Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 13, Issue. 2 : 2022
ISSN : **1906-9685**

ENHANCING DATA SECURITY IN WIRELESS SENSOR NETWORKS THROUGH DIFFERENTIATED DELAY SERVICES AND DYNAMIC ROUTING

[#1]Mr.GURRALA SANDEEP REDDY, *Assistant Professor*
[#2]Mr.JANGA RAVICHANDER, *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Because of the rapid advancement of computer and sensor technologies, Wireless Sensor Networks (WSNs) have had a significant impact on modern society. These WSNs are made up of tens of thousands of randomly distributed sensor nodes. They can receive data, process it, and send it to other devices. Emerging technologies can address the cost, scalability, layout customization, and energy consumption challenges that plague wireless sensor networks. Applications that use the same Wireless Sensor Network (WSN) technology must frequently comply to differing Quality of Service (QoS) criteria. We demand information that is secure and handled quickly. These two desires, however, cannot always be met at the same time. To overcome this issue, we introduce IDDR, a multi-path dynamic routing technique, in this paper. Its origins can be traced back to the scientific idea of potential. IDDR provides a virtual hybrid potential field based on the weight assigned to each packet that splits packets of applications with differing QoS criteria. This improves data integrity for applications that value it while decreasing end-to-end latency for the same applications. We demonstrate the stability of IDDR using the Lyapunov drift approach. IDDR offers data protection and delay compensation services based on the outcomes of the exercise.

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

1. INTRODUCTION

There has recently been a surge in interest in wireless sensor networks (WSNs). This is partly because Micro-Electro-Mechanical Systems (MEMS) technology has made it easier to manufacture smart gadgets. These sensors are less expensive despite being smaller and having less computer capacity than others. These sensor nodes are capable of sensing, measuring, and capturing environmental data.

Then, based on a local decision-making process, they may communicate this information to the user. Smart sensor nodes are low-power, small devices that include a radio, actuator, processor, memory, power supply, and storage. They could have several sensors.

The future generation of networks will rely heavily on WSNS, which are utilized to perceive the external environment. Because WSNs support such a wide range of complex applications, researchers are increasingly focused on the QoS potential of these networks.

WSNs should be able to run multiple applications on the same platform because they are part of an information infrastructure. QoS needs may differ between systems. A fire monitoring program, for example, should promptly notify the sink in the event of a fire alert. Certain applications, on the other hand, need that the vast majority of their packets arrive safely at the basin regardless of when they arrive. Packets arriving late is okay in habitat monitoring applications, for example, but the sink should still receive the majority of them.

The two most important quality of service

requirements for wireless sensor networks are low latency and good data integrity. These requirements lead to delay-sensitive and high-integrity applications. Both objectives are often met in low-traffic networks.

will be straightforward to achieve. If the network becomes overcrowded, it will become backed up, increasing the end-to-end delay time.

Despite network congestion, our goal is to improve fidelity for high-integrity applications while reducing end-to-end latency for delay-sensitive applications. We create a new method for data routing based on potential using the physics concept of a potential field. IDDR is an acronym that stands for integrity and delay differentiated routing. IDDR can be used for two different things:

Improve fidelity for high-integrity applications.

The primary goal is to acquire as much buffer space as possible from paths that are not in use or are not active enough to hold excess packets that would otherwise be dropped on the quickest route. As a result, the first task is to find these unoccupied or little trafficked pathways.

The second challenge is successfully storing the packets for later transmission. To discover vacant routes, IDDR generates a potential field from depth1 and queue length data. The bits that must be particularly secure will be transmitted with less traffic to the following step. The goal of Implicit Hop-by-Hop Rate Control is to increase packet caching performance.

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 Each application is given a weight based on its sensitivity to delays. IDDR enables heavier packets to choose faster routes by generating regional dynamic potential fields with slopes that vary depending on the weight values of the transmitted packets. IDDR also uses a priority queue to limit the amount of time packets that cannot wait spend in the queue.

IDDR automatically avoids the tradeoff between high integrity and low delay. The high-integrity packets are stored on the underloaded paths, which have longer end-to-end delays due to more hops, and the delay-sensitive packets travel shorter paths to reach the sink as rapidly as feasible. We show that IDDR is stable using Lyapunov's theory of drift. Furthermore, the results of many models run on the TOSSIM platform show that the IDDR approach is effective and practical.

2. RELATED WORK AND MOTIVATION

Related Work

Because they must locate paths and reserve resources from scratch, the majority of QoS provisioning systems designed for ordinary ad hoc networks are prohibitively expensive. As a result, they are unsuitable for WSNs with minimal resources. A few approaches for providing QoS services to WSNs have been developed. The most important issue in this case is determining dependability and delay.

Providing Real-Time Service

RAP makes efficient use of the concept of speed and offers a speed-based scheduling strategy to reduce the amount of missed deadlines. However, in order to complete your duty, you must have deep knowledge of network structure. To deliver real-time service, Implicit Earliest Deadline First (EDF) principally leverages a medium access control protocol.

In this situation, rather using control packets, as is the case with the majority of other protocols, the inferred priority is employed. SPEED maintains the intended delivery speed throughout the network by integrating feedback control with non-deterministic QoS-aware regional forwarding. A two-hop neighbor information-based gradient routing algorithm is proposed to increase real-time performance. The pathways are determined using two-hop information and the number of travels from a source to a sink.

Providing Reliability Service

The Adaptive Forwarding Scheme (AFS) is in charge of determining how and how reliably packets are forwarded. It makes use of the notion of dynamic packet states to reduce the number of lines required to achieve the desired level of reliability. However, in order to use both AFS and ReInforM, you must be conversant with the global network architecture.

LIEMRO analyzes the quality of active paths using a dynamic path maintenance system and changes the amount of traffic that travels each

path based on its present quality. When determining and updating the active route traffic rate, the active nodes' buffer capacity and service rate are ignored.

Providing Real-Time and Reliability Services

SPEED is used to ensure probabilistic QoS and differentiate services. It uses the same approach as SPEED as well as additional lines to assure reliability and meets the delay requirements of various sorts of traffic. A change to the MAC layer function enables reliable multicast transmission of packets to many peers as well as faster access. Despite the fact that the network is congested, all source nodes continue to send packets to the sink in a variety of ways without taking any further precautions, such as temporarily holding packets. This diminishes dependability and slows down delay-sensitive components.

The Energy-Efficient and Quality-of-Service (QoS)-based Multipath Routing Protocol (EQSR) employs a lightweight XOR-based Forward Error Correction (FEC) technique. It improves protocol reliability by sending duplicate data during the transfer phase. To meet the latency needs of various applications, EQSR also manages real-time and non-real-time traffic using a queuing architecture. DARA takes into account factors such as dependability, latency, and energy remaining.

Motivation

Figure 1 illustrates a WSN component. Assume node 1 is a hotspot and that packets arriving from nodes A, B, and C include both high integrity and delay-sensitive packets (represented by porous and solid rectangles, respectively). A well-functioning routing program will choose the best path for each packet. Figure displays one example. Everyone is directed to node 1 by the shortest path tree (SPT) route. 1a. Due to this, there will be a considerable lot of congestion, which will result in the loss of multiple packets with high integrity and a lengthy wait for packets that are sensitive to delay. Fig. 1 is an illustration of a multipath routing approach. 1b might go in a variety of routes to avoid hotspots. However, little latency and great throughput nearly seldom occur simultaneously.

Here are the causes:

- When packets with high integrity are dropped, the problem worsens because delay-sensitive packets use buffer space and bandwidth.
- High-integrity packets block the shortest pathways, which causes delay-sensitive packets to take longer to reach the sink, hence increasing the delay.
- High-integrity packets use buffer space, causing delay-sensitive packets to wait longer.

We will create a strategy to overcome these concerns by routing delay-sensitive packets along the shortest path and accuracy-sensitive packets along a route that protects them from being lost at hotspots. This is how data integrity and delay-differentiated services can coexist on the same network. We offer the IDDR protocol, a potential-based multi-path dynamic routing algorithm, because we are aware of this.

Fig. 1 demonstrates this. No high-integrity messages are delivered to Node 1 because it must wait so long (Figure 1c). To prevent these packets from being lost in the hotspot, they are appropriately cached and sent along other, less-busy paths, such as path Sink and Sink. IDDR, on the other hand, prioritizes delay-sensitive transmissions on the shortest path, thereby reducing latency. Moreover, IDDR can select multiple routes for packets that cannot wait, such as path:

A Sink in Fig., if the shortest route is congested. In case 1d, the link between node 1 and the sink is so congested that node A or B will send packets to the sink via alternative, less-used routes in order to prevent packet loss. Using the weight numbers contained within the packet header, IDDR can differentiate between various types of packets and respond accordingly.

It begins with populating the appropriate potential fields so that the optimal route decisions can be made for various packet types. The potential-based IDDR algorithm will then be explained in detail. get a lot of attention due to their high operating costs. In conventional networks, where targets are assigned at random, it is prohibitively expensive to create a distinct virtual field for each target. In contrast, the many-to-one flow pattern in WSNs functions significantly better with the potential-based routing algorithm.

In certain circumstances and applications, there may be more than one receptacle. In contrast,

nodes typically only need to transmit their sample data to one of the data-centric WSNs.

In this study, we create a unique virtual potential field in order to tailor a multipath dynamic routing method that identifies the most efficient routes for packets with strict integrity and latency requirements to reach the sink. The potential-based route method for WSNs with a solitary sink will be discussed next. It is simple to implement the method in WSNs with multiple sinks.

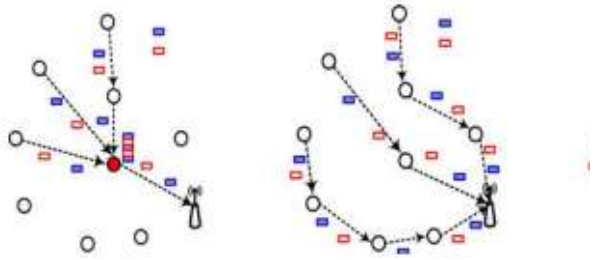

Figure 1: (a) The SPT's actions. (b) The operation of the multipath router. c) The IDDR's actions. RFID equipped with a beacon

3. EXISTING SYSTEM

- Most QoS provisioning approaches for normal ad hoc networks necessitate significant extra effort to reserve resources and select the best way from one end to the other. As a result, they are inappropriate for WSNs with limited resources. There have been a number ways explored for providing QoS services to WSNs.
- Based on the importance of each packet, the Adaptive Forwarding Scheme (AFS) calculates how to reliably deliver data packets.
- LIEMRO uses a dynamic path maintenance system to analyze the quality of active paths and adjusts the amount of traffic that travels each path based on its current quality.

Disadvantages of Existing System

- It does not consider the buffer capacity or service rate of active nodes when determining and modifying the traffic rate of active routes.
- Congestion will develop, leading in the loss of numerous high-integrity packets and a considerable end-to-end delay for packets that cannot tolerate delays.
- When high-integrity packets are dropped, the situation intensifies because delay-sensitive packets use buffer space and bandwidth.
- Because high-integrity packets block the quickest paths, delay-sensitive packets take longer to reach the sink, increasing the delay.
- Because high-integrity packets consume buffer space, delay-sensitive packets must wait longer.

4. PROPOSED SYSTEM

Regardless of network congestion, our goal is to increase fidelity for high-integrity applications while decreasing end-to-end latency for delay-sensitive applications. Using the physics idea of a potential field, we develop a new way for data routing based on potential. The term IDDR stands for integrity and delay differentiated routing. IDDR can be used for two purposes:

Enhance fidelity for applications that require high integrity. The primary purpose is to obtain as much buffer space as possible from paths that are not in use or are insufficiently active to keep extra packets that would otherwise be lost on the shortest route. As a result, the initial objective is to identify these empty or less traveled paths. The second problem is storing the packets successfully for later transmission. IDDR creates a potential field from depth1 and queue length data to find vacant routes. The bits that must be very secure will be sent with less traffic to the next step. Implicit Hop-by-Hop Rate Control aims to improve packet caching performance.

Reduce the time it takes from start to finish for programs that require it. Each application is weighted according to its susceptibility to delays. IDDR allows heavier packets to pick faster routes by generating regional dynamic potential fields with slopes that vary based on the weight values of the transmitted packets. IDDR also employs a priority queue to limit the time packets that cannot wait spend in the queue.

Advantages of Proposed System

- IDDR eliminates the tradeoff between high integrity and low delay automatically. This is because high-integrity packets are stored on underutilized paths, where they will face significant end-to-end delay due to extra hops, but delay-sensitive packets remain on shorter channels to reach the sink as soon as feasible.
- We show that the IDDR is stable using the

notion of Lyapunov drift.

- Furthermore, the outcomes of numerous models performed on the TOSSIM platform demonstrate that the IDDR strategy is both effective and practicable.

5. IMPLEMENTATION

Service Provider

The service provider will review the data file, configure the router nodes, and transmit it to the right individuals in this part. The service provider sends the data file to the router, which finds the shortest path to the intended receiver.

Router

The router allows for the management of different networks as well as data storage. The network has n nodes numbered from 1 to 5. The router's service provider has access to information regarding afflicted nodes and is aware of their identities. The service provider sends the data file to the router, which finds the shortest path to the intended receiver. When a node detects an offender, the router connects to another node and sends a message to the offender.

IDS Manager

This module's IDS Controller is divided into two phases. If the router identifies problems with data integrity or malicious activities, the IDS controller is triggered. In the first phase, DNS packets, Net flow, Traffic filter, and IDS client detection are detected at a fine grain level. The goal is to identify every host on the monitored network that communicates with IDS. To reduce network flows induced by IDS software, we execute a pre-filtering step on raw data detected at the network's interface. The remaining data is then examined, and a set of statistical features are extracted to identify transactions done by IDS customers. Our system evaluates IDS client data and divides it into three categories: genuine IDS clients, IDS Integrity Data, and malicious data. Coarse-grained IDS identifies Integrity or Malicious Data in the second phase, fine-grained IDS identifies clients, and Integrity or Malicious Data is identified.

Receiver (End User)

The file can be retrieved from the router by the recipient of this device. The service provider will send a file to the server, which will subsequently deliver it to the intended recipient. Before sending the file to the recipients, no changes are done to it. Access to specific file categories is restricted on the network.

Attacker

Someone is considered an attacker if they send destructive data to the correct node and change its bandwidth. An attacker can trick a node into using a bogus internet connection. The router's bandwidth will vary once the nodes have been impacted.

6. CONCLUSION

An IDDR dynamic multipath routing method is proposed in this paper as a way to meet both the QoS requirements of high data integrity and low end-to-end delay across a single WSN. The foundation of this strategy is the physics idea of potential. The IDDR technique's stability is demonstrated using Lyapunov's drift theory. Furthermore, by dispersing packets from multiple applications across space and time, IDDR can considerably boost the throughput of high-integrity applications and reduce the end-to-end delay of delay-sensitive applications.

This has been proved by experiments on a small test platform and simulations using TOSSIM. IDDR is scalable and easy to deploy because it just requires local data. Furthermore, the additional labor performed by IDDR for communication is justified.

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.