A HYBRID APPROACH ON OPTIMIZING ENERGY CONSUMPTION IN WIRELESS SENSOR NETWORKS

Dr H K Shankarananda
HOD, E&C Department
TMAES Polytechnic (Govt Aided)
Hosapete.

ABSTRACT

Wireless network is the one in which, computer devices communicate with each other without any wire. The communication medium between the computer devices is wireless. When a computer device wants to communicate with another device, the destination device must lays within the radio range of each other. Users in wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are getting more and more popular because of its mobility, simplicity and very affordable and cost saving installation. With the advancement in communication and internet technologies, recently there have been many research efforts in the area of Wireless Sensor Networks (WSNs) to conserve energy. Energy consumption is one of the main problems in the sensor networks and if the consumption of energy increases then the node failure increases which results the failure of the nodes in the sensor networks. The main evaluation indexes include performance of Pareto optimal solution sets, the life cycle of network, the energy consumption of sensor nodes, the energy consumption of relay nodes, the number of living nodes, and the running time of algorithms. Deploying relay nodes is a significant mechanism to prolong the network lifetime of wireless sensor networks (WSNs). However, most existing studies overlook the energy consumption of relay nodes, leading to imperfections in the optimization process.

Keywords: *Wireless network, Energy consumption, internet technologies, conserve energy, optimization process.*

INTRODUCTION

The transmission power in nodes decays in direct proportion to the distance within nodes or between nodes and sink by a 'distance factor squared' or higher order. In case of those applications, where Region of Interest (ROI) covers a large area, the long-haul transmission from far placed nodes communicating in a single-hop lead to their energy depletion. Recent advances in miniaturization and low-power design have led to the development of small-sized battery-operated sensors that are capable of detecting ambient conditions such as temperature and sound. Sensors are generally equipped with data processing and communication capabilities. The sensing circuitry measures parameters from the environment surrounding the sensor and transforms them into an electric signal. Processing such a signal reveals some properties about objects located and/or events happening in the vicinity of the sensor. Each sensor has an onboard radio that can be used to send the collected data to interested parties. In this study, Genetic Algorithm-based Optimized Clustering (GAOC) protocol is designed for optimized CH selection by integrating the parameters of residual energy, distance to the sink and node density in its formulated fitness function. Furthermore, to pact with the Hot-Spot problem, and to shorten the communicating distance from the nodes to the sink, Multiple data Sinks based GAOC (MS-GAOC) is proposed. The optimization technique for CH selection aims to minimize its energy consumption. However, the optimized CH selection towards most energy efficient routing is a non-deterministic polynomial-time hard (NP-hard) problem. Nevertheless, the

selection of CH can be optimized through some metaheuristics methods that incorporate some key factors for CH selection in the process of building up the fitness function.

LITERATURE REVIEW

Noman Hassany (2024) In this study, we propose an improved clustering algorithm for wireless sensor networks (WSNs) that aims to increase network lifetime and efficiency. We introduce an enhanced fuzzy spider monkey optimization technique and a hidden Markov model-based clustering algorithm for selecting cluster heads. Our approach considers factors such as network cluster head energy, cluster head density, and cluster head position. We also enhance the energy-efficient routing strategy for connecting cluster heads to the base station. Additionally, we introduce a polling control method to improve network performance while maintaining energy efficiency during steady transmission periods. Simulation results demonstrate a 1.2% improvement in network performance using our proposed model.

Hend Marouane (2024) Communication in cyber-physical systems relies heavily on Wireless Sensor Networks (WSNs), which have numerous uses including ambient monitoring, object recognition, and data transmission. However, they are vulnerable to cyberattacks because they are connected to the IoT. The effectiveness of recommendation systems is improved with the introduction of context awareness. To lessen the burden on the computer, we first do a principal component analysis and singular value decomposition on the raw traffic data. The system was tested on two datasets, yielding extremely high accuracy results. This is evidence of the system's strength, even when the dataset is changed. On the WSN-DS dataset, the suggested SG-IDS model achieved a 96% accuracy rate, outperforming state-of-the-art algorithms with higher rates of 98% accuracy, 96% recall, and 97% F1-measurement. In an evaluation on an IoMT dataset, the SG-IDS performed admirably, with an accuracy of 0.87 and a precision of 1.00 in intrusion detection tasks.

Shakir Zaman (2022) Information and Communication Technology (ICT) has changed the computing paradigm. Various new channels for communication are created through these developments, and the Internet of Things (IoT) is one of them. Internet of Medical Things (IoMT) is a part of IoT in which medical devices are connected through a network. IoMT has resolved many traditional health-related problems and has some security concerns. This study uses three Machine Learning algorithms, Random Forest, Gradient Boosting, and Support Vector Machine (SVM), to detect cyberattacks. Machine Learning models are best for performing cyberattack detection. Machine Learning models are evaluated on the WUSTL EHMS 2020 dataset, which consists of main in-the middle, data injection, and spoofing attacks. The evaluation of the result analysis shows that the proposed Machine Learning models outperformed existing techniques.

M. Dinesh (2022) Internet of Medical Things (IoMT) is network of interconnected medical devices (smart watches, pace makers, prosthetics, glucometer, etc.), software applications, and health systems and services. IoMT has successfully addressed many old healthcare problems. But it comes with its drawbacks essentially with patient's information privacy and security related issues that comes from IoMT architecture. Using obsolete systems can bring security

vulnerabilities and draw attacker's attention emphasizing the need for effective solution to secure and protect the data traffic in IoMT network. Recently, intrusion detection system (IDS) is regarded as an essential security solution for protecting IoMT network. In the past decades, machines learning (ML) algorithms have demonstrated breakthrough results in the field of intrusion detection. Notwithstanding, to our knowledge, there is no work that investigates the power of machines learning algorithms for intrusion detection in IoMT network.

Nourah Ali (2021) In recent years, the Industrial Internet of things (IIoT) is a fastest advancing innovative technology with a potential to digitize and interconnect many industries for huge business opportunities and development of global GDP. IIoT is used in diverse range of industries such as manufacturing, logistics, transportation, oil and gas, mining and metals, energy utilities and aviation. Although IIoT provides promising opportunities for the development of different industrial applications, they are prone to cyberattacks and demands for higher security requirements. The enormous number of sensors present in the IIoT network generates a large amount of data and has attracted the attention of cybercriminals across globe. The intrusion detection system (IDS) that monitors the network traffic and detects the behaviour of the network is considered as one of the key security solutions for securing IIoT application from attacks. Recently, the application of machine and deep learning techniques have proved to mitigate multiple security threats and enhance the performance of intrusion detection.

Dynamic Voltage Scaling (DVS) Techniques

Authors in describe a cooperative optimization technique that applies DVS and Dynamic Modulation Scaling (DMS) to minimize the power consumption. This technique uses a prediction mechanism to estimate the processor load and the radio communication device based on the log data for a good cooperation. However, it does not rely on the variability of the CPU load parameter which generates temporal irregularity inducing an erroneous result. Therefore, this solution proved to be ineffective to corroborate the performance criteria specific to WSNs.

The paper in aims to minimize the energy of the digital part of a node. To do this, the Quasi Delay Insensitive (QDI) asynchronous logic is used with the software/hardware partitioning of the application. This method implements certain functions of an energy-intensive application on software. The specification of a DVS coprocessor, which is another contribution of this work, allows the control of the processor speed according to a software set point.

Dynamic Voltage and Frequency Scaling (DVFS)

While the frequency (F) is proportional to the voltage (V), the dynamic power is proportional to the square of the voltage. Thus, lowering both (F, V) induces a cubical drop in power. This DVFS hardware strategy hinders the overall performance and brings overheads penalties due to the changes of the (F, V). Software solutions come into play to counter this limitation, including task migration, injection of idle cycles and scheduling that balances the load between the processors to enhance overall energy consumption.

Energy Harvesting Solutions

The emerging trend whereby demand for energy is satisfied, is deploying energy harvesting solutions. The motes provide extra energy by gathering, kinetic (wind, waves, gravity, vibration), piezo, electromagnetic (radio frequencies, photovoltaic), or thermal energy (solar, temperature gradients) for an unlimited amount of time. Harvested energy from irregular and fluctuating sources such as wind power, photovoltaics, capacitive methods, etc., are low and not continuously available to meet the demand of a power system. Indeed, they are often produced away from the consumer places, where local infrastructure is less robust. In smart health applications, recovering energy brings risks and skin infections. Consequently, it would be wise not to equip the network more but to implement an efficient energy management strategy allowing reliable control of the nodes.

HEEPS: A Hybrid Energy-Efficient Power Manager Scheduling

Applying several energy management strategies at once provides more energy benefits than settling on one method. Therefore, we propose an online HEEPS power manager that incorporates three energy management strategies. This results from the trade-off between time constraints and power-modes. By providing a functional modeling of a low power energy manager, the need for manual intervention is minimized. The advent of functional and structural failure risks is eliminated through the use of a robust verification methodology. A low consumption system level model is presented that acts on the wireless sensor network both at the local node level and at the global level, i.e., at the network level.

Model in homogeneous wireless networks

The solution proposed by is to create different schedules, each one associated with a time interval that activates only the set of sensor nodes necessary to satisfy the coverage and connectivity restrictions. The employment of different schedules keeps from occurring the premature starvation from some of the nodes, bringing about a more homogeneous models energy consumption level across the whole network. Moreover, this is provided because the alternation of active nodes among the schedules is often a design outcome, as it optimizes the overall network energy consumption taking into account all time intervals, coverage, and connectivity restrictions.

RESEARCH METHODOLOGY

A Hybrid Tree Construction (HTC) algorithm to achieve the delay aware data aggregation in Wireless Sensor Network is proposed in this chapter. In HTC, a node which has high residual energy is chosen as sink. Each node chooses their corresponding parent and child node among their neighbors through implementing a two-hop tree construction model. The HTC algorithm is developed to construct a data aggregation tree that is suitable for any network scenario as well as that can adopt any aggregation scheduling algorithms. Rest of the nodes chooses their corresponding parent and child node among their neighbors based on its energy level and the distance with neighbors. Distance is measured by the response time (in seconds) of each node for the broadcast request of other nodes. A two-hop tree construction method is followed by all the nodes to find its child and parent nodes. The performance of the proposed algorithm has been studied by applying the delay aware data aggregation algorithm on the data aggregation tree constructed by HTC.

Distance is measured by the response time of each node for the broadcast request in seconds. When a node selects its parent and child, it follows a binary search tree model to construct the aggregation tree. The twohop tree structure is the reason behind the selection of binary search tree model for constructing aggregation tree. The least child nodes send their data to its parent nodes in first time slot. And the parent nodes send the data to its upstream nodes. Similarly, the data aggregation has been performed at the root node through all the parent nodes from its child nodes.

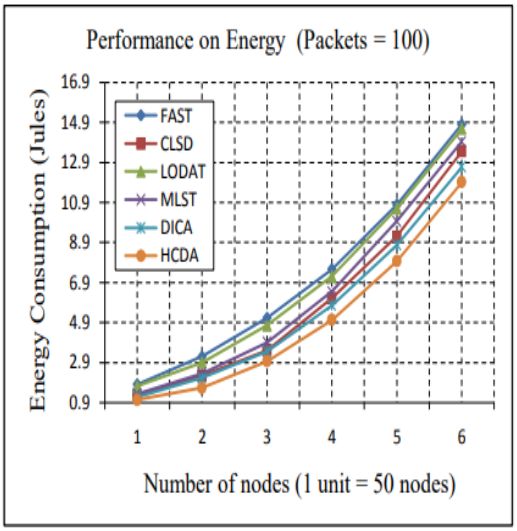
RESULTS AND DISCUSSIONS

For all simulation scenarios, only one node was selected as a sink node which has high residual energy and attached with gateway. The sink is located anywhere in surveillance area. All the nodes in the network generate a broadcast reply of size 64 bytes. Each source generates random data reports of size 136 bytes when it senses data with a constant bit rate (CBR) of 1 packet/sec. Table 1 represents the consolidated simulation parameters and values used to evaluate the algorithm performance. Even the algorithm CLSD, LODAT, MLST and ATC proposed the hybrid scheduling; they did not achieve collision free fast data aggregation. The performance of HCDA has been compared with the existing aggregation scheduling algorithms FAST, CLSD, LODAT, MLST and DICA to prove the efficiency.

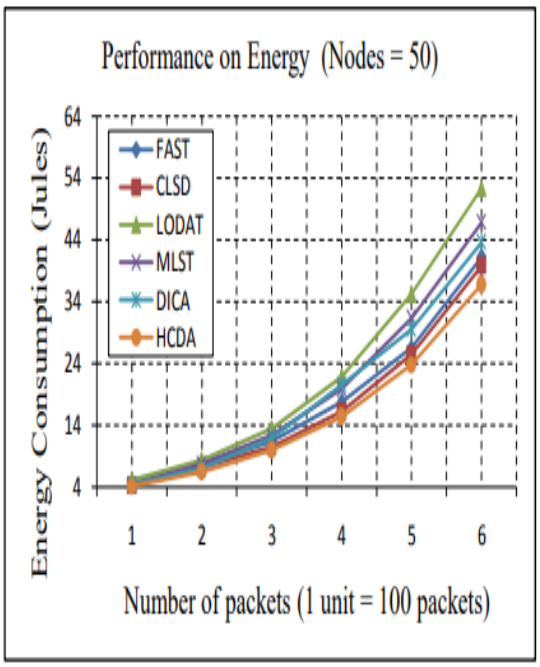
Table 1: Simulation parameters

Simulation Parameters	Values
Simulation Area	200m X 300m
Sink node	1
Number of nodes	50 to 300
Communication radius (m)	15m
mulation time (m)	12
nitial Energy (J)	15
Transmit Energy	660mW
Receive Energy	395mW
Data Packet Size	136 bytes

For all simulation scenarios, only one node was selected as a sink node. The average energy consumption of HCDA has been calculated and compared with the average energy consumed in the existing algorithms. The energy utilization of the sensor nodes is analysed in terms of Joule.



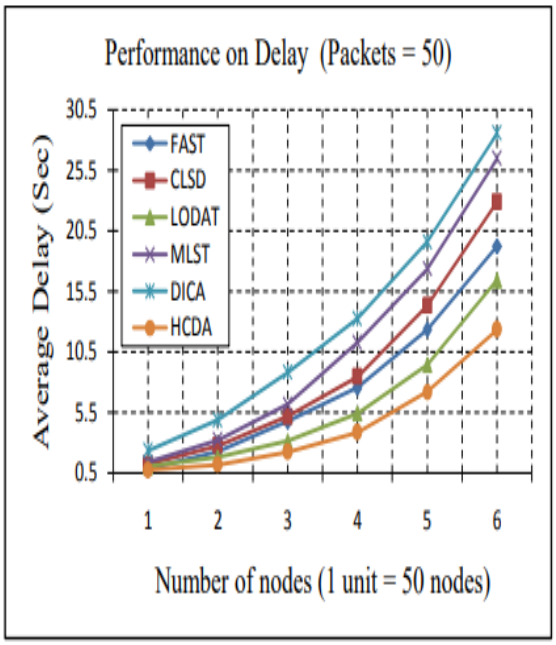
Graph 1: Average energy utilization when packets are constant



Graph 2: Average energy utilization when nodes are constant

Graph 1 and graph 2 show the performance of HCDA on energy. In graph 3 the simulation results were compared with existing models based on the number of nodes to be aggregated in the network. By varying the number of node from 50 to 300 in increments of 50 nodes, the individual energy consumption has been evaluated using equation 4.3 at each node.

The proposed system shows a significant improvement when aggregating 50 packets with 300 nodes. The HCDA aggregates 50 packets with 300 nodes in 12.34 sec which is very less than other compared models.



Graph 3: Average delay when packets are constant

CONCLUSIONS

HEEPS acts on the local and global level when most of the works focuses on the network aspect of the WSNs. Additionally, more power modes are considered compared to other researches. Similarly, the power manager stands out by its hybrid aspect and its combination of several methodologies DPM (time-out2) DVFS (inter task) and GEDF scheduler contributing to more optimality in terms of scheduling. Two conditions of scheduling are combined, which are Goossens, Funk, and Baruah and Srinivasan and Belkadi and non-exploited mainly under the WSNs context. Besides, the STORM simulator is selected to focus more on its many advantages. A significant contradiction is that the battery in the sensor cannot be recharged in most cases, so, the design of the protocols concentrates more on how to reduce energy consumption. The proposed algorithm effectively addresses common challenges such as uneven node distribution, biased cluster head elections, and accelerated energy depletion among

cluster heads. By incorporating load-balancing techniques and ensuring equal opportunities for all nodes to serve as cluster heads, the algorithm enhances network efficiency and prolongs node lifespan. Additionally, features from Adaptive LEACH are integrated to optimize the hop count of transmitted data during the transmission phase from cluster heads to the Base Station (BS), thereby balancing energy consumption and extending network survival time.

REFERENCES

1. *Caroline, B. (2016), "Hybrid Energy-Efficient Transmission Protocol for Heterogeneous Wireless Sensor Networks", Circuits and Systems, issn:2153-1293, vol.7, pages.897-906.*
2. *D. Zeghlache (2010), "Priority-Based Hybrid MAC for Energy Efficiency in Wireless Sensor Networks," Wireless Sensor Network, issn:1945-3086, Vol.2, No.10, pages.755-767.*
3. *Hend Marouane (2024), "Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning", IEEE Access, issn:2169-3536, vol.(99), pages.1-1.DOI:10.1109/ACCESS.2023.3349248*
4. *M. Dinesh (2022), "An investigation and comparison of machine learning approaches for intrusion detection in IoMT network", The Journal of Supercomputing, issn:1573-0484, vol.78(4), DOI:10.1007/s11227-022-04568-3*
5. *Noman Hassany (2024), "A Hybrid Approach for Energy Consumption and Improvement in Sensor Network Lifespan in Wireless Sensor Networks", Sensors, issn:1424-8220, vol.24(5), pages.1353.https://doi.org/10.3390/s24051353*
6. *Nourah Ali (2021), "Deep Learning Approaches for Intrusion Detection in IIoT Networks – Opportunities and Future Directions", International Journal of Advanced Computer Science and Applications, issn:2156-5570, vol.12(4), DOI:10.14569/IJ ACSA.2021.0120411*
7. *Shakir Zaman (2022), "Cyberattacks Detection in IoMT using Machine Learning Techniques", Journal of Computing & Biomedical Informatics, issn:2710-1614, vol.4(01), DOI:10.56979/401/2022/80*
8. *Tao Li (2020), "DeepFed: Federated Deep Learning for Intrusion Detection in Industrial Cyber-Physical Systems", IEEE Transactions on Industrial Informatics, issn:1941-0050, vol.17(8), pages.5615-5624.DOI:10.1109/TII.2020.3023430*
9. *Venugopal, K. (2009), "Dynamic Hierarchical Communication Paradigm for Wireless Sensor Networks: A Centralized, Energy Efficient Approach", Wireless Sensor Network, issn:1945-3086, vol.1, pages.340-349.*
10. *Y. Pan (2009), "An Energy-Aware Clustering Approach for Wireless Sensor Networks," International Journal of Communications, Network and System Sciences, issn:1913-3723, Vol.2, No.2, pages.131-141.*