attack tolerance of complex networks," Nature, pp.406–378, 2000.

[72] K. Klemm and VM Eguiluz, "Growing scale-free networks with small-world behavior", Physics Review E 65, 057102, 2002.

[73] Adilson E. Motter, Takashi Nishikawa, and Ying-Cheng, Lai, "Range-based attack on links in scale-free networks: are long-range links responsible for the small world phenomenon?" Physics Review E 66, 065103, 2002.

[74] "Types of ZigBee Networks," http://www.stg.com/wireless/ZigBee_netw.html, last accessed on Jan 2006.

[75] Khanh Tuan Le, "Transceiver Design for IEEE 802.15.4 and ZigBee Complaint Systems", Microwave Journal, Sept 2005.

[76] S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, "A Taxonomy of Wireless Microsensor Network Models," ACM Mobile Computing and Communications Review, Vol.1, No.2, pp.1-8, 2002.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Chairman, Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

4. Professor Tri T. Ha, Code EC/Ha
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

5. Professor Weilian Su, Code EC/Su
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA