IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Trust Aware Framework For Optimizing Misdirection Attacks In Storm

Shibin Sebastian[1], K. Sankar Ganesh[2], R. Gopi[3].

[1]Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan Engineering College, Perambalur-621212, India.

[2]Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan Engineering College, Perambalur-621212, India.

[3]Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan Engineering College, Perambalur-621212, India.

Abstract

STORM is a cross-layer framework for the effective dissemination of real-time and elastic traffic in multihop wireless Adhoc networks. The routes established in STORM are shown to be loop-free and real time packets forwarded along these routes are shown to have bounded end-to-end delays. STORM is best suited for ad hoc networks subject to a variety of multicast and unicast traffic, subject to delay or bandwidth constraints. STORM offers little protection against identity deception through replaying routing information. An adversary can exploit this defect to launch various harmful or even devastating attacks against the routing protocols. To overcome this attack an efficient trust aware routing framework has been implemented. TARF proves effective against those harmful attacks developed out of identity deception. This paper focuses on the kind of attacks in which adversaries misdirect network traffic by identity deception through replaying routing information.

Keywords: Unicast, Multicast, end to end delay, bandwidth, Trust Aware Routing, STORM.

1. Introduction

The field of wireless networking emerges from the integration of personal computing, cellular technology, and the Internet. This is due to the increasing interactions between communication and computing, which is changing information access from "anytime anywhere" into "all the time, everywhere". STORM (Scheduling and traffic management in orders routing meshes) is the first cross-layering scheme that provides flow-ordered routing meshes consisting of multiple paths from sources to destinations over which relays are capable of establishing channel reservations that meet the end-to-end requirements of the flows being routed. STORM establishes and maintains loop-free routes from sources to destinations and, just as important, that the reservations established along these paths provide bounded end-to-end delays. STORM can provide some performance improvements even in those cases where the traffic is unicast and elastic (e.g., http), because it avoids most packet collisions and limits the signaling overhead needed for routing. The multihop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. The multihop routing of WSNs often becomes the target of malicious attacks. An attacker may tamper nodes physically, create traffic collision with seemingly valid transmission, drop or misdirect messages in routes.

The most existing routing protocols for WSNs either assume the honesty of nodes or focus on energy efficiency [8], or attempt to exclude unauthorized participation by encrypting data and authenticating packets. It is also critical to incorporate security as one of the most important goals meanwhile, even with perfect encryption and authentication [5], by replaying routing information, a malicious node can still participate in the network using another valid node's identity. The cryptographic methods trust and reputation management [6] has been employed in generic ad hoc networks and WSNs to secure routing protocols. WSNs are concerned, secure routing solutions based on trust and reputation management rarely address the identity deception through replaying routing information [4], [3]. The countermeasures proposed so far strongly depends on either tight time synchronization or known geographic information while their effectiveness against attacks exploiting the replay of routing information has not been examined yet [9].

2. Existing System

2.1 STORM Framework.

STORM provides scheduling, routing, and traffic Management functions of a multihop wireless network in a way that sources and destinations of flows perceive the network as a virtual link .A single wireless channel organized into time frames consisting of a fixed number of time slots. Accessing the time slots of each frame is based on a combination of distributed elections of available time slots and reservations of time slots. Time slots that have not been reserved, nodes use a distributed election algorithm based on hashing functions of node identifiers. The schedules generated by STORM are such that delay guarantees can be enforced on a per-hop and end-to-end basis.

STORM provides an extra path provide by routing meshes that can be used in the case of line breaks. Routing algorithm establishes enclaves, which restrict the dissemination of

control information to those nodes that are likely to participate as forwarders of a given data flow. Nodes reserve time slots on behalf of real-time data flows according to their end-to-end schedules and use a priority-based queuing system to select the packets that are transmitted on each slot. STORM uses reservations and a priority-based queuing system to implement and preserve the per-flow channel access schedules. Queuing system composed of signaling packets and real time data, packets are selected according to priority of the packets. Thus STORM establishes a dedicated queuing network for each real-time flow and non real time packets.

2.2 Traffic Management

STORM frame is composed of N time slots (from slot 0 to slot N - 1) and use the position of a slot within the STORM frame as the identifier of the slot. A STORM frame does not have any particular structure and any time slot can be used to transmit a sequence of packets (signaling or data). When a node is allowed to transmit over a time slot, it fits as many packets as possible in it. Packets are selected from the local transmission queues, which are FIFO and are served using a priority-based algorithm. Reservation packets have the highest priority, the next priority is given to network-layer signaling packets, and data packets waiting in data queues have the lowest priority, Hello packets are transmitted with the lowest priority.

2.3 Neighbor protocol

To gather information from the neighbor node additional protocol is introduce in STORM. The neighborhood of a node consists of those nodes whose transmissions the node can decode, which call one-hop neighbors, and the one-hop neighbors of those nodes are called two-hop neighbors. To gather two-hop neighborhood information, each node transmits hello messages periodically every hello period seconds, and each such message contains a list of tuples. Each tuple is composed of a node identifier, a list of the identifiers of the time slots reserved by the node, and the length of the list of reserved slots.

Neighbor protocol [3] is also used for resolving conflict reservation. When two nodes select same time slots, node with large identifier get the given timeslot, the node with the lower identifier has to give up its current reservation and start a new reservation transaction over a different slot. The neighborhood information contained in hello messages allows nodes to detect these collisions before the conflicting nodes become one-hop neighbors.

2.4 Channel Access Algorithm

Transmission Scheduling Algorithm is used by node to select the particular timeslot in the STORM framework, On every slot t with identifier (t mode N) node u with identifier idu first checks if it is the owner of the slot (i.e., if (t+idu)mod N=0)and if so, u can access the channel. If node u does not own the slot, it checks if the owner is present in its two-hop neighborhood, if this is the case, then node u listens to the channel. If the owner of the time slot is not present in the two-hop neighborhood, node u checks if it has a reservation on the slot (t mod N), in which case it can access the channel. Otherwise it checks the neighbor node for the reservation. If none of the two previous conditions are met, node u employs a hash-based election scheme; Node u computes the priority of each node v in its two-hop neighborhood. Node u can access the channel if ptu > ptv for any node v in its two-hop neighborhood. Otherwise, node u listens to the channel.

2.5Meshes and Routes

Routing meshes and destination meshes are used for sending the packet. To integrate unicast and multicast routing, a destination D is treated as a connected destination mesh containing one or more nodes. In the case of a unicast data flow, D is a singleton that contains a node with identifier D, in the case of a multicast data flow, D contains the members of a multicast group, as well as a set of nodes needed to keep D connected. The routing meshes used in STORM have the restriction that each node in those paths is flow ordered. Elastic flows are routed using simple loop-free paths from sources to destinations, and they have no end-to-end restrictions, given that they do not have to be flow ordered. Enclaves are used to confine the dissemination of signaling packets into connected regions of the network that contain those nodes with interest in a given data flow. The enclave of a destination D is the union of the destination D, the set of active sources S, the routing meshes used to connect the elements of S with D, as well as nodes located one hop away from them.

The first source that becomes active for a given destination sends its first data packet piggybacked in a Mesh Request (MR) packet that is flooded up to a horizon threshold. Destination node receiving the request processes the request and establishes a routing path between source and destinations.

2.6 Mesh Announcement (MA) and Packet Forwarding

STORM uses mesh announcements to establish and maintain routing and destination meshes, to publish the availability of time slots in their corresponding flow ordered intervals, to coordinate end-to-end schedules for real-time flows and, in the case of a multicast group, to elect the core of the group. A node transmits MAs to inform other nodes about updates in its routing state. Reception of a MR, a multicast group member first determines whether it has received a MA from the core of that group within the last two MA-periods. If that is the case, no further action is needed otherwise; the receiver considers itself the core of the group and starts transmitting MAs to its neighbors, stating itself as the core of the group.

When a source has data to send, it checks whether it has received an MA advertising the intended destination within the last three MA periods. If that is the case, the sender simply broadcasts the data packet; otherwise, it broadcasts an MR. Upon reception of a data packet, a node checks for a hit in its data-packet cache. Otherwise, the receiving node inserts the Pair in its cache and determines whether it has to relay the data packet or not. If the node is part of the destination, it also passes the data packet to upper layers.

2.7 Identity deception attacks

The multihop routing of WSNs often becomes the target of malicious attacks a malicious node simply replays all the outgoing routing packets from a valid node to forge the latter node's identity the malicious node then uses this forged identity to participate in the network routing, thus disrupting the network traffic. It may drop packets received, forward packets to another node not supposed to be in the routing path, or even form a transmission loop through which packets are passed among a few malicious nodes infinitely. STORM framework is highly susceptible to malicious mode attack, especially Sinkhole and Wormhole attack. Sinkhole attacks are another kind of attacks that can be launched after stealing a valid identity. The harm of such malicious attacks based on the technique of replaying routing information is further aggravated by the introduction of mobility and introduce TARF concept to reduce malicious attack.

3. Proposed Methodology

3.1 Design Assumptions

TARF secures the multihop routing in WSNs against intruders misdirecting the multihop routing by evaluating the trustworthiness of neighboring nodes. It identifies which is the malicious node by the low trust value, and reroute the traffic to another high trust value node, thus secure the WSN from malicious attack.

Neighbor: A neighbor (neighboring node) of N is a node that is reachable from N with one-hop wireless transmission.

Trust level: The trust level of the neighbor is N's estimation of the probability that this neighbor correctly delivers data received to the base station.

Energy cost: The energy cost of a neighbor is the average energy cost to successfully deliver a unit sized data packet with this neighbor as its next-hop node.

3.2 Overview

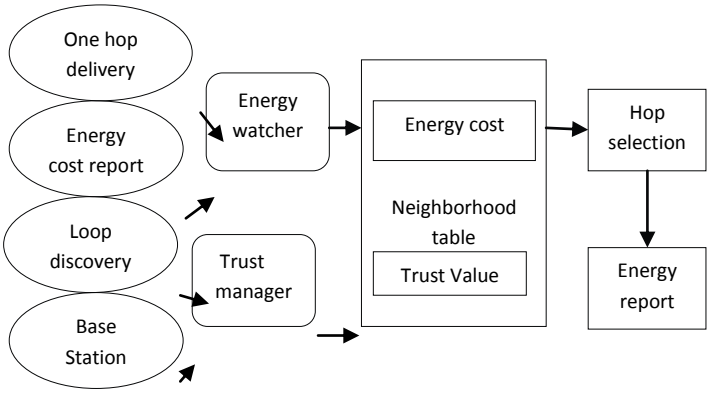

Fig.1. Each node selects a next-hop node based on its neighborhood table and broadcast it's energy cost.

TARF-enabled node N to route a data packet to the base station, N only needs to decide to which neighboring node it should forward the data packet considering both the trustworthiness and the energy efficiency. N maintains a neighborhood table with trust level values and energy cost values for certain known neighbors. In addition to data packet transmission, there are two types of routing information that need to be exchanged broadcast messages from the base station about data delivery and energy cost report messages from each node. Each delivery message collects information about the neighborhood node and collected information mention in the delivered report. This periodic collection helps in periodic updating of Table thus enables the routing information progress.

TARF enabled Node have two components such as *energy watcher and trust manager* .Energy Watcher is responsible for recording the energy cost for each known neighbor. A compromised node may report extremely low energy cost energy. Trust Manager is responsible for tracking trust level values of neighbors based on network loop discovery and broadcast messages from the base station about data delivery.

3.3 Routing Procedure

TARF run as periodic service. The length of that period determines how frequently routing information is exchanged and updated. Beginning of each period, the base station broadcasts a message about data delivery during last period to the whole network consisting of a few contiguous packets. Whenever a node receives such a broadcast message from the base station, it knows that the most recent period has ended and a new period has started. During each period, Energy Watcher on a node monitors energy consumption of one-hop transmission to its neighbors and processes energy cost reports from those neighbors' to maintain energy cost entries in its neighborhood table. Trust Manager also keeps track of network loops and processes broadcast messages from the base station about data delivery to maintain trust level entries in its neighborhood table.

To maintain the stability of its routing path, a node may retain the same next-hop node until the next fresh broadcast message from the base station occurs. To reduce traffic, its energy cost report could be configured to not occur again until the next fresh broadcast message from the base station. If a node does not change its next-hop node selection until the next broadcast message from the base station that guarantees all paths to be loop-free, as can be deducted from the procedure of next-hop node selection.

3.4 Energy Watcher

Energy Watcher is responsible for calculating energy of the neighbor node Energy Watcher computes the energy cost E_nb for its neighbor b in N's neighborhood table. E_nb mentioned is the average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N's next-hop node being responsible for the remaining route.

3.5 Calculating Energy Cost

Energy cost can be calculated by energy watcher using an equation calculated energy cost is stored in neighborhood table. Routing decision is taken with the help of this table.

$E_nb = E_{n->b} + E_b$. (1)

Where,

E_nb is Average energy cost of successfully delivering a unit-sized data packet from N to the base station, with b as N's next-hop node

$E_{n->b}$ is Average energy cost of successfully delivering a data packet from N to its neighbor b with one hop.

E_b is Energy cost of the one hop neighbor.

3.6 TrustManager

A node N's Trust Manager decides the trust level of each neighbor based on the following events discovery of network loops, and broadcast from the base station about data delivery. To minimize the effort to integrate TARF and the existing protocol and to reduce the overhead, when an existing routing protocol does not provide any anti-loop mechanism, adopt the following mechanism to detect routing loops. A binary variable loop is used to record the result of loop discovery 0 if a loop not received loop value is 1.

3.7 Calculating Trust Value

Trust value is calculated by the formula:

$$T_{new} = \begin{cases} (1-w_d)* \text{Told} + w_d * \text{loop.} \\ \qquad \text{if loop=0.} \\ (1-w_u)* \text{Told} + w_u * \text{loop.} \\ \qquad \text{If loop=1.} \end{cases} \quad (2)$$

T_{new} is the trust value of a sensor node. The two parameters w_d and w_u allow flexible application requirements. W_d and w_u represent the extent to which upgraded and degraded performance are rewarded and penalized, respectively. So calculating the trust value and energy value of each neighbor node the malicious node can easily identified and routing inside STORM framework can be improved.

4. Results and Discussions

Java network simulator is used for experimental setup. JNS is a tool for simulating network components and resources. But JNS do not run independently it run's with the help of IDE Netbeans and the simulated result shown in Netbeans.

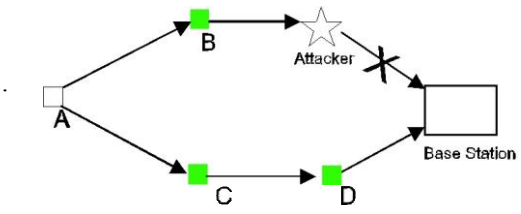

Fig. 2. Illustrate how *Trust-manager* Works.

TrustManager on one node does not take any recommendation from the TrustManager on another node. If an attacker forges false energy report to form a false route, such intention will be defeated by TrustManager: when the TrustManager on one node finds out the many delivery failures from the broadcast messages of the base station, it degrades the trust level of its current next-hop node. TrustManager identities the low trust worthiness of various attackers misdirecting the multihop routing, especially those exploiting the replay of routing information. TrustManager significantly improves data delivery ratio in the existence of attack attempts of preventing data delivery. TrustManager encourages a node to choose another route when its current route frequently fails to deliver data to d the base station

The TrustManager on node A starts to degrade the trust level of its current next-hop node B although node B is absolutely honest. Once that trust level becomes too low, node A decides to select node C as its new next-hop node. In this way, node A identifies a better and successful route (A - C - D - base). Link layer encryption and authentication mechanisms may be reasonable first approximation for defense against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

4.1 Evaluation of Energy Watcher and TrustManager

The energy cost report is the only information that a node is to passively receive. It appears that such acceptance of energy cost report could be a pitfall when an attacker or a compromised node forges false report of its energy cost. The main interest of an attacker is to prevent data delivery rather than to trick a data packet into a less efficient route, considering the effort it takes to launch an attack. As far as an attack aiming at preventing data delivery is concerned, TARF mitigates the effect of this pitfall through the operation of TrustManager. The TrustManager on one node does not take any recommendation from the TrustManager on another node. If an attacker forges false energy report to form a false route, such intention will be defeated by TrustManager: when the TrustManager on one node finds out the many delivery failures from the broadcast messages of the base station, it degrades the trust level of its current next-hop node; when that trust level goes below certain threshold, it causes the node to switch to a more promising next-hop node.

TrustManager identities the low trust worthiness of various attackers misdirecting the multihop routing, especially those exploiting the replay of routing information. It is noteworthy that TrustManager does not distinguish whether an error or an attack occurs to the next-hop node or other succeeding nodes in the route. It seems unfair that TrustManager downgrades the trust level of an honest next-hop node while the attack occurs somewhere after that next-hop node in the route. TrustManager significantly improves data delivery ratio in the existence of attack attempts of preventing data delivery. It is often difficult to identify an attacker who participates in the network using an id "stolen" from another legal node.. With the Link-connectivity protocol [11] each node selects its next-

hop node among its neighborhood table according to a link estimator based on exponentially weighted moving average [12]. The simulation results show, in the presence of misbehaviors, the throughput in TARF is often much higher than that in Link connectivity; the hop-per delivery in the Link-connectivity protocol is generally at least comparable to that in TARF.

4.2 Limitations of secure multi-hop Routing

A multi-hop routing topology around a fixed set of base stations is that those nodes within one or two hops of the base stations are particularly attractive for compromise. After a significant number of these nodes have been compromised, all is lost. After a set of virtual base stations have been selected, a multi-hop topology is constructed using them. The virtual base stations then communicate directly with the real base stations. The set of virtual base stations should be changed frequently enough to make it difficult for adversaries to choose the "right" nodes to compromise.

The main remaining problem is that location information advertised from neighboring nodes must be trusted. A compromised node advertising [13] its location on a line between the targeted node and a base station will guarantee it is the destination for all forwarded packets from that node. Probabilistic selection of a next hop from several acceptable destinations or multipath routing to multiple base stations can help with this problem, but it is not perfect. Restricting the structure of the topology can eliminate the requirement for nodes to advertise their locations if all nodes' locations are well known.

5. Simulation

Emulator of wireless sensor networks on a 3D plane with JNS to test TARF. Initially, 18 nodes are randomly distributed within a 50000 rectangular area, with unreliable wireless transmission. All the nodes have the same power level and the same maximal transmission range of 100 m. Each node samples six times in every period. The timing gap between every two consecutive samplings of the same node is equivalent. Simulate the sensor network in 784 consecutive periods.

The performance of TARF is compared to that of a link connectivity-based routing protocol the link connectivity-based routing protocol as Link connectivity. The simulation results show, in the presence of misbehaviors, the throughput in TARF is often much higher than that in Link connectivity; the hop-per delivery in the Link-connectivity protocol is generally at least comparable to that in TARF. This new implementation integrating TARF requires moderate program storage and memory usage.. The Multihop Oscilloscope application, with certain modified sensing parameters for our later evaluation purpose, periodically makes sensing samples and sends out the sensed data to a root via multiple routing hops.

5.1 Implementation and empirical evaluation

The detection of routing loops and the corresponding reaction are excluded from the implementation of TrustManager since many existing protocols, such as Collection Tree Protocol and the link connectivity-based protocol already provide that feature. the existing protocols provide many nice. Features, such as the analysis of link quality, the loop detection and the routing decision mainly considering the communication cost. Instead of providing those features, implementation focuses on the trust evaluation based on the base broadcast of the data delivery, and such trust information can be easily reused by other protocols.

The TrustManager component in TARF is wrapped into an independent TinyOS configuration named Trust Manager. TrustManager uses a dedicated logic channel for communication and runs as a periodic service with a configurable period, thus not interfering with the application code. Though it is possible to implement TARF with a period always synchronized with the routing protocol's period that would cause much intrusion into the source code of the routing protocol. The Trust Control interface provides the commands to enable and disable the trust evaluation, while the Record interface provides the commands for a root, i.e., a base station, to add delivered message record, for a no root node to add forwarded message record, and for a node to retrieve the trust level of any neighboring node.

6. Conclusion

STORM, a cross-layer protocol framework for wireless ad hoc networks that integrates interest-driven routing with priority-based queuing for traffic management, end-to-end bandwidth reservations controlled by the routing, and distributed transmission scheduling. All these components work together to provide end-to-end delay and bandwidth guarantees to real-time unicast and multicast data flows in multihop wireless networks even when nodes move. Hence proved that the routing meshes established with STORM are loop-free at any time and that the end-to-end reservations established along routing meshes provide bounded delays to real-time data packets. Hence storm didn't concentrate much on the security issues where to overcome this TARF protocol has been corporate with the current protocol to tolerate the dynamic attacks in the network.

7. Future Enhancements

In future, security of Enhance STORM is improved by adding additional modules to the TARF framework, also this TARF module can be integrated into existing routing protocols with the least effort, thus producing secure and efficient fully functional protocols. Thus by enhancing TARF framework by enhancing the modules Adhoc network can able to withstand any attacks. Especially Denial of Service Attack, TARF framework do not address the attack of injecting into the network a number of packet contain false sensing data. If the attacker intends to inject a few packets cause wrong routing, such attack also defended by TARF through Trust-Manager. Module description enable many theoretical relationships with corrected route module help in route identification and incorrect information .If an attacker gave unnecessary

information the protocol inside the framework help to correlate the previous value.

References

[1] Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, pp. 2826-2841, Oct. 2007

[2] L. Bao and J.J. Garcia-Luna-Aceves, "A New Approach to Channel Access Scheduling for Ad Hoc Networks," Proc. AC M Mobile Com,
pp. 210-221, 2001.

[3] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou, "FBSR: Feedback-Based Secure Routing Protocol for Pervasive Computing and Comm., vol. 4,
pp. 61-76, 2008.

[4] E. Carlson, C. Prehofer, C. Bettstetter, H. Karl, and A. Wolisz, "Secure routing in wireless sensor network: Attacks and countermeasures" IEEE J. Selected Areas in Comm., vol. 24, no. 11, pp. 2018-2027, Nov. 2006.

[5] Chang, S. Shieh, W. Lin, and C. Hsieh, "An Efficien t Broadcast Authentication Scheme in Wireless Sensor Networks," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '06), pp. 311-320, 2006.

[6] J. Garcia-Luna-Aceves and Rolando Menchaca-Mendez, "STORM: A Framework For Integrated Routing, Scheduling and Traffic Management in Adhoc network,"

[7] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang, "A Gro up Mobility Model for Ad Hoc Wireless Networks," Proc. ACM/IEEE Secon d Int'l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM '99), pp. 53-60, 1999.

[8] P. Jacquet, A. Laouiti, P. Minet, and L. Viennot, " Multipath Routing in Wireless Sensor Networks: Survey and Research Challenges" Proc. Second IFIP-TC6 Networking Conf., May 2002.

[9] C. Karl of and D. Wagner, "Secure Routing in Wireless Sensor networks Attacks and Countermeasures," Proc. First IEEE Int' l Workshop Sensor Network Protocols and Applications, 2003.

[10] A. Perrig, R. Szewczyk, W. Wen, D. Culler, and J. Tygar, "SPINS: Security Protocols for Sensor Networks," Wireless N etworks J., vol. 8, no. 5, pp. 521-534, Sept. 2002.

[11] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A Link Layer Security Architecture for Wireless Sensor Networks," Proc. ACM Int'l Conf. Embedded Networked Sensor Systems (SenSys '04), Nov. 2004.

[12] Q. Zheng, X. Hong, and S. Ray, "Recent Advances in Mobility Modeling for Mobile Ad Hoc Network Research," Proc. 42nd Ann.Southeast Regional Conf. (ACM-SE 42), pp. 70-75, 2004.

[13] Woo, T. Tong, and D. Culler, "Taming the Underlying Challenges of Reliable Multihop Routing in Sensor Networks," Proc. First ACM Int'l Conf. Embedded Networked Sensor Systems (SenSys '03), Nov. 2003.