



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

P.VARALAKSHMI¹, R.HIMAJA², E.SIRISHA³, K.SHANKAR⁴

¹Department of CSE, VITS College of Engineering, Sontyam, Visakhapatnam, India

²Department of CSE, VITS College of Engineering, Sontyam, Visakhapatnam, India

³Department of CSE, VITS College of Engineering, Sontyam, Visakhapatnam, India

laxmivara777@gmail.com, himajaramaswamy@gmail.com, sirisha2422@gmail.com, shankarkopanati@gmail.com

Abstract- 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.

I. INTRODUCTION

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. WSNs have two basic QoS requirements: low delay and high data integrity, leading to what are called delay sensitive 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 potential based routing algorithm, which is called integrity and delay differentiated routing (IDDR).

II. OBJECTIVE

To find the data integrity and delay differentiated services in wireless sensor networks.

III. MODULE DESCRIPTION AND IMPLEMENTATION

In this paper there are five modules to implement they are

- **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 changed in a router.

IV. CONCLUSION

In this project, 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.

REFERNCES

- [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 multihop 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.