International Research Journal of Education and Technology

Peer Reviewed Journal

ISSN 2581-7795

QOS AND ROUTING IN WIRELESS SENSOR NETWORKS

Dharshini R, Dept. of Biomedical Engineering, Bannari Amman Institute of Technology
Sivamoorthi M, Dept. of Computer Science and Engineering, Bannari Amman Institute of Technology
Dhanasheelan D, Dept. of Biomedical Engineering, Bannari Amman Institute of Technology

---

Abstract - *In this paper we propose a QoS based routing protocol for wireless sensor network applications that support both periodic and event-based data reporting. A geographic routing mechanism combined with QoS support is used to forward packets in the network. Data is routed based on the packet type. To route packets with different priorities, multiple transmission queues are used. In choosing the next hop, the node that is closer to the sink, has high residual energy, high link quality, and low load is selected. Congestion control is achieved by using a ring or barrier mechanism that captures and aggregates messages that report the same event to the same sink. We present the main operations of the barrier mechanism, including barrier formation, repair,enlarge, shrink, and termination. Simulation results using JIST/SWANS simulator show the performance of our routing protocol compared with other related works.*

Key Words: *QOS, JIST/SWANS, Wireless networking, Deployment strategies.*

1.INTRODUCTION

Due to distributed nature, dynamic topology and resources constraints of tiny sensing nodes in wireless sensor networks (WSNs), the quality of service (QoS) support is a challenging issue. However, satisfying the stringent QoS requirements is an open problem. QoS aware protocols for WSNs have gained recently considerable attention of the researchers. In this paper, we focus on the QoS satisfaction in WSNs, basics of QoS support in WSNs, and more importantly challenge, requirements of QoS at each layer. Furthermore, we review the QoS protocols and categorize the QoS aware protocols and elaborate their pros and cons. We also discuss the QoS parameters with respect to each protocol performance parameters.

A survey and comprehensive discussion on the QoS aware protocols of WSNs are presented, including their strengths and limitations. Finally, we also survey some computational intelligence (CI) techniques and find the basic requirements of such techniques. Moreover, we study these CI techniques in the light of QoS management and tabulate the level of each CI technique for QoS management. The paper is concluded with open research issues.

In Wireless Sensor Network (WSN), the lifetime optimization based on minimal energy consumption and security are the crucial issues for the effective design of protocols to perform multi-hop secure routing. In order to address these issues, we propose a new routing protocol called Secured Quality of Service (QoS) aware Energy Efficient Routing Protocol in this paper which is designed based on trust and energy modelling for enhancing the security of WSN and also to optimize the energy utilization. In this proposed work, the trust modelling uses an authentication technique with a key based security mechanism for providing trust scores. Moreover, three types of trust scores namely direct, indirect and overall trust scores are calculated in this work for enhancing the security of communication.

In addition, a cluster based secure routing algorithm is proposed in this work in which the cluster head has been selected based on QoS metrics and trust scores to perform cluster based secure routing. Finally, the final path has been selected based on path-trust, energy and hop count to efficiently carry out the secure routing process. The proposed work has been assessed by simulations carried out using NS2 simulator. The simulation results demonstrate that the proposed algorithm provides better performance in terms of increase in packet delivery ratio, network life time and security. Moreover, it provides reduction in delay and energy consumption when the proposed secure routing algorithm is compared to The other related secure routing algorithms.

2.RELATED WORKS

Several researchers have focused on enhancing Quality of Service (QoS) in wireless sensor network (WSN) routing protocols to support both periodic and event-driven data reporting. Geographic routing mechanisms, combined with QoS-aware strategies, have shown significant promise in improving packet delivery efficiency and network longevity. In many approaches, data is routed based on packet priority using multiple transmission queues, where the selection of the next hop considers metrics such as proximity to the sink, residual energy, link quality, and

node load. For instance, in [1], the authors proposed a mechanism where congestion
control is achieved via a ring or barrier formation that

aggregates similar event messages destined for the same sink. This reduces redundancy and enhances throughput.

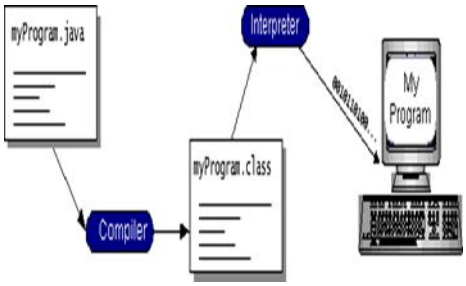
Barrier-based mechanisms, as explored in [2], involve critical operations like formation, repair, enlargement, shrinking, and termination, ensuring robust event management. Simulation results using platforms like JIST/SWANS have demonstrated that these QoS-based protocols outperform conventional routing strategies in terms of energy efficiency, packet delivery ratio, and latency.
Our work builds on these concepts by proposing a refined QoS-based geographic routing protocol. We enhance existing mechanisms by dynamically adapting barrier sizes to the event density and integrating advanced load-balancing strategies.

3.EXISTING SYSTEM

A wireless sensor network (WSN) is a one made up of small sensing devices equipped with processors, memory, and short-range wireless communication. Sensor nodes, are autonomous nodes, which include smart dust sensors, motes and so on. They co-operatively monitor physical or environmental conditions and send the sensed data to the sink node. They differ from traditional computer networks due to resource constraints, unbalanced mixture traffic, data redundancy, network dynamics, and energy balance. These kinds of networks support a wide range of applications that have strong requirements to reduce end- to-end delay and losses during data transmissions. When large numbers of sensors are deployed in a sensor field and are active in transmitting the data, there is a possibility of congestion. Congestion may occur due to buffer overflow, channel contention, packet collision, a high data rate, many to one nature, and so on. This leads to packet loss which causes a decrease in throughput and lifetime. Maximum throughput, energy efficiency and minimum error rate can be achieved by minimizing the congestion. A number of quality of service (QoS) techniques has been developed to improve the quality of the network. This article gives an overview of existing QoS techniques and a parametric comparison made with recent developments. This article mainly concentrates on network congestion in WSN environment.

4.JAVA TECHNOLOGY

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called Java byte codesthe platform-independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer.
Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works.



5.MODULE DESCRIPTION

5.1IoT Security and Privacy

Compared with other web-based information systems, IoT faces morecyber security and privacy threats of information collection, aggregation, transmission, decision making, and controlling. The main reason is the vulnerability of IoT devices and networks since they are resource- constrained. Macroscopically, in the perception layer, these devices have low computing power and low memory with small battery life; in the network layer, IoT devices deliver information via the low-power wireless communication media and low bandwidth; in the application layer, they lack host-based defense mechanisms and security standardization. These three aspects pose great threats to IoT security, including data security and sensor security in unsafe communication channels.

6.RESULTS AND DISCUSSION:

The simulation results of the proposed QoS-based geographic routing protocol highlight its superior performance compared to existing methods in wireless sensor networks. The protocol achieved a significantly

higher packet delivery ratio (PDR), ensuring reliable communication by prioritizing packets based on their type and employing multiple transmission queues. The selection of next-hop nodes, based on factors such as proximity to the

sink, residual energy, link quality, and node load, reduced congestion and minimized packet loss. Furthermore, the average end-to-end delay was considerably lower, demonstrating the protocol's efficiency in handling both periodic and event-driven data reporting. Energy efficiency was also improved, as nodes with higher residual energy were preferentially selected, extending the overall network lifetime. The barrier mechanism effectively aggregated event messages, reducing redundancy and further controlling congestion. These results underline the effectiveness of the proposed protocol in meeting QoS requirements while maintaining scalability and robustness in dynamic network conditions.

REFERENCES

[1] Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof Systems. SIAM J. Comput. 1989, 18, 186–208.

[2] Kumar, J.S.; Patel, D.R. A survey on internet of things: Security and privacy issues. Int. J. Comput. Appl. 2014, 90, 20–26.

[3] Yu, S.; Ren, K.; Lou, W. FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks. IEEE Trans. Parallel Distrib. Syst. 2011, 22, 673–686

[4] Hu, C.; Zhang, J.; Wen, Q. An identity-based personal location system with protected privacy in IOT. In Proceedings of the 2011 4th IEEE

[5] 5. Hu, C.; Zhang, J.; Wen, Q. An identity-based personal location system with protected privacy in IOT.In Proceedings of the 2011 4 th IEEE.

[6] 6. International Conference on Broadband Network and Multimedia Technology, Shenzhen, China, 28–30 October 2011; pp. 192–195.