ISSN: 2581-3404 (Online) IF: 5.445 (SJIF)

IJIRTM, Volume-7, Issue-3, June-2023.

Greedy Perimeter Vector Routing Protocol for Underwater Acoustic Wireless Sensor Networks Using NS-2

Sukhmeet Singh Oberai[1], Gowreesh Malhan[2], Aryan[3], Ananya Sharma[4]
Department of CSE (AI&ML)[1,2,3,4]
Panipat Institute of Engineering and Technology, Panipat, India[1,2,3,4]
sukhmeetoberoi@gmail.com[1], gowreeshgm1@gmail.com[2], kharbaryan2000@gmail.com[3],
ananyasharma242004@gmail.com[4]

Abstract: *The underwater environment offers considerable scope for sensor-network deployment across several application domains. As with terrestrial wireless sensor networks (WSNs), security and energy consumption remain the two most pressing design constraints for underwater acoustic sensor networks (UASNs). A number of energy-aware clusters and data-aggregation schemes have been proposed to reduce power drain while still preventing malicious nodes from accessing sensitive data; such schemes couple energy harvesting with delay-tolerant security mechanisms. In this work, an enhanced Sparsity-aware Energy Efficient Clustering (SEEC) protocol is developed to jointly address data aggregation and network security. The design introduces a backup cluster head (CH) that assumes control whenever the primary CH fails, ensuring that ongoing operations are not interrupted and continue to execute on schedule. Simulation results obtained in NS-2 show that the proposed clustering-based SEEC variant outperforms the reference protocol on the standard networking metrics evaluated. Future work will extend this direction with additional security- and energy-aware protocols for underwater deployments.*

Keywords: Underwater acoustic sensor network; WSN; cross-layer protocol; cluster head; SEEC.

Introduction

The underwater sensor networks (UWSNs) are expected to find a wide range of applications such as seismic surveys and pollution monitoring, tactical surveillance, oceanographic data collection, equipment monitoring, offshore exploration and disaster mitigation and assisted navigation. A fleet of Autonomous Underwater Vehicles (AUVs) with various underwater sensors may be deployed to survey underwater resources and to gather mission-critical data for later analysis. To achieve these applications, it is required to maintain reliable communication between underwater nodes, and to provide timely exchange of time-critical information between nodes and vehicles by them sharing their state information (such as sensed readings, and dynamic topology) autonomously. This has led to the development of wireless communication under water for such uses. An underwater acoustic sensor network (UASN) usually consists of many sensors and mobile devices that self-organise a distributed network that is suitable for the characteristics of the ocean environment [9]. Underwater ad hoc networking is seen as a low-cost communication substrate for distributed users in this regard.

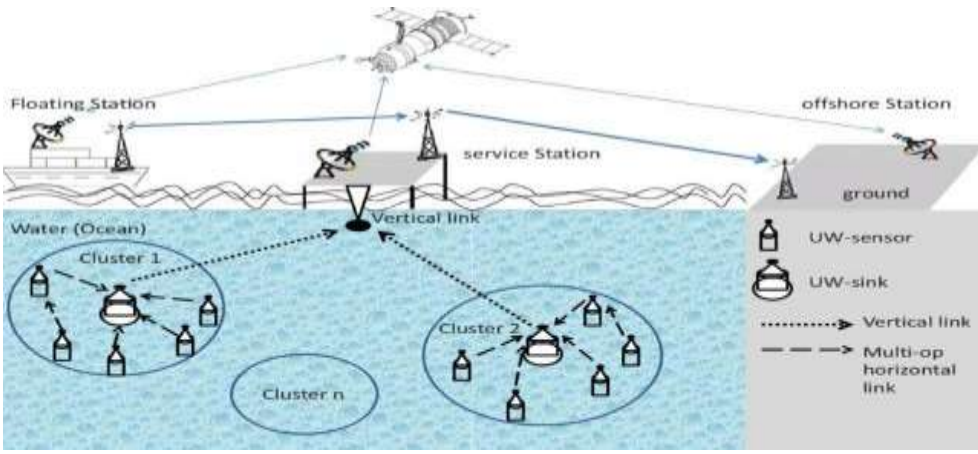

Figure 1: Underwater acoustic sensor network.

UASNs are characterized by a distributed architecture, node mobility and a constantly changing topology, all of which make network formation and maintenance considerably harder than in terrestrial networks. Over the past decade a substantial body of work has targeted improved routing performance for such networks by addressing these challenges. WSNs more broadly have become established technology, having been deployed successfully in demanding settings such as battlefield surveillance, smart-home automation, traffic monitoring and habitat monitoring, among other domains [10].

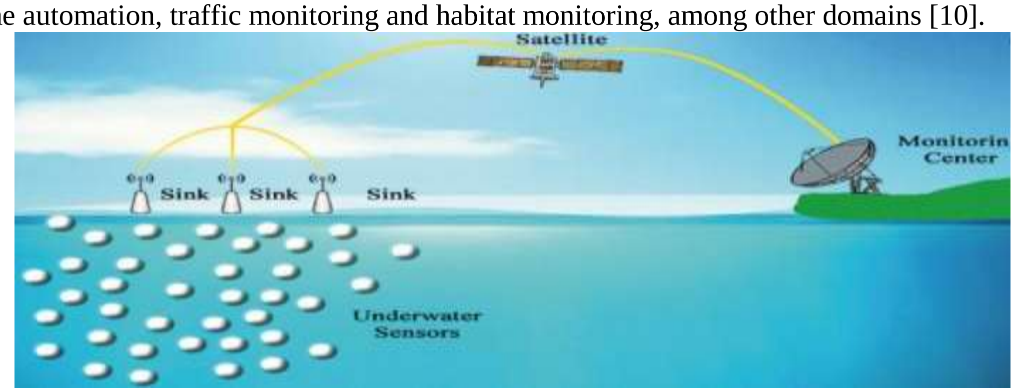

Figure 2: Underwater sensor node.

II. Related Work

Underwater deployments continue to attract growing research interest, and recent years have seen renewed focus on the opportunities that large-scale sensor networks offer in the underwater domain [6], [7]. Underwater wireless networking has emerged as a leading technology for ocean-related applications, with nodes and vehicles expected to autonomously exchange topology and sensing information.

Alzubaidi and Shaker [1] observe that security remains one of the most significant open challenges for WSNs: as networking technology advances, deployed networks become increasingly exposed to a growing range of attacks. Because individual sensor nodes cannot be provisioned with large power and memory budgets, adversaries can introduce malicious nodes that compromise network operation, which is why security mechanisms are difficult to implement effectively in this setting. Combining sensing capability with power-aware management and wireless communication makes such networks useful in practice, but wireless communication itself introduces a range of security threats; the authors survey the principal categories of attack encountered in WSNs. Koutsonikola et al. [14] provide a broad survey of research challenges in ad hoc wireless networks, tracing the origins of ad hoc networking and its subsequent evolution. Their analysis is organised around several dimensions — application domains, network characteristics, topology, node capability and design constraints — that collectively differentiate ad hoc networks from conventional infrastructure networks. The survey also identifies open research problems spanning quality of service, energy efficiency and security. Zhu et al. [4] have proposed an authenticated trust and reputation calculation and management mechanism (ATRCM) for the sensor network cloud service integration. The proposed ATRCM system aims at (i) authenticating the cloud service providers (CSPs) and sensor-network providers (SNPs) in order to avoid impersonation attacks, (ii) auditing the integrity and quality of the services provided by the CSPs and SNPs, and (iii) assisting cloud service users to choose an appropriate CSP and the appropriate sensor-network provider (SNP), respectively, by the CSP. To recommend an effective and efficient ATRCM design, the authors statistically analyze, simulate and conduct a security evaluation.

Methodology

Sensor placement can follow several deployment models depending on the environmental conditions and application requirements. UASN communication architectures are generally classified as two-dimensional (2-D) or three-dimensional (3-D). Energy consumption, network reliability and the overall network topology are the dominant factors that determine achievable performance under either architecture.

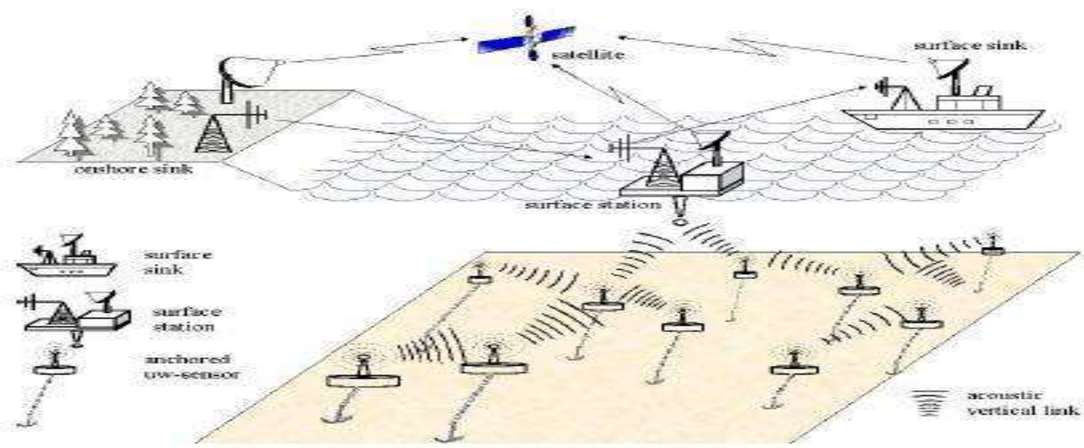

Figure 3: Architecture of a 3-D underwater sensor network.

Because UASN topologies are inherently dynamic and susceptible to a range of attacks, the network design must incorporate robust security mechanisms alongside an appropriate topology. In a 3-D deployment, sensor depth can be actively controlled, allowing the same nodes to be repositioned for surveillance of different ocean phenomena. A 3-D AUV network is typically composed of a static component built from anchored (berthed) sensors together with a mobile component realised through autonomous vehicles.

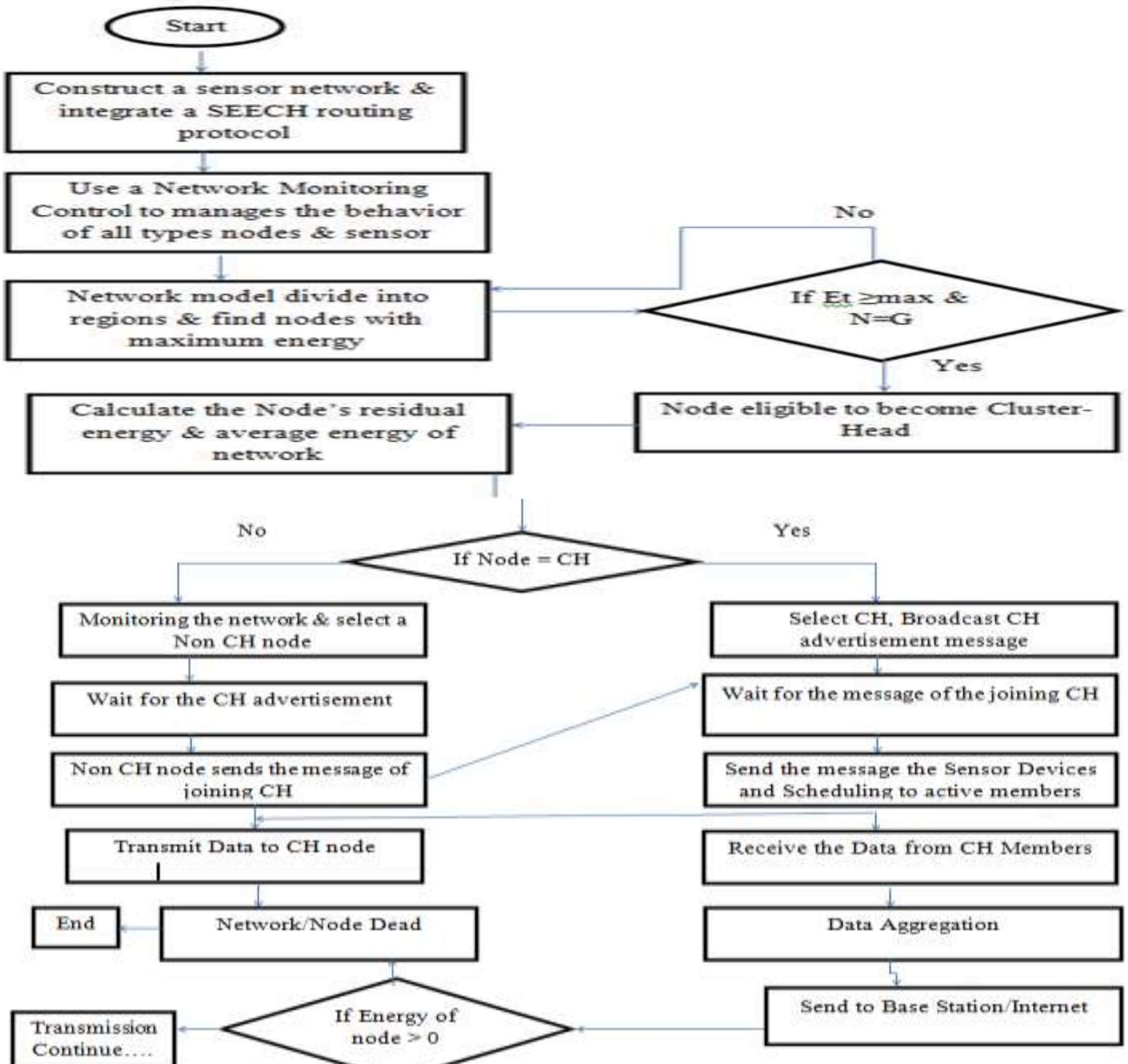

Figure 4: Flowchart of the proposed work.

Simulation Results

Several simulation environments are available for characterising wireless-network behaviour, including NS-2, J-Sim, OMNeT++, MATLAB and GloMoSim. This work uses NS-2.35 to implement and evaluate the proposed protocol.

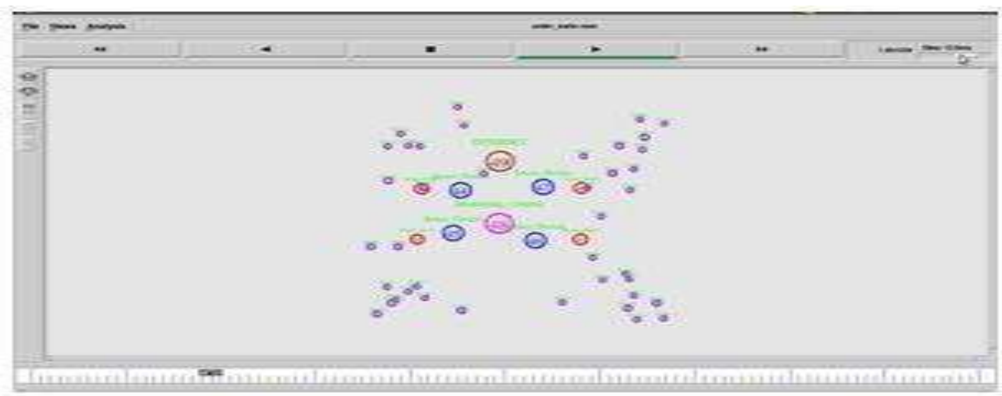

Figure 5: Cluster-head-based monitoring and control.

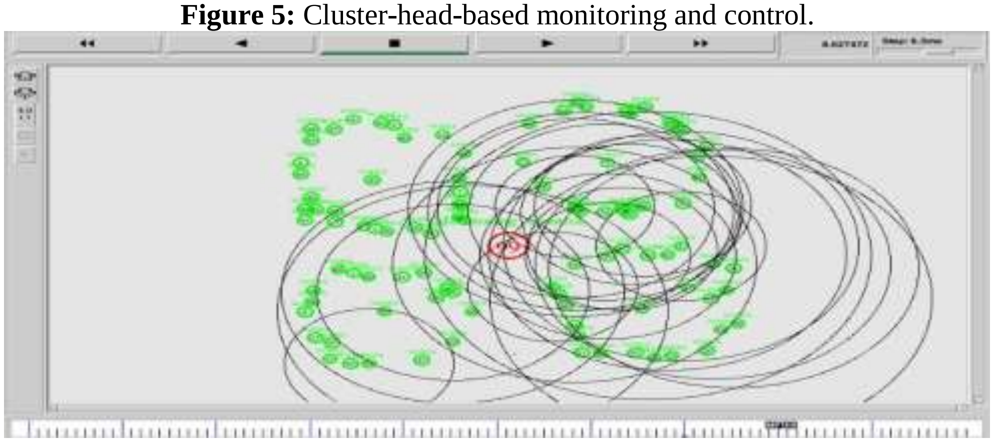

Figure 6: Communication process between sensor nodes.

A. Throughput

The number of packets which are delivered successfully from the transmitting node to the receiving node is known as throughput.

Figure 7: Average throughput.

B. Average End-to-End Delay

When a packet travels from source to destination over an optimum multi-hop route, the elapsed time before it reaches the destination constitutes the end-to-end delay. This metric aggregates several component delays, including those introduced by routing-protocol processing, buffer/queuing delay and transmission delay.

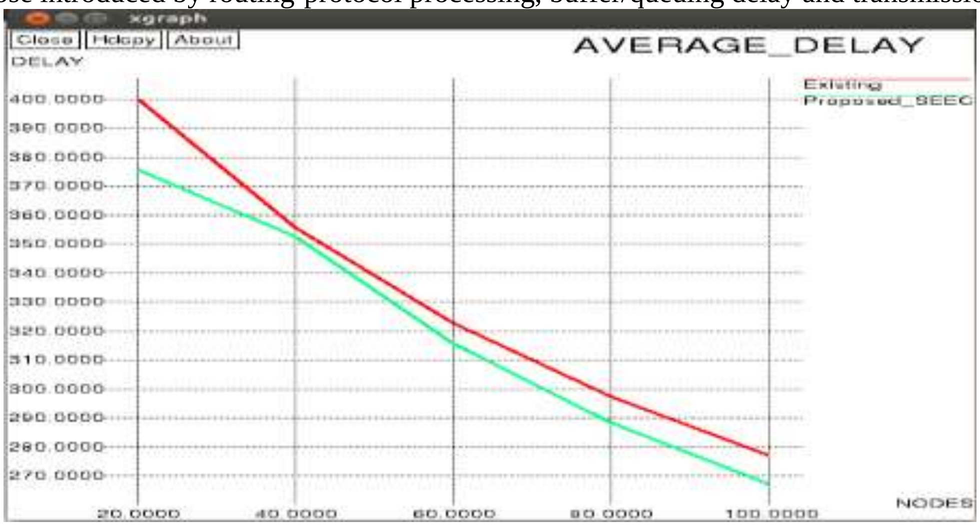

Figure 8: Average end-to-end delay.

C. Energy Consumption

Packet transmission consumes energy at each sensor node, and the amount consumed depends on the node's role — transmitter, cluster head or receiver. A lower measured energy consumption indicates a more energy-efficient routing protocol.

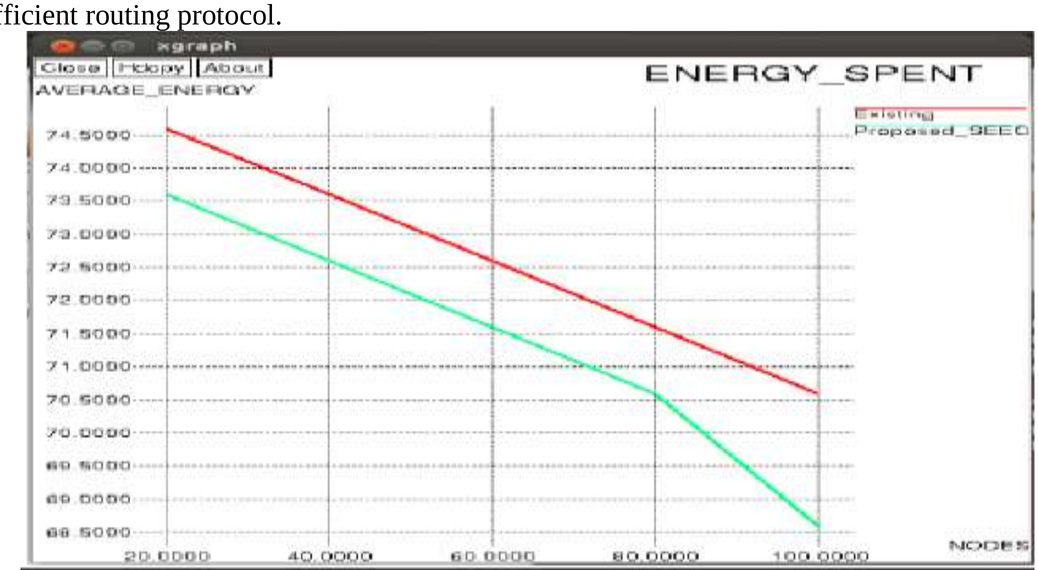

Figure 9: Energy consumption.

D. Packet Delivery Ratio

The packet delivery ratio (PDR) indicates the effective throughput achieved by the network, which is the percentage of packets that arrive at a receiver. A higher PDR means more efficient the network is.

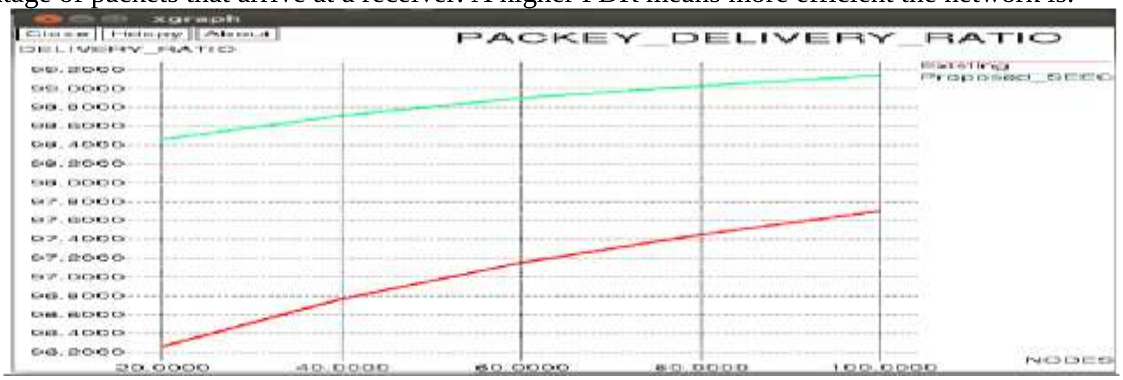

Figure 10: Packet delivery ratio.

Conclusion

Energy-efficient data-aggregation schemes combined with robust security mechanisms can protect crucial network information from malicious nodes while conserving energy through harvesting and delay-tolerant security. The enhanced SEEC protocol proposed here improves the packet delivery ratio, which in turn improves overall data transmission while reducing the incidence of spoofing. Simulation results show that the clustering-based variant of SEEC outperforms the reference protocol on the metrics considered. Because network survivability is governed largely by the energy consumed by the deployed sensor nodes, the demonstrated power efficiency of the enhanced SEEC protocol is a significant outcome. The primary objective of this work — to design, implement and test a cluster-based routing protocol for underwater deployments — was achieved with satisfactory simulation results.

References

[1] W. Kh. Alzubaidi and S. H. Shaker, "Methods of secure routing protocol in wireless sensor networks," J. Al-Qadisiyah Comput. Sci. Math., vol. 10, no. 3, pp. 2521–3504, 2018.

[2] I. Azam, A. Majid, I. Ahmad, and U. Shakeel, "SEEC: Sparsity-aware energy efficient clustering protocol for underwater wireless sensor networks," in Proc. IEEE 30th Int. Conf. Advanced Information Networking and Applications (AINA), 2016.

[3] H. Yu, N. Yao, T. Wang, G. Li, Z. Gao, and G. Tan, "WDFAD-DBR: Weighting depth and forwarding area division DBR routing protocol for UASNs," Ad Hoc Netw., 2016.

[4] C. Zhu, H. Nicanfar, V. C. M. Leung, et al., "An authenticated trust and reputation calculation and management system for cloud and sensor networks integration," IEEE Trans. Inf. Forensics Security, vol. 10, no. 1, pp. 118–131, 2015.

[5] J. Wu, L. Zhang, Y. Bai, and Y. Sun, "Cluster-based consensus time synchronization for wireless sensor networks," IEEE Sensors J., vol. 15, no. 3, pp. 1404–1413, Mar. 2015.

[6] G. Han, J. Jiang, L. Shu, and M. Guizani, "An attack-resistant trust model based on multidimensional trust metrics in underwater acoustic sensor networks," IEEE Trans. Mobile Comput., Feb. 2015.
[7] F. Yuan, Y. Zhan, and Y. Wang, "Data density correlation degree clustering method for data aggregation in WSN," IEEE Sensors J., vol. 14, no. 4, pp. 1089–1098, Apr. 2014.
[8] H. Lin and H. Uster, "Exact and heuristic algorithms for data-gathering cluster-based wireless sensor network design problem," IEEE/ACM Trans. Netw., vol. 22, no. 3, pp. 903–916, Jun. 2014.
[9] T. Ali, L. T. Jung, and I. Faye, "End-to-end delay and energy efficient routing protocol for underwater wireless sensor networks," Wireless Pers. Commun., vol. 79, no. 1, pp. 339–361, Nov. 2014.
[10] K. Ovaliadis, N. Savage, and V. Tsiantos, "A new approach for a better recovery of cluster head nodes in underwater sensor networks," in Proc. IEEE Int. Conf. Telecommunications and Multimedia (TEMU), Jul. 2014, pp. 167–172.
[11] N. Goyal, M. Dave, and A. K. Verma, "Fuzzy based clustering and aggregation technique for underwater wireless sensor networks," in Proc. IEEE Int. Conf. Electronics, Communication and Aerospace Technology (ICECS), Feb. 2014, pp. 1–5.
[12] Y. Han, J. Tang, Z. Zhou, M. Xiao, L. Sun, and Q. Wang, "Novel itinerary-based KNN query algorithm leveraging grid division routing in wireless sensor networks of skewness distribution," Pers. Ubiquitous Comput., vol. 18, no. 8, pp. 1989–2001, Dec. 2014.
[13] Y.-P. Chi and H. P. Chang, "An energy-aware grid-based routing scheme for wireless sensor networks," Telecommun. Syst., vol. 54, no. 4, pp. 405–415, Dec. 2013.
[14] D. Koutsonikola, S. Das, H. Y. Charlie, and I. Stojmenovic, "Hierarchical geographic multicast routing for wireless sensor networks," Wireless Netw., vol. 16, no. 2, pp. 449–466, 2010.