2581-4575

International Journal For Recent Developments in Science & Technology

Crossref

A Peer Reviewed Research Journal

DYNAMIC ROUTING FOR DATA INTEGRITY AND DELAY DIFFERENTIATED SERVICES IN WIRELESS SENSOR NETWORKS

N.SANGEETA[1] & K. LAKSHMI[2]

[1]Assistante Professor, Department of Electronics and Communication Engineering, Narsimha Reddy College of Engineering, Hyderabad, T. S., India

[2]Associate Professor, Department of Electronics and Communication Engineering, Narsimha Reddy College of Engineering, Hyderabad, T. S., India

E-Mail ID: sangeetha@nrcmec.org ,K.Lakshmi@nrcmec.org

ABSTRACT

Applications running on the same Wireless Sensor Network (WSN) platform usually have different Quality of Service (QoS) requirements. The major networking performance parameters are lowering delay and high data integrity and data security. However, in most situations, these three requirements cannot be satisfied simultaneously. In this paper, based on the concept of material science, i propose IDDR and Diffie Hellman, IDDR is a multi-path dynamic routing algorithm, to resolve this conflict. By constructing a virtual hybrid potential field, IDDR separates packets of applications with different QoS requirements according to the weight assigned to each packet, and routes them towards the sink through different paths to improve the data fidelity for integrity-sensitive applications as well as reduce the end-to-end delay for delay-sensitive ones. Diffie Hellman is used for distributing key from sink to all for increasing data security; i prove the IDDR plus Diffie Hellman are stable for above requirements. Simulation results demonstrate that a proposed technique provides extended performance for data integrity and delay differentiated services with prolonged network lifetime

Keywords: QOS,N IDDR, WSN, ROUTING, VIRTUAL HYBRID POTENTIAL

1. INTRODUCTION

1.1 Domain Introduction

Dynamic Routing mechanisms in the Internet have normally has based on shortest-path routing for best traffic effort. This causes traffic congestion, particularly if bottleneck joins on the shortest path surely restrict the effective bandwidth between the source and the destination. Dynamic routing means building up the routing efficient when source sent the root request that time follow the packet delivery ratio, IDDR protocol . WSNs, which are utilized to senses the physical elements in the area, will play an important role in the next generation networks. Due to the diversity and complexity of applications running over WSNs and the QoS ensure in such increasing the networks gains consideration in the research community. As a one of the part of a data base, WSNs should be able to support different applications over the same platform. Different applications may have different QoS necessities. WSNs have two essential QoS prerequisites low delay and high data integrity, in a system with light

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


load, both necessities can be promptly fulfilled. However, a heavily loaded network will suffer congestion, and then expands end-to-end delay. Wireless Sensor network is the vibrant and emerging research area in the field of system due to its expanding application over the whole globe. Some of its application fields are zone observation, home security, brilliant spaces, natural checking, and target tracking.

Wireless Sensor Network comprises of sensor hubs that will be distributed in offered region to sense or screen the physical or natural conditions like Temperature, Pressure, and Sound and so on. A distributed system is a system in which parts situated on networked computers communicate and facilitate their activities by passing messages. There are two types of distributed networks; Dense Network and Sparse Network. A dense system is a system in which the quantity of connections of every hub is near the most extreme number of hubs. A sparse network, by complexity, is associated by a low number of connections only. Sensor Network under consideration are those systems that are densely distributed.

These sensor hubs sense the nature and collect the data. These collected data will be transmitted to the destination utilizing wireless means Sensor hubs are only hubs which is comprised of radio handset, Micro-Controller and Battery. Radio Transceiver comprises of an inherent receiving in antenna or an externally connected antenna. Small scale Controller is the one that will interface between the energy source and sensing device. Now the third component is the energy source, usually battery is used as a energy source to sensor hubs. Since these sensor hubs are conveyed over remote areas, furthermore these sensor hubs are generally by little battery and also frequent recharging of battery is also not possible.

1.2 Problem Statement

1.2.1 IDDR

We get the idea of potential field from the control of material science and configuration a novel potential based routing algorithm, which is called integrity and delay differentiated routing (IDDR). IDDR is able to provide the following two functions.

A. Improve fidelity for high-integrity applications

The fundamental idea is to find as much buffer space as could be expected from the idle and/or under-loaded paths to cache the excessive packets that might be dropped on the shortest path. Therefore, the first task is to find out the idle and/or under loaded paths, then the second task is to cache the bundles efficiently for subsequent transmission. IDDR develops a potential field to the depth1 and line length data to find the underutilized ways. The bundles with high integrity requirement will be forwarded to the next hop with smaller queue length.

B. Decrease end-to-end delay for delay-sensitive applications

Every application is assigned a weight, which represents the degree of sensitivity to the delay. Through building nearby dynamic potential fields with various slopes indicated by weight values carried by packets, IDDR allows the packets with larger weight to

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


choose shorter paths. In addition, IDDR also employs the priority queue to further decrease the queuing delay of delay-sensitive packets.

C. IDDR inherently avoids the conflict between high integrity and low delay

The high-integrity packets are cached on the under loaded paths along which packets will endure a huge end-to-end delay due to more hops and the delay-sensitive packets travel along shorter paths to approach the sink as soon as possible.

2. DIFFIE-HELLMAN

Diffie–Hellman is a particular strategy for Generation keys. It is one of the most punctual reasonable cases of key Generation executed inside the field of cryptography. The Diffie–Hellman key Generation technique permits two gatherings that have no earlier learning of each other to mutually build up a common secret key over an insecure communications channel. This key can then be utilized to encrypt subsequent communications utilizing a symmetric key cipher. This scheme was first distributed by Whitfield Diffie and Martin Hellman in 1976, although it had been separately invented a few years earlier within GCHQ, the British signs knowledge office, by James H. Ellis, Clifford Cocks and Malcolm J. Williamson yet was kept arranged. Despite the fact that Diffie–Hellman key agreement itself is an a mysterious key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's vaporous models This method was followed short time later by RSA ,an implementation of public key cryptography utilizing asymmetric algorithms.

The framework has following gotten to be known as Diffie–Hellman key Generation. While that framework was initially depicted in a paper by Diffie and me, it is an open key dispersion framework; an idea created by Markel, and hence should be called 'Diffie–Hellman–Merkle key Generation „if names are to be connected with it. I hope this small pulpit might help in that attempt to perceive Markel‟s equal contribution to the invention of open key cryptography.

Diffie–Hellman builds up a common secret that can be utilized for secret communications while Generation data over a an open system.. The following diagram represents the general idea of the key Generation by utilizing colors instead of a very large number. Diffie-Hellman is very secure, the keying material is set as the output of a key-derivation function that maps the secret value to the (bit-string) keys of the symmetric algorithms .The Diffie-Hellman (DH) key generation, as well as some generalizations, were initially designed to protect against a passive adversary that only eavesdrops on messages. However, when it comes to implement these schemes in a dispersed system‟s security architecture a much stronger adversary must be taken into account. Hackers have a great lot of control over our Internet communications.

2.1 Caesar Ciphers

Cryptography and encryption/decryption techniques fall into two general classifications symmetric and open key. In

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

symmetric cryptography, In symmetric cryptography, here and there called traditional cryptography, Therefore, before utilizing a symmetric cryptography system, the users must somehow come to an agreement on a key to use. An obvious problem arises when the parties are separated by large distances which are common place in today‟s worldwide digital communications. If the parties did not meet prior to their separation, They could send a trusted courier to exchange keys, however that is not achievable, if time is a critical factor in their communication. The problem of securely distributing keys used in symmetric ciphers has challenged cryptographers for many years.

Caesar's cipher, to which reference was made in the David Kahn quote toward the start of this area, was a straightforward substitution figure, but it had a memorable key. For Caesar's cipher, "letters were replaced by letters standing three places further down the alphabet," Here is the key to Caesar‟s cipher.

Plaintext letters
abcdefghijklmnopqrstuvwxyz
Cipher text letters
DEFGHIJKLMNOPQRSTUVWXYZABC

The key can be memorized because there is a pattern to it the cipher text alphabet is just the plaintext alphabet moved to the right three places. Sender and receiver just need to remember the movement obviously, different movements could be utilized. All such move, or interpretation, ciphers are now presently called Caesar ciphers. Here is the plaintext/cipher text correspondence for a Caesar cipher.

Plaintext letters
abcdefghijklmnopqrstuvwxyz
Cipher text letters
IJKLMNOPQRSTUVWXYZABCDEFGH

For each of these ciphers, the technique for encryption is the Caesar cipher and the key is the shift. Knowing the key, the sender and receiver can make the plaintext/cipher text correspondence as required. There is no need to keep a written copy of the plaintext/cipher text correspondence in this manner; key security is less of an issue than it is for the more general simple substitution cipher.

Throughout the years, cryptographers have made disk or slide devices to show the plaintext/cipher text correspondence for use when encrypting and decrypting. The Italian cryptologist Leon Battista Alberti (1404 – 1472), who is known as the Father of Western Cryptology, built up a cipher disk.

The disk that is shown has the letters in the cells in the typical request. Sender and receiver must agree which circle corresponds to plaintext and which circle corresponds to cipher text. The disk that is pictured has cipher text on the littler circle and plaintext on the bigger circle. The disk has been set to Caesar‟s original cipher.

Thinking about the cipher text alphabet "turning round to bite its tail" Caesar ciphers are sometimes called rotation ciphers. Unfortunately, Caesar ciphers have a little key space, and messages encoded with Caesar ciphers can be easily broken by brute

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


force if it is recognized that the message has been encrypted with a Caesar cipher.

2.2 Objectives

- Reducing end to end delay.
- Increasing overall performance of the network.
- Achieving high packet deliver ratio.
- Probability of security.
- Routing Overhead.

3. LITERATURE SURVEY

Before we start developing the project we should have a complex idea abt the project. In order to get detailed abt the project we carry out the literature survey. We do complex survey on the project, we can examine the background of the present plan which supports to discover faults in the existing schemes and monitors us are the unresolved problem‟s and which can be sold out.so, the following area not only the background of the projects and defects which motivated us to propose a new solution and work on this application.

Paper 1: Accurate and scalable simulation of entire TinyOS applications

Author: P. Levis, N. Lee, M. Welsh, and D. Culler (2003)

Accurate and scalable simulation has historically been a key enabling factor for systems research. We present TOSSIM, a simulator for TinyOS wireless sensor networks. By exploiting the sensor network domain and TinyOS‟s design, TOSSIM can capture network behavior at a high fidelity while scaling to thousands of nodes. By using a probabilistic bit error model for the network, TOSSIM remains simple and efficient, but expressive enough to capture a wide range of network interactions. Using TOSSIM, we have discovered several bugs in TinyOS, ranging from network bit level MAC interactions to queue overflows in an ad-hoc routing protocol. Through these and other evaluations, we show that detailed, scalable sensor network simulation is possible.

Paper 2: QoS routing performance in multihop multimedia wireless networks

Author: T. Chen, J. Tsai, and M. Gerla (1997)

In this paper, we propose an approach to QoS (Quality of Service) routing in a multimedia, multi hop, wireless network. The wireless net can be either stand alone, or connected to the wired net. The main focus of the paper is the QoS routing procedure which can inform the source of the bandwidth and quality of service available to any destination in the wireless network. This knowledge enables the establishment of QoS connections within the wireless network and the efficient support of real time, multimedia traffic. In addition, it enables more effective call acceptance control. In the case of ATM interconnection, QoS information permits to extend the ATM virtual circuit service to the wireless network, with possible renegotiation of QoS parameters at the gateway. Simulation experiments show the efficiency of QoS routing in selected multi hop, mobile radio network scenarios.

Paper 3: Core extraction distributed ad hoc routing algorithm

Author: R. Sivakumar, P. Sinha, and V. Bharghavan (Aug 1999)

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal


In this paper, we present CEDAR, a Core-Extraction Distributed Ad hoc Routing algorithm for QoS routing in ad hoc network environments. CEDAR has three key components: (a) the establishment and maintenance of a self-organizing routing infrastructure called the core for performing route computations, (b) the propagation of the link-state of high-bandwidth and stable links in the core through increase/decrease waves, and (c) a QoS route computation algorithm that is executed at the core nodes using only locally available state. Our performance evaluations show that CEDAR is a robust and adaptive QoS routing algorithm that reacts quickly and effectively to the dynamics of the network while still approximating link-state performance for stable networks.

Paper 4: Distributed quality-of-service routing in ad hoc networks

Author: S. Chen and K. Nahrstedt (Aug 1999)

In an ad hoc network, all communication is done over wireless media, typically by radio through the air, without the help of wired base stations. Since direct communication is allowed only between adjacent nodes, distant nodes communicate over multiple hops. The quality-of-service (QoS) routing in an ad hoc network is difficult because the network topology may change constantly, and the available state information for routing is inherently imprecise. In this paper, we propose a distributed QoS routing scheme that selects a network path with sufficient resources to satisfy a certain delay (or bandwidth) requirement in a dynamic multi hop mobile environment. The proposed algorithms work with imprecise state information. Multiple paths are searched in parallel to find the most qualified one. Fault tolerance techniques are brought in for the maintenance of the routing paths when the nodes move, join, or leave the network. Our algorithms consider not only the QoS requirement, but also the cost optimality of the routingpath to improve the overall network performance. Extensive simulations show that high call admission ratio and low-cost paths are achieved with modest routing overhead. The algorithms can tolerate a high degree of information imprecision.

Paper 5: Achieving real-time guarantees in mobile ad hoc wireless networks

Author: B. Hughes and V. Cahill (2003)

Timely wireless communication is essential to allow real-time mobile applications, such as communication between mobile robots or inter-vehicle communication to be realized. The real-time event-based communication paradigm has been recognized as an appropriate high level communication scheme to connect autonomous components in large distributed control systems. We investigate whether real-time event constraints can be guaranteed in a mobile ad hoc wireless network. In this work in progress paper we present our analysis of the impact of mobile ad hoc wireless networks on achieving real-time guarantees. We introduce our ongoing work on the use of a proactive routing and resource reservation protocol using mobility awareness and prediction to reduce the unpredictability of a dynamic mobile ad hoc wireless network.

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

Paper 6: MMSPEED: Multipath Multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks

Author: E. Felemban, C.-G. Lee, and E. Ekici (Jun 2003)

In this paper, we present a novel packet delivery mechanism called Multi-path and Multi-Speed Routing Protocol (MMSPEED) for probabilistic QoS guarantee in wireless sensor networks. The QoS provisioning is performed in two quality domains, namely, timeliness and reliability. Multiple QoS levels are provided in the timeliness domain by guaranteeing multiple packet delivery speed options. In the reliability domain, various reliability requirements are supported by probabilistic multipath forwarding. All these for QoS provisioning are realized in a localized way without global network information by employing localized geographic packet forwarding augmented with dynamic compensation, which compensates the local decision inaccuracy as a packet travels towards its destination. This way, MMSPEED can guarantee end-to-end requirements in a localized way, which is desirable for scalability and adaptability to large scale dynamic sensor networks. Simulation results show that MMSPEED provides QoS differentiation in both reliability and timeliness domains and, as a result, significantly improves the effective capacity of a sensor network in terms of number of flows that meet both reliability and timeliness requirements.

Paper 7:Real-Time Communication Architecture for large-Scale wireless sensor networks

Author: C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He (2002)

Large-scale wireless sensor networks represent a new generation of real-time embedded systems with significantly different communication constraints from traditional networked systems. This paper presents RAP, new real-time communication architecture for large-scale sensor networks. RAP provides convenient, high-level query and event services for distributed micro-sensing applications. Novel location-addressed communication models are supported by a scalable and light-weight network stack. We present and evaluate a new packet scheduling policy called velocity monotonic scheduling that inherently accounts for both time and distance constraints. We show that this policy is particularly suitable for communication scheduling in sensor networks in which a large number of wireless devices are seamlessly integrated into a physical space to perform real-time monitoring and control. Detailed simulations of representative sensor network environments demonstrate that RAP significantly reduces the end-to-end deadline miss ratio in the sensor network.

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

4. METHODOLOGY

4.1. System Architecture

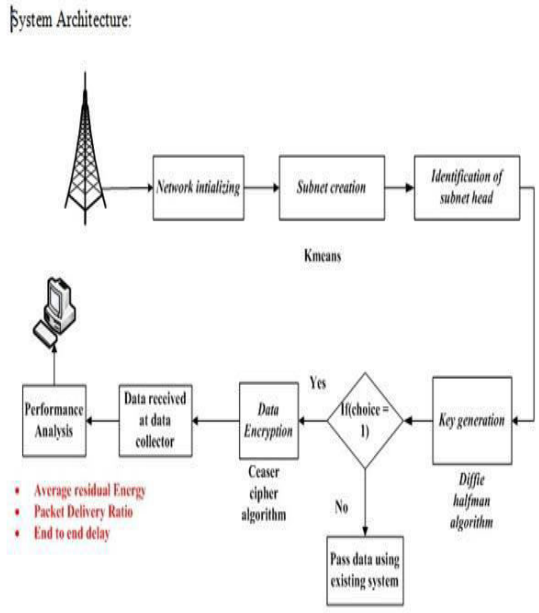

Figure 1. System Architecture

Module Description:

1. Network Initialization

Here Network can be instated with some number of centers say (N =20), close by the zone of 100*100, center can be depicted using xloc and yloc with early on center properties, here starting essentialness of the center point is 100j, moreover center points can be perceived using Unique identity number and work can be done on 802_11 Mac type with random waypoint mobility Model. (This is created the network).

2. Subnet creation

The Main Objective of the project is to provide better service for delay reduction and prolonged network lifetime for reduction in energy consumption, here by using k-means techniques for sub network creation it's possible to assign different cluster heads based on network.

3. Key Generation

Security is an most valuable parameter for networking, because of relay node selection while transmitting data from source to destination, here for key generation Diffie Hellman algorithm is used for secured data. The Diffie-Hellman protocol is a method for two computer users to generate a shared private key with which they can then exchange information across an insecure channel, before receiving data authentication can be done from destination nodes.

4. Data transmission

After applying security algorithms, next step is to transmit data from source to destination, here based on distance network can be chosen for all users, and data transmitted one after the another based on authentication, if users found to be unknown, for the proposed scheme, we are denying to access the data, data received only in case of successful authentication.

5. Performance analysis

Here based on network performance the following networking performance parameters can be measured, that is routing overhead, probability of security, average delay and packet delivery ratio, and improvements can done for all parameters by choosing an efficient techniques, hence increased network lifetime of the network.

Data Flow Diagram

1. The Data Flow Diagram is moreover called as air pocket diagram. It is a fundamental graphical formalism that can be utilized to address a framework regarding data to the

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

structure, unmistakable taking care of did on this data and the yield data is delivered by this framework.

2. The Data Flow Diagram is a champion amongst the most demonstrating devices. It is utilized to demonstrate the framework areas. These segments are the framework procedure, the data utilized by the strategy, an outside component that interfaces with the structure and the information streams in the framework.
3. Data Flow Diagram demonstrates how the information goes through the framework and how it is changed by a development of changes. It is a graphical system that outlines information stream and the progressions that are related as data moves from commitment to yield.
4. Data Flow Diagram may be utilized to address a system at any level of consultation. Data Flow Diagram may be separated into levels that address developing information stream and utilitarian reason of interest.

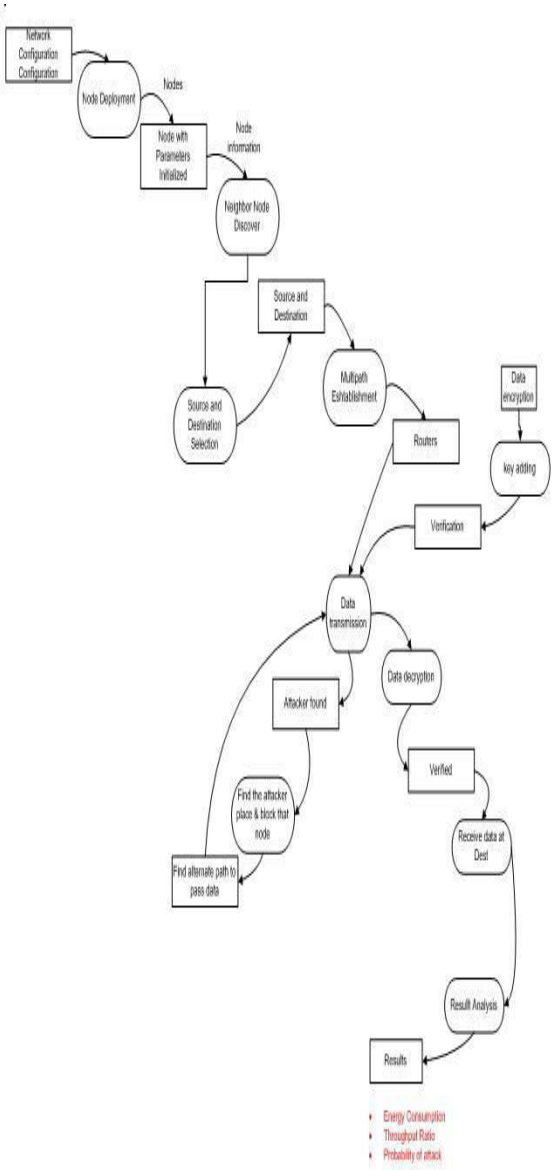

Figure 2. Data Flow Diagram

5. CONCLUSION AND FUTURE SCOPE

This work goals to simultaneously improve the fidelity for high- honesty applications and decrease the end-to-end delay for delay-sensitive ones, even when the network is congested. The proposed system naturally avoids the conflict between high integrity and low delay, the high-integrity packets are

2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

stored on the under loaded paths along which packets will suffer a large end-to-end delay because of more hops and the delay-sensitive packets travel along shorter paths to approach the sink as soon as possible. The proposed IDDR protocol is an energy efficient, likelihood of security and highly reliable routing overhead protocol that prolongs the network lifetime, and then by using Caesar ciphers algorithm data integrity is achieved i.e., data decryption and encryption is done by Caesar ciphers algorithm.

Future Scope

In future we require enhance the throughput of data transmission and reduce the routing overhead.

REFERENCE –

1. P. Levis, N. Lee, M. Welsh, and D. Culler, "TOSSIM: Accurate and scalable simulation of entire TinyOS applications," in Proc. 1st Int. Conf. Embedded Networked Sensor Syst., 2003,pp. 126–137.
2. T. Chen, J. Tsai, and M. Gerla, "QoS routing performance in multi hop multimedia wireless networks," in Proc. IEEE Int. Conf. Universal Personal Commun., 1997, pp. 557–561.
3. R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: Core extraction distributed ad hoc routing algorithm," IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1454–1465, Aug. 1999.
4. R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: Core extraction distributed ad hoc routing algorithm," IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1454–1465, Aug. 1999.
5. B. Hughes and V. Cahill, "Achieving real-time guarantees in mobile ad hoc wireless networks," in Proc. IEEE Real-Time Syst.Symp., 2003.
6. E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," IEEE Trans. Mobile Comput.,vol. 5, no. 6, pp. 738–754, Jun. 2003.
7. C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, "RAP: Areal-time communication architecture for large-scale wireless sensor networks," in Proc. IEEE 8th Real-Time Embedded Technol. Appl.Symp., 2002, pp. 55–66.
8. E. Felemban, C.-G. Lee, and E. Ekici, "MMSPEED: Multipath multi-speed protocol for QoS guarantee of reliability and timeliness in wireless sensor networks," IEEE Trans. Mobile Comput., vol. 5, no. 6, pp. 738– 754, Jun. 2003.
9. C. Lu, B. Blum, T. Abdelzaher, J. Stankovic, and T. He, "RAP: A real-time communication architecture for large-scale wireless sensor networks," in Proc. IEEE 8th Real-Time Embedded Technol. Appl. Symp., 2002, pp. 55–66.

10. M. Caccamo, L. Zhang, L. Sha, and G. Buttazzo, "An implicit prioritized access protocol for wireless sensor networks," in Proc. IEEE Real-Time Syst. Symp., 2002, pp. 39–48.
11. T. He, J. Stankovic, C. Lu, and T. Abdelzaher, "SPEED: A stateless protocol for real-time communication in sensor networks," in Proc. IEEE 23rd Int. Conf. Distrib. Comput. Syst., 2003, pp. 46–55.
12. P. T. A. Quang and D.-S. Kim, "Enhancing real-time delivery of gradient routing for industrial wireless sensor networks," IEEE Trans. Ind. Inform., vol. 8, no. 1, pp. 61–68, Feb. 2012.
13. S. Bhatnagar, B. Deb, and B. Nath, "Service differentiation in sensor networks," in Proc. Int. Symp. Wireless Pers. Multimedia Commun., 2001.
14. B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: Reliable information forwarding using multiple paths in sensor networks," in Proc. IEEE Intl Conf. Local Comput. Netw., 2003, pp. 406–415.