IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Enhancement of Network Lifetime in WSN Using Symmetric AES

S.Veevi Fathima[1], Mrs.D.Jacinth Annie Pearlin[2]

[1]M.E, Computer Science and Engineering, S.Veerasamy Chettiar College of Engineering, Puliangudi, Tirunelveli

[2]M.TECH, Assistant Professor, Computer Science and Engineering, S.Veerasamy Chettiar College of Engineering, Puliangudi, Tirunelveli

Abstract

The main objective of this paper is to enhance the life time of the wireless sensor network. In a wireless sensor network (WSN), the area around the Sink forms a bottleneck zone where the traffic flow is maxi-mum. Thus, the lifetime of the WSN network is dictated by the lifetime of the bottleneck zone. It has been observed that there is a reduction in energy consumption in the bottleneck zone with the proposed approach. This in-turn will lead to increase in network lifetime. Although, packet latency is high for low node density but with increase of node density the proposed approach has significantly low latency than forwarding without network coding in a duty cycled WSN. A significant improvement in packet delivery ratio has been achieved with the proposed network coding approach.

Index Terms— *WSN, Qos, ALERT, MAC Protocol, Duty Cycle*

1.INTRODUCTION

Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes that are small in size and communicate unmetered in short distances. These tiny sensor nodes, which consist of sensing, data processing, and communicating components, leverage the idea of sensor networks based on collaborative effort of a large number of nodes. Sensor networks represent a significant improvement over traditional sensors, which are deployed in the following two ways: Sensors can be positioned far from the actual phenomenon, i.e., something known by sense perception. In this approach, large sensors that use some complex techniques to distinguish the targets from environmental noise are required.

Several sensors that perform only sensing can be deployed. The positions of the sensors and communications topology are carefully engineered. They transmit time series of the sensed phenomenon to the central nodes where computations are performed and data are fused. A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

The above described features ensure a wide range of applications for sensor networks. Some of the application areas are health, military, and security. For example, the physiological data about a patient can be monitored remotely by a doctor. While this is more convenient for the patient, it also allows the doctor to better understand the patient's current condition. Sensor networks can also be used to detect foreign chemical agents in the air and the water. They can help to identify the type, concentration, and location of pollutants. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. It is envisioned that, in future, wireless sensor networks will be an integral part of our lives, more so than the present-day personal computers.

Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks are outlined below: The number of sensor nodes in a sensor net-work can be several orders of magnitude higher than the nodes in an ad hoc network. Sensor nodes are densely deployed. Sensor nodes are prone to failures. The topology of a sensor network changes very frequently. Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications. Sensor nodes are limited in power, computational capacities, and memory.

Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors. Since large numbers of sensor nodes are densely deployed, neighbor nodes may be very close to each other. Hence, multihop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations. Multihop communication can also effectively overcome some of the signal propagation effects experienced in long-distance wireless communication. One of the most important constraints on sensor nodes is the low power consumption requirement.

Sensor nodes carry limited, generally irreplaceable, power sources. Therefore, while traditional net-works aim to achieve high quality of service (QoS) provisions, sensor network protocols must focus primarily on power conservation. They must have inbuilt trade-off mechanisms that give the end user the option of prolonging network lifetime at the cost of lower throughput or higher transmission delay.

Many researchers are currently engaged in developing schemes that fulfill these requirements. In this paper, a survey of protocols and algorithms proposed thus far for sensor networks is proposed in this paper. The aim is to provide a better understanding of the current research issues in this field. An investigation into pertaining design constraints and outline the use of certain tools to meet the design objectives is also attempted.

Some environmental applications of sensor networks include tracking the movements of birds, small animals, and insects; monitoring environmental conditions that affect crops and livestock; irrigation; macroinstruments for large-scale Earth monitoring and planetary exploration; chemical/ biological detection; precision agriculture; biological, Earth, and environmental monitoring in ma-rine, soil, and atmospheric contexts; forest fire detection; meteorological or geophysical research; flood detection; bio-complexity mapping of the environment; and pollution study.

Forest fire detection: Since sensor nodes may be strategically, randomly, and densely deployed in a forest, sensor nodes can relay the exact origin of the fire to the end users before the fire is spread uncontrollable. Millions of sensor nodes can be deployed and integrated using radio frequencies/ optical systems. Also, they may be equipped with effective power scavenging methods , such as solar cells, because the sensors may be left unat-tended for months and even years. The sensor nodes will collaborate with each other to perform distributed sensing and overcome obstacles, such astrees and rocks, that block wired sensors'line of sight.

Biocomplexity mapping of the environment:

A biocomplexity mapping of the environment re-quires sophisticated approaches to integrate in-formation across temporal and spatial scales. The advances of technology in the remote sensing and automated data collection have enabled higher spatial, spectral, and temporal resolution at a geometrically declining cost per unit area. Along with these advances, the sensor nodes also have the ability to connect with the Internet, which allows remote users to control, monitor and observe the biocomplexity of the environment.

Although satellite and airborne sensors are useful in observing large biodiversity, e.g., spatial complexity of dominant plant species, they are not fine grain enough to observe small size biodiversity, which makes up most of the biodiversity in an ecosystem. As a result, there is a need for ground level deployment of wireless sensor nodes to observe the biocomplexity. One example of biocomplexity mapping of the environment is done at the James Reserve in Southern California. Three monitoring grids with each having 25–100 sensor nodes will be implemented for fixed view multimedia and environmental sensor data loggers.

Flood detection: An example of flood detection is the ALERT system deployed in the US. Several types of sensors deployed in the ALERT system are rainfall, water level and weather sensors. These sensors supply information to the centralized database system in a pre-defined way. Research projects, such as the COUGAR Device Database Project at Cornell University and the Data Space project at Rutgers , are investigating distributed approaches in interacting with sensor nodes in the sensor field to provide snapshot and long-running queries. Precision Agriculture: Some of the benefits is the ability to monitor the pesticides level in the drinking water, the level of soil erosion, and the level of air pollution in real-time.

Health applications: Some of the health applications for sensor net-works are providing interfaces for the disabled; integrated patient monitoring; diagnostics; drug administration in hospitals; monitoring the movements and internal processes of insects or other small animals; tele monitoring of human physiological data; and tracking and monitoring doctors and patients inside a hospital.

Telemonitoring of human physiological data: The physiological data collected by the sensor net-works can be stored for a long period of time, and can be used for medical exploration. The installed sensor networks can also monitor and detect elderly people's behavior, e.g., a fall. These small sensor nodes allow the subject a relater freedom of movement and allow doctors to identify pre-defined symptoms earlier . Also, they facilitate a higher quality of life for the subjects compared to the treatment centers . A ''Health Smart Home'' is designed in the Faculty of Medicine in Grenoble —France to validate the feasibility of such system. Tracking and monitoring doctors and patients inside a hospital: Each patient has small and light weight

sensor nodes attached to them. Each sensor node has its specific task. For example, one sensor node may be detecting the heart rate while another is detecting the blood pressure. Doctors may also carry a sensor node, which allows other doctors to locate them within the hospital. Drug administration in hospitals: If sensor nodes can be attached to medications, the chance of getting and prescribing the wrong medication to patients can be minimized. Because, patients will have sensor nodes that identify their allergies and required medications. Computerized systems as described have shown that they can help minimize adverse drug events.

Previously proposed sensor network data dissemination schemes require periodic low-rate flooding of data in order to allow recovery from failure. Here two kinds of multi paths is considered to enable energy efficient recovery from failure of the shortest path between source and sink. Disjoint multipath has been studied in the literature. a novel braided multipath scheme is proposed, which results in several partially disjoint multipath schemes. It is found that braided multipaths are a viable alternative for energy-efficient recovery from isolated and patterned failures.

A new class of problems called network information flow is introduced which is inspired by computer network applications. Consider a point-to-point communication network on which a number of information sources are to be mulitcast to certain sets of destinations. It is assumed that the information sources are mutually independent. The problem is to characterize the admissible coding rate region. This model subsumes all previously studied models along the same line. In this paper, the problem with one information source, and we have obtained a simple characterization of the admissible coding rate region are studied. Our result can be regarded as the Max-flow Min-cut Theorem for network information flow. Contrary to one's intuition, our work reveals that it is in general not optimal to regard the information to be multicast as a "fluid" which can simply be routed or replicated. Rather, by employing coding at the nodes, which referred to as network is coding, bandwidth can in general be saved. This finding may have significant impact on future design of switching systems.

A capacity-achieving coding scheme for unicast or multicast over lossy packet networks is presented. In the scheme, intermediate nodes perform additional coding yet do not decode nor even wait for a block of packets before sending out coded packets. Rather, whenever they have a transmission opportunity, they send out coded packets formed from random linear combinations of previously received packets. All coding and decoding operations have polynomial complexity.

It shows that the scheme is capacity-achieving as long as packets received on a link arrive according to a process that has an average rate. Thus, packet losses on a link may exhibit correlation in time or with losses on other links. In the special case of Poisson traffic with losses, an error exponents is given that quantify the rate of decay of the probability of error with coding delay. Our analysis of the scheme shows that it is not only capacity-achieving, but that the propagation of packets carrying "innovative" information follows the propagation of jobs through a queuing network, and therefore fluid flow models yield good approximations. Networks with both lossy point-to-point and broadcast links are considered, allowing us to model both wired and wireless packet networks.

II. PROPOSED SYSTEM

The sensor nodes are usually scattered in a sensor field as shown in Fig. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink and the end users. Data are routed back to the end user by a multi hop infrastructure less architecture through the sink. The sink may communicate with the task manager node via Internet or Satellite. The protocol stack used by the sink and all sensor nodes is given. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the application layer, transport layer , network layer, data link layer , physical layer , power management plane , mobility management plane, and task management plane. Depending on the sensing tasks, different types of application software can be built and used on the application layer. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer. Since the environment is noisy and sensor nodes can be mobile, the MAC protocol must be power aware and able to minimize collision with neighbors' broadcast. The physical layer addresses the needs of a simple but robust modulation, transmission and receiving techniques. In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall power consumption.

The power management plane manages how a sensor node uses its power. For example, the sensor node may turn off its receiver after receiving a message from one of its neighbors. This is to avoid getting duplicated messages. Also, when the power level of the sensor node is low, the sensor node broadcasts to its neighbors that it is low in power and cannot participate in routing messages. The remaining power is reserved for sensing.

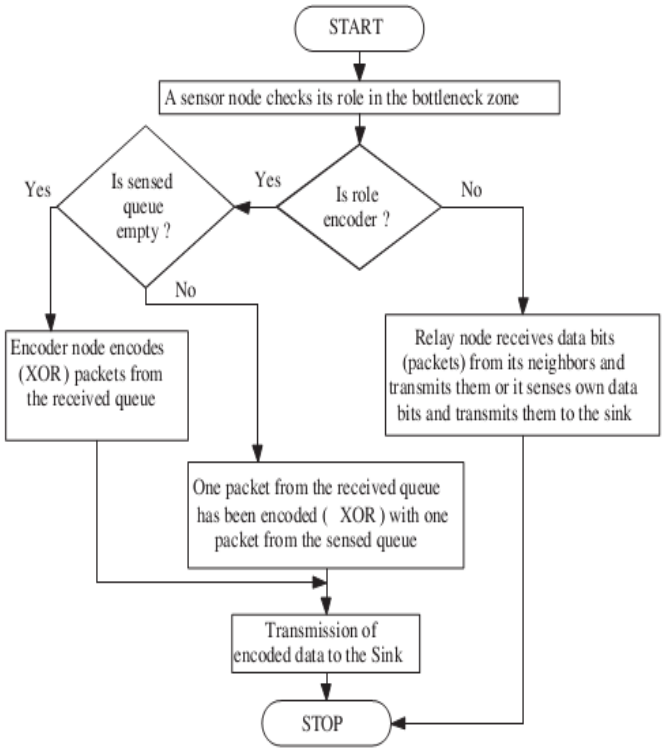

Fig 1 Flow Diagram of the Proposed System

The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes. By knowing who the neighbor sensor nodes are, the sensor nodes can balance their power and task usage. The task management plane balances and schedules the sensing tasks given to a specific region. Not all sensor nodes in that region are required to perform the sensing task at the same time. As a result, some sensor nodes perform the task more than the others depending on their power level. These management planes are needed, so that sensor nodes can work together in a power efficient way, route data in a mobile sensor net-work, and share resources between sensor nodes. Without them, each sensor node will just work individually. From the whole sensor network standpoint, it is more efficient if sensor nodes can collaborate with each other, so the lifetime of the sensor networks can be prolonged.

The network coding technique improves the capacity of an information network with better utilization of bandwidth. In a multi-hop communication with network coding ,the intermediate nodes of a network can appropriately encode the incoming data packets before forwarding the coded packets to the next node. The network coding technique also improves reliability of the network. .A network coding based communication paradigm in the bottle-neck zone has been proposed to reduce the traffic load which enhances the network lifetime. The major contributions of this work can be summarized as follows: The network lifetime through bottleneck zone analysis in (a) random duty-cycled WSN
(b) non-duty cycled WSN using network coding in the bottleneck zone (c) random duty-cycled WSN using network coding in the bottleneck zone.

It has been shown that the duty cycle and network coding techniques can be integrated to utilize the network resources efficiently. The energy consumption in the bottleneck zone has been reduced to improve the lifetime of the overall WSN. Simulations have been carried out to show the efficacy of the proposed approach in terms of network lifetime, packet delivery ratio and packet latency.

WSN Establishment

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring.

Duty Cycle

The ratio between the time during which a sensor node is in active state and the total time of active/dormant states is called duty cycle. The duty cycle depends on the node density of the monitored area for better coverage and connectivity. Usually for a dense WSN the duty cycle of a node is very low.

Network Coding

Network coding is a technique which allows the intermediate nodes to encode data packets received from its neighboring nodes in a network.

Encoding Operation

A node, that wants to transmit encoded packets, chooses a sequence of coefficients =(q1,q2, ...,qn), called encoding vector, from GF(2s).A set of n packets Gi(i=1,2,3,4, ..., n)that are received at a node are linearly encoded into a single output packet.

Decoding Operation

A receiver node solves a set of linear equations to retrieve the original packets from the received coded packets. The encoding vector q is received by the receiver sensor nodes with the encoded data. Let, a set(q1,Y1), ...,(qm,Ym) has been received by a node. The symbols Yj and qj denote the information symbol and the coding vector for the jth received packet respectively.

Network Lifetime

The density property of the WSNs it is possible to enhance the network life time and also efficiently balance the energy consumption load across the network Lifetime maximization: Energy/Power Consumption of the sensing device should be minimized and sensor nodes should be energy efficient since their limited energy resource determines their lifetime. To conserve power the node should shut off the radio power supply when not in use.

Performance Analysis

Performance analysis involves gathering formal and informal data to help customers and sponsors define and achieve their goals. Performance analysis uncovers several perspectives on a problem or opportunity, determining any and all drivers towards or barriers to successful performance, and proposing a solution system based on what is discovered. Performance analysis is the front end of the front end. Some synonyms are planning, scoping, auditing, and diagnostics.

Symmetric Key AES algorithm

For the security purpose we can use these Symmetric AES(Advanced Encryption Standard) Algorithm. Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.[1] This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to encryption. This is also known as private key encryption.

Types of Symmetric Key AES algorithm

Symmetric-key encryption can use either stream ciphers or block ciphers. (i) Stream ciphers encrypt the digits (typically bytes) of a message one at a time, (ii) Block ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the block size. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm approved by NIST in December 2001 uses 128-bit blocks.

Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemenand Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

ALGORITHM 1

PacketProcess(Pi) : Packet processing
at a node inside the network coding layer
Require: Packet transmission and reception starts, received packets inserted
into the RecvQueue()
Ensure: Encoded packet transmitted or discarded
1. Pick a packet Pi from RecvQueue(Pi)
2. If Packet Pi ∈ ForwardPacketSet(Pi) exit;
3. If Node n ∈ EncoderNodeSet() continue;
4. If native(Pi) then
5. CN =XorEncode();
6. Node n transmits the coded packet CN to Sink
7. Insert the processed packet Pi to ForwardPacketSet();
8. else
9 Discard(Pi);
10 endif
10. else
11. Node n acts as relay and transmits the packet Pi to the *Sink;*
12. endif
13. endif
14. If (RecvQueue() _= empty)
15. goto step 1;
16. else exit;
17. endif

ALGORITHM 2

XorEncode() : Encoding algorithm
Require: A received queue RecvQueue() and a sensed queue SensQueue() is maintained at an encoder node
Ensure: Generation of network coded packet CN
1. If SensQueue() is not empty then continue;
2. Pick a packet Pi from head of the RecvQueue();
3. Pick a packet Pj from head of the SensQueue();
4. CN = Pi ⊕ Pj ;
5. else
6. Pick next packet Pi+1 from the RecvQueue();
7. CN = Pi ⊕ Pi+1;
10. endif;
11. return CN

III. Conclusion and Future Work

In a wireless sensor network (WSN), the area around the Sink forms a bottleneck zone where the traffic flow is maximum. Thus, the lifetime of the WSN network is dictated by the lifetime of the bottleneck zone. The lifetime upper bounds have been estimated with (i) duty cycle, (ii) network coding and (iii) combinations of duty cycle and network coding. It has been observed that there is a reduction in energy consumption in the bottleneck zone with the proposed approach. This in-turn will lead to increase in network lifetime. A significant improvement in packet delivery ratio has been achieved with the proposed network coding approach. Although, packet latency is high for low node density but with increase of node density the proposed approach has significantly low latency than forwarding without network coding in a duty cycled WSN.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey,"Computer Networks, vol. 38, no. 4, pp. 393– 422, 2002.
[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, no. 12, pp. 2292–2330, 2008.
[3] C. F. Hsin and M. Liu, "Randomly duty-cycled wireless sensor networks: dynamic of coverage,"IEEE Trans. Wireless Commun.,vol.5,no.11, pp. 3182–3192, 2006.
[4] X. Y. Wang, R. K. Dokania, and A. Apsel, "PCO-based synchronization for cognitive duty-cycled impulse radio sensor networks,"IEEE Sensors J., vol. 11, no. 3, pp. 555–563, 2011.
[5] Q. Wang and T. Zhang, "Bottleneck zone analysis in energy-constrained wireless sensor networks,"IEEE Commun. Lett., vol. 13, no. 6, pp. 423– 425, June 2009.
[6] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," ACM SIGMOBILE Mobile Computing and Commun. Rev., vol. 5, no. 4, pp. 11–25, 2001.
[7] R. Ahlswede, N. Cai, S. Y. R. Li, and R. Yeung, "Network information flow,"IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, July 2000.
[8] O. M. Al-Kofahi and A. E. Kamal, "Network coding-based protection of many-to-one wireless flows,"IEEE J. Sel. Areas Commun.,vol. 27, no. 5, pp. 797–813, 2009.
[9] S.-Y. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, 2003.
[10] S. Lee and S. H. Lee, "Analysis of network lifetime in cluster-based sensor networks," IEEE Commun. Lett., vol. 14, no. 10, pp. 900–902, 2010.
[11] M. Bhardwaj, T. Garnett, and A. Chandrakasan, "Upper bounds on the lifetime of sensor networks," in Proc. 2001 IEEE ICC, pp. 785–790.
[12] H. Zhang and J. C. Hou, "On the upper bound ofα−lifetime for large sensor networks," ACMTrans.Sen.Netw., vol. 1, no. 2, pp. 272–300,2005.
[13] H. R. Karkvandi, E. Pecht, and O. Y. Pecht, "Effective lifetime-awarerouting in wireless sensor networks," *IEEE Sensors J.*, vol. 11, no. 12,pp. 3359–3367, 2011.
[14] F. Wang and J. Liu, "RBS: a reliable broadcast service for large-scalelow duty-cycled wireless sensor networks," in *Proc. 2008 IEEE ICC*,pp. 2416–2420.
[15] Y. Gu, T. Zhu, and T. He, "ESC: Energy synchronized communication insustainable sensor networks," in *Proc. 2009 IEEE Int. Conf. on NetworkProtocols*, pp. 52–62.
[16] S. Lai and B. Ravindran, "Efficient oppertunistic broadcasting over dutycycledwireless sensor networks," in *Proc. 2010 IEEE INFOCOM*, pp.1–2
[17] D. Lun, M. Medard, R. Koetter, and M. Effros, "On coding for reliablecommunication over packet networks," *Physical Commun.*, vol. 1, pp.3–20, 2008.
[18] R. R. Rout, S. K. Ghosh, and S. Chakrabarti, "A network coding basedprobabilistic routing scheme for wireless sensor network," in *Proc. 2010 Int. Conf. on Wireless Communication and Sensor Networks*, pp. 27–32.
[19] S. Yang and J. Wu, "Efficient broadcasting using network coding and directional antennas in MANETs," *IEEE Trans. Parallel Distrib. Syst.*,vol. 21, no. 2, pp. 148–161, 2010.
[20] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.