

Energy Efficient Routing Protocol for Wireless Sensor Networks at Node Level Routing and Multihop Routing

Pavan R. Jagtap, Dheeraj D. Shirbhate and Harshal D. Gurad

¹Asst. Professor, JDIET, Yavatmal
pvnjacks50@gmail.com

²Asst. Professor, JDIET, Yavatmal
shirbhate.dhiraj@gmail.com

³Asst. Professor, JDIET, Yavatmal
guradharshal@gmail.com

ABSTRACT

The objective of energy efficient routing protocol is to increase the operational lifetime of the wireless sensor networks. Multipath routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among multiple paths instead of a single optimal path. The disjoint multipath routing scheme with secret sharing is widely recognized as one of the effective routing strategies to ensure the safety of information. To this end, a three-phase disjoint routing scheme called the Security and Energy-efficient Disjoint Route (SEDR) is proposed. Based on the secret-sharing algorithm, the SEDR scheme dispersively and randomly delivers shares all over the network in the first two phases and then transmits these shares to the sink node. New distributed topology control technique is presented that enhances energy efficiency and reduces radio interference in wireless sensor networks. Each node in the network makes local decisions about its transmission power and the culmination of these local decisions produces a network topology that preserves global connectivity. Central to this topology control technique is the novel Smart Boundary Yao Gabriel Graph (SBYaoGG) and optimizations to ensure that all links in the network are symmetric and energy efficient. Our protocol assumes generic MAC protocols and aims at prolonging the lifetime of networks by making residual energy of sensor nodes more evenly distributed. One of the generic application define as Underwater sensor network (UWSN) has emerged in recent years as a promising networking technique for various aquatic applications. Due to specific characteristics of UWSNs, such as high latency, low bandwidth, and high

energy consumption, it is challenging to build networking protocols for UWSNs. Here, we carried out the observation among the routing protocol for WSNs in the direction of topology control, disjoint multihop, Reinforcement Learning technique and Improve the security using the asymmetric (public) key crypto system. To generate the digital signature, MD5 hash function is used. The private and public keys are generated using the RSA algorithm. It is a widely used public key crypto system. It may be used to provide both secrecy and digital signatures.

Keywords: energy efficiency, security, disjoint multipath routing

1. INTRODUCTION

Energy efficient routing protocol refers the efficient delivery of the packet at the destination. In such networks applied routing strategy should ensure the mining of energy consumption and hence extend lifetime of networks. Topology control plays an important role in the design of wireless ad hoc and sensor networks; it is capable of constructing networks that have desirable characteristics such as sparser connectivity, lower transmission power, and a smaller node degree. The objective of energy efficient routing protocol is to increase the operational lifetime of the wireless sensor networks. Multipath routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among multiple paths instead of a single optimal path. We propose an adaptive, energy-efficient, and lifetime-aware routing protocol based on reinforcement learning, e.g. QELAR. Our protocol assumes generic MAC protocols and aims at prolonging the lifetime of

networks by making residual energy of sensor nodes more evenly distributed. In sensor networks the sensor node are small size and communicate unrestrictedly over short distance. Wireless sensor networks (WSNs) have been widely deployed for an extensive range of operation, such as transform each packet into several shares to improve security of transmission. A secure mode disjoint multipath routing protocol for WSN network is proposed. Here, the data packets are transmitted in a secure manner by using the digital signature crypto systems. new distributed topology control technique is presented that enhance energy efficiency and reduce of radio interference in wireless sensor network.

2. BACKGROUND

Methodology for routing protocol is a hybrid of **proactive** and **reactive** protocol, where nodes only keep the routing information of their direct neighbor nodes which is a small subset of the network, so that the drawbacks of both proactive and reactive routing protocols are avoided. The routing information is updated by one hop broadcasts rather than flooding

Proposed methodology proceed with following point of view

- Low Overhead
- Dynamic Network Topology
- Load Balance.
- General Framework

SEDR Methodology is composed of three phases:

- Regional dispersive routing;
- Disjoint identical-hop routing; and
- least-hop routing.

Proposed the SEDR Methodology framework to maximize both the network lifetime and the security . Specifically, SEDR focuses on increasing security by utilizing available energy to forward shares with disjoint routes. In WSNs must aims to security it provides more security by using the digital signature crypto system. This crypto system uses the MD5 hash function and RSA algorithm. Public key encryption is a cryptographic method which uses in WSNs.Asymmetric-key pair: a public key and a private key. Asymmetric key pair is used to encrypt and decrypt messages. Symmetric-key pair: Public key crypto system's counterpart is the symmetric key crypto system and is also used in WSN security. The symmetric key crypto system, uses the same key for both

encrypting and decrypting data. Based on reactive routing proposed Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol. It is a source initiated, reactive (Node/link) disjoint multipath routing protocol. AOMDV extends the Ad hoc On-demand Distance Vector (AODV) protocol to discover multiple paths between the source and the destination in every route discovery

There are several different approaches to topology control and it is possible to organize them into a coherent taxonomy.

1) Control transmitter power

The power control approaches act on the transmission power of nodes using several different techniques. The first distinction to make of power control approaches is between

- homogeneous :Homogeneous topology control is the easier of the two in which nodes are assumed to use the same transmitting power and the problem of topology control becomes in essence one of finding the value of the transmitter range that satisfies a certain network wide property
- nonhomogeneous: In nonhomogenous topology control nodes are allowed to select different individual transmitting powers up to a certain maximum that they can support which means that they will have different transmitting ranges. This form of topology control can be split into three different categories according to the type of information that is used to generate the topology. These three categories are location based, direction based, and neighbor based.

2) Hierarchical approaches change the logical structure of the network in terms of node adjacencies and may be broken down into approaches that use clustering and those that use dominating sets.

4. PREVIOUS WORK DONE

The major technical challenges for realization of industrial WSNs are resource constraints, dynamic topologies and harsh environmental conditions, Quality-of-Service (QoS) requirements, data redundancy, packet errors and variable-link capacity, security, large-scale deployment and ad hoc architecture, and integration with internet and other networks. Most QoS metrics are interdependent such that improving one may degrade the other node [2].Energy efficiency has also been a major design concern for sensor networks. In

underwater environment, because of the much higher transmission and receiving power consumptions of acoustic modems (e.g., 10 W and 3 W of transmission and receiving power, respectively, for the popular WHOI Micro-Modem versus 105 mW and 54 mW for the Crossbow Mica2)[1], the lifetime of a network is prolonged by allowing interleaving recovery time during battery usage. However, it assumes geographical information known to each node [1].

Along with the disjoint multipath routing this can be generally summarized as follows:

- 1) Deterministic disjoint multipath routing and
- 2) Randomly disjoint multipath routing

Both routing strategies focus on transmitting copies of packets along the disjoint routes, which are calculated by some multipath routing algorithms. Randomly disjoint multipath routing does not have a fixed candidate route for selection. Some works combine secret sharing and randomly disjoint multipath routing to further enhance the security of WSNs maximize both the network security and lifetime by exploiting an effective randomly disjoint multipath routing scheme with secret sharing [3]. Optimal path between the source and destination is selected by the routing protocols to satisfy the resource constraints such as energy, bandwidth and computation power. The routing protocols take into account the metrics like minimum hop, minimum transmission cost, high residual energy etc to route the data [4]. Topology control is one of the most important techniques used in WSNs to reduce energy consumption and radio interference. It lends itself to the mechanisms of multihop communication and energy-efficient operation. Topology control aims to control the graph representing communication links between nodes, with the purpose of meeting a global property of the graph such as connectivity, while reducing energy consumption and radio interference [2]. In the SEDR (secure and energy efficient disjoint multipath routing) scheme, focus on transmitting the shares of packets along the routes distributed in the whole network to enhance the security of the network. Intuitively, the diversity of routes is proportional to the network security. However, the energy consumption of sensor nodes may increase at the same time, which may also lead to a decrease in network lifetime [3]. To simplify the analysis of the relationship between network security and lifetime, the impact of different parameters, such as energy consumption and distance from the sink node to the sensors, As the energy

consumption of sensor nodes is uneven caused by the many-to-one traffic pattern, we analyze the relationship between sensor nodes' energy consumption and locations in each phase [3].

5. EXISTING METHODOLOGY

In the recent past various proposed work attempted to implement security in WSNs using public key encryption. Public key cryptography provides authentication and confidentiality. The high processing overhead and energy cost make the implementation of public key cryptography in WSNs impractical. Public key encryption is a cryptographic method which uses an asymmetric-key pair: a public key and a private key. Asymmetric-key pair is used to encrypt and decrypt messages. The public key is made public and is distributed widely and freely. The private-key need not be distributed and it is kept secret. Symmetric-key pair: Public key crypto system's counterpart is the symmetric key crypto system and is also used in WSN security. The symmetric key crypto system uses the same key for both encrypting and decrypting data.

Energy Efficient Node Disjoint Multipath routing Protocol (EENDMRP) is a sink initiated, proactive node disjoint multipath routing protocol. The sink node starts the multipath route construction phase to generate its routing tables. During this process, Route CONstruction (RCON) packets are exchanged between the nodes. Each sensor node broadcasts the RCON packet once and maintains its own routing table. The format of the RCON packet is as shown in the Fig. 1. EENDMRP detail in two phases: (i) route construction phase and (ii) data transmission phase (shows in fig). The security in EENDMRP is designed using the asymmetric (public) key crypto system. To generate the digital signature, MD5 hash function is used. The private and public keys are generated using the RSA algorithm. It is a widely used public key crypto system. It may be used to provide both secrecy and digital signatures. Its security is based on the intractability of the integer factorization problem.

Packet Type	Hop Count	Forward ID	Threshold Energy	Route	Forwarder's Public Key
1 Byte	2 Bytes	2 Bytes	4 Bytes	2 Bytes	4 Bytes

Fig. 1. Format of route construction (RCON) packet.

NODE ID	Hop Count	Node Cost	Residual Energy	Node Disjoint Paths	Neighboring node's Public Key
---------	-----------	-----------	-----------------	---------------------	-------------------------------

Fig. 2. Format of node routing table.

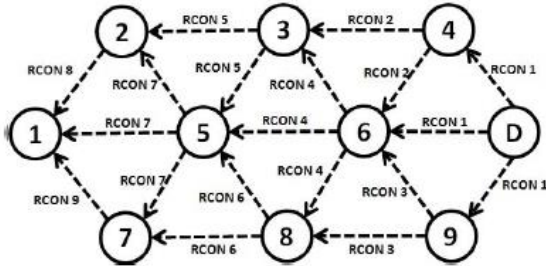


Fig. 3. Route construction phase in EENDMRP.

Fig. phase of EENDMRP[1]

SEDR Methodology describe framework to maximize both the network lifetime and the security. Specifically, SEDR focuses on increasing security by utilizing available energy to forward shares with disjoint routes. SEDR Methodology is composed of three phases:

- 1) Regional dispersive routing;
- 2) Disjoint identical-hop routing; and
- 3) least-hop routing.

Based on the (T, M) -threshold secret sharing mechanism, such as the Shamir's algorithm, to break the packet into M shares, the M shares are sent to M randomly selected sensor nodes in the regional dispersive routing phase. In the disjoint identical-hop routing phase, M shares are transmitted to other sensor nodes that are dispersive distributed in the network with disjoint routes, where all the sensor nodes along the same routing path have equal hops to the sink node. Finally, the SEDR scheme uses the shortest routing path to forward the M shares to the sink node.

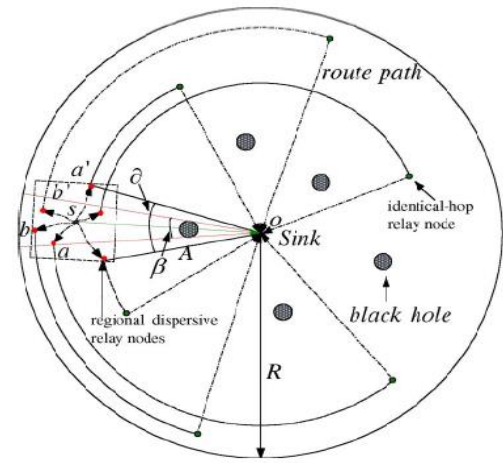


Fig. 4 Example of the SEDR scheme [3]

In order to develop a technique that produced a network topology that met the objectives that have been set out and that adhered to the identified requirements and conformed to the choices made, it was decided to create a graph algorithm that is a hybrid of different proximity graph algorithms. The algorithm is a mixture of the Gabriel graph algorithm and the Yao graph algorithm, with the use of smart region boundaries. The algorithm is referred to as the Smart Boundary Yao Gabriel Graph (SBYaoGG).

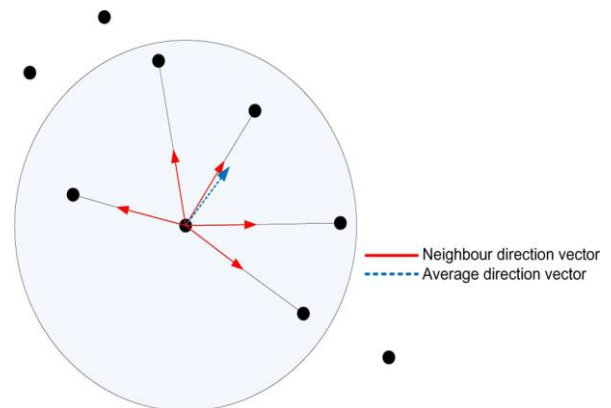


Fig. 5. Neighbor direction vectors and the average direction vector.

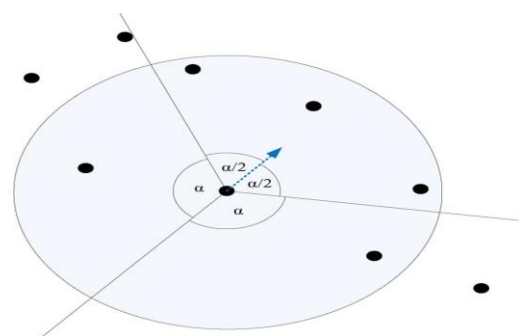


Fig. 6. Yao graph boundaries using an average direction vector.

The cones of the Yao graph are as shown in Fig. 6. corresponding to a Yao graph with three cones. It can be seen that aligning the axis of one of the cones to the average direction vector, results in a cone where a high number of neighbor nodes fall into. It is possible that in certain arrangements all the neighbors will fall into this cone, which will mean that the number of edges calculated during topology control will be reduced.

An option was to use the neighbor centroid, for the following reason: Opposed to the average direction vector, the centroid has the drawback that neighbors that are further away will have coordinates that dominate over closer neighbor coordinates. The average of unit direction vectors overcomes this drawback. Selection of Yao graph is necessary to maintain connectivity. The largest value of Yao graph was used in simulations when setting the boundaries of the Yao graph, in order to reduce the node degree as much as possible, while maintaining connectivity.

The major contribution of our approach is that for the first time, apply the Q-learning technique in a distributed routing protocol for UWSNs to balance workload among sensor nodes for longer network lifetime, to reduce networking overhead for higher energy efficiency, and to learn the environment effectively and efficiently for better adaptability to dynamic networks.

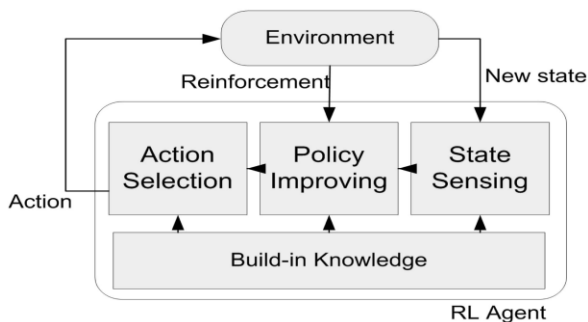


Fig. 6. The framework of reinforcement learning

Reinforcement Learning technique (RL), which is the theoretical basis for our protocol. We then describe the Q-learning algorithm, and adopt it in our routing protocol. We map the routing problem to the state space formulated in the general framework of RL. The technique of Reinforcement Learning (RL) provides us a framework, by which a system can learn to achieve a goal in control problems based on its experience. Fig. 1 depicts the framework of RL. An agent in RL chooses actions according to the current state of a system and the reinforcement it receives from the environment. Most RL algorithms are based on estimating value functions,

functions of states (or of state-action pairs), which evaluate how good it is for the agent to be in a given state

6. ANALYSIS AND DISCUSSION

Energy Efficient Node Disjoint Multipath routing Protocol (EENDMRP) is a sink initiated, proactive node disjoint multipath routing protocol as discussed earlier. The security in EENDMRP is designed using the asymmetric_(public) key crypto system. To generate the digital signature, MD5 hash function is used. The private and public keys are generated using the RSA algorithm. It is a widely used public key crypto system. It may be used to provide both secrecy and digital signatures. Its security is based on the intractability of the integer factorization problem.

SEDR scheme is composed of three phases: 1) regional dispersive routing; 2) disjoint identical-hop routing; and 3) least-hop routing. Based on the (T, M) -threshold secret sharing mechanism, such as the Shamir's algorithm. As the typical many-to-one traffic pattern leads to uneven energy consumption, the sensor nodes close to the sink node have much higher chances of power outage. When one of the sensor nodes is out of energy in WSNs, the nodes far away from the sink node normally have only used 10% of their batteries. More specifically, in our Q-learning-based routing algorithm, the energy consumption of sensor nodes and residual energy distribution among groups of nodes are novel considerations that are put into the reward function. With such a reward function, the forwarding policy can be improved at runtime, so as to achieve high energy efficiency and uniform energy distribution, and thus, prolong the network lifetime. Thus, proposed scheme aims at utilizing the redundant energy to dispersively distribute the shares of packets all over the WSNs and then forward these shares to the sink node along the randomized disjoint routes. The scheme enhances the network security by increasing the diversity of disjoint routes, which significantly decreases the probability of packet interception by adversaries. In the meantime, the least required number of shares M is reduced with the improvement of security, which leads to energy savings. Topology control is one of the most important techniques used in WSNs to reduce energy consumption and radio interference. There were two design objectives in developing the envisaged topology control technique for WSNs. The first objective was that it should be energy efficient and the second was that it should have low interference. Performance measures were used to determine

how well these objectives were met. The relative performance of the new technique compared to other well-known approaches to topology control was also used to evaluate how well these objectives were met. It lends itself to the mechanisms of multihop communication and energy-efficient operation. Topology control aims to control the graph representing communication links between nodes, with the purpose of meeting a global property of the graph such as connectivity, while reducing energy consumption and radio interference.

energy-efficient, and lifetime-aware routing protocol, QELAR, to address the issues mentioned above based on Q-learning technique, which is a reinforcement learning technique that solves decision problems. Q-learning is a framework that can be easily extended. Its behavior is largely determined by the reward function, which is used to give a positive or negative reinforcement to the agent after it makes a decision. The effects of different weights in the reward function on the network performance are thoroughly evaluated in simulations. Without any assumption of the underlying MAC, the routing protocol monitors the environment closely and learns to extract needed information, such as the network topology and residual energy of surrounding nodes, since nodes are able to directly exchange the information with its one-hop neighbor nodes to aid each node in choosing adequate forwarders for the next hop.

7. PROPOSED METHODOLOGY

Energy saving at Node Level

This Methodology describes the basic components of wireless sensor node. Suggestions regarding the choice of node components and batteries have been made and the node architecture was studied in detail.

The methods in which energy savings can be affected or can be classified under two heads:

1. Device Level -Hardware component selection and their configuration to achieve low energy consumption in a wireless sensor node.
2. Network Level -Choice of communication methods and protocols to minimize energy consumption. Overall Design

In a Sensor node there are four essential parts: processing unit, sensing unit, transceiver unit and, power unit. This part of Wireless sensor mote (WSM) is built on the Integrated Chip (IC). One needs to choose proper Peripheral of WSM and

configure the entire network which will be more energy efficient. The basic diagram of wireless sensor mote is shown in figure.7 below.

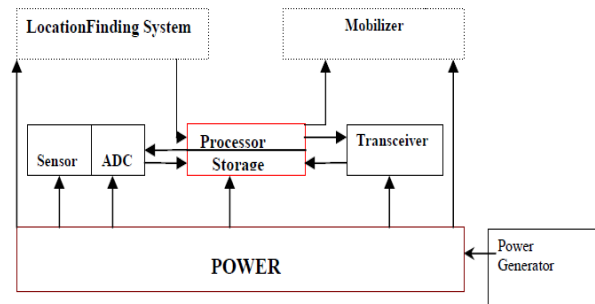


Figure 7: The basic block diagram of the WSN

Processing unit is a part of microcontroller unit which can read sensor data, perform some minimal computations and make a packet ready for transfer in the wireless communication channel. The local memory requirements will not be high and emphasis will be placed on the modes of operation to facilitate low-power operation. The Communication module/unit is typically an RF transceiver that should support the 802.15.4. This unit helps in collecting information and to exchange or control data acquisition. The maximum amount of energy is used in communication module when compared to the two other modules. Sharing information between sensor nodes will consume more amount of energy than implementing the calculation within individual node. In Sensing unit, sensors are literally used for sensing temp, images, gas etc. Sensors to sense different things require different amount of energy, but to sense gas, sensors require more amount of energy than any other applications. Energy saving at Node Level methodology is able to consume less energy which effectively used in design of routing protocol for WSNs. energy efficiency in node can improve using this method it is advantageous for WSNs. Some sensor node parameter may affect on the energy efficiency such as hardware component being used.

8. POSSIBLE OUTCOME AND RESULT

The EENDMRP model is compared with the AOMDV model from different perspectives such as packet delivery fraction, end-to-end delay, normalized routing load and average energy spent. The ratio of the data packets delivered to the destinations to those generated by the constant bit rate (CBR) sources is known as Packet Delivery Fraction (PDF). Average

end-to-end delay includes all possible delays due to buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times of data packets. The AOMDV model is a reactive multi-path routing protocol. When the source node gets data to send, the route discovery is done from the source node to the sink. Normalized Routing Load (NRL) is the number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission. Average energy spent by the sensor nodes in the network is one of the important metrics to evaluate energy efficiency of the proposed routing protocol. Because of the inaccurate residual energy, the energy variance becomes larger as the measurement error increases, which means residual energy is distributed less and less uniformly. However, for the same routing tasks, the energy consumption almost keeps the same, because the number of hops to destination does not change much with the inaccurate energy measurement. At the same time, residual energy error almost has no influence on the packet delivery rate. Since the residual energy of each node is an important factor in our routing protocol, and it may not be accurate with the current estimation system in sensor nodes, we then evaluate the effect of inaccurate battery measurement on the protocol performance. Each time the hardware reports a residual energy value, we introduce a random noise with the maximum value from 0 percent to 10 percent of the residual energy.

Design parameters of our protocol are affecting the network performance, such as delivery rate, latency, energy consumption, and residual energy distribution in QELAR routing protocol. The performance of the SBYaoGG algorithm was evaluated using several performance metrics and compared with that of other topology control algorithms. The metrics that were chosen were those that measure energy efficiency, interference, and the routing efficiency that will be a result of using the topology controlled graph as input to a routing protocol. Theoretical analysis and extensive simulation results show that the SEDR scheme outperforms I-walk in both network security and lifetime under various parameters. The SEDR always outperforms I-walk with the same security requirement since the shares transmitted by the SEDR have lower probability to be intercepted by the adversary, which

leads to a lower required number of shares M and releases the burden of the sensor node with maximal energy consumption.

9. CONCLUSION

Ad hoc on-demand multipath distance vector routing protocol it shows better results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the ad hoc on-demand multipath distance vector routing. This crypto system uses the MD5 hash function and RSA algorithm it provides more security by using the digital signature crypto system. These algorithms provide the security in routing protocol with concern to privacy, authentication and non-repudiation of the data in the network. The multipath routing increases the probability of reliable data delivery. In multi-path routing, the energy cost overhead for data retransmissions due to link failure or node failure and an alternate path construction is minimized due to WSN suffers from many attacks like spoofing or altering the route information, selective forwarding, sinkhole attack, sybil attack, wormhole attack, HELLO flood attack, byzantine attack, resource depletion attack, routing table overflow, routing table poisoning. The disjoint multipath routing scheme with secret sharing is widely recognized as one of the effective routing strategies to ensure the safety of information. In our work, we jointly consider both network security and lifetime issues while aim at designing an efficient secret-sharing-based disjoint multipath routing scheme to enhance both the security and lifetime performance of WSNs. As the typical many-to-one traffic pattern leads to uneven energy consumption, the sensor nodes close to the sink node have much higher chances of power outage. WSNs brings about flexibility, self-organization, self-configuration, inherent intelligent-processing capability, and enables rapid deployment. The major technical problems for realization of industrial WSNs are resource constraints, dynamic topologies and harsh environmental conditions, Quality-of-Service (QoS) requirements, data redundancy, packet errors and variable-link capacity, security, large-scale deployment and ad hoc architecture, and integration with internet and other networks. Most QoS metrics are interdependent such that improving one may degrade the other node. Wireless sensor networks (WSNs) have been widely deployed for an extensive range of applications, such as intelligent transportation, military, and civilian domains.

Designing routing strategies to bypass sensor is one of effective methods for addressing such kind of security issues.

Wireless solutions have benefits in industrial applications such as enhanced physical mobility, reduced danger of breaking cables, less hassle with connectors and ease of upgrading. WSNs, therefore, are an attractive option for industrial applications. WSNs effectively used in underwater sensor network (UWSNs) can be employed in a wide spectrum of aquatic applications, such as environmental observation for scientific exploration, coastline surveillance and protection, commercial exploitation, disaster prevention, assisted navigation, and mine detection.

10. FUTURE SCOPE

In the near future it will likely to the metrics that were chosen were those that measure energy efficiency, interference, and the routing efficiency, focus on new metric measuring energy and QoS parameter with link reliability, and implement security in routing protocol with concern to privacy using crypto algorithm that will be a result of using the topology controlled graph as input to a routing protocol and design an energy-efficient and secure routing scheme for WSNs, considering both packet loss and delay due to the fading channel.

11. REFERENCES

- [1] Tiansi Hu, and Yunsi Fei, "QELAR: A Machine-Learning-Based Adaptive Routing Protocol for Energy-Efficient and Lifetime-Extended Underwater Sensor Networks," *IEEE Transactions On Mobile Computing*, VOL. 9, NO. 6, PP 796-809, JUNE 2010
- [2] Tapiwa M. Chiwewe and Gerhard P. Hancke, "A Distributed Topology Control Technique for Low Interference and Energy Efficiency in Wireless Sensor Networks", *IEEE Transactions on Industrial Informatics*, VOL.8, NO. 1, PP 11-19, February 2012
- [3] Anfeng Liu, Zhongming Zheng, Chao Zhang, Zhigang Chen, and Xuemin (Sherman) Shen, Fellow, "A Secure and Energy-Efficient Disjoint Multipath Routing for WSNs" *IEEE Transactions On Vehicular Technology*, VOL. 61, NO. 7, PP. 3255-3265, SEPTEMBER 2012
- [4] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks"

IEEE Sensors Journal, VOL. 12, NO. 10, PP 2941-294,9
OCTOBER 2012