International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Dynamic Routing for Data Integrity and Delay Differentiated Services in Wireless Sensor Networks

Dr. Mohammed Abdul Waheed[1], Heena Khanum[2]

[1]Associate Professor, Department of Computer Science and Engineering, V.T.U P.G Centre, Kalaburagi, Karnataka-India

[2]P.G Student, Department of Computer Science and Engineering, V.T.U P.G Centre, Kalaburagi, Karnataka-India

Abstract: ***With the enormous advancement in the field of embedded computer and sensor technology, Wireless Sensor Networks (WSNs) have made remarkable impact in today's world. These WSNs consist of several thousands of sensor nodes deployed randoml y, are capable of sensing, actuating, and communicating the collected information. Since wireless sensor networks are constrained by cost, scalability, topology change and power consumption, new technologies are being considered to overcome these and many other issues.Applications running on the same Wireless Sensor Network (WSN) platform usually have different Quality of Service (QoS) requirements. Two basic requirements are low delay and high data integrity. However, in most situations, these two requirements cannot be satisfied simultaneously. In this paper, based on the concept of potential in physics, we propose IDDR, 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. Using the Lyapunov drift technique, we prove that IDDR is stable. Simulation results demonstrate that IDDR provides data integrity and delay differentiated services.***

Keywords: Wireless sensor networks, potential field, dynamic routing, data integrity, delay differentiated services.

1. Introduction

Wireless sensor networks (WSNs) have gained worldwide attention in recent years, particularly with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology which has facilitated the development of smart sensors. These sensors are small, with limited processing and computing resources, and they are inexpensive compared to traditional sensors. These sensor nodes can sense, measure, and gather information from the environment and, based on some local decision process, they can transmit the sensed data to the user. Smart sensor nodes are low power devices equipped with one or more sensors, a processor, memory, power supply, radio, and an actuator.

WSNS, which are used to sense the physical world, will play an important role in the next generation networks. Due to the diversity and complexity of applications running over WSNs, the QoS guarantee in such networks gains increasing attention in the research community.

As a part of an information infrastructure, WSNs should be able to support various applications over the same platform. Different applications might have different QoS requirements. For instance, in a fire monitoring application, the event of a fire alarm should be reported to the sink as soon as possible. On the other hand, some applications require most of their packets to successfully arrive at the sink irrespective of when they arrive. For example, in habitat monitoring applications, the arrival of packets is allowed to have a delay, but the sink should receive most of the packets.

WSNs have two basic QoS requirements: low delay and high data integrity, leading to what are called delaysensitive applications and high-integrity applications, respectively. Generally, in a network with light load, both requirements can be readily satisfied. However, a heavily loaded network will suffer congestion, which increases the end-to-end delay.

This work aims to simultaneously improve the fidelity for high-integrity applications and decrease the end-to-end delay for delay-sensitive ones, even when the network is congested. We borrow the concept of potential field from the discipline of physics and design a novel potentialbased routing algorithm, which is called integrity and delay differentiated routing (IDDR). IDDR is able to provide the following two functions:

[1] Improve fidelity for high-integrity applications.
The basic idea is to find as much buffer space as possible 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 these idle and/or underloaded paths, then the second task is to cache the packets efficiently for subsequent transmission. IDDR constructs a potential field according to the depth1 and queue length information to find the under-utilized paths. The packets with high integrity requirement will be forwarded to the next hop with smaller queue length. A mechanism called Implicit Hop-by-Hop Rate Control is designed to make packet caching more efficient.

[2] Decrease end-to-end delay for delay-sensitive applications.
Each application is assigned a weight, which represents the degree of sensitivity to the delay. Through building local dynamic potential fields with different slopes according to the weight values carried by packets, IDDR allows the packets with larger weight to choose shorter paths. In addition, IDDR also employs the priority queue to further decrease the queuing delay of delay sensitive packets.

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 suffer 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. Using the Lyapunov drift theory, we prove that IDDR is stable. Furthermore, the results of a series of simulations conducted on the TOSSIM platform demonstrate the efficiency and feasibility of the IDDR scheme.

2. Related Work and Motivation

2.1 Related Work

Most QoS provisioning protocols proposed for traditional ad hoc networks have large overhead caused by end-to-end path discovery and resource reservation. Thus, they are not suitable for resource-constrained WSNs. Some mechanisms have been designed to provide QoS services specifically for WSNs. Here we mainly focus on the metrics of delay and reliability.

2.1.1 Providing Real-Time Service

RAP exploits the notion of velocity and proposes a velocity-monotonic scheduling policy to minimize the ratio of missed deadlines [7]. However, the global information of network topology is required. Implicit Earliest Deadline First (EDF) mainly utilizes a medium access control protocol to provide real-time service [8]. The implicit prioritization is used instead of relying on control packets as most other protocols do. SPEED maintains a desired delivery speed across the network through a novel combination of feedback control and non-deterministic QoS-aware geographic forwarding [9]. In [10], a two-hop neighbor information-based gradient routing mechanism is proposed to enhance real-time performance. The routing decision is made based on the number of hops from a source to the sink and the two-hop information.

2.1.2 Providing Reliability Service

Adaptive Forwarding Scheme (AFS) employs the packet priority to determine the forwarding behavior to control the reliability [11]. ReInforM uses the concept of dynamic packet states to control the number of paths required for the desired reliability [12]. However, both of AFS and ReInforM require to know the global network topology. LIEMRO [13] utilizes a dynamic path maintenance mechanism to monitor the quality of the active paths during network operation and regulates the injected traffic rate of the paths according to the latest perceived paths quality. However, it does not consider the effects of buffer capacity and service rate of the active nodes to estimate and adjust the traffic rate of the active paths.

2.1.3 Providing Real-Time and Reliability Services

MMSPEED extends SPEED for service differentiation and probabilistic QoS guarantee [6]. It uses the same mechanism as SPEED to satisfy the delay requirements for different types of traffic, and uses redundant paths to ensure reliability. The MAC layer function is modified to provide prioritized access and reliable multicast delivery of packets to multiple neighbors. However, when the network is congested, all the source nodes still continuously transmit packets to the sink along multipaths without taking some other mechanisms, such as caching packets for some time. This not only deteriorates reliability but also retards the delay-sensitive packets. Energy-Efficient and QoS-based Multipath Routing Protocol (EQSR) [14] improves reliability through using a lightweight XOR-based Forward Error Correction (FEC) mechanism, which introduces data redundancy in the data transmission process. Furthermore, in order to meet the delay requirements of various applications, EQSR employs a queuing model to manage real-time and non-real-time traffic. DARA [15] considers reliability, delay and residual energy.

2.2 Motivation

Fig. 1 illustrates a small part of a WSN. Suppose node 1 is a hotspot and there are both high integrity packets (hollow rectangles) and delay-sensitive packets (solid rectangles) from source nodes A, B and C. A commonly used routing algorithm will choose the optimal path for all the packets. For example, the standard shortest path tree (SPT) routing will forward all of them to node 1 as shown in Fig. 1a. This will cause congestion and thus lead to many highintegrity packets loss and large end-to-end delay for delay sensitive packets. A multipath routing algorithm as shown in Fig. 1b can utilize more paths to avoid hotspots. However, the low delay and high throughput are hardly met simultaneously.

The reasons are:

- Delay-sensitive packets occupy the limited bandwidth and buffers, worsening drops of high-integrity ones.
- High-integrity packets block the shortest paths, compelling the delay-sensitive packets to travel more hops before reaching the sink, which increases the delay.
- High-integrity packets occupy the buffers, which also increases the queuing delay of delay-sensitive packets.

To overcome the above drawbacks, we intend to design a mechanism which allows the delay-sensitive packets to move along the shortest path and the packets with fidelity requirements to detour to avoid possible dropping on the hotspots. In this way, the data integrity and delay differentiated services can be provided in the same network. Motivated by this understanding, we propose the IDDR scheme, a potential-based multi-path dynamic routing algorithm.

As shown in Fig. 1c, the high-integrity packets do not choose node 1 due to its large queue length. Some other idle and/or under loaded paths, such as path 2 → 3 → Sink and 4 → 5 → 6 →Sink, are used to cache and route these packets efficiently so as to protect them from being dropped in the hotspot. On the other hand, IDDR gives delay-sensitive packets priority to go ahead in the shortest path to achieve low delay. Furthermore, if the traffic on the shortest path is heavy, IDDR can also select other paths for the delay-sensitive packets, such as path: A → 4 → 5 → 6 → Sink shown in Fig. 1d, the link from node 1 to the sink is so busy that node A or B will bypass node 1 and send packets to the sink along other under-utilized paths to avoid packets being dropped. IDDR distinguishes different types of packets using the weight values inserted into the header of packets,

and then performs different actions on them. Its cornerstone is to construct proper potential fields to make right routing decisions for different types of packets. Next the potential-based IDDR algorithm will be described in detail. attract widespread attention because of its huge management overhead. It is quite expensive to build an exclusive virtual field for each destination in traditional networks where numerous destinations might be distributed arbitrarily. On the contrary, the potential-based routing algorithm is much suitable for the many-to-one traffic pattern in WSNs. In some special applications and environments, more than one sink may exist. However, generally the data-centric WSNs only require nodes to transmit their sampling data to one of them. Therefore, in this work, we build a unique virtual potential field to customize a multipath dynamic routing algorithm, which finds proper paths to the sink for the packets with high integrity and delay requirements. Next, the potential-based routing algorithm for WSNs with one sink is described. It is straightforward to extend the algorithm to work in WSNs with multiple sinks.

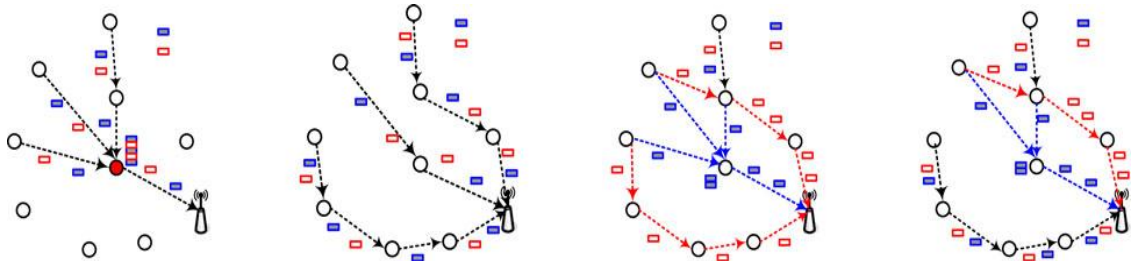

Figure 1: (a) Action of SPT. (b) Action of multipath router. (c) Action of IDDR. (c) IDDR with hotspot

3. Existing System

1) Most QoS provisioning protocols proposed for traditional ad hoc networks have large overhead caused by end-to-end path discovery and resource reservation. Thus, they are not suitable for resource-constrained WSNs. Some mechanisms have been designed to provide QoS services specifically for WSNs.
2) Adaptive Forwarding Scheme (AFS) employs the packet priority to determine the forwarding behavior to control the reliability
3) LIEMRO utilizes a dynamic path maintenance mechanism to monitor the quality of the active paths during network operation and regulates the injected traffic rate of the paths according to the latest perceived paths quality.

3.1 Disadvantages of Existing System

1) It does not consider the effects of buffer capacity and service rate of the active nodes to estimate and adjust the traffic rate of the active paths.
2) This will cause congestion and thus lead to many high integrity packets loss and large end-to-end delay for delay sensitive packets.
3) Delay-sensitive packets occupy the limited bandwidth and buffers, worsening drops of high-integrity ones.
4) High-integrity packets block the shortest paths, compelling the delay-sensitive packets to travel more hops before reaching the sink, which increases the delay.
5) High-integrity packets occupy the buffers, which also increases the queuing delay of delay-sensitive packets.

4. Proposed System

This work aims to simultaneously improve the fidelity for high-integrity applications and decrease the end-to-end delay for delay-sensitive ones, even when the network is congested. We borrow the concept of potential field from the discipline of physics and design a novel potential based routing algorithm, which is called integrity and delay differentiated routing (IDDR). IDDR is able to provide the following two functions:

Improve fidelity for high-integrity applications. The basic idea is to find as much buffer space as possible 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 these idle and/or underloaded paths, then the second task is to cache the packets efficiently for subsequent transmission. IDDR constructs a potential field according to the depth1 and queue length information to find the under-utilized paths. The packets with high integrity requirement will be forwarded to the next hop with smaller queue length. A mechanism called Implicit Hop-by-Hop Rate Control is designed to make packet caching more efficient.
Decrease end-to-end delay for delay-sensitive applications. Each application is assigned a weight, which represents the degree of sensitivity to the delay. Through building local dynamic potential fields with different slopes according to the weight values carried by packets, IDDR allows the packets with larger weight to choose shorter paths. In addition, IDDR also employs the priority queue to further decrease the queuing delay of delay-sensitive packets.

4.1 Advantages of Proposed System

1) 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 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.
2) Using the Lyapunov drift theory, we prove that IDDR is stable.
3) Furthermore, the results of a series of simulations conducted on the TOSSIM platform demonstrate the efficiency and feasibility of the IDDR scheme.

5. Implementation

- **Service Provider**

In this module, the service provider will browse the data file, initialize the router nodes and then send to the particular receivers. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver.

- **Router**

The Router manages a multiple networks to provide data storage service. In network n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and attacked nodes. Service provider will send their data file to router and router will select smallest distance path and send to particular receiver. If any attacker is found in a node then router will connect to another node and send to particular user.

- **IDS Manager**

In this module, the IDS Controller consists of two phases. If Integrity or Malicious Data is occurs in router then IDS controller is activated. In a first phase DNS packets, Net flow, Traffic filter and Fine-grained IDS client detection are present. Aim is that detecting all hosts within the monitored network that engage in IDS communications. We analyze raw traffic collected at the edge of the monitored network and

apply a pre-filtering step to discard network flows that are unlikely to be generated by IDS applications. We then analyze the remaining traffic and extract a number of statistical features to identify flows generated by IDS clients. In the second phase, Coarse-grained IDS Integrity or Malicious Data detection, Fine-grained IDS client detection and Integrity or Malicious Data are present; our system analyzes the traffic generated by the IDS clients and classifies them into either legitimate IDS clients or IDS Integrity or Malicious Data.

- **Receiver (End User)**

In this module, the receiver can receive the data file from the router. Service provider will send data file to router and router will send to particular receiver. The receivers receive the file by without changing the File Contents. Users may receive particular data files within the network only.

- **Attacker**

Attacker is one who is injecting malicious data to the corresponding node and also attacker will change the bandwidth of the particular node. The attacker can inject fake bandwidth to the particular node. After attacking the nodes, bandwidth will have changed in a router.

6. Conclusion

In this paper, a dynamic multipath routing algorithm IDDR is proposed based on the concept of potential in physics to satisfy the two different QoS requirements, high data fidelity and low end-to-end delay, over the same WSN simultaneously. The IDDR algorithm is proved stable using the Lyapunov drift theory. Moreover, the experiment results on a small test bed and the simulation results on TOSSIM demonstrate that IDDR can significantly improve the throughput of the high-integrity applications and decrease the end-to-end delay of delay sensitive applications through scattering different packets from different applications spatially and temporally. IDDR can also provide good scalability because only local information is required, which simplifies the implementation. In addition, IDDR has acceptable communication overhead.

References

[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] S. Chen and K. Nahrstedt, “Distributed quality-of-service routing in ad hoc networks,” IEEE J. Selected Areas Commun., vol. 17, no. 8, pp. 1488–1505, 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: 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.
[8] 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.
[9] 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.
[10] 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.
[11] S. Bhatnagar, B. Deb, and B. Nath, “Service differentiation in sensor networks,” in Proc. Int. Symp. Wireless Pers. Multimedia Commun., 2001.
[12] 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.
[13] M. Radi, B. Dezfouli, K. A. Bakar, S. A. Razak, and M. A. Nematbakhsh, “Interference-aware multipath routing protocol for QoS improvement in event-driven wireless

sensor networks," Tsinghua Sci. Technol., vol. 16, no. 5, pp. 475–490, 2011.
[14] J. Ben-Othman and B. Yahya, "Energy efficient and QoS based routing protocol for wireless sensor networks," J. Parallel Distrib. Comput., vol. 70, no. 8, pp. 849–857, 2010.
[15] M. Razzaque, M. M. Alam, M. MAMUN-OR-RASHID, and C. S. Hong, "Multi-constrained QoS geographic routing for heterogeneous traffic in sensor networks, ieice transactions on communications," IEICE Trans. Commun., vol. 91B, no. 8, pp. 2589–2601, 2008.
[16] D. Djenouri and I. Balasingham, "Traffic-differentiation-based modular qos localized routing for wireless sensor networks," IEEE Trans. Mobile Comput., vol. 10, no. 6, pp. 797–809, Jun. 2010.
[17] A. Basu, A. Lin, and S. Ramanathan, "Routing using potentials: A dynamic traffic-aware routing algorithm," in Proc. Conf. Appl., Technol., Architectures, Protocols Comput. Commun., 2003, pp. 37–48.
[18] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: Congestion detection and avoidance in sensor networks," in Proc. 1st Int. Conf. Embedded Netw. Sensor Syst., 2003, pp. 266–279.
[19] L. Georgiadis, M. J. Neely and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," Found. Trends Netw., vol. 1, no. 1, pp. 1–144, 2006.
[20] A. Papadoulos and J. A. Mccann, "Towards the design of an energy-efficient, location-aware routing protocol for mobile, ad-hoc sensor networkFs," in Proc. Int. Workshop Database Expert Syst. Appl., 2004, pp. 705–709.