Air Force Institute of Technology

AFIT Scholar

Theses and Dissertations

Student Graduate Works

3-2006

Supplementing an AD-HOC Wireless Network Routing Protocol with Radio Frequency Identification (RFID) Tags

LeRoy S. Willemsen

SUPPLEMENTING AN AD HOC WIRELESS NETWORK ROUTING PROTOCOL WITH RADIO FREQUENCY IDENTIFICATION (RFID) TAGS

THESIS

LeRoy S. Willemsen, Captain, USAF

AFIT/GE/ENG/06-56

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government.

AFIT/GE/ENG/06-56

SUPPLEMENTING AN AD HOC WIRELESS NETWORK ROUTING PROTOCOL WITH RADIO FREQUENCY IDENTIFICATION (RFID) TAGS

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

LeRoy S. Willemsen, BSEE

Captain, USAF

March 2006

AFIT/GE/ENG/06-56

SUPPLEMENTING AN AD HOC WIRELESS NETWORK ROUTING PROTOCOL WITH RADIO FREQUENCY IDENTIFICATION (RFID) TAGS

LeRoy S. Willemsen, BSEE

Captain, USAF

Approved:

/signed/

_____________________________________ ________

Rusty O. Baldwin, Ph.D. (Chairman) Date

/signed/

_____________________________________ ________

Barry E. Mullins, Ph.D. (Member) Date

/signed/

___________________________________ ________

Richard A. Raines, Ph.D. (Member) Date

Acknowledgments

I would like to express my sincere appreciation to my faculty advisor Dr. Rusty Baldwin for his guidance and support throughout the course of this thesis effort. I would also like to thank my family, whose support and encouragement throughout this endeavor have been instrumental and vital to my success.

LeRoy S. Willemsen

.

Table of Contents

Page

List of Figures

Page

List of Tables

Page

AFIT/GE/ENG/06-56

Abstract

Wireless sensor networks (WSNs) have a broad and varied range of applications, yet all of these are limited by the resources available to the sensor nodes that make up the WSN. The most significant resource is energy; a WSN may be deployed to an inhospitable or unreachable area leaving it with a non-replenishable power source. This research examines a technique of reducing energy consumption by augmenting the nodes with radio frequency identification (RFID) tags that contain routing information. It was expected that RFID tags would reduce the network throughput, AODV routing traffic sent, and the amount of energy consumed. However, RFID tags have little effect on the network throughput or the AODV routing traffic sent. They also increase ETE delays in sparse networks as well as the amount of energy consumed in both sparse and dense networks. Furthermore, there was no statistical difference in the amount of user data throughput received. The density of the network is shown to have an effect on the variation of the data but the trends are the same for both sparse and dense networks. This counter-intuitive result is explained and conditions for such a scheme to be effective are discussed.

SUPPLEMENTING AN AD HOC WIRELESS NETWORK ROUTING PROTOCOL WITH RADIO FREQUENCY IDENTIFICATION (RFID) TAGS

I. Introduction

A wireless sensor network (WSN) is an infrastructureless network of small nodes which can communicate over short distances. Each node has a sensor, memory, data processor, power source, and a communications component. The applications for a WSN are broad and varied but all are limited by the resources available to each node. Extending the resources of the nodes is paramount to extending the capabilities of the WSN.

1.1 Overview

A WSN can contain thousands of randomly deployed nodes with no pre-existing infrastructure. However, low node density or a small population of nodes within a WSN may mean nodes cannot communicate directly with each other. Therefore, each node must also act as a router to forward packets to a destination. Several routing protocols have been developed to facilitate the routing of information packets within a network. The ad hoc on-demand distance vector (AODV) routing protocol is the basis of this research. The nodes in a WSN are limited in what they can accomplish due to the limited resources of each node, the most limiting of which is power [ASS02a, Nat05]. The lifetime of the node and the network itself is determined by the lifetime of the battery.

Radio frequency identification (RFID) is a method of remotely storing and retrieving data using devices called tags. RFID tags can be passive or active. A passive tag has no battery. Instead, it gets power from the interrogator (reader) which generates an electromagnetic field (EMF) to read the contents of the tag. The tag uses a portion of this EMF power to respond eliminating the need for a battery. An active tag has an internal power source and responds to the reader using its own power source when energized. This gives the active tags longer range with more storage capability. The operation of both tags is similar; when a reader energizes a tag, it responds by transmitting its memory contents or a portion thereof.

1.2 Motivation and Goals

WSNs have a broad range of applications, especially military applications, such as detecting enemy movement, Chemical, Biological, or Nuclear agents or an explosion or other phenomena [Nat05]. The manner in which WSNs may be deployed and their location may render them inaccessible. Nodes deployed from an aircraft to an extreme environment (enemy territory, toxic area) would be an example of inaccessibility.

The goal of this research is to analyze the effect of incorporating RFID tags on energy consumption and other network performance metrics when using the AODV routing protocol. Measuring the effect RFID tags have on the AODV protocol and energy consumption provides insight into which node configuration (no tags, passive tags, or active tags) to use in different situations.

1.3 Thesis Organization

This chapter introduces WSNs and RFID tags and the motivation for this research. Chapter II introduces common routing protocols for both mobile ad hoc networks (MANET) and WSNs. Chapter III discusses the experimental methodology used for this research. Chapter IV provides the results and analysis of the experiments.

Chapter V presents the conclusions drawn from the results and analysis and indicates areas for further research.

II. Literature Review

This chapter provides an overview of WSNs, RFID tags, and routing protocols for both MANETs and WSNs. Section 2.1 discusses WSNs and provides an example of a commonly used sensor node. Section 2.2 introduces RFID tags and their operation. Section 2.3 introduces routing protocols for MANETs and WSNs. Section 2.4 provides a brief description of some table-driven routing protocols. Section 2.5 discusses some common on-demand routing protocols. Section 2.6 presents the Zone Routing Protocol, a hybrid routing protocol. Section 2.7 discusses some WSN routing protocols. Section 2.8 provides a summary for this chapter.

2.1 Wireless Sensor Networks

A wireless sensor network is an infrastructureless network of small nodes. Nodes are about the size of a deck of cards and can communicate over short distances, about 150 meters [Cro05]. Each node typically has a sensor, memory, data processor (to process data prior to sending it), power source and a communication component. A WSN can consist of thousands of densely-deployed nodes possibly moving independently within the network. The position of these nodes are not necessarily pre-determined [ASS02a] which allows many different deployment scenarios, some of which may be to areas that are inhospitable. It is this lack of organization that forces WSN routing protocols to be self-organizing [Nat05].

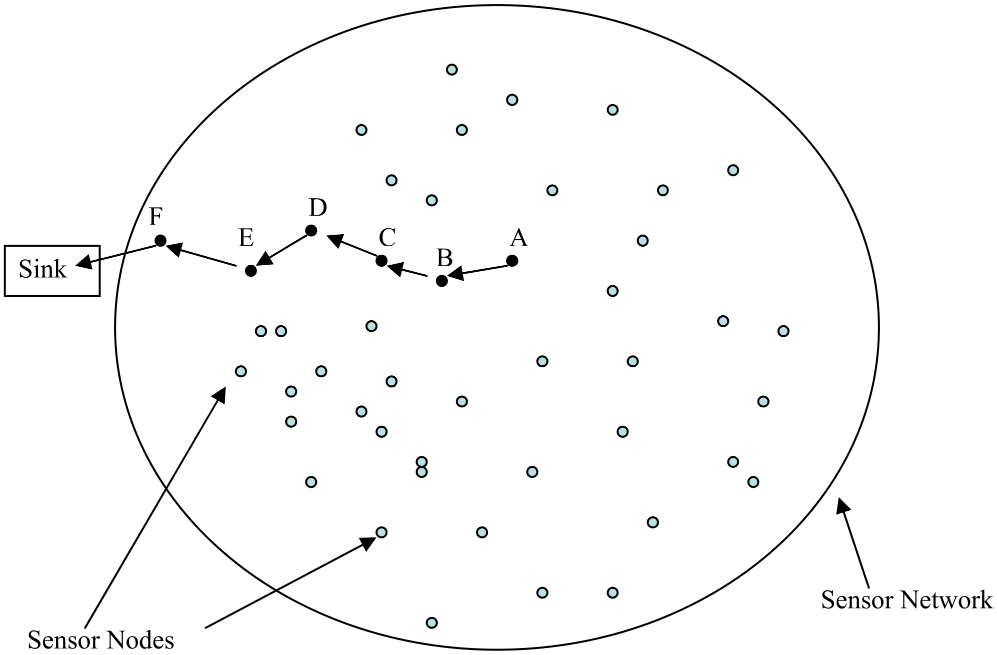


Figure 1: Wireless Sensor Network

Figure 1 shows a possible sensor network topology. Node A is a sensor node with data to send. The arrows indicate a path the data may follow to reach the destination (Sink). Low node density or a small population within a WSN may mean nodes are not able to communicate directly with each other. Therefore, each node in the network must also act as a router to forward packets along a path to the destination, a process which may require multiple hops to reach the destination.

The nodes in a WSN are limited in what they can accomplish because they have limited resources. The most limiting resource is power. The lifetime of the node and the network itself is determined by the life of the battery [ASS02a, Nat05]. Node memory and data processing capabilities are also scarce resources. For example, the processing unit of the Crossbow Technologies MICA2 platform uses the Atmel ATmega 128L microcontroller. This microcontroller has 128 KB of Programmable Flash, 4 KB EEPROM and 4 KB SRAM [Atm04, Cro05]. The communication component consists of an RF transmitter and receiver to communicate with other nodes. In terms of power, transmitting is the most expensive operation a node performs [Cro05]. Since the nodes typically have a non-replenishable power source, conserving energy is paramount, and minimizing transmissions is one way to extend the life of the network.

2.2 Radio Frequency Identification (RFID)

Radio frequency identification (RFID) is a method of remotely storing and retrieving data using devices called tags. RFID tags come in several sizes and can be passive or active. A passive tag has no battery; instead, it gets its power from the interrogator (reader) which generates an electromagnetic field (EMF) to read the contents of the tag. The tag uses a portion of this EMF to generate its power eliminating the need for a battery. Passive tags have a very short transmission range, on the order of about 1 - 3 meters, and a limited read/write memory of 32 – 256 bits of data. Figure 2 shows a passive RFID tag, actual size is 1.81” x 3.11” x 0.051”. This is one of many possible sizes and shapes for a passive tag.

Figure 2: Passive RFID tag [Int04]

Active tags contain a battery and therefore have greater capabilities. Active tags have ranges on the order of 1 – 50 meters with read/write memory of 256K – 1M bits [Ass05]. Figure 3 shows an active RFID tag, actual size is 2.4” x 1.2” x 0.4”. This is just one of many different sizes and shapes.

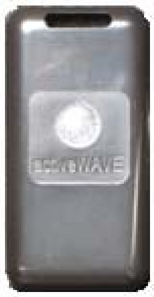


Figure 3: Active RFID Tag [Act05]

Typical frequency ranges for both types of tags are:

- 300-500KHz
- 850-900MHz
- 2.4GHz-2.5GHz

The ranges associated with each frequency band are dependent on obstructions near the devices; however, higher frequencies tend to have shorter ranges for the passive tags [Int04]. In order to communicate RFID tags use a version of ALOHA medium access control (MAC). When an RFID tag sends a response it delays that response by randomly selecting a slot then transmits within the slot. The slot size is based on the packet size and data rate. The actual implementation of the MAC protocol is specific to the RFID manufacturer but are based on the ALOHA protocol.

2.3 Routing Protocols

Routing protocols are schemes to facilitate the transfer of messages between nodes in a network. There are many different protocols, but they can be separated into three different categories: table-driven, source initiated, and hybrid. Table driven protocols, also called proactive protocols, try to provide consistent, up-to-date routing information to each node in the network resulting in a common global view of the network. These protocols must maintain several tables to store this routing information. Changes to the network are propagated throughout the network to maintain the routing tables [RoT99]. Some proactive routing protocols include:

- Destination–Sequenced Distance-Vector Routing Protocol (DSDV)
- Clusterhead Gateway Switch Routing Protocol (CGSR)
- Wireless Routing Protocol (WRP)

Source initiated protocols, also called reactive or on-demand, create routes only as needed and do not maintain a table with routes to all destinations. When a source needs to send a message it establishes a route to the destination and sends the message. The route is maintained as long as the path exists or until the source no longer needs it [RoT99]. Some on-demand routing protocols include:

- Dynamic Source Routing (DSR)
- Ad hoc On-Demand Distance Vector Routing (AODV)
- Temporally Ordered Routing Algorithm (TORA)

Hybrid Routing Protocols combine table-driven routing protocols with on-demand routing protocols, using table-driven protocols in some parts of the network and on-demand in others. These protocols allow nodes in close proximity to minimize the cost of route discovery by maintaining a table of routes to nearby nodes and establish routes on-demand to distant nodes [AWD04, LWZ03]. One popular hybrid routing protocol is the Zone Routing Protocol (ZRP) but there are several others. ZRP is used in this chapter as a reference protocol to discuss the basic function of hybrid protocols. Each routing protocol has strengths and weaknesses, and the network configuration will ultimately determine the most suitable routing protocol to implement.

The aforementioned protocols are primarily designed for MANETs and are not well suited for WSNs. WSNs require more scalable and energy-efficient routing protocols. This new and emerging field is the subject of much research at this time. The Wireless Sensor Network routing protocols that are discussed are:

- Sensor Protocols for Information via Negotiation (SPIN)
- Directed Diffusion
- Low Energy Adaptive Clustering Hierarchy (LEACH)

These are only a few of many protocols available for use in WSNs but they are representative of many that have been proposed.

2.4 Table-Driven Routing Protocols

Table-driven routing protocols try to maintain the current network state accurately in a series of tables and use this information to determine the best route to a destination. The following is a brief discussion on some table-driven routing protocols.

2.4.1 Destination–Sequenced Distance-Vector Routing Protocol

The Destination–Sequenced Distance-Vector Routing Protocol (DSDV) algorithm is a table-driven routing protocol in which every node maintains a routing table with all possible destinations and the number of hops required to reach them. This algorithm provides loop free routes by giving each table entry a sequence number assigned by the destination [PeB94]. These sequence numbers are used to distinguish stale routes from new ones thus providing loop free routes [RoT99].

2.4.1.1 DSDV Operation

There are two types of update messages used in DSDV, 'full dump' and 'incremental' messages. Full dump messages contain all of the routing information in a node. Full dump messages are sent whenever a change to network topology is detected, such as when a new node joins the network. The new node will broadcast its route table; the first node to receive this message will update its own route table and broadcast the new table. This process is repeated throughout the network.

The incremental message contains only the information that has changed since the last full dump and is used to capture rapid changes in network topology created by mobile nodes. The incremental messages are smaller than full dump messages. An incremental message is limited to one packet length while full dump messages can consist of multiple packets. The incremental messages are used until the size of the updates can no longer fit into one packet, at that time a full dump message is scheduled. Incremental messages a sent more frequently based on the mobility of the nodes.

When a node receives new routing information, it compares that information to its own routing table. Any routes with a greater sequence number are used and the route with the old sequence number is discarded. If the sequence numbers are equal the node chooses the route with a better metric, hop count, and discards the other. DSDV does not scale well to large networks due to this large overhead [AWD04].

2.4.2 Clusterhead Gateway Source Routing Protocol (CGSR)

Clusterhead Gateway Source Routing Protocols are hierarchical routing protocols. Nodes are grouped together to form a cluster with the clusterhead performing all routing to destinations outside the cluster. The clusterhead is elected using a distributed clusterhead election algorithm. All nodes within transmission range of the clusterhead belong to that cluster. As non-clusterhead nodes move between clusters, no clusterheads are changed, only cluster members. When a clusterhead moves into another cluster it challenges the current clusterhead, and the clusterhead with the highest priority will remain a clusterhead. The clusterhead priority scheme should be well defined, could be related to node connectivity or node identification. When a non-clusterhead node moves out of its cluster and does not enter a new cluster it becomes a new clusterhead creating a new cluster. CGSR uses DSDV as the underlying routing scheme and therefore has the same overhead. Clusterheads route traffic outside the cluster through a gateway node, which is a node that can communicate with at least two clusterheads. Nodes within a cluster first route a packet to the clusterhead which in turn routes it to the appropriate gateway, which forwards the packet along to the appropriate clusterhead or nearest clusterhead along the path to the destination. Each node within a cluster must maintain a cluster member table that is periodically updated. Each node also maintains a complete routing table as in DSDV.

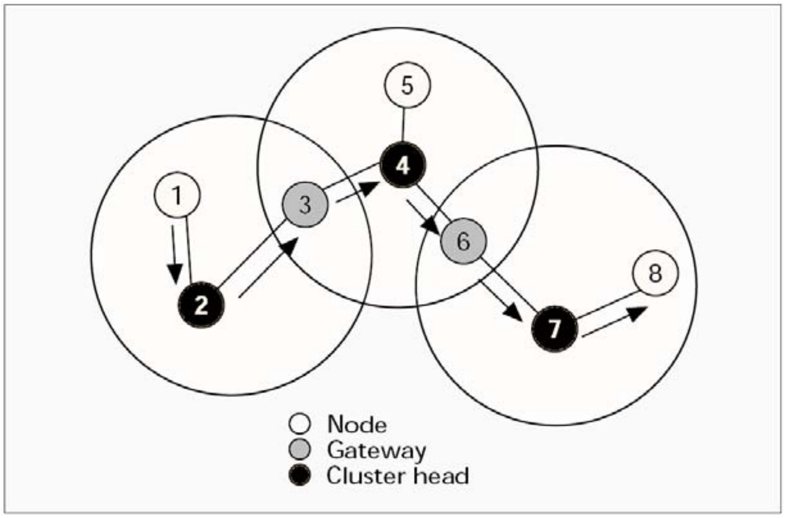


Figure 4: CGSR Packet Routing [RoT99]

Figure 4 illustrates the routing scheme in CGSR. Routing a packet from node 1 to node 8 begins with node 1 sending the packet to its clusterhead (node 2). Node 2 the clusterhead forwards this packet to its gateway (node 3). Node 3 forwards the packet to the next clusterhead along the path to the destination (node 4). Node 4 forwards the packet to node 6 which is a gateway; node 6 forwards to node 7 the clusterhead for node 8. Finally node 7 forwards the data packet to the destination node, node 8. In addition to the high overhead of DSDV, CGSR introduces critical nodes (clusterheads) and single points of failure at the clusterhead. If a clusterhead fails, the cluster must re-elect a clusterhead introducing more overhead and delay [AWD04, CWL97, RoT99].

2.4.3 Wireless Routing Protocol (WRP)

The Wireless Routing Protocol, like DSDV, ensures loop free routing but requires that each node maintain four routing tables [MuG96]:

- Distance Table
    - Distance of each destination via each neighbor

- Routing Table
    - Distance of each destination from source
    - The predecessor and the successor of the source node
    - Tag to identify if path is simple, loop or invalid
- Link-Cost Table
    - Cost of the link to each neighbor
    - Number of timeouts since an error-free message received from neighbor
- Message Retransmission Table (MRL)
    - Sequence number of the update message
    - Retransmission counter
    - Acknowledgement flag vector, one entry per neighbor
    - List of updates sent in the update message

Link changes are propagated through the network using update messages. These messages are only sent between neighboring nodes. An update message contains: the identification of the sending node, a sequence number assigned by the sending node, an update list which contains the actual updates, and a response list. The update list specifies a destination, a distance to the destination (hop count), and a predecessor to the destination. The response list is a list of nodes that should send an ACK to the update message. After receiving an update message a node is required to send a positive acknowledgement (ACK) indicating that it has processed that update message and therefore, has good radio connectivity. Each node propagates changes after it receives an update. If a node is not sending data messages, it still sends hello messages to indicate it is operational. WRP provides loop free routing by detecting changes in links. With each link change, a node checks the consistency of its neighbors [RoT99]. However, due to the number of tables required to support this protocol, the memory requirements are substantial [AWD04].

2.5 On-Demand Routing Protocols

On-demand routing protocols do not maintain the state of the network but rather create routes on an as needed basis. These routes are maintained as long as the route is required or until the route is no longer available. There are several on-demand routing protocols. The following is a discussion of some of these protocols.

2.5.1 Dynamic Source Routing (DSR)

In Dynamic Source Routing, nodes are required to maintain route caches to all destinations the node is aware of. These route caches are continually updated as the network topology changes using route discovery and route maintenance messages [JOM96].

2.5.1.1 Route Discovery

Route discovery is initiated when a node has data to send but no route to a destination, or an expired route to a destination in its route cache. The node broadcasts a *route request* packet, which includes the destination address, source address and a unique identification number. As each intermediate node receives this request it determines if it has a route to the destination. If it does, it returns a *route reply* to the source node. However, if an intermediate node does not have a route to the destination, it adds its address to the route record of the packet and forwards the packet if it has not received this packet before and its address is not contained in the route record. This eliminates loops in *route requests*. The *route reply* packet is sent from either the destination node or an intermediate node with a route to the destination. If bidirectional links are available, the packet is sent in the reverse direction to the source according to the route record in the packet. Otherwise, the node uses a route in its route cache. If no route exists it will piggy back the reply with a *route request* to the source, thus reducing route discovery packets. To further reduce the number of route discoveries generated for the same destination, the source node uses an exponential back-off algorithm which doubles the timeout between successive *route requests* for the same destination [JMH03].

2.5.1.2 Route Maintenance

Route maintenance is accomplished using *route error* packets. A *route error* packet is generated when the forwarding node determines a link is no longer available. This forwarding node sends the route error packet to the source node. The route error packet contains the address of the host that detected the error and the address of the host to which the packet was destined. Upon receiving a *route error* packet, all routes which contain the node reporting the error are removed from the route cache [JOM96].

2.5.2 Ad hoc On-Demand Distance Vector Routing (AODV)

Ad hoc On-Demand Distance Vector Routing (AODV) builds on the DSDV algorithm. AODV minimizes the number of broadcasts by creating routes on-demand, rather than maintaining a complete list of routes as in DSDV. AODV has the same route discovery scheme as DSR. The main difference is an AODV packet contains the destination address while a DSR packet carries the entire route. AODV employs two functions: route discovery and route maintenance [PeR99].

2.5.2.1 Route Discovery

When a node needs to forward data and there is no valid entry in the route table, it broadcasts a route request packet (RREQ) to its neighbors. The RREQ packet contains the following fields:

- Source address
- Source sequence number
- Broadcast ID
- Destination address
- Destination sequence number
- Hop count (initially set to 0)

The source address and the broadcast id uniquely identify each RREQ. The broadcast id is incremented each time the source transmits a new RREQ. The source sequence numbers are maintained by each node and are used to maintain information about the reverse path to the source. The destination sequence number is the most recent sequence number the source has for the destination. A node with a path to the destination can only reply to the RREQ if it has a destination sequence number greater than or equal to the one contained in the RREQ. As a RREQ propagates through the network, intermediate nodes record the address of the first neighbor from which the packet was received, and build the reverse path back to the source. Intermediate nodes also increment the hop counter and rebroadcast the packet to their neighbors with its address in the address field of the RREQ packet. When the RREQ reaches the destination node or an intermediate node with a fresh path to the destination, a route reply (RREP) packet is sent. This packet contains the following fields:

- Source address
- Destination address
- Destination sequence number
- Hop count
- Lifetime

The RREP packet is unicast to the neighbor from which the first RREQ is received. As this packet is routed back along the reverse path, nodes along the path update the forward route table entries with the address from which the RREP was received.

2.5.2.2 Route Maintenance

Route maintenance is accomplished using a RREP packet with a fresh sequence number (incremented by one) and the hop count set to infinity. This packet is generated by the node that detects a link failure and is propagated to all upstream neighbors. The upstream nodes update their route table and forward the message to their neighbors and so on until all nodes are notified. If a node still requires a route to this destination it can restart the discovery process using a RREQ message. One additional feature of the protocol is the hello message. Hello messages are periodically broadcast by a node to indicate a node's presence. The use of hello messages is not a requirement of the protocol and its use is a function of the application.

2.5.3 Temporally Ordered Routing Algorithm (TORA)

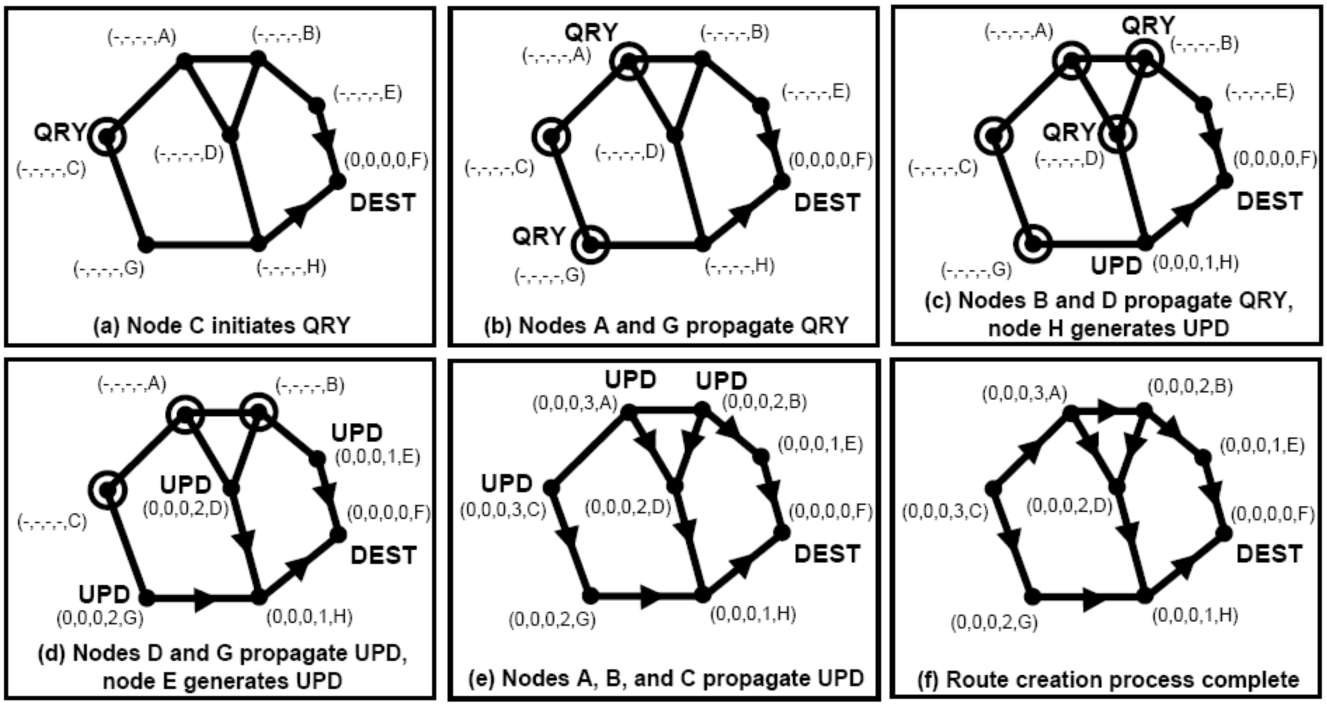
The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, loop-free, distributed routing algorithm based on the concept of link reversal. TORA provides multiple paths to the destination while limiting the propagation of control messages to a small set of nodes near the occurrence of a topological change. TORA performs three functions: route creation, route maintenance and route erasure [PaC97, RoT99].

2.5.3.1 Route Creation

Route creation assigns directions to links in an undirected network [PaC97]. During route creation nodes use a height metric which is represented as a quintuple, $H_i = (\tau_i, oid_i, r_i, \delta i, i)$ where:

- τ_i – is the time of a link failure, represents the first element of the reference level, initially set to null for route creation
- oid_i – originator-id, ID of the node that defines a new reference level this is the second element of the reference level
- r_i – a single bit used to divide each reference level into 2 sub-levels. This bit is used to distinguish between the original reference level and the new reference level. Represents the third and final element of the reference level.
- δ_i – integer that orders nodes with respect to a unique reference level.
- i – unique identifier of the node.

Links are assigned a direction (upstream or downstream) based on the height metric of neighboring nodes. A query (QRY) packet is used for route creation as well as an update (UPD) packet. Creating a route with TORA requires establishing a sequence of directed links to the destination which is only done when a node has no directed links to the destination. A QRY packet consists of a destination ID (*did*) which identifies the destination. A UPD packet consists of a *did* and the height of the node which broadcasts the packet. Each node maintains a route required flag which is initially clear. When a node requires a route to the destination, it broadcast a QRY and sets its route required flag.



(a) Node C initiates QRY

(b) Nodes A and G propagate QRY

(c) Nodes B and D propagate QRY, node H generates UPD

(d) Nodes D and G propagate UPD, node E generates UPD

(e) Nodes A, B, and C propagate UPD

(f) Route creation process complete

Figure 5: TORA Route Creation Process [PaC97]

Figure 5 illustrates the route creation process, notice that the height quintuple of all nodes except the destination are set to (-,-,-,-,*i*). Node C in Figure 5a initiates a QRY and sets its route required flag to true, indicated by the circle around the node. Figure 5b shows nodes A and G forwarding the QRY and setting their route required flags to true. Nodes B and D propagate the QRY and node H sends a UPD in Figure 5c. Notice that the height quintuple of node H now contains (0, 0, 0, 1, H) indicating it is the first node away from node F the destination. In Figure 5d nodes D and G are propagating a UPD while node E generates a UPD. The height of each node has changed showing their order to the destination. Also notice that nodes D and G no longer have their route required flags set to true (no circles). Figure 5e shows the propagation of the UPD with all nodes clearing their route required flags and their heights adjusted. Figure 5f shows the completed route creation with no messages in transit.

When a node receives a QRY packet it performs the following:

- If the node has no downstream links and its route required flag is clear, it rebroadcasts the packet and sets its route required flag.
- If the node has at least one downstream link and the route required flag is set, it discards the packet.
- If the node has at least one downstream link and its height is NULL, it sets its height to the minimum height of its non-NULL neighbors and broadcasts a UPD packet.
- If the node has at least one downstream link and its height is not-NULL, it compares the time the last UPD packet was broadcast to the time the link over which the QRY packet was received became active. If a UPD packet has been broadcast since the link became active it discards the QRY packet; otherwise, it broadcasts a UPD packet.

If a node has the route required flag set when a new link is established, it broadcasts a QRY packet [PaC97, RoT99].

2.5.3.2 Route Maintenance

Route maintenance uses the QRY and UPD packets. When a DAG route is broken, route maintenance is used to re-establish a DAG. When a node detects a downstream link failure it generates a new reference level and propagates it to neighboring nodes. Links are reversed to reflect the change to the new reference level. This reverses the direction of one or more links when a node has no downstream links.

TORA assumes all nodes have synchronized logical clocks because the height metric is dependent on the logical time of a link failure. The reference level is comprised of the first three elements of the height quintuple. This reference level is redefined each time a node loses its downstream link.

2.5.3.3 Route Erasure

Route erasure uses a CLR packet which is flooded through the network to erase invalid routes. A route becomes invalid when a link failure creates a partition of part of the network [PaC97, RoT99]. This partition is no longer part of the greater network and clears all routes that do not exist within the partition. This allows the communication within the partition to continue without wasting resources trying to route data to unreachable destinations.

2.6 Hybrid Routing Protocols

Hybrid routing protocols combine proactive and reactive protocols. These protocols increase scalability by allowing nodes in close proximity to work together to perform routing duties. This is done primarily using proactive techniques to maintain routes to nearby nodes and reactively determining routes to distant nodes [AWD04]. What follows is a brief description of the Zone Routing Protocol.

2.6.1 Zone Routing Protocol (ZRP)

In ZRP, nodes establish a routing zone; each node within the zone must maintain network connectivity in a proactive manner and the range of this zone is defined in hops.

This ensures that all nodes within the zone are immediately available. Routes to nodes not in the zone are determined as needed. ZRP is not so much a distinct protocol but rather provides the framework for other protocols.

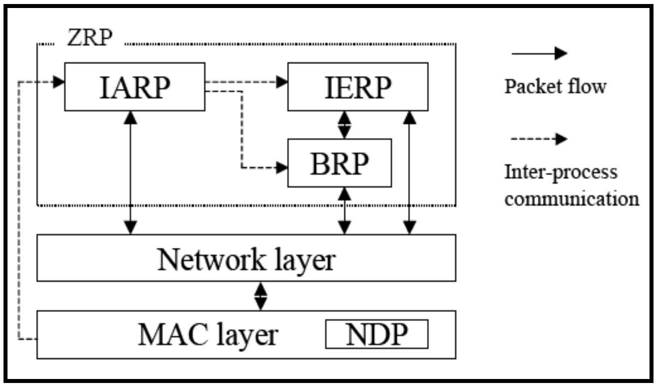


Figure 6: ZRP Architecture [HPS02]

Figure 6 shows the relationship between the different protocols within the Zone Routing Protocol framework. The protocols used with ZRP are Neighbor Discovery Protocol (NDP), Intrazone Routing Protocol (IARP), Interzone Routing Protocol (IERP) and Bordercast Resolution Protocols (BRP) [HPS02].

Route updates are triggered by NDP which relies on the MAC layer to detect neighboring nodes. NDP transmits HELLO messages at regular intervals. Upon receipt of a HELLO message, the neighbor table is updated. When a HELLO message is not received within a specific time, entries are removed from the neighbor table. NDP notifies IARP of updates to the neighbor table. IARP communicates with the interior nodes of its zone. IARP maintains routes to nodes within the zone proactively; a node's zone is determined by a certain number of hops known as the zone radius. Each node maintains it own routing zone which has the added benefit that routing zones of neighboring nodes overlap. IARP is restricted to routing within the zone. IERP uses a reactive approach to communicate with nodes in other zones. Route queries between different zones are used on-demand, that is, only when a request for a route is made. The delay caused by the route discovery is minimized through the use of bordercasting. IERP uses the routing table of IARP to respond to route queries which are forwarded with BRP. BRP directs the route requests initiated by IERP to the peripheral nodes. It uses the routing table provided by IARP to construct a bordercast tree which directs queries away from the covered zone. BRP also uses the routing table of IARP to guide route queries away from the source.

2.6.1.1 ZRP Routing

Routing in ZRP has several facets and is dependent on the scenario. If a node has a packet to send, it determines if the destination is within its zone by checking the IARP. If the destination is within the zone, the node routes the packet according to the proactively determined route. If, however, the destination lies outside the zone reactive routing is used to find a route to the destination.

Reactive routing occurs in two phases, *route request* and *route reply*. Route request starts with the generation of a route request packet sent to the peripheral nodes using BRP. If the receiving node has a route to the destination it responds with a route reply packet, otherwise the node will continue bordercasting the packet. A route reply is sent when the packet reaches the destination or a node with a valid route to the destination. The route reply is sent in the reverse direction of the request using the sequence of addresses contained in the request.

Route maintenance uses NDP at the MAC layer. When a link is found to be defective or no longer available, the neighbor table is updated and forwarded as described earlier.

2.7 Wireless Sensor Network Routing Protocols

Due to the limited resources available to nodes in a WSN and the number of nodes in a network, a WSN routing protocol must be:

- Scalable
- Self-organizing
- Have low overhead
- Energy-efficient

There has been considerable research done in the area of routing in sensor networks. WSN routing protocols fall into three main categories; data centric, hierarchical, or location based [ALK04]. Data centric protocols prolong the life of the network by aggregating the data, therefore reducing the amount of data transmitted. Hierarchical protocols establish zones or clusters to reduce the amount of network traffic. Nodes in a zone or cluster communicate with the clusterhead which aggregates the data and forwards it to a base-station. Location based protocols use position information to relay data to the desired region of the network instead of the entire network. The following section discusses only a few of the routing protocols for wireless sensor networks. These include:

- Sensor Protocols for Information via Negotiation (SPIN)
- Directed Diffusion
- Low Energy Adaptive Clustering Hierarchy (LEACH)

2.7.1 Sensor Protocols for Information via Negotiation (SPIN)

The SPIN protocol [HKB99] is a family of protocols that disseminates all the information a node has to every node in the network under the assumption that all nodes are potential base-stations. This enhances fault tolerance since all nodes have a copy of all the data in the network. Thus the user can query any node to get the required information making SPIN a query based protocol. SPIN operates under the premise that nodes in close proximity have similar data, requiring nodes to only forward data that other nodes do not have. This reduces the amount of unnecessary data being transmitted across the network, saving valuable resources. The SPIN protocol uses two basic ideas; negotiation and resource adaptation.

2.7.1.1 Negotiation

Nodes using SPIN negotiate with each other prior to transmitting data to prevent "implosion". Implosion occurs when a node sends its data to all of its neighbors which can lead to two copies arriving at the same destination wasting valuable network resources. By negotiating before sending data, SPIN ensures that only useful data is forwarded. To negotiate, nodes must be able to fully describe their data using what is known as meta-data. The format for meta-data is not specified which eliminates limitations on what can or must be contained in the meta-data.

2.7.1.2 Resource Adaptation

Each SPIN node queries a resource manager prior to transmitting. The resource manager tracks node energy consumption and calculates the amount of energy available. The resource manger can also calculate the energy cost of performing computations and sending and receiving data. With this information a node can make an informed decision about using its resources. When a node approaches its low-energy threshold it will cutback on certain activities of the SPIN protocol, for example the node may no longer forward third party data, saving its resources for its own data. If energy is abundant the node fully participates in the protocol. As energy resources are consumed to a particular level the node will only participate when it is certain that it can complete all stages of the protocol.

2.7.1.3 SPIN Messages

SPIN is a three phase protocol; each node uses three types of messages:

- ADV is a new data advertisement. When a node has data to share it advertises this fact in an ADV message containing meta-data.
- REQ is a request for data sent when a node wishes to receive some data.
- DATA is the data message which contains the actual data with a meta-data header.

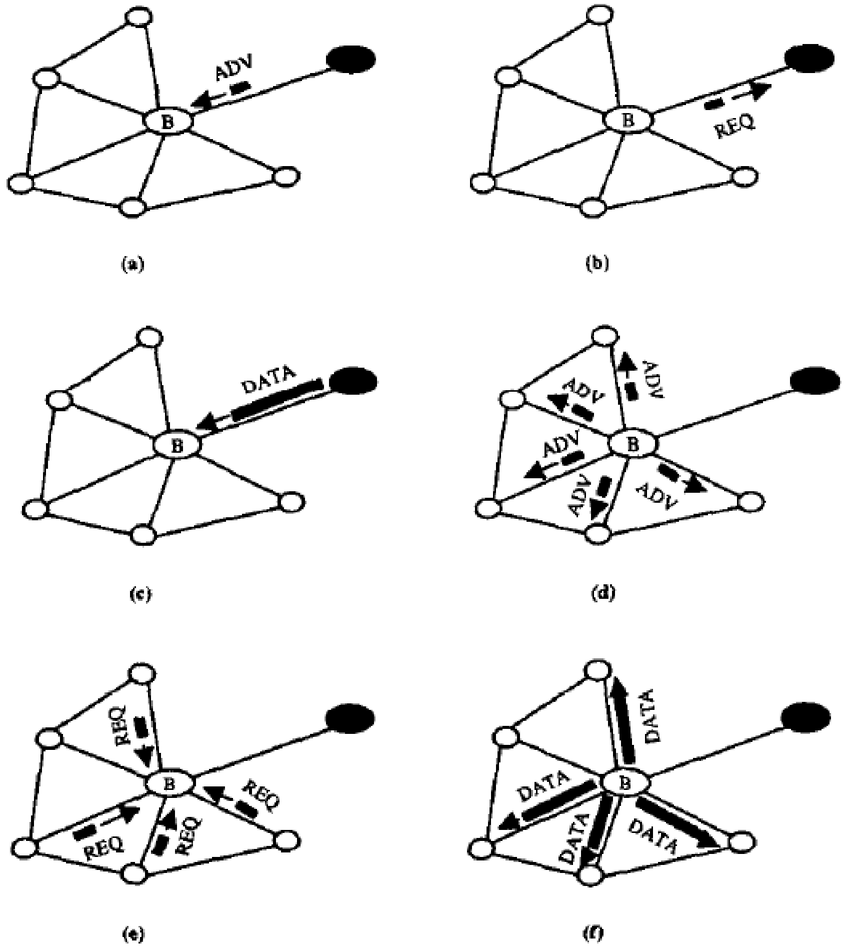


Figure 7: The SPIN Protocol [HKB99]

Figure 7 illustrates the operation of the SPIN protocol. When node A obtains new data it sends an ADV message to its neighbors (Figure 7(a)). Upon receiving an ADV message, node B checks to see if it has already received or requested the advertised data. If it has not received the data, it sends a REQ message back to node A for the data (Figure 7(b)). Node A transmits the data to node B (Figure 7(c)). Once node B receives this new data it repeats this process transmitting an ADV message to its neighbors (Figure 7(d)), the neighbors respond with REQ messages (Figure 7(e)) and node B transmits the data to its neighbors (Figure 7(f)).

2.7.1.4 SPIN Protocols

The two main SPIN protocols are SPIN-1 and SPIN-2. Both incorporate negotiation before transmitting data. SPIN-1 is the three stage protocol discussed above and the SPIN-2 protocol is an extension of SPIN-1. SPIN-2 has a threshold-based resource awareness mechanism incorporated in addition to negotiation. This resource awareness allows the node to fully participate in the protocol when energy is plentiful using the three stages of SPIN-1. When the energy of a node reaches the low threshold it reduces its participation in the protocol and participates only when it believes it can complete all stages of the protocol without going below the threshold. Other protocols of the SPIN family are [KHB02]:

- SPIN-PP designed for point-to-point communication
- SPIN-EC adds an energy heuristic to SPIN-PP
- SPIN-BC designed for broadcast media
- SPIN-RL reliable version of SPIN BC, used for lossy channels.

The SPIN protocols are well suited for environments where the sensors are mobile because forwarding decisions are based on local neighborhood information.

2.7.2 Directed Diffusion

Directed diffusion [IGE00] is a data aggregation paradigm for WSNs. Directed diffusion is data centric with all data generated by a node named by attribute-value pairs. A base-station requests data by broadcasting *interests* for named data. The main idea of the data aggregation paradigm is to combine data coming from different nodes enroute to the base-station [ALK04]. Data that matches this *interest* is routed toward the base-station with the creation of gradients. A gradient specifies an attribute value (data rate) and a direction. The attribute value can be defined using different semantics as determined by the designer and may be application specific.

2.7.2.1 Directed Diffusion Messages

Each sensor measures events and creates gradients of information in their neighborhoods. A base-station broadcasts an *interest* message which describes a task to be performed by the network. Each node maintains an *interest* cache, and each item in this cache represents a distinct *interest*. An *interest* cache entry has the following fields:

- Timestamp – indicates the timestamp of the last received matching interest
- Gradient – no more than one per neighbor, indicates the data rate (derived from the interval indicated in the *interest* message) and the direction (neighbor ID).
- Duration – derived from the timestamp and indicates the lifetime of the interest

Interests are diffused through the network by each node to its neighbor. As this *interest* message propagates throughout the network gradients are established to 'draw' any data that satisfies the query of the *interest* message toward the requesting base-station. When a node receives an *interest*, it checks its *interest* cache to see if a match exists. If no match exists, an *interest* entry is created in the cache. This entry has a single gradient toward the neighboring node from which it was received with the specified data rate. It must be possible to distinguish individual neighbors using some unique neighbor ID. If an *interest* entry already exists in the cache but no gradient exists for the sender, a gradient is added with the specified value and the timestamp and duration of the entry are updated. If an interest entry exists and has a gradient, just the timestamp and duration are updated. Once a node has received an *interest*, it may re-send the *interest* to its neighbors. This *interest* appears to have originated at this node, when in fact it could have originated at some distant base-station.

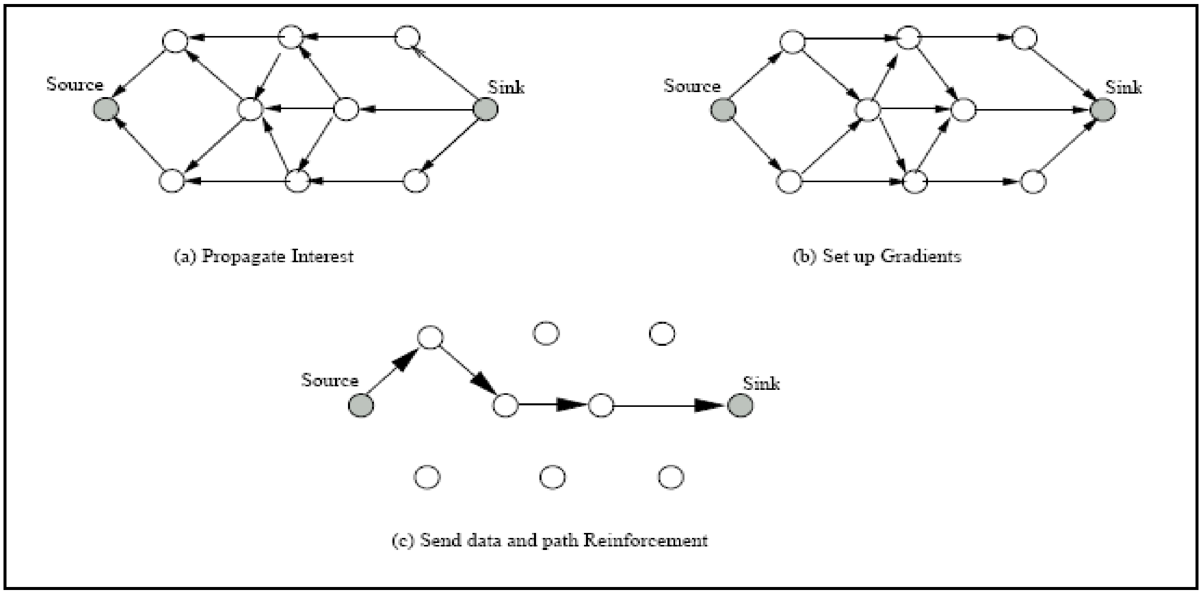


Figure 8: Directed Diffusion [IGE00]

In Figure 8(a) a sink sends an *interest* message. Figure 8(b) shows the gradients being setup, in a multi-path fashion back to the destination. Through the process of reinforcement, the best paths are chosen, based on the speed of the link. When the sink originated its interest message, it included an interval field set to a low data rate (such as) one event per second. As data begins to arrive from multiple sources at this low data rate, the sink will re-send the interest with a higher data rate to the neighbor from which it first received data. This is the fastest route. This node will do the same to its neighbor and so on until the source is reached. The source will transmit the data using the path with a higher data rate. Figure 8(c) shows the data being disseminated along the reinforced path. Data is aggregated along the way to reduce communication costs.

Direct diffusion is unsuitable for one-time queries since it is not worth the effort of setting up gradients for queries which will use a path only once. It is also not well suited for applications that require continuous data delivery because directed diffusion is an on-demand protocol.

2.7.3 Low Energy Adaptive Clustering Hierarchy (LEACH)

LEACH [HCB00] is a hierarchical clustering algorithm. LEACH randomly selects a few sensor nodes as clusterheads, and the role of clusterhead is circulated throughout the network to evenly distribute the energy load of the network [ALK04]. The clusterheads compress data received from nodes within the cluster and send an aggregated packet to the base station. This reduces the amount of data that must be transmitted. LEACH operates in two phases; setup and steady state. The steady state phase is longer than the set-up phase to minimize overhead.

2.7.3.1 Cluster Set-Up Phase

To establish clusters, each node decides whether or not to become a clusterhead based on an a priori determination of the percentage of clusterheads required for the network. The election of a clusterhead occurs as follows. A node chooses a random number between 0 and 1. If this random number is less than a threshold value $T(n)$, the node becomes a clusterhead for the current round. The threshold value $T(n)$ is:

$$T(n) = \frac{p}{1 - p(r \bmod (\frac{1}{p}))} \quad n \in G \tag{2.1}$$

where *p* is the desired percentage of clusterheads required for the network, *r* is the current round, and *G* is the set of nodes that have not been clusterheads in the last 1/*p* rounds.

Once a node is elected as clusterhead it sends an advertisement message to the rest of the nodes in the network indicating it is the new clusterhead. All non-clusterhead nodes decide which cluster they belong to after receiving this advertisement based on the signal strength of the advertisement. Once all the nodes have responded to a clusterhead requesting inclusion in the cluster, the clusterhead creates a Time Division Multiple Access (TDMA) schedule based on the number of nodes in the cluster and broadcasts this schedule to all nodes within the cluster.

2.7.3.2 Steady State Phase

After the cluster has been established, nodes forward data to the clusterhead according to the TDMA schedule. The clusterhead aggregates the data received from all cluster nodes and forwards the aggregated data to the base station. After a certain time, determined a priori, the next round of clusterhead election begins. Each cluster communicates using a different Code Division Multiple Access (CDMA) code to reduce interference from neighboring cluster nodes.

The LEACH protocol assumes all nodes can transmit with enough power to reach the base station and that each node can support two different MAC protocols: TDMA and CDMA. Due to the randomness of the clusterhead elections the clusterhead distribution could be concentrated in one part of the network leaving a large portion of the network without a path to the base station.

2.8 Summary

This chapter describes routing protocols, wireless sensor networks and RFID tags. Several different MANET routing protocols are discussed including table-driven, on-demand and hybrid protocols. A description of several wireless sensor network routing protocols is also provided.

III. Methodology

This chapter describes the methodology to evaluate the effect of augmenting nodes with RFID tags and using the AODV routing protocol. Section 3.1 discusses the problem definition, as well as the goals and hypothesis. Section 3.2 introduces the system boundaries. Section 3.3 discusses the system services. Section 3.4 presents the system workload. Section 3.5 introduces the performance metrics related to the system. Section 3.6 discusses the system and workload parameters. Section 3.7 introduces the factors of the system. Section 3.8 discusses the evaluation technique used for this research. Section 3.9 presents the experimental design. Section 3.10 discusses how the results of this research will be analyzed and interpreted. Section 3.11 summarizes this chapter.

3.1 Problem Definition

The main problem with WSNs is the limited resources that each node has. If the node resources are not used in an efficient manner, the operation of the network can terminate prematurely. Routing data in an efficient manner is one way to extend the life of the network. Several routing techniques are available, but the main types are table-driven, source-initiated, and hybrid. Table-driven protocols try to produce consistent, up-to-date routing information and so maintain a global view of the network. Source-initiated protocols create routes as needed and do not maintain a table with routes to all destinations. When a source needs to send a message, it establishes a route to the destination then sends the message. Hybrid protocols combine table-driven with on-demand protocols using a table for a portion of the network and a demand approach in others. Hybrid protocols minimize the cost of route discovery by maintaining a table of routes to nearby nodes and establishing routes on-demand to distant nodes. The AODV routing protocol, which is the target of this research, is an on-demand protocol

3.1.1 Goals and Hypothesis

Due to the limited energy resources available to a sensor node, a WSN has a limited operational lifetime. To increase the lifetime of the WSN, the number of transmissions must be reduced since transmissions are the most energy consuming operation a node performs. The goal of this research is to increase the lifetime of a WSN using the RFID tag Augmented AODV Routing System (RAARS). It is expected that RFID tags will reduce the AODV RREQ packet transmissions since nodes are able to get next hop information from the RFID tags and will not generate a RREQ packet. Furthermore, such packets will not be received and retransmitted by other nodes saving more energy. The time to determine a path from the RFID tags is expected to result in increased End-To-End delay of the network but the total energy expended will likely decrease using the RAARS, as this system will determine routes using RFID tags rather than broadcasting and propagating an AODV route request message.

3.1.2 Approach

To prove this hypothesis the OPNET discrete event simulation tool will be used to account for the energy cost of transmitting and receiving plus the cost of RFID tag transmissions and receptions. These results are compared to the standard AODV routing protocol transmitting and receiving costs.

3.2 System boundaries

The system under test (SUT) shown in Figure 9 is made up of sensor nodes, sink nodes, the mobility of the sinks, as well as the sensor node distribution, the MAC layer protocol, and the RFID tags (passive or active). The component under test (CUT) is the augmented AODV Routing Protocol. It is assumed that only sink nodes are mobile and all sensor nodes are randomly deployed and stationary. All nodes and sinks share the same transmission medium.

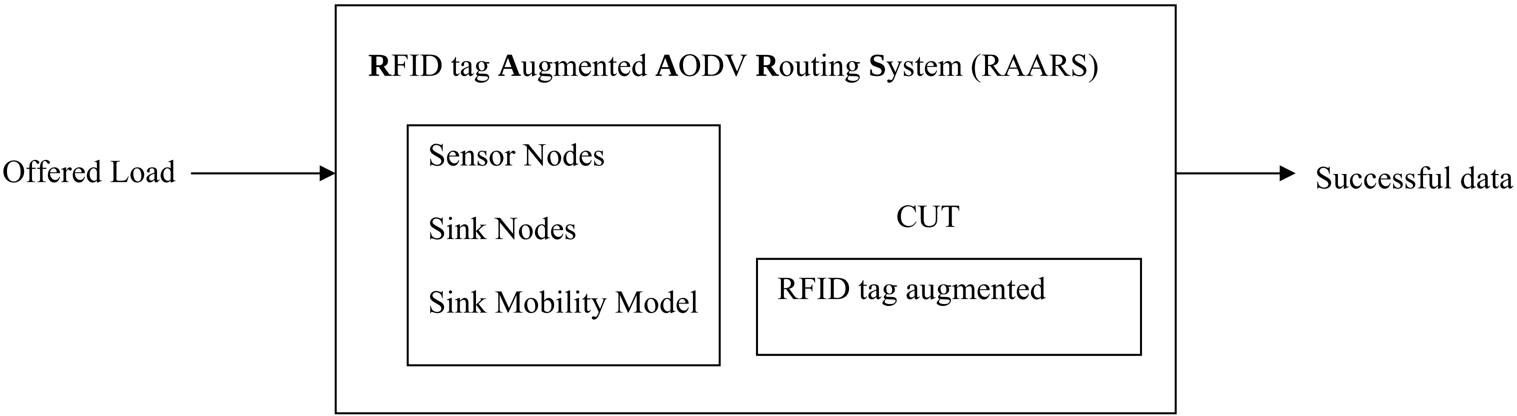


Figure 9: System Under Test

3.3 System Services

The SUT provides a data transfer service from the nodes within the network to the mobile sinks as well as routing information packets between the nodes and the sinks. The routing information packets provide nodes with a path to the sink. This path is used to forward data from the node to the sink. A success occurs when the sink receives the data from the node. Failure occurs when the sink does not receive the data from the node.

3.4 Workload

The workload for the SUT consists of both routing and sensor data. Sensor data is the information collected by each sensor in the network and forwarded to the sink at predetermined intervals. Routing data is generated by nodes to establish a path to the destination. Sensor data is forwarded along this path through the network to the sink in a multi-hop fashion. The workload is 4 packets per second, exponentially distributed, with a packet size of 64 bytes. The AODV route request packets are 24 bytes while route reply and route error packets are 20 bytes long and are generated as needed by the routing protocol. Each node in the network is assumed to be similar to the Crossbow Mica2 which has an Atmel ATmega 128L microcontroller with 4 KB of RAM, 128 KB of flash, and a CC1000 radio. The radio operates at 433 MHz and transmits at a rate of 38.4 Kbps with Manchester encoding.

3.5 Performance Metrics

To measure the network performance the following metrics are used:

a. **Throughput** – The ratio of successfully transmitted bits per unit time for the entire network. This includes all routing data and user data.

b. **End to End Delay** – The time elapsed between the creation of a packet at its source and its destruction at the destination, measured in seconds.

c. **Routing Traffic Sent –** Amount of routing traffic sent in bits/sec for the entire network. This measures the effect of RFID tags on routing overhead.

d. **Power Consumed** – This metric determines the amount of energy expended during network operations. The metric is measured in milliamp hours (ma-h) and is determined by calculating the average number of bits transmitted and received per node then multiplying by the cost of the communication activity. The energy required for processing is assumed to be constant and is not used in this calculation.

3.6 Parameters

3.6.1 System

- **Number of Sink Nodes –** The number of sink nodes, also known as destinations, in the network affects the performance of the routing protocol and the total successfully transmitted packets. The number of sink nodes will also affect the connectivity of the network.
- **Number of Sensor Nodes** – The number of sensor nodes affects the connectivity of the network as well as the amount of data sent throughout the network since sensor nodes are sources. Sensor nodes will randomly select, with a uniform distribution, a destination from a list of available sinks and reselect a destination every ten seconds.
- **Simulation Area** – The area the WSN is deployed in affects the density of the network and also determines the number of nodes needed for coverage of the area. The density of the network will have a direct effect on the system performance. A sparse network may not be a connected network and an overly dense network may overload the network. The simulation area for this research is 300 meters by 300 meters.

- **Node Speed –** Since sink nodes are mobile, the rate of their respective movement affects the performance of the system because it causes changes in network topology. This forces the AODV routing protocol to re-establish paths to the destinations. All sink nodes move at different pre-determined rates. All sensor nodes are stationary once deployed. Deployment of sensor nodes is random with a uniform distribution.
- **Node Configuration –** The type of sensor node used has a direct affect on system performance. Nodes may have different transmission frequencies, memory allocation and processing power. The standard OPNET MANET model is used for node configurations in this research.
- **Antenna Type** – The antenna used has a dramatic affect on the system performance. Directional antennas allow communication in only one direction and can result in a partitioned network. Omni-directional antennas transmit in all directions and are assumed for this research.
- **Transmission Range** – The transmission range of sensor nodes is limited by the radio. These radios determine which nodes are reachable. Based on [Cro05] the transmission range for the nodes is assumed to be 150 meters.

- **Routing Protocol –** The routing protocol also affects the performance of the network. Table-driven routing requires the entire network routing table be periodically broadcast to ensure all nodes have up to date information. This induces overhead and is an inefficient use of resources. On-demand routing protocols such as AODV discover routes as needed, thus reducing the overhead and saving resources. The routing protocol used for this research is AODV.
- **RFID Tag -** The type of tag used determines the communication range of the tag as well as the amount of information that can be stored. Passive tags have much smaller transmission ranges and less memory.

3.6.2 Workload

- **Sensed Events –** The number of sensed events affects the amount of data sent through the network depending on the node configuration. Some nodes are configured for continuous periodic transmission while others transmit upon sensing an event. As the number of sensed events increases, so does the amount of data. Nodes are assumed to transmit in the continuous mode at predetermined intervals.
- **Number of Sensor Nodes** – The number of sensor nodes determines the amount of traffic generated by the network. Since each sensor

node generates a constant amount of traffic, the more nodes present in the network, the higher the amount of traffic.

- **Arrival Rate** – The arrival rate of packets could easily overload the network and cause unacceptable delays in the network. An exponentially distributed arrival rate of 4 packets per second is assumed, similar to [HJB04].
- **Packet Size** – The size of the packet directly affects network performance, since larger packets use more bandwidth and resources. Data packets are fixed at 64 bytes. This is a large data packet and will stress the network to determine performance under this load. Routing packet sizes vary depending on the type of packet generated. Route Request packets are 24 bytes while route reply and route error packets are 20 bytes long.

3.7 Factors

a. Number of Sensor Nodes – The number of sensor nodes contained in a WSN can vary between 2 and several hundred nodes. The levels chosen are intended to capture the effects of node density on the network performance.

- **Sparse** – 10 sensor nodes deployed in the simulation area
- **Dense** – 200 sensor nodes deployed in the simulation area

b. Number of Sinks – The number of sinks can affect delay with an increase in sinks the data is forwarded to more destinations rather than just two, which may create a bottleneck in the network. The increase in possible destinations should remove bottlenecks in the network, as the data will be headed in multiple directions instead of just two.

- **Few** – 2 mobile sinks available for nodes to forward data. Sinks are positioned on opposite sides of the simulation area.
- **Several** – 12 mobile sinks available for nodes to forward data. Provides uniform coverage around the simulation area.

c. **RFID Tag –** RFID tags provide source nodes with information about neighbors that have paths to a requested destination. An energy burst of 6ms is assumed to initiate the tags. This value is assumed based on the size of the passive tag memory capacity of 128 bits. It is assumed that the time required to energize the RFID tag will be less than the time to transmit the tags' memory.

- **Passive Tags** – Have a transmission range of 3 meters and 128 bits of memory. The data rate is assumed to be 5333 bps [Int04].
- **Active Tags** – Have a transmission range of 50 meters and 256K bits of memory. The data rate is assumed to be 5333 bps [Int04].
- **No Tags** – No RFID tags used, standard AODV routing protocol implementation.

3.8 Evaluation Technique

The evaluation technique is simulation using OPNET 10.5. The motivating factor for choosing this technique is the maturity of the system under test. WSNs are a new technology and there are few resources available for direct measurement. The OPNET Discrete Event Simulation package contains an AODV module. This module is modified to provide the source node with the capability to request information from the RFID tags of neighboring nodes and determine which, if any, of its neighbors have a route to the destination prior to sending a standard AODV route request packet, this modification and others are described in more detail in Appendix A. This modification alleviates the need for transmission from neighboring nodes allowing the source node to determine which of its neighbors has a route to the destination. Upon finding a neighbor with a route to the destination, the routing table of the source node is updated with next hop information for that destination and a data packet sent. If the information returned does not contain a route to the destination, a route request is generated according to the AODV protocol.

3.9 Experimental Design

The design of this experiment is a full factorial design. With two factors having two levels and one factor having three, there are 2*2*3 = 12 experiments. It is expected that variance between experiments will be slight so 10 replications of each experiment will provide enough information for statistical analysis. The total number of experiments required, then, is 120. The random seed used for random number generation is changed at the beginning of each simulation. At the start of each simulation the sensor nodes are distributed according to a random uniform distribution within a user defined region prior to any data being generated. Once the sensor nodes are in place, they remain static for the duration of the simulation. Sink nodes are deployed within regions defined along the border of the sensor node simulation area as shown in Figure 10 below. Figure 10 shows the 200 node network with 12 sinks deployed around the simulation area. The blue regions indicate the North, South, East, and West areas of mobility for the sink nodes. Sink node movement is limited to the region it is assigned to.

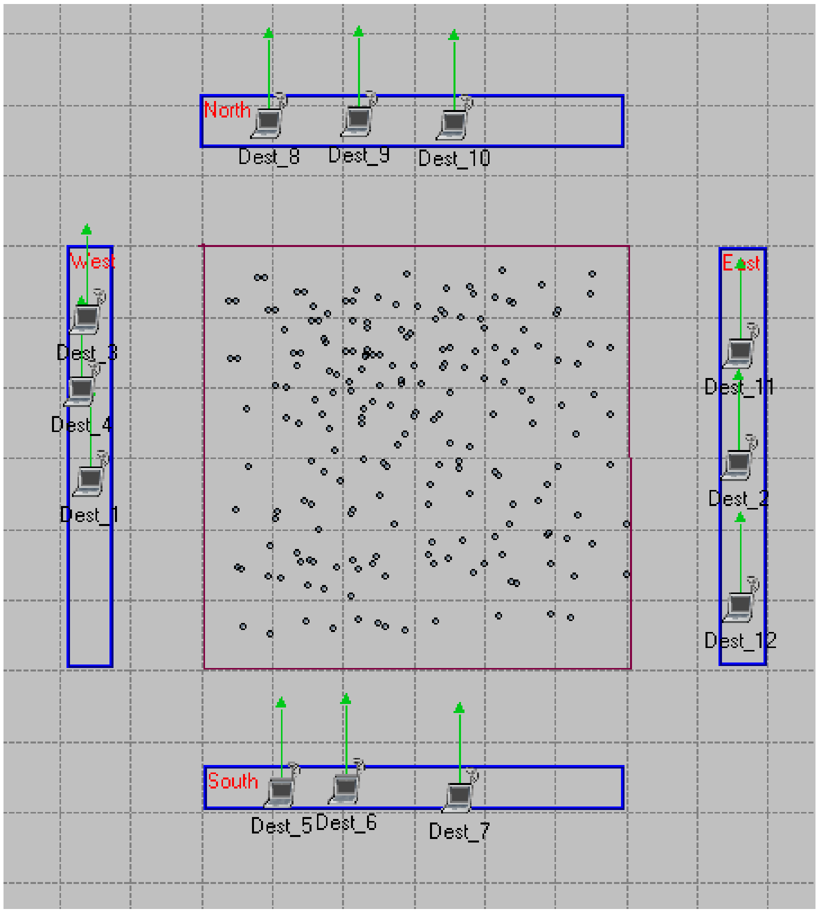


Figure 10: 200 Node Network with 12 Sinks

The sink nodes are active at the beginning of the simulation and ready to receive data. Each sink node moves within the specified domain with pause/move intervals defined by the user using the OPNET configuration editor. The assumptions are that the relationship between the response and the factors is linear and errors are statistically independent, normally distributed and have a constant standard deviation. The error assumptions for independence and constant standard deviation are verified with a scatter plot of the error and the predicted response obtained from the regression analysis. The normality assumption is verified using a normal quantile – error quantile plot.

3.10 Analyze and Interpret results

The data collected from simulation is compared to two alternatives, AODV and AODV with the use of RFID tags. Confidence intervals are used for before and after comparisons using a 95% confidence interval (CI). To determine the statistical difference between the alternatives, the Tukey simultaneous method of comparisons is used. If the 95% CI includes zero, there is no statistical difference between the alternatives. The analysis of variance (ANOVA) methods are used to determine the variation due to error and the variation due to the factors.

3.11 Summary

Wireless sensor networks are a new technology with a vast array of applications. However, WSNs are limited by the resources available to each node in the network. To save resources a more efficient method for routing the data through the network must be developed. The goal of this research is to determine the effect of RFID tags on the execution of the AODV routing protocol within a WSN. This chapter first discussed the system services then the workload and performance metrics are discussed in detail. From the list of performance metrics the factors to be changed are selected. The evaluation technique and experimental design are presented in the following two sections. Finally, a discussion on the use of the data collected to interpret the results of the experiment.

IV. Analysis and Results

This chapter presents the results of this research and an analysis of those results. Section 4.1 presents the validation of the AODV OPNET model and discusses the verification of modifications made to the AODV model. Section 4.2 presents the energy consumed results and analysis. Section 4.3 discusses the total network throughput results with analysis. Section 4.4 introduces the AODV routing traffic sent results and presents an analysis of the results. Section 4.5 discusses the ETE delay results and provides an analysis of the results. Section 4.6 presents the results for the user data throughput with analysis. Section 4.7 discuss the results of this research and provides an explanation for the results. Section 4.8 presents a summary of this chapter.

4.1 Verification of OPNET AODV Implementation

The verification of the OPNET implementation of the AODV routing protocol [Ric05] shows that the OPNET implementation follows a similar trend to the results in the original AODV protocol [DPR00]. Figure 11 shows that there are some differences but these can be attributed to different implementations of the protocol.

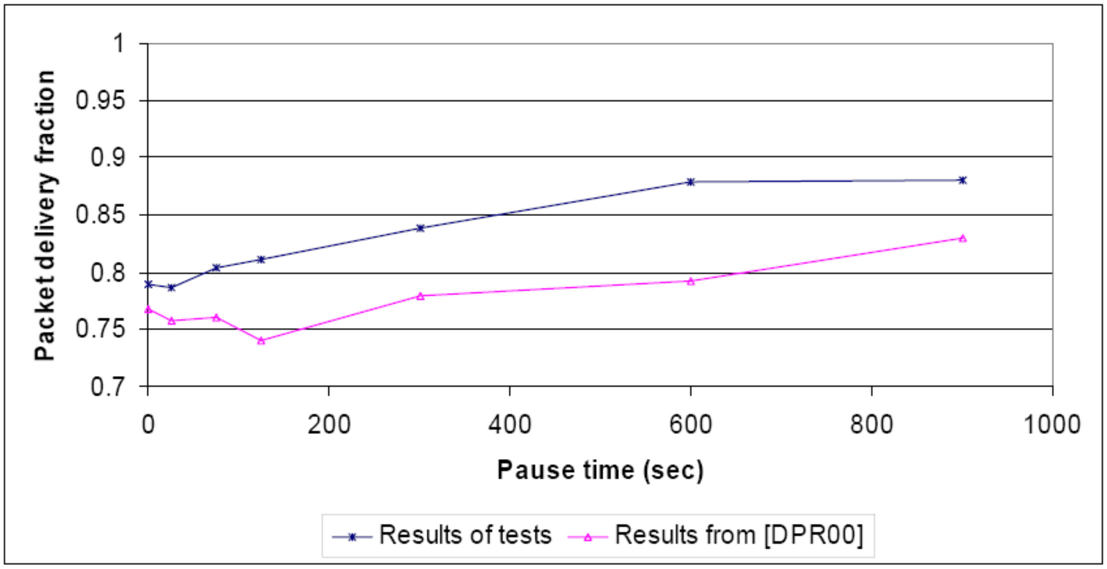


Figure 11: Verification of OPNET AODV Implementation [Ric05]

The OPNET AODV models are implemented according to RFC 3651 [Opn04].

The modifications made to the AODV model are detailed in Appendix A. All modifications made to the AODV model and other OPNET models are verified using the OPNET debug program with the use of "printf" statements. These statements are used to ensure that the changes made produced the desired affect. For example, when no RFID responses are received or no valid route updates are produced the system should behave similar to the standard AODV model. Figure 12 shows the 200 network throughput interval plot. From this figure it can be seen that the passive tag scenarios are statistically not different from the no tag scenarios (standard AODV model), verified with the Tukey method. This verifies that when no RFID responses are received or no route table updates made due to the use of the RFID tags the system behaves similar to the standard AODV model.

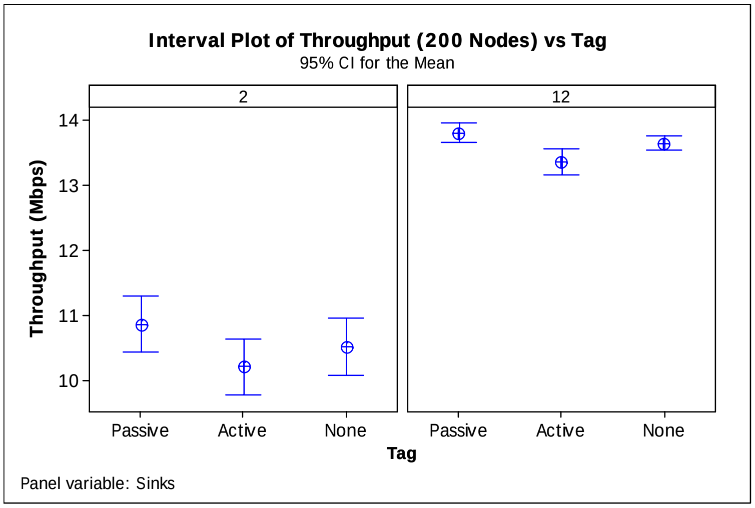


Figure 12: Verification of AODV Modifications

4.2 Energy Consumption Analysis

The mean energy consumed per node is determined by calculating the total time spent transmitting and receiving. This time is then multiplied by the current draw for the particular operation. The sum of energy consumed per operation results in mean total node energy consumed.

$$E_{tx} = \left({}^{bits}\!/_{data\_rate(bps)}\right) * \left({}^{1hour}\!/_{3600\sec}\right) * 27ma \tag{4.1}$$

$$E_{rx} = \left({}^{bits}\!/_{data\_rate(bps)}\right) * \left({}^{1hour}\!/_{3600\sec}\right) * 10ma \tag{4.2}$$

$$E_{total} = E_{tx} + E_{rx} \tag{4.3}$$

Figure 13 is an interval plot with 95% CI of this data. Figure 13 is separated into two panels (10 and 200). Each panel represents the number of nodes used in the simulation. It shows that the total energy consumed by an average node in the network is greater when using RFID tags in both the 10 node (sparse) and 200 node (dense) networks.

RFID tags consume more energy since a node must expend extra energy to activate an RFID tag and to receive the data returning from the activated RFID tags.

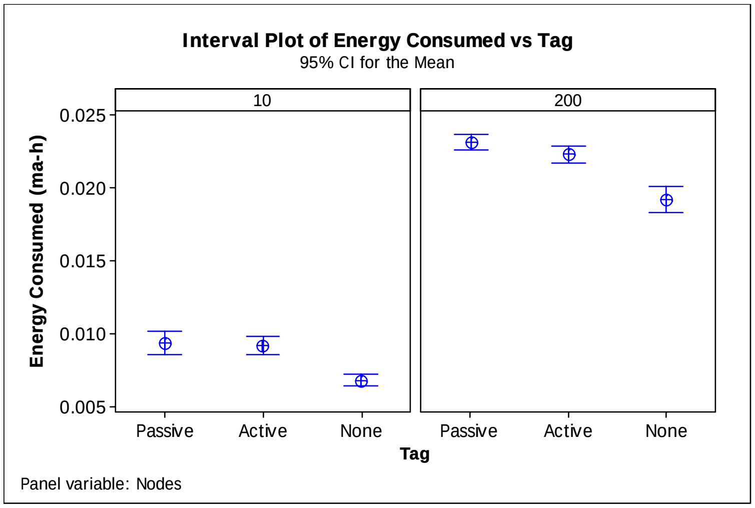


Figure 13: Energy Consumed per Node

Since the difference in energy consumed between the 10 and 200 node networks is obvious, the energy consumed is analyzed separately for each network. The 10 node network energy consumed data did not satisfy the assumptions for an ANOVA. Therefore, the interval plot of Figure 14 is used to analyze the results for the 10 node network; the two panels (2 and 12) represent the number of sinks available.

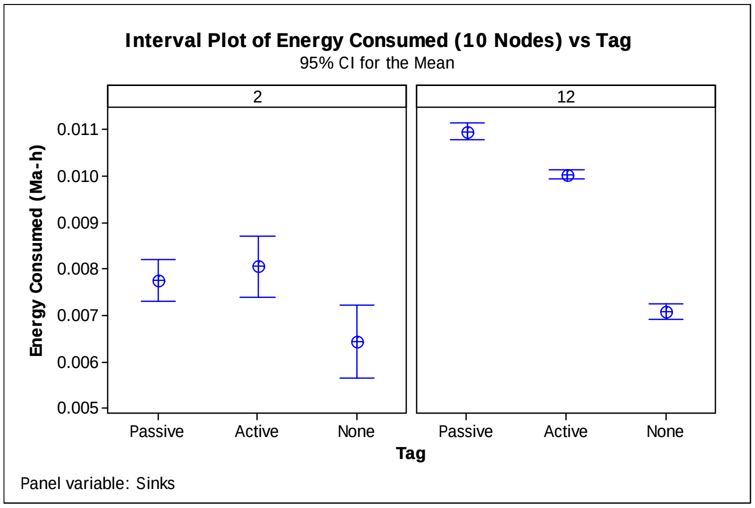


Figure 14: Energy Consumed per Node (10 Node Network)

From Figure 14 it appears that using RFID tags increases the energy consumed per node regardless of the number of sinks present. To determine the statistical difference between the tags for the 2 sink and 12 sink scenarios, the Tukey simultaneous method of comparison is used. This method is shown in Table 1 below. It can be seen using the adjusted p-value from Table 1 that for the 2 sink scenario the passive and active tags are statistically not different from each other at the 95% confidence level and that they both consume more energy than the no tag alternative. The results of the Tukey method for the 12 sink scenario support what is shown in Figure 14.

Table 1: 10-Node, 2-Sink Comparison of Alternatives

Tag = Passive				
Tag	Difference of Means	SE of Difference	T-Value	Adjusted P-Value
Active	0.000293	0.000405	0.724	0.7513
None	-0.001319	0.000405	-3.258	0.0082
Tag = Active				
Tag	Difference of Means	SE of Difference	T-Value	Adjusted P-Value
None	-0.001612	0.000405	-3.982	0.0013

Figure 15 shows that the energy consumed per node in the 200 node network is similar to the 10 node network in that the use of RFID tags increases the energy consumed.

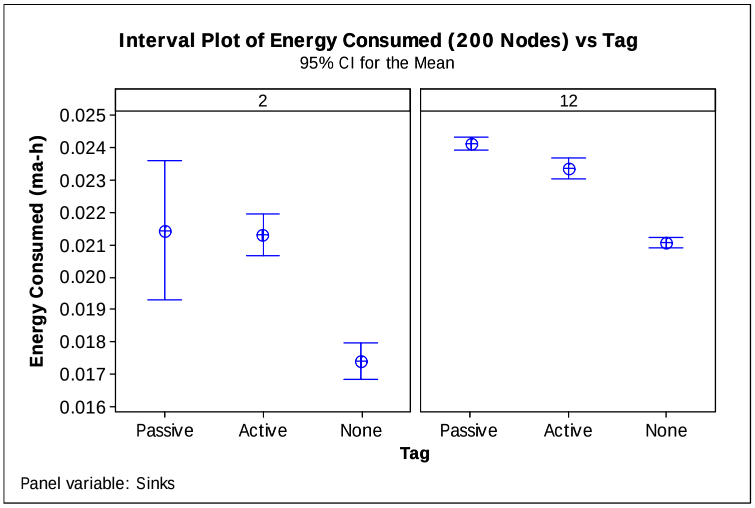


Figure 15: Energy Consumed per Node (200 Node Network)

The Tukey method of comparison verifies the use of RFID tags does indeed increase energy consumption. Furthermore, the energy consumed when using the passive tags is greater than that of the active tags for the 12 sink scenario. An ANOVA for the 200 node network is shown in Table 2. The majority of variation is due to the factors of the experiment as opposed to error. In particular, RFID tags account for more than 57% of the variation with the number of sinks accounting for more than 31%.

Table 2: 200 Node Energy Consumed ANOVA

Source	DF	Seq SS	% Variation	Adj MS	F Ratio	Prob > F
Tag	2	1.750E-04	57.70	8.750E-05	199.12	0.000
Sinks	1	9.460E-05	31.19	9.460E-05	215.24	0.000
Tag*Sinks	2	9.900E-06	3.26	5.000E-06	11.29	0.000
Error	54	2.370E-05	7.81	4.000E-07		
Total	59	3.033E-04				

R-Sq = 92.17% R-Sq(adj) = 91.45%

Figure 16 shows the visual test used to verify the ANOVA assumptions. The normality of the residuals is presented in Figure 16(a) and Figure 16(c). While the independence of the residuals can be seen in Figure 16(b) this figure also shows that the standard deviation is constant. To verify that there are no systematic, errors Figure 16(d) is used to show the residuals in their observed order. If any trends appear it may indicate a problem with the simulation setup or metric measurement/calculation. Figure 16(d) seems to show a convergence of the data. This is due to the fact that the first 30 samples are associated with the scenarios in which only 2 sinks are present. The last half of the graph are the residuals related to the 12 sink scenario. When separated based on the sinks of each scenario it can be seen that there is no systematic error. The graphs of the visual tests for ANOVA assumptions of the other performance metrics are not included in this chapter but can be found in Appendix B.

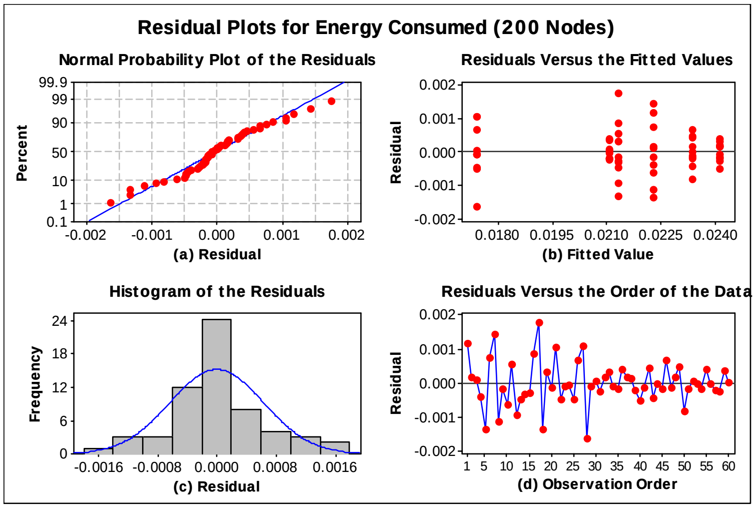


Figure 16: Visual Tests for 200 Node Energy Consumed ANOVA Assumptions

4.3 Throughput Results and Analysis

The total network throughput was measured and since the network sizes are significantly different (10 nodes versus 200 nodes), the throughput analysis is separated accordingly. Figure 17 shows the 95% CI throughput plot for the 10 node network.

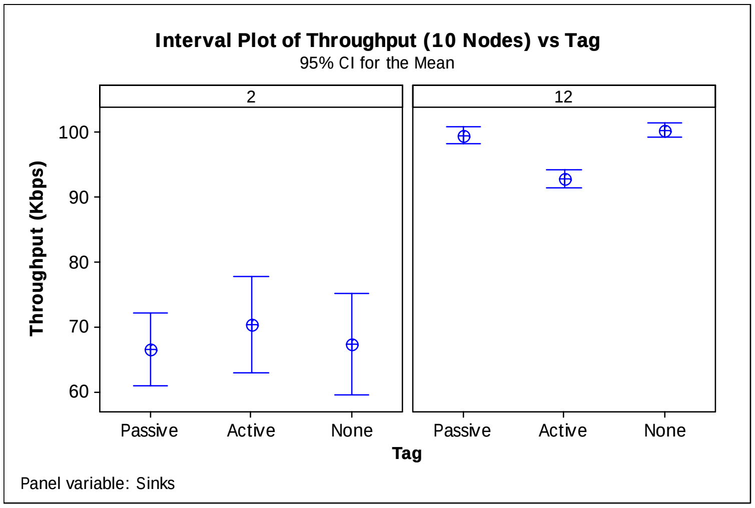


Figure 17: Throughput for 10 Node Network

For the 2 sink scenario there is no statistical difference in the throughput; however in the 12 sink scenario, active tags have less throughput than the other scenarios. The Tukey method of comparison verified that for the 2 sink scenario the throughput is not statistically different between any of the three alternatives. In the 12 sink scenario the passive tag and no tag scenarios are not statistically different but the active tag is statistically different from both the passive tag and no tag scenarios. The differences in variation between the 2 sink and 12 sink scenarios may be associated with network connectivity. When only 2 sinks are available the network may not be connected at certain times during the simulation while the 12 sink scenario may have a greater chance of remaining connected when presented with mobility. The data for either scenario does not satisfy the assumptions of ANOVA; several transformations of the data failed to satisfy the ANOVA assumptions.

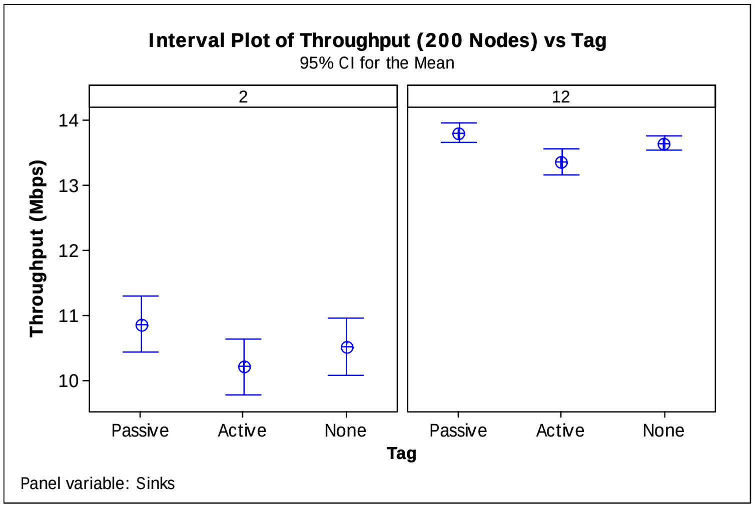


Figure 18: Throughput for 200 Node Network

The 95% CI plot for the 200 node network throughput is shown in Figure 18. As with the 10 node scenario when only 2 sinks are present, the throughput shows no statistical difference between the alternatives. The simultaneous method of comparison verifies that in the 12 sink scenario the passive tag and no tag scenarios are not statistically different but the active tag is statistically different from both the passive tag and no tag scenarios. However, the use of active RFID tags decreases the throughput by only 2%. Table 3 shows the ANOVA for the 200 node network throughput. The number of sinks account for over 90% of the variation. While the RFID tags account for less than 2% of the variation.

Table 3: 200 Node Throughput ANOVA

Source	DF	Seq SS	% Variation	Adj MS	F Ratio	Prob > F
Tag	2	3.066	1.960	1.533	7.47	0.001
Sinks	1	142.151	90.872	142.151	692.34	0.000
Tag*Sinks	2	0.127	0.081	0.063	0.31	0.736
Error	54	11.087	7.088	0.205		
Total	59	156.43				

R-Sq = 92.91% R-Sq(adj) = 92.26%

4.4 AODV Routing Traffic Sent Results and Analysis

As with the throughput, the AODV routing traffic sent for the 10 node and 200 node scenarios is discussed separately. The 95% CI AODV routing traffic sent plot for the 10 node network is shown in Figure 19; this figure shows that the AODV routing traffic is not statistically different when using RFID tags. This was verified using the Tukey method.

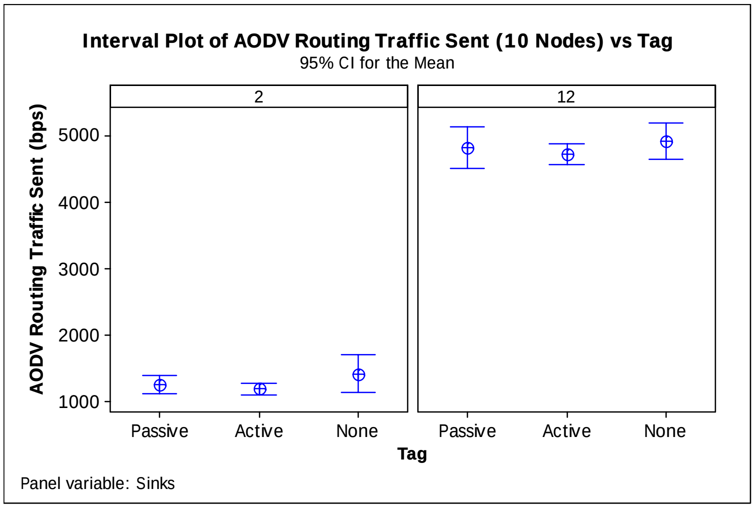


Figure 19: AODV Routing Traffic Sent for 10 Node Network

Table 4 shows the ANOVA for the 10 node scenario AODV routing traffic sent. It shows approximately 80% of the variation comes from the number of sinks available and that the RFID tags only account for about 10% of the variation. The interaction between the RFID tags and the number of sinks account for less than 10% of the variation

Table 4: 10 Node AODV Routing Traffic Sent ANOVA

Source	DF	Seq SS	% Variation	Adj MS	F Ratio	Prob > F
Tag	2	1.227E+07	10.45	6.134E+06	79.08	0.00
Sinks	1	9.338E+07	79.56	9.338E+07	1203.89	0.00
Tag*Sinks	2	7.534E+06	6.42	3.767E+06	48.57	0.00
Error	54	4.188E+06	3.57	7.756E+04		
Total	59	1.174E+08				

R-Sq = 97.25% R-Sq(adj) = 97.00%

For the 200 node network it can be seen in Figure 20 that using active RFID tags reduces the amount of AODV routing traffic sent. The Tukey method verifies that there is no statistical difference between the passive tag and no tag scenarios and using active tags does indeed reduce the amount of routing traffic sent for both the 2 sink and 12 sink scenarios

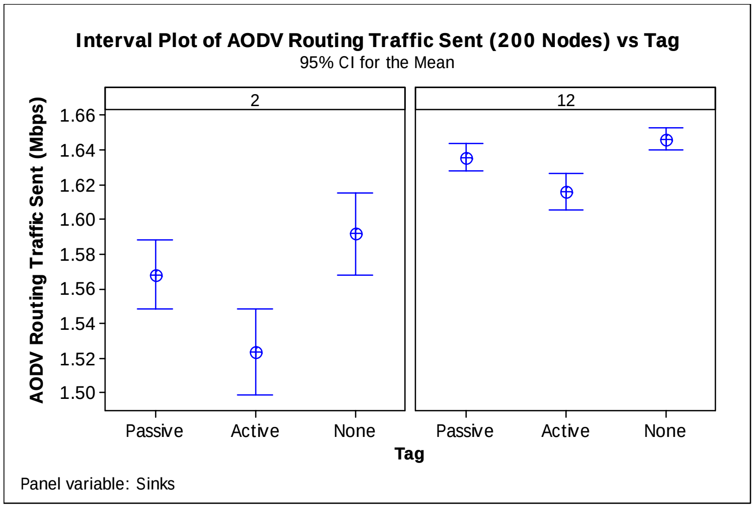


Figure 20: AODV Routing Traffic Sent for 200 Node Network

The data for the 200 node AODV routing traffic sent did not satisfy the assumption for ANOVA; therefore, the ANOVA is not used in this analysis.

4.5 End-to-End Delay Results and Analysis

Due to the differences between the 10 node and 200 node scenarios, the data for each will be presented separately. The data for ETE delay for the 10 node network did not satisfy the assumptions for ANOVA; Figure 21 shows the 95% CI plot for the ETE delay for this network.

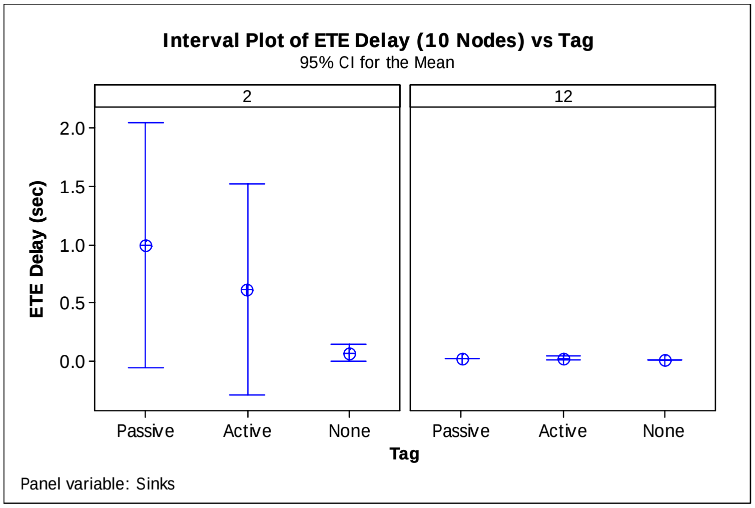


Figure 21: ETE Delay for 10 Node Network

It can be seen that the use of RFID tags has no effect on the delay other than increasing the variation. This variation, which is not as great in the 12 sink scenario, is believed to be due to the network not being connected at certain times during the simulation due to the mobility of the sink nodes. With only 2 sinks present and 10 nodes in the network, this is a sparse network and the probability of not being connected is greater than when there are 12 sinks available. A pilot study was completed to verify this assumption. In the pilot study the sensor nodes are deployed as normal, the only difference is that the sink nodes remain static throughout the simulation, there are no further changes made. The results from the pilot study shown in Figure 22, show that with a static network the ETE delay behaved as expected with the delays being much shorter with less variation. Figure 22 also shows that the use of RFID tags (passive or active) in a static network increase the ETE delay. There is no statistical difference between passive and active RFID tags, and both tags have greater ETE delay than the no tag scenario, the Tukey method verifies this.   This pilot study supports the assumption the mobile sinks around a sparse network may lead to a non-connected network which has a great effect on delay.

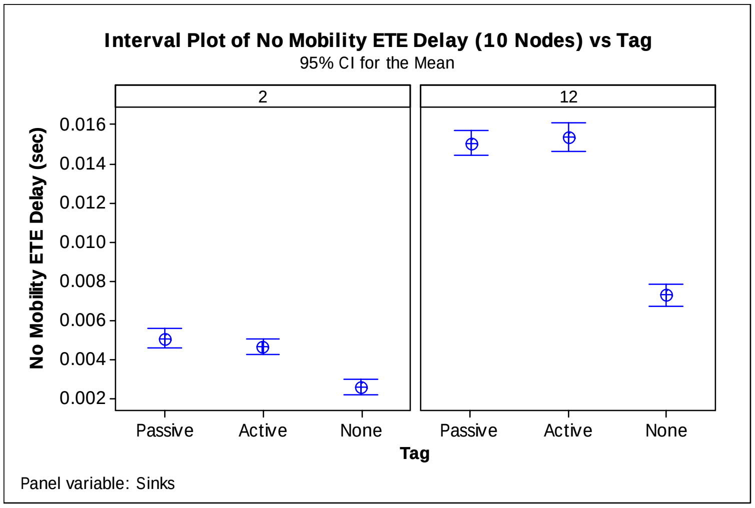


Figure 22: ETE Delay for 10 Node Network No Mobility

The 200 node ETE delay shown in Figure 23 shows that the RFID tags appear to have no effect on the delay of the network for the 2 sink scenario; this is verified with the Tukey method of comparison. The reduced delay when 12 sinks are present is believed to be related to dynamic routing. When only 2 sinks are available, they are always on opposite sides of the network. When a node reselects a destination for its data, which occurs every ten seconds, it may have to establish a path in the opposite direction. When there are 12 sinks present they are distributed around the network and the changes in routing that result are less dramatic than when 2 sinks are present. It can also be seen in Figure 23 that for the 12 sink scenario the passive tags have less ETE delay than the active tags. The Tukey method verifies this. It also shows that there is no statistical difference between the passive tag and no tag scenarios as well as the fact that there is no statistical difference between the active tag and no tag scenarios.

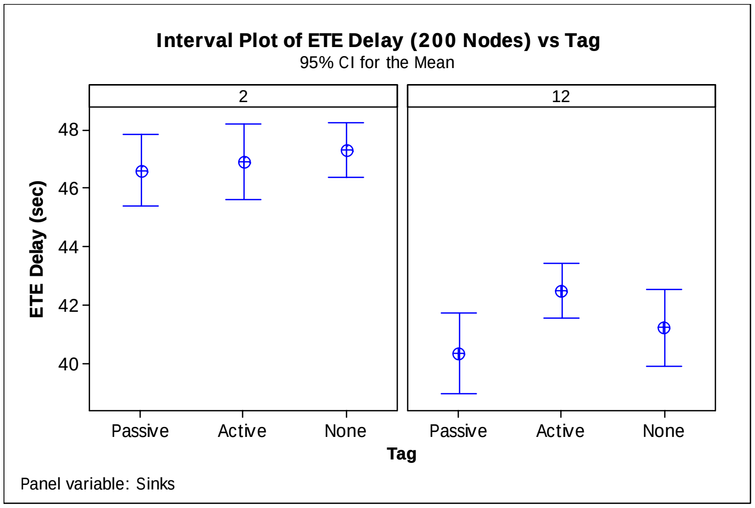


Figure 23: ETE Delay for 200 Node Network

An ANOVA could not be performed because the data does not meet the assumptions for ANOVA.

4.6 Data Received Results and Analysis

The data received metric is the actual user data that was successfully transmitted from the source and received by the destination. The results for the 10 node network data received are shown in Figure 24. From this graph it appears that the data received when only 2 sinks are present is statistically not different, yet when 12 sinks are present the use of active tags decreases the data received. This is verified using the Tukey method of comparison.

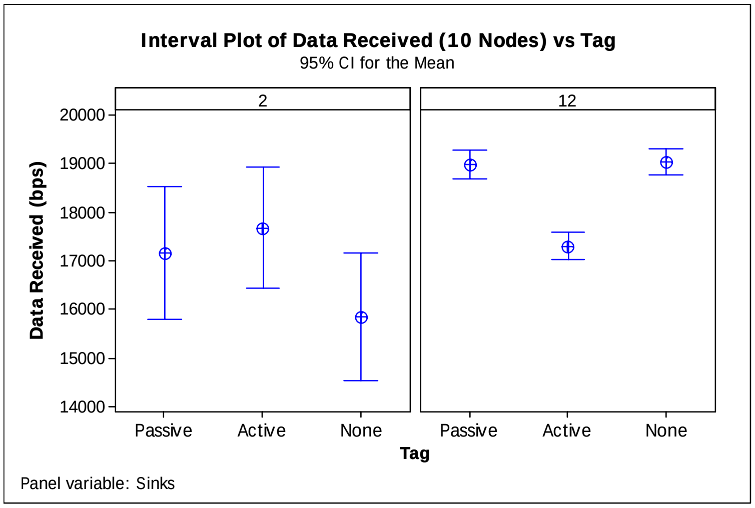


Figure 24: Data Received for 10 Node Network

The ANOVA for the 10 node data received could not be performed since the data did not satisfy the ANOVA assumptions.

The results for data received for the 200 node network are shown in Figure 25. From this graph it can be seen that the data received when using RFID tags is statistically not different from the scenario when no RFID tags are used. The only difference is that passive tags receive more user data than active tags in the 12 sink scenario.

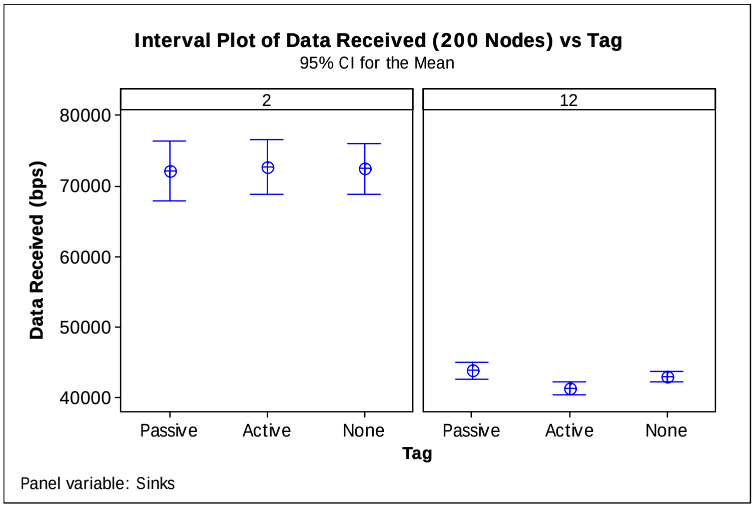


Figure 25: Data Received for 200 Node Network

The largest difference appears to occur when more sinks are present; this tends to reduce that amount of data that is received. An ANOVA for the 200 node data could not be performed either; this data also did not satisfy the ANOVA assumptions.

4.7 Discussion of Results

The results presented in this chapter do not support the hypothesis. One possible reason for this may be associated with the RFID tag MAC layer. Recall that the nodes are generating data packets at a rate of 4 packets per second, exponentially distributed. This equals roughly one packet every 250 ms. The RFID tags use a version of slotted ALOHA. When an RFID tag sends a response it delays that response by randomly selecting a slot (10 slots available) then transmits within the slot. The slot size is based on the packet size and data rate. Both parameters are fixed in this research. Active tags have a slot size of 216 ms. For the passive tags the slot size is 30 ms. For active tags this delayed transmission results in few tags being received before the next data packet is generated, when a new data packet is generated and no RFID responses have been received or have not updated the route table, the standard AODV route request is generated. For the passive tags the transmission delay is not a limiting factor; their range limits their effectiveness. A node requesting a response will only receive a response from neighbors within the 3 meter range of the passive RFID tags.

4.8 Summary

This chapter discusses the verification of the OPNET implementation of the AODV routing protocol. The results of performance metrics are presented and analyzed. When possible an ANOVA table is used to show that the factors are the main source of variation. All comparisons between factors using confidence intervals are made using the Tukey simultaneous method of comparison.

V. Conclusions and Recommendations

This chapter presents the research conclusions, significance of research, and recommendations for future research. Section 5.1 discusses the research conclusions, Section 5.2 describes the significance of the research, and Section 5.3 discusses possible avenues of future research.

5.1 Research Conclusions

The hypothesis of this research is that using RFID tags to augment the AODV routing protocol will decrease the total energy consumed in a WSN. Data presented in Chapter 4 shows this hypothesis is not correct. Rather, the use of RFID tags to augment the AODV routing protocol increased the energy consumed. The overall effects on the network performance showed that using the RFID tags in a sparse or dense network with 2 sinks had no effect on the throughput of the network. However, in the 12 sink scenarios the network throughput decreases when active tags are used. In a sparse network the use of RFID tags had no effect on the amount of AODV routing traffic sent, regardless of the number of sinks present. In a dense network, active tags reduce the amount of AODV routing traffic sent in both the 2 sink and 12 sink scenarios. This reduction in AODV routing traffic sent is minor however, around 4% for the 2 sink scenario and 2% for the 12 sink scenario. The ETE delay for a sparse network with limited sinks showed a 10 fold increase in the variation of the results due to node mobility. In the pilot study when the mobility was not present, the ETE delay increased using the RFID tags as expected. The 2 sink scenario shows a 96% increase in the ETE delay and the 12 sink scenario shows a 111% increase in the ETE delay. There is no difference in the ETE delay for the dense network, except that the 2 sink scenario incurs a

14.8% greater ETE delay than the 12 sink scenario due to dynamic routing. The amount of user data received when using the RFID tags was statistically not different from when the standard AODV protocol was used, except in a sparse network with 12 sinks present using active tags. In this scenario the user data throughput decreases by 9%. One possible explanation for these results may be the delay associated with the RFID tag responses. RFID tag responses experience substantial delay waiting to transmit due to the MAC protocol (ALOHA). It is believed that if this delay could be removed or lessened, the benefits of using RFID tags would be realized by allowing more RFID responses to be received by the source node.

5.2 Significance of Research

This research is the first WSN study to introduce RFID as a means for reducing energy consumption. While this research showed RFID tags have little effect on the network performance, RFID tags are still a promising avenue of research. There are other protocols to test this hypothesis on, as well as varying additional factors of the RFID tags and the sensor nodes.

5.3 Recommendations for Future Research

An area of future research would be to further examine the RFID tags MAC layer protocol on the performance of the AODV routing protocol. The routing protocol used for this research was one of many available for use in MANETs. Another area of future research would be to extend this study to other routing protocols. There are limitations as to what can be studied using the OPNET simulation tool, because at this time OPNET only provides models for AODV, DSR and the TORA MANET routing protocols.

Another area of research would be to expand the OPNET model library to include WSN routing protocols, such as:

- LEACH
- SPIN
- Directed Diffusion

RFID tags are a new and rapidly expanding technology. Additional research could focus on the RFID tag/reader MAC protocols.

Appendix A

In order to get the desired changes incorporated into OPNET several changes to the OPNET models had to be made. Section A.1 presents the process model created to provide for the random deployment of the sensor nodes at the beginning of the simulation. Section A.2 discusses the MANET traffic generation process model. Section A.3 discusses the RFID MAC process model created to send and receive as well as generate RFID MAC bursts and responses. Section A.4 introduces the transceiver pipeline stage closure model used to limit the range of particular transmissions. Section A.5 presents the AODV process model created to enable the use of RFID tags and discusses minor changes to other process to facilitate this change. Section A.6 discusses how these new process models are actually implemented.

A.1 Random Node Deployment Process Model

To facilitate the random deployment of sensor nodes at the beginning of the simulation the node deployment process model was created. This process model enabled the user to define a deployment region based on x and y coordinates (in meters). The user, for example, enters a range in the x direction (x_min and x_max) and a range in the y direction (y_min and y_max). A random number uniformly distributed is generated between the x_min and x_max values as well as between the y_min and y_max these two randomly generated numbers are then assigned to the nodes attributes as the x position and y position. This occurs at simulation time zero and only occurs once per simulation for each sensor node in the network.

A.2 MANET Traffic Generation Process Model

The MANET traffic generation process model is a standard OPNET process model used to generate data packets for the source nodes. During this packet generation process the packet type and size as well as destination address are set. This process model is modified to incorporate random destinations, as well as the capability to generate a burst packet. The burst packet is a 32 bit packet used to initiate the RFID tags of the network and simulates a 6 ms burst of RF energy. The AODV routing protocol sends a remote interrupt to this process when a burst packet is required. With the remote interrupt the AODV process passes a pointer to the AODV route table. This process will generate the burst packet and forward it to the RFID MAC process model. In order to incorporate random destinations an array is created in this process at the beginning of the simulation. This array is randomly populated with possible destination addresses (sink addresses). The size of the array is 200 elements. A node will reselect a destination from this array every ten seconds, the 200 array entries aloud for a 2000 second simulation. The simulations actually ran for 1000 second.

A.3 RFID MAC Process Model

The RFID MAC process model was created to facilitate the RFID tags transmissions and receptions. Since the RFID tags operate at a different frequency, this ensured there are no collisions with any routing or data packets. The functions of the RFID MAC process model include:

- Forwarding RFID burst packets received from higher layer
- Generating and forwarding an RFID response, when an RFID burst packet is received from the lower layer.

- Forwarding RFID response packets received from lower layer to the AODV routing protocol.
- Implements the slotted ALOHA protocol for the RFID tags.

The operation of this process model is as follows: when a burst packet is received from the MANET traffic generation process model it is immediately forwarded to the RFID transmitter for transmission. Since this is a burst packet there is no delay the packet is immediately broadcast with the full transmission range of the node (150m).

When a burst packet is received by the RFID MAC process model from the lower layer it is determined if the packet has incurred any collisions, if it has the packet is discarded and no statistics are updated. If the packet is received free of collisions the RFID MAC process model generates an RFID response packet. The process gets the AODV route table pointer from the MANET traffic generation process model, and uses this pointer to fill the fields of the RFID response packet with valid destination from the node AODV routing table. The number of entries is based on the RFID response; a passive response can only contain one entry, while the active response can hold 12 entries. The RFID response packets use a version of slotted ALOHA MAC. Therefore, each response packet is randomly assigned a slot number (10 slots available). The slot size is determined by the packet size and the data rate. Once the slot is determine the packet is delayed until its slot time arrives, then transmitted using the OPNET transceiver pipeline.

When the RFID MAC process model receives an RFID response packet from the lower layer it determine if the packet has incurred any collisions, if it has the packet is discarded and no statistics are updated. If the packet is received free of collisions the packet is forwarded to the AODV routing process model for further processing.

A.4 Transceiver Pipeline Stage Closure Model

In order to limit the transmission range of the nodes and the RFID responses the transceiver pipeline stage closure model is modified. The modifications are straight forward. Once a packet arrives at this stage of the pipeline the packet format is determined. The transmission range is determined by the packet format. All transmissions are limited to 150 meters; this represents the maximum transmission range for the Crossbow MICA2 sensor node [Cro05]. If the packet format was an RFID response then the type of response limits the range of transmission. An active tags' response is set to 50 meters, and a passive tags' response is set to 3 meters. The closure stage is the third stage of 14 pipeline stages if closure exists, meaning the nodes can communicate, the packet continues through the pipeline. If closure does not exist the packet is discarded. Therefore, when an RFID active response is transmitted it can only travel 50 meters. Nodes outside this area will not receive the RFID response packet.

A.5 AODV Routing Process Model

To incorporate the RFID tags into the AODV routing protocol the standard OPNET AODV routing process model is modified. When a data packet arrives from the higher layer (MANET traffic generation process model) and no route exists to the destination a burst packet is generated to initiate the RFID tags instead of the standard route request. All AODV route request are created by the same function "aodv_rte_route_request_send()". The burst are active after 5 seconds of simulation time. This allows the AODV protocol time to establish routes. When the node changes destinations after ten seconds of simulation and no route exists to the destination a burst packet is generated by the AODV protocol send a remote interrupt to the MANET traffic generation process. Once this remote interrupt is sent a flag is set indicating that a burst packet has been generated. The next time this function is called since the burst sent flag is set it will generate a standard AODV route request. The burst sent flag is reset so that the following request will generate a new burst packet.

When the AODV routing process model receives an RFID response packet from the RFID MAC process model the "RFID_response_pkt_arrival()" function is called. This function is added to the standard AODV routing process model to allow for processing of RFID response packets. This function examines the contents of the RFID response packet and determines which if any of its entries will update the AODV route table. Each packet entry is compared to the AODV route table, if no route exists a new entry is created using the standard AODV routing process model, and all packets queued to for this destination are forwarded out this path. If a packet entry already exists in the AODV routing table the hop count and sequence numbers are compared. Packet entries with the same sequence number and lower hop count update the AODV route table. Packet entries with the same sequence number update invalid route entries in the AODV route table. After each AODV route table update all packets queued for that destination are forwarded. Once all the packet entries are examined the packet is destroyed.

A.6 Implementing New Process Models

To implement these new models the process models are brought together in a new node model. Figure 26 shows the new node model created using these new process models. The Node_deployment process model is shown on the right side of this model.

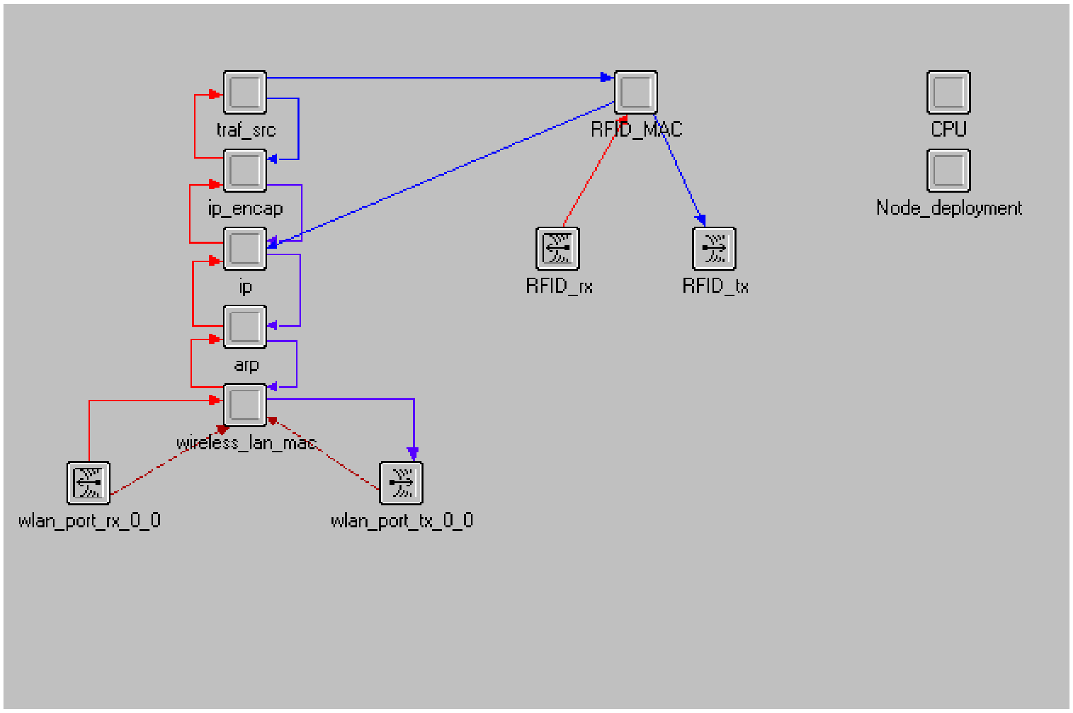


Figure 26: New RFID Node Model

The traf_src model is the MANET traffic generation process model, the blue line connecting it to the RFID_MAC model is the stream that the RFID burst packet travels to get transmitted. The RFID_MAC model also has a blue line connecting it to the IP model. This is the path the RFID response packets travel to get to the AODV routing process model for further processing. Once the node model is created it can be placed into a larger network as shown in Figure 27. The 200 sensor nodes are deployed within the 300 x 300 meter area with 12 sink nodes deployed around this area.

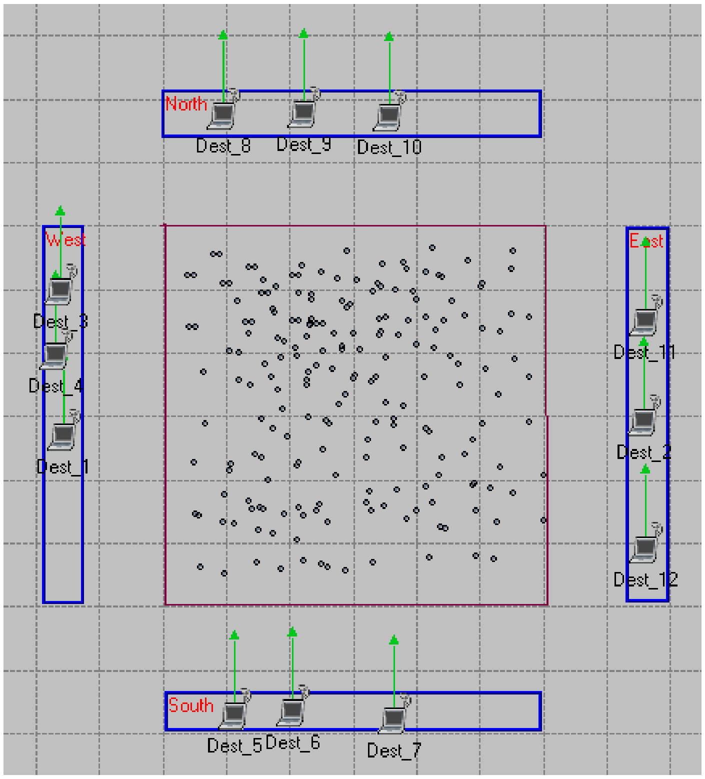


Figure 27: 200-Node, 12-Sink Simulation Scenario

Appendix B

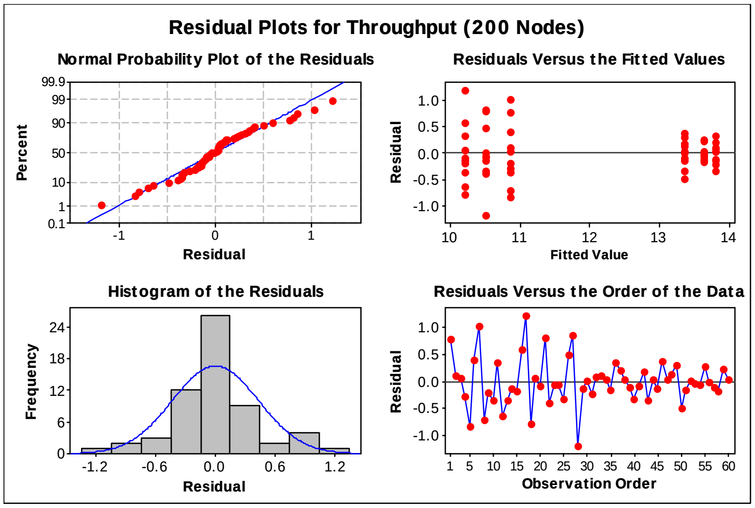


Figure 28: Visual Test 200 Node Throughput ANOVA Assumptions

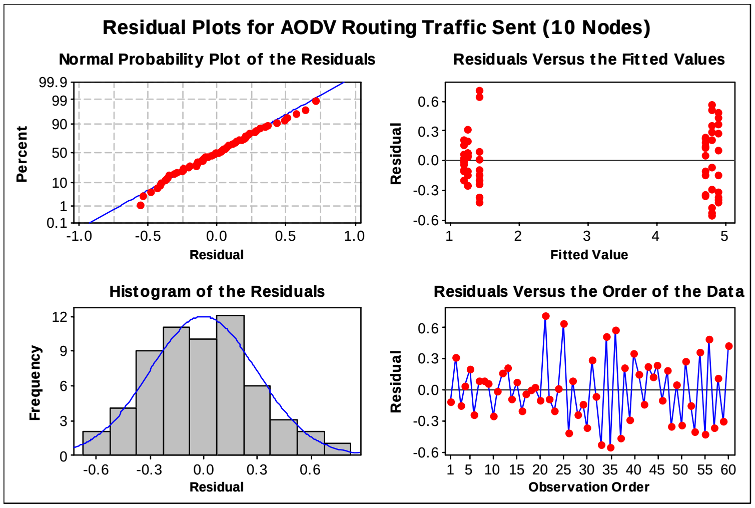


Figure 29: Visual Test 10 Node AODV Routing Traffic Sent ANOVA Assumptions

Bibliography

[Act05] ActiveWave Inc. "Compact Tag Specification Sheet". CompactTagv7, 2005.

[ALK04] Al-Karaki, J.N., and Kamal, A.E. "Routing Techniques in Wireless Sensor Networks: A Survey". Wireless Communications, IEEE Volume 11 Issue 6, Dec 2004.

[ASS02a] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci E. Wireless Sensor Networks: A Survey. Computer Networks, Volume 38, Issue 4, 15 March 2002, Pages 393-422.

[ASS02b] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci E. A Survey of Sensor Networks. IEEE Communication Magazine, pp 102 – 114, August 2002.

[Ass05] Association for Automatic Identification and Mobility (AIM). "What is Radio Frequency Identification (RFID)?" http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp#top Accessed 11 May 2005.

[Atm04] Atmel "ATMEL 8-bit Microcontroller with 128K Bytes In-System Programmable Flash, ATmega 128L Data Sheet". Rev. 2467MS–AVR–11/04.

[AWD04] Abolhasan, M., Wysocki, T., and Dutkiewicz, E. "A review of routing protocols for mobile ad hoc networks". Ad Hoc Networks, Volume 2, Issue 1, January 2004, Pages 1-22. http://www.sciencedirect.com Accessed 15 May 2005.

[Cro05] Crossbow "MICA2 Wireless Measurement System". Document Part Number: 6020-0042-07 Rev A.

[CWL97] Chiang, C. C., Wu, H.K., Liu W., and Gerla, M. "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel". In Proceedings of IEEE SICON '97, April 1997.

[DPR00] Das, S. R., Perkins, C. E., Royer, E. M. "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," In Proceedings of IEEE INFOCOM 2000, Tel Aviv, Israel, Mar. 2000.

[HCB00] Heinzelman, W., Chandrakasan, A., and Balakrishnan, H. "Energy-Efficient Communication Protocol for Wireless Microsensor Networks". In Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[HJB04] Hull, B., Jamieson, K., and Balakrishnan, H."Mitigating Congestion in Wireless Sensor Networks". In Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04), Baltimore, MD, November 2004. ACM Press, New York, NY.

[HKB99] Heinzelman, W., Kulik, J., and Balakrishnan, H. "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks". In Proceedings of the 5th ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA, August 1999.

[HPS02] Haas, Z. J., Pearlman, M. R., and Samar P. "The zone routing protocol (ZRP) for ad hoc networks," IETF, MANET Internet Draft, July 2002.

[IGE00] Intanagonwiwat, C., Govindan, R., and Estrin, D. "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks". In Proceedings of ACM Mobicom '00, Boston, MA, 2000.

[Int04] Intermec "The Intermec Guide to RFID Tag Selection". http://www.intermec.com Accessed 03 June 2005.

[JMH03] Johnson, D., Maltz, D., and Hu, Y. C. "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", 16-Apr-03, draft-ietf-manet-dsr-09.txt.

[JOM96] Johnson, D. and Maltz, D. "Dynamic Source Routing in Ad Hoc Wireless Networks". Mobile Computing, Kluwer Academic publishers, 1996.

[KHB02] Kulik, J., Heinzelman, W., and Balakrishnan, H. "Negotiation-Based protocols for Disseminating Information in Wireless Sensor Networks". Wireless Networks, Volume 8, 2002.

[LWZ03] Lu, Y., Wang, W., Zhong, Y., and. Bhargava, B. "Study of Distance Vector Routing Protocols for Mobile Ad Hoc Networks," *percom*, Volume 00, 2003.

[MuG96] Murthy, S., and Garcia-Luna-Aceves, J.J. “An Efficient Routing Protocol for Wireless Networks”. ACM Mobile Networks and Applications Journal, Special Issue on Routing in Mobile Communication Networks, October 1996.

[Nat05] National Institute Of Standards and Technology (NIST). Advanced Network Technologies Division, Wireless Ad Hoc Networks. Wireless Ad Hoc Sensor Networks. http://www.antd.nist.gov/wahn_ssn.shtml

[Opn04] OPNET Product Documentation Team, “Modeling Wireless Networks,” *Wireless Module Users Guid*e, OPNET Modeler 10.5.A Product Documentation, 2004.

[PaC97] Park V. and Corson, M. “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks”. In Proceedings of INFOCOM ’97, Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution, 1997.

[PeB94] Perkins, C. E., and Bhagwat, P. “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”. In Proceedings of SIGCOMM ’94, August 1994.

[PeR99] Perkins, C. E., and Royer, E. M. “Ad Hoc On-Demand Distance Vector Routing.” In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb 1999.

[Ric05] Rickmon, A. “Evaluation of the Ad hoc On-Demand Distance Vector Routing Protocol for Mobile Ad hoc Networks” AFIT Thesis AFIT/GCS/ENG/05-15, (Mar 05).

[RoT99] Royer, E, and C-K Toh. “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks”. In IEEE Personal Communications, Apr. 1999.

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 074-0188*

1. REPORT DATE *(DD-MM-YYYY)* 23-03-2006	**2. REPORT TYPE** Master's Thesis	**3. DATES COVERED** *(From – To)* August 2004 – March 2006

4. TITLE AND SUBTITLE **SUPPLEMENTING AN AD HOC WIRELESS NETWORK ROUTING PROTOCOL WITH RADIO FREQUENCY IDENTIFICATION (RFID) TAGS**	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Willemsen, LeRoy S., Captain, USAF	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way, Building 640 WPAFB OH 45433-8865	**8. PERFORMING ORGANIZATION REPORT NUMBER** AFIT/GE/ENG/06-56
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Mr. William Koenig AFRL/IFSC 2241 Avionics Circle WPAFB, OH 45433 DSN785-4709x3172	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Wireless sensor networks (WSNs) have a broad and varied range of applications, yet all of these are limited by the resources available to the sensor nodes that make up the WSN. The most significant resource is energy; a WSN may be deployed to an inhospitable or unreachable area leaving it with a non-replenishable power source. This research examines a way of reducing energy consumption by augmenting the nodes with radio frequency identification (RFID) tags that contain routing information. It was expected that RFID tags would reduce the network throughput, AODV routing traffic sent, and the amount of energy consumed. However, RFID tags have little effect on the network throughput or the AODV routing traffic sent. They also increase ETE delays in sparse networks as well as the amount of energy consumed in both sparse and dense networks. Furthermore, there was no statistical difference in the amount of user data throughput received. The density of the network is shown to have an effect on the variation of the data but the trends are the same for both sparse and dense networks. This counter-intuitive result is explained and conditions for such a scheme to be effective are discussed.

15. SUBJECT TERMS

Mobile Ad Hoc Network (MANET), Wireless Sensor Network (WSN), Routing Protocols, Radio Frequency Identification (RFID) tags

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Rusty O. Baldwin, Ph.D. (AFIT/ENG)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(Include area code)*
U	U	U	UU	91	(937) 255-6565, ext 4445 (Rusty.Baldwin@afit.edu)