International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501

A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013

http://www.ijeemc.com

AN EMPIRICAL COMPARATIVE ANALYSIS ON ASSORTED ROUTING PROTOCOLS

Er. Simranjeet Sandhu, Deepinder Singh Wadhwa

Introduction

Wireless Ad Hoc Networks can be mobile or static networks in which wireless terminals cooperate to maintain network connectivity and to exchange information. WLANs are an alternative to the high installation and maintenance cost incurred by traditional changes in wired LAN infrastructures. Moreover, deployment of such networks is inevitable in cases where wired network installation is not possible, such as in battlefields, old monuments and concrete buildings with no previous network cabling [1]. Unlike conventional WLANs, where the access point enforces centralized control over its neighborhood, in ad hoc networks, the terminals must act co- operatively as routers that forward data packet from sources to destinations.

In order for ad hoc networks to operate as efficiently as possible, appropriate on-demand routing protocols have to be incorporated, which can find efficient routes from a source to a destination node, taking into consideration the mobility of the terminals. Mobility affects the ongoing transmissions, since a mobile node that receives and forwards packets may move beyond the coverage range of its neighbors. As a result, some (or all) of the links with its neighbors can break over time. In that case, a new route must be established, before the data flows are restored. Thus, a quick route recovery should be one of the main characteristics of a well-designed routing protocol.

Volume 2 Issue 1 January 2013

http://www.ijeemc.com

Routing Protocols - Generally

According to their characteristics, routing protocols can be divided in two different categories: table-driven (proactive) and on-demand (reactive). Table-driven routing protocols enforce mobile nodes to maintain tables with path information from every terminal to every other terminal in the wireless network [2]. This information is updated by transmitting messages containing network topology changes, so as for each node to have at least one possible route towards any in- tended receiver. The most popular table-driven protocol is DSDV (Destination-Sequenced Distance-Vector Routing protocol).

IP routing protocols Background

Dynamic routing protocols have evolved over several years to meet the demands of changing network requirements. Although many organizations have migrated to more recent routing protocols such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), many of the earlier routing protocols, such as Routing Information Protocol (RIP), are still in use today. Dynamic routing protocols have been used in networks since the early 1980s. The first version of RIP was released in 1982, but some of the basic algorithms within the protocol were used on the ARPANET as early as 1969. One of the earliest routing protocols was RIP. RIP has evolved into a newer version: RIPv2 [3].

However, the newer version of RIP still does not scale to larger network implementations. To address the needs of larger networks, two advanced routing protocols were developed: OSPF and Intermediate System–to–Intermediate System (IS-IS). Cisco developed Interior Gateway Routing Protocol (IGRP) and Enhanced IGRP (EIGRP). EIGRP also scales well in larger network implementations. Additionally, there was the need to interconnect different internetworks and provide routing among them. Border Gateway Protocol (BGP) is now used between Internet service providers (ISP) as well as between ISPs and their larger private clients to exchange routing information. With the advent of numerous consumer devices using IP, the IPv4 addressing space is nearly exhausted.

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013

http://www.ijeemc.com

Classification of routing protocols

The design space for routing algorithms for WSNs is quite large and we can classify the routing algorithms for WSNs in many different ways. Routing protocols are classified as node centric, data-centric, or location-aware (geo-centric) and QoS based routing protocols. Most Ad-hoc network routing protocols are node-centric protocols where destinations are specified based on the numerical addresses (or identifiers) of nodes [4]. In WSNs, node centric communication is not a commonly expected communication type. Therefore, routing protocols designed for WSNs are more data-centric or geocentric. In data-centric routing, the sink sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute based naming is necessary to specify the properties of data. Here data is usually transmitted from every sensor node within the deployment region with significant redundancy.

In location aware routing nodes know where they are in a geographical region. Location information can be used to improve the performance of routing and to provide new types of services. In QoS based routing protocols data delivery ratio, latency and energy consumption are mainly considered. To get a good QoS (Quality of Service), the routing protocols must possess more data delivery ratio, less latency and less energy consumption. Routing protocols can also be classified based on whether they are reactive or proactive. A proactive protocol sets up routing paths and states before there is a demand for routing traffic. Paths are maintained even there is no traffic flow at that time. In reactive routing protocol, routing actions are triggered when there is data to be sent and disseminated to other nodes. Here paths are setup on demand when queries are initiated. Routing protocols are also classified based on whether they are destination-initiated (Dst-initiated) or source-initiated (Src-initiated). A source-initiated protocol sets up the routing paths upon the demand of the source node, and starting from the source node. Here source advertises the data when available and initiates the data delivery. A destination initiated protocol, on the other hand, initiates path setup from a destination node. Routing protocols are also classified based sensor network architecture.

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts
Volume 2 Issue 1 January 2013
http://www.ijeemc.com

Some WSNs consist of homogenous nodes, whereas some consist of heterogeneous nodes. Based on this concept we can classify the protocols whether they are operating on a flat topology or on a hierarchical topology. In Flat routing protocols all nodes in the network are treated equally. When node needs to send data, it may find a route consisting of several hops to the sink. A hierarchical routing protocol is a natural approach to take for heterogeneous networks where some of the nodes are more powerful than the other ones. The hierarchy does not always depend on the power of nodes. In Hierarchical (Clustering) protocols different nodes are grouped to form clusters and data from nodes belonging to a single cluster can be combined (aggregated).The clustering protocols have several advantages like scalable, energy efficient in finding routes and easy to manage.

Comparison of Table-Driven and On-Demand Routing Protocols

The table-driven ad hoc routing approach is similar to the connectionless approach of forwarding packets, with no regard to when and how frequently such routes are desired. It relies on an underlying routing table update mechanism that involves the constant propagation of routing information. This is not the case, however, for on-demand routing protocols. When a node using an on-demand protocol desires a route to a new destination, it will have to wait until such a route can be discovered [5]. On the other hand, because routing information is constantly propagated and maintained in table-driven routing protocols, a route to every other node in the ad hoc network is always available, regardless of whether or not it is needed. This feature, although useful for datagram traffic, incurs substantial signaling traffic and power consumption. Since both bandwidth and battery power are scarce resources in mobile computers, this becomes a serious limitation.

AODV

The Ad hoc On-demand Distance Vector routing protocol is based on the table- driven DSDV. However as an on-demand protocol, it does not maintain global routing information for the whole network. Nodes that do not belong to a route do not need to keep information about that route. Such nodes do not send or receive topology-update packets, so they have information only for their active routes; a node considers a route as active, if it sends, receives or forwards packets for that route and through which there is at least one data packet transmitted within a fixed time interval. (For some routing protocols, a node considers a route as active, if it overhears routing information that makes it realize that the route is active).

DSR

The Dynamic Source Routing protocol also allows mobile sources to dynamically discover paths towards any desired destination. Every data packet includes a complete list of nodes, which the packet must pass before it reaches the destination. Hence, all nodes that forward or overhear these packets may store important routing information for future use. Even though nodes may move at any time and even continuously, DSR can support fast network topology changes. Moreover, DSR can support asymmetric links; it can successfully find paths and forward packets in unidirectional link environments. Moreover, like AODV, it has a mechanism for on-demand route maintenance, so there are no periodic topology update packets. When link failures occur, only nodes that forward packets through those links must receive proper routing advertisements. In addition, DSR allows source nodes to receive and store more than one path towards a specific destination. Intermediate nodes have the opportunity to select another cached route as soon as they are informed about a link failure. By this way, less routing overhead is required for path recovery, something that reduces the overall data packet delay.

Destination-Sequenced Distance-Vector (DSDV) protocol

The Table-driven DSDV protocol is a modified version of the Distributed Bellman-Ford (DBF) Algorithm that was used successfully in many dynamic packet switched networks. The Bellman-Ford method provided a means of calculating the shortest paths from source to destination nodes, if the metrics (distance-vectors) to each link are known. DSDV uses this idea, but overcomes DBF’s tendency to create routing loops by including a parameter called destination-sequence number. In DSDV, each node maintains a routing table that contains the shortest distance and the first node on the shortest path to every other node in the network. A sequence number created by the destination node tags each entry to prevent loops, to counter the count – to-infinity problem and for faster convergence [6]. The tables are exchanged between neighbors at regular intervals to keep an up to date view of the network topology.

The tables are also forwarded if a node finds a significant change in local topology. This exchange of table imposes a large overhead on the whole network. To reduce this potential traffic, routing updates are classified into two categories. The first is known as “full dump” which includes all available routing information [7]. This type of updates should be used as infrequently as possible and only in the cases of complete topology change. In the cases of occasional movements, smaller “incremental” updates are sent carrying only information about changes since the last full dump. Each of these updates should fit in a single Network Protocol Data Unit (NPDU), and thus significantly decreasing the amount of traffic. Table updates are initiated by a destination with a new sequence number which is always greater than the previous one. Upon receiving an updated table a node either updates its tables based on the received information or holds it for some time to select the best metric received from multiple versions of the same update from different neighbors.

STAR

STAR is a table-driven routing protocol. Each node discovers and maintains topology information of the network, and builds a shortest path tree (source tree) to store preferred paths to destinations. The basic mechanisms in STAR include the detection of neighbors and exchange of topology information (update message) among nodes.

Comparison of MANETS and sensor networks

MANETS (Mobile Ad-hoc NETworkS) and sensor networks are two classes of the wireless Adhoc networks with resource constraints. MANETS typically consist of devices that have high capabilities, mobile and operate in coalitions [8]. Sensor networks are typically deployed in

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts
Volume 2 Issue 1 January 2013
http://www.ijeemc.com

specific geographical regions for tracking, monitoring and sensing. Both these wireless networks are characterized by their ad hoc nature that lack pre deployed infrastructure for computing and communication. Shares some characteristics like network topology are not fixed, power is an expensive resource and nodes in the network are connected to each other by wireless communication links. WSNs differ in many fundamental ways from MANETS as mentioned below. Sensor networks are mainly used to collect information while MANETS are designed for distributed computing rather than information gathering.

- Sensor nodes mainly use broadcast communication paradigm whereas most MANETS are based on point-to-point communications.
- The number of nodes in sensor networks can be several orders of magnitude higher than that in MANETS.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.
- Sensor nodes are much cheaper than nodes in a MANET and are usually deployed in thousands.
- Sensor nodes are limited in power, computational capacities, and memory where as nodes in a MANET can be recharged somehow.
- Usually, sensors are deployed once in their lifetime, while nodes in MANET move really in an Ad-hoc manner.
- Sensor nodes are much more limited in their computation and communication capabilities than their MANET counterparts due to their low cost.

Dynamic versus Static Routing

Feature	Dynamic Routing	Static Routing

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts
Volume 2 Issue 1 January 2013
http://www.ijeemc.com

Configuration complexity	Generally independent of the network size	Increases with network size
Required administrator knowledge	Advanced knowledge required	No extra knowledge required
Topology changes	Automatically adapts to topology changes	Administrator intervention required
Scaling	Suitable for simple and complex topologies	Suitable for simple topologies
Security	Less secure	More secure
Resource usage	Uses CPU, memory, and link bandwidth	No extra resources needed
Predictability	Route depends on the current topology	Route to destination is always the same

Static Routing Usage, Advantages, and Disadvantages

Static routing has several primary uses, including the following:

- Providing ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- Routing to and from stub networks.
- Using a single default route, used to represent a path to any network that does not have a more specific match with another route in the routing table.

Static routing advantages are as follows:

- Minimal CPU processing
- Easier for administrator to understand
- Easy to configure

Static routing disadvantages are as follows:

- Configuration and maintenance are time-consuming.
- Configuration is error-prone, especially in large networks.
- Administrator intervention is required to maintain changing route information.
- Does not scale well with growing networks; maintenance becomes cumbersome.
- Requires complete knowledge of the entire network for proper implementation.

Dynamic Routing Advantages and Disadvantages

Dynamic routing advantages are as follows:

- Administrator has less work in maintaining the configuration when adding or deleting networks.
- Protocols automatically react to the topology changes.
- Configuration is less error-prone.
- More scalable; growing the network usually does not present a problem.

Dynamic routing disadvantages are as follows:

- Router resources are used (CPU cycles, memory, and link bandwidth).
- More administrator knowledge is required for configuration, verification, and troubleshooting.

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501

A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013

http://www.ijeemc.com

Comparison of IP routing protocols

	RIP v1	**RIP v2**	**OSPF**	**Integrated IS-IS**	**EIGRP**	**BGP**
Type	IGP	IGP	IGP	IGP	IGP	EGP
Convergence	Slow	Slow	Fast	Fast	Very Fast	Average
Class	Distance vector	Distance vector	Link state	Link state	Hybrid (advanced distance vector)	Path vector
AD	120	120	110	115	5 (summary) 90 (internal) 170 (external)	20 (external) 200 (internal)
Metric	Hop Count (max 15)	Hop Count (max 15)	cost	cost	Lowest best Composite (BW + DLY) Hop Count 100 (max 224)	Path attributes (Usually AS-path)
Classless	NO	YES	YES	YES	YES	YES
Algorithm	Bellman-Ford	Bellman-Ford	Dijkstra (SPF)	Dijkstra (SPF)	Dual	Best path
Transport type	UDP/port520	UDP/port520	IP protocol 89 (OSPF)	Layer 2	IP protocol 88 (EIGRP)	TCP/179

Routing updates	Every 30 seconds full table broadcast 255.255.255.255	Every 30 seconds full table multicast address 255.0.0.9	Only when changes occurs multicast address 224.0.5-6	Only when changes occur	Multicast address 224.0.0.10 or Unicast (RTP) only when change occurs	Only when changes occurs (Unicast updates)
Propagate a default route	Default-information originate	Default-information originate	Default-information originate	Default-information originate	Redistribute static	Default-information originate

1) Type - exchange routing information within (interior IGP) or between (exterior EGP) an autonomous system (AS). Autonomous system (AS) - a collection of IP networks and routers under the control of one entity.

2) Convergence - the status of a set of routers having the same knowledge of the surrounding network topology.

3) Protocol Class (Type) - routing algorithms used by varying routing protocols to determine the metric for routing (Distance Vector - Uses hop count, Link State - Uses Shortest Path First, Common View of Network, Hybrid - Distance vector with more accurate update metrics).

4) Administrative distance (AD) - preference of routing protocol - is how a router determines which source of routes it should use if it has two identical routes from different sources. In other words, the router needs to be able to determine which routes to trust if it's

receiving the same information from two different sources (which is most trustworthy). The lower the administrative distance - is best

5) Metric - Routers use various metrics and calculations to determine the best route for a packet to reach its final network destination. Each routing protocol uses its own algorithm with varying weights to determine the best possible path (only one from all).

6) Classful routing protocols do not carry subnet mask information on their routing updates the same subnet mask everywhere is needed to avoid routing black holes), Classless routing protocols include the subnet mask along with the IP address when advertising routing information.

IP supports a broad variety of IGPs. In the distance vector category, IP supports the Routing Information Protocol (RIP) and the Interior Gateway Routing Protocol (IGRP). In the hybrid category, IP supports the Enhanced Interior Gateway Routing Protocol (EIGRP). In the link-state category, IP supports the Open Shortest Path First (OSPF) protocol and the Integrated Intermediate System to Intermediate System (Integrated IS-IS) protocol. IP also supports two EGPs: the Exterior Gateway Protocol (EGP) and the Border Gateway Protocol (BGP). RIP is the original distance vector protocol. RIP and its successor, RIP version 2 (RIPv2), enjoyed widespread use for many years [9]. Today, RIP and RIPv2 are mostly historical. RIP employs classful routing based on classful IP addresses. RIP distributes routing updates via broadcast. RIPv2 enhances RIP by supporting classless routing based on variable-length subnet masking (VLSM) methodologies.

Other enhancements include the use of multicast for routing update distribution and support for route update authentication. Both RIP and RIPv2 use hop count as the routing metric and support load balancing across equal-cost paths. RIP and RIPv2 are both IETF standards. IGRP is a Cisco Systems proprietary protocol. IGRP was developed to overcome the limitations of RIP [10]. The most notable improvement is IGRP's use of a composite metric that considers the delay, bandwidth, reliability, and load characteristics of each link. Additionally, IGRP expands

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts
Volume 2 Issue 1 January 2013
http://www.ijeemc.com

the maximum network diameter to 255 hops versus the 15-hop maximum supported by RIP and RIPv2 [9]. IGRP also supports load balancing across unequal-cost paths. IGRP is mostly historical today. EIGRP is another Cisco Systems proprietary protocol. EIGRP significantly enhances IGRP. Although EIGRP is often called a hybrid protocol, it advertises routing-table entries to adjacent routers just like distance vector protocols. However, EIGRP supports several features that differ from typical distance vector protocols.

Among these are partial table updates (as opposed to full table updates), change triggered updates (as opposed to periodic updates), scope sensitive updates sent only to affected neighbor routers (as opposed to blind updates sent to all neighbor routers), a "diffusing computation" system that spreads the route calculation burden across multiple routers, and support for bandwidth throttling to control protocol overhead on low-bandwidth WAN links. EIGRP is a classless protocol that supports route summaries for address aggregation, load balancing across unequal-cost paths, and route update authentication [11]. Though waning in popularity, EIGRP is still in use today. OSPF is another IETF standard protocol. OSPF was originally developed to overcome the limitations of RIP. OSPF is a classless protocol that employs Dijkstra's Shortest Path First (SPF) algorithm, supports equal-cost load balancing, supports route summaries for address aggregation, and supports authentication. To promote scalability, OSPF supports the notion of areas. An OSPF area is a collection of OSPF routers that exchange LSAs. In other words, LSA flooding does not traverse area boundaries. This reduces the number of LSAs that each router must process and reduces the size of each router's link-state database. One area is designated as the backbone area through which all inter-area communication flows.

Each area has one or more Area Border Routers (ABRs) that connect the area to the backbone area. Thus, OSPF implements a two-level hierarchical topology. All inter-area routes are calculated using a distance-vector algorithm. Despite this fact, OSPF is not widely considered to be a hybrid protocol. OSPF is very robust and is in widespread use today. IS-IS was originally developed by Digital Equipment Corporation (DEC) [12]. IS-IS was later adopted by the ISO as

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501
A Scientific and Scholarly Resource for Publication of Research Manuscripts
Volume 2 Issue 1 January 2013
http://www.ijeemc.com

the routing protocol for its Connectionless Network Protocol (CLNP). At one time, many people believed that CLNP eventually would replace IP. So, an enhanced version of IS-IS was developed to support CLNP and IP simultaneously. The enhanced version is called Integrated IS-IS. In the end, the IETF adopted OSPF as its official IGP.

OSPF and Integrated IS-IS have many common features. Like OSPF, Integrated IS-IS is a classless protocol that employs Dijkstra's SPF algorithm, supports equal-cost load balancing, supports route summaries for address aggregation, supports authentication, and supports a two-level hierarchical topology. Some key differences also exist. For example, Integrated IS-IS uses the Dijkstra algorithm to compute inter-area routes. EGP was the first exterior protocol [13]. Due to EGP's many limitations, many people consider EGP to be a reach ability protocol rather than a full routing protocol. EGP is mostly historical today. From EGP evolved BGP. BGP has since evolved from its first implementation into BGP version 4 (BGP-4). BGP-4 is widely used today. Many companies run BGP-4 on their Autonomous System Border Routers (ASBRs) for connectivity to the Internet.

Likewise, many ISPs run BGP-4 on their ASBRs to communicate with other ISPs. Whereas BGP-4 is widely considered to be a hybrid protocol, BGP-4 advertises routing table entries to other BGP-4 routers just like distance vector protocols [14]. However, a BGP-4 route is the list of AS numbers (called the AS_Path) that must be traversed to reach a given destination. Thus, BGP-4 is called a path vector protocol. Also, BGP-4 runs over TCP. Each BGP-4 router establishes a TCP connection to another BGP-4 router (called a BGP-4 peer) based on routing policies that are administratively configured. Using TCP relaxes the requirement for BGP-4 peers to be topologically adjacent. Connectivity between BGP-4 peers often spans an entire AS that runs its own IGP internally. A TCP packet originated by a BGP-4 router is routed to the BGP-4 peer just like any other unicast packet. BGP-4 is considered a policy-based routing protocol because the protocol behavior can be fully controlled via administrative policies [15]. BGP-4 is a classless protocol that supports equal-cost load balancing and authentication.

International Journal of Electrical, Electronics and Mechanical Controls ISSN (Online) : 2319 – 7501

A Scientific and Scholarly Resource for Publication of Research Manuscripts

Volume 2 Issue 1 January 2013

http://www.ijeemc.com

References

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankaraubramaniam, and Erdal Cayirci: *A Survey on sensor networks*, IEEE Communications Magazine (2002).

[2] José A. Gutierrez, Marco Naeve, Ed Callaway,Monique Bourgeois,Vinay Mitter, Bob Heile, IEEE 802.15.4: *A Developing Standard for Low-Power Low-Cost Wireless Personal Area Networks*, IEEENetwork, pp. 12-19 (September/October 2001).

[3] Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez, Marco Naeve, Bob Heile, Venkat Bahl: *A Developing Standard for Low-Rate Wireless Personal Area Networks; IEEE Communications Magazine*, pp. 70-77 (August 2002).

[4] Sarjoun S. Doumit, Dharma P. Agrawal: *Self-Organizing and Energy-Efficient Network of Sensors*, IEEE, pp. 1-6 (2002).

[5] Elaine Shi, Adrian Perrig: *Designing Secure Sensor Networks IEEE Wireless Communications,* pp. 38-43 (December 2004).

[6] Chien-Chung Shen, Chavalit Srisathapornphat, Chaiporn Jaikaeo: *Sensor Information Networking Architecture and Applications*, IEEE Personal Communications, pp. 52-59

[7] Al-Karaki,J.N,Al-Mashagbeh: Energy-Centric Routing in Wireless Sensor Networks Computers and Communications, ISCC 06 Proceedings, 11th IEEE Symposium (2006).

[8] Kay Romer, Friedemann Mattern: *The Design Space of Wireless Sensor Networks*, IEEE Wireless Communications, pp. 54-61 (December 2004).

[9] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci: A Surveyon Sensor Networks, *IEEE Communications Magazine*, pp. 102-114 (August 2002).

[10] Wendi B. Heinzelman, Amy L. Murphy, Hervaldo S. Carvalho, Mark A. Perillo: *Middleware to Support Sensor Network Applications*, IEEE Network, pp. 6-14,

[11] W. Heinzelman, J. Kulik, and H. Balakrishnan: Adaptive Protocols for Information Dissemination in Wireless Sensor Networks, Proc. 5th *ACM/IEEE Mobicom*, Seattle, WA, pp. 174–85 (Aug. 1999).

[12] J. Kulik, W. R. Heinzelman, and H. Balakrishnan: Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks, *Wireless Networks*, vol. 8, pp. 169–85 (2002).

[13] C. Intanagonwiwat, R. Govindan, and D. Estrin: Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks, Proc. *ACM Mobi- Com* 2000, Boston, MA, pp. 56–67 (2000).

[14] D. Braginsky and D. Estrin: Rumor Routing Algorithm for Sensor Networks, in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA.

[15] C. Schurgers and M.B. Srivastava: Energy efficient routing in wireless sensor networks, in the MILCOM Proceedings on Communications for Network-Centric Operations: *Creating the Information Force*, McLean, VA (2001).