Multi Hop Secure and Energy Aware Routing in Wireless Sensor Network

R. Logeswari[1]Mr.V.Manimaran[2]

[1]PG Scholar, [2]Assistant Professor, Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamil Nadu

ABSTRACT - *Sensor nodes widely used to gather and forward sensed information and are mostly treated as smart devices. However, besides intrinsic constraints on sensor nodes are vulnerable to a variety of security threats. In this paper an (ESMR) energy-aware and secure multi-hop routing protocol by using a secret sharing scheme to increase the performance of energy efficiency with multi-hop data security against malicious actions are proposed. The ESMR protocol comprises three main aspects. In this first, based on the node selection the network field is segmented into inner and outer zones. Furthermore, in each zone, on the basis of node neighborhood vicinity numerous clusters are generated. Second aspect is, the data transmission from cluster heads in each zone towards the sink node is secured using the proposed efficient secret sharing scheme. The proposed solution evaluates the quantitative analysis of data links to minimize the routing disturbance, in the end. This work provides a lightweight solution with secure data routing in multi-hop approach for the wireless sensor networks (WSNs).*

Keywords: *Clusters formation, multi-hop, secret sharing, secure routing, route maintenance, PDV, throughput.*

I. INTRODUCTION

Wireless Sensor Networks (WSN) are composed of multiple wireless sensor nodes, that has the advantages of low power consumption, low cost, distributed protection, self-organization and so on. WSN is mainly used in environmental and medical monitoring, military surveillance, intelligent transportation and so on. In this case, WSN nodes typically work in an untrusted environment. [1]. Mainly the basic goal of WSNs is to distribute sensor nodes randomly in unattended locations. It provides the connectivity wirelessly. [2] Mostly in traditional networks, different routing algorithms are developed to the development of network and to increase the performance in terms of delivery ratio and latency [3].

In Wireless Sensor Networks to transfer the data from source to destination, the source node can directly interact with the destination node or may interact with the router nodes that can act as an interface between source and destination nodes. Thosenetwork with router nodes is known as multi-hop networks [4-6]. The lifetime of WSN depends upon following characteristics: communication medium, resource limitations, coverage and connectivity, fault tolerance, (quality of service) QoS requirements, mobility and deployment [7]. Any time, sensor nodes can leave and joins a network and change their locations, hence WSN uses a highly dynamic network topology [8]. Due to the (broadcast) deployment nature of WSNs, Sensor Networks are less reliable, failure-prone and susceptible to several attacks, such security attacks like on-off attack, Sybil attack, etc. [9][10]. The trade-off analysis between transmission distances and energy consumption, the multipath collaborative communication is compared with the single-input-single-output (*SISO*) system. *SISO* is suitable for short distances Collaborative communication performs better over the long distance [11]. First construct an Energy Efficient model under FD scheduling with power control in multi-hop wireless networks. By exploiting the Reformulation Linearization Technique (RLT) to reformulate the objective function term and SINR term, and the piece-wise linearization method [12].

Sensor Networks divide the network into clusters, each of which has a cluster head (*CH*) and serving as an intermediate between the aka member nodes, cluster nodes, and the base station (*BS*) [13].Cluster Headhas the highest energy level in the cluster and the CH gathers data, aggregates them and delivers them to the (*BS*).In WSN behavior of sensor nodes can be monitored by neighbor nodes. Sensor nodes are highly constrained in computing power, memory, bandwidth and energy, by monitoring the behavior of nodes it is not enough to judge the trust degree of nodes only [14]

II. RELATED WORK

In recent years, due to low cost smart devices the wireless technology provided a chance to design and maintain the coverage area. Smart devices are always known as sensor nodes that have various functionalities. Sensor nodes are always interconnected in ad-hoc infrastructures by means of wireless links to capture the information, process it, and send it back towards the BS or sink node. Hence Sensor nodes are broadly explored in various applications, i.e., smart homes, smart cities, agriculture, military, and healthcare. For the improvement of network scalability, network lifetime, and communication overheads, cluster based solutions have been presented by the research community. As open media are full of network threats and malicious activities the proposed solutions are overlooked in security perspective. The selection of cluster head is the leading part in the cluster formation process, as it has to perform various other activities rather than its local information gathering.

For the energy-efficient WSN with a mobile sink node a novel ring partitioned based MAC (RP-MAC) protocol. Weighted Voronoi diagram (WVD) algorithm initiates a clustering phase is initiated by assigning a weight value for each node. By enabling novel RP-MAC scheduling in each cluster due to idle listening Energy consumption is minimized. In the network collision-free data transmission is achieved by RP-MAC protocol. To minimize energy consumption by reducing the number of transmissions a TFDA scheme is proposed for the data aggregation phase. Routing phase supports both inter-cluster routing and intra-cluster routing [18].

A (TSSRM) trust sensing-based secure routing mechanism with the ability to resist many common attacks and the lightweight characteristics simultaneously, the security route selection algorithm is also optimized at the same time by taking QoS metrics and trust degree into account. [19].LEACH, using greedy algorithm all nodes are organized in the kind of a chain. Via their next-hops all nodes can send and receive data.

III. PROBLEM FORMULATION

Motivation with problem formulation introduces the proposed ESMR protocol with its architecture and algorithms. Network assumptions and model. Different solutions have been presented by researchers for WSNs to facilitate the community in various domains. However, because of the constrained battery power on the part of sensor nodes, mostly proposed solutions have compromised network lifetime. As a result, many researchers are focused to design and implement the solutions in order to prolong the energy efficiency with improved data delivery performance.

Furthermore, as sensor nodes perform communications in open media, malicious nodes can capture the information or even interrupt the data transmission. Although different solutions are presented to secure wireless sensor communication, most of them have network and computational overheads. In addition, the presented solutions provide end-to-end secure communications without evaluating the security on intermediate nodes. Intermediate nodes are treated as forwarders and it might happen that they are compromised. To stripy nodes the forwarders may expose secret information, in such condition. Security threats can be divided into active or passive attacks. In a passive attack, a malicious node only captures congenital data, while on the other hand, in active attacks, a malicious node first captures the information and then changes it and further transmits to its neighbor nodes. Therefore, applying security in a distributed and multi-hop manner by imposing a lightweight solution is another challenging task. In recent years, cluster based solutions have been presented by the research community for the improvement of network scalability, network lifetime, and communication overheads.

IV. PROPOSED MODULES

A. ENERGY-AWARE AND SECURE MULTI-HOP ROUTING (ESMR) PROTOCOL

The following diagram depicts the block diagram for Energy-aware and secure multi-hop routing (ESMR) protocol.

ESMR Protocol segments the network field into inner and outer zones based on the node location. In each zone clusters are generated. Second the data transmission from cluster heads in each zone towards the sink node is secured using multi key generation technique. Third aspect is the proposed solution evaluates the quantitative analysis of data links to minimize the routing disturbance.

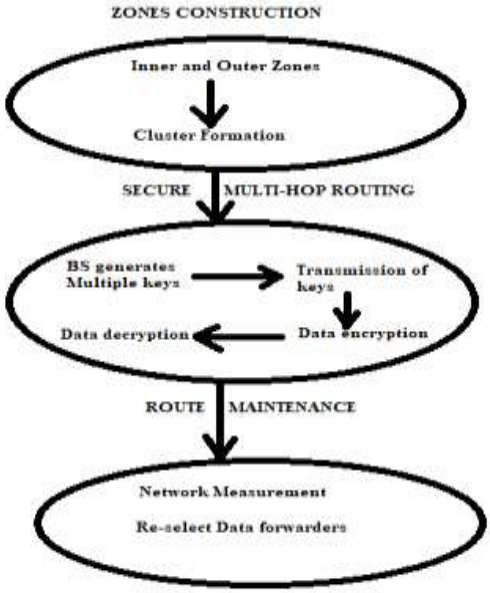

Figure 1

Algorithm

Step 1: Network construction

Step 2: Zones construction

Step 3: Calculating neighbors distance and produce a routing

Step 4: Calculating Dynamic Distance for all nodes

Step 5: Decompose the nodes into particular zones(Location)

Step 6: Calculating parts the zone nodes into clusters

Step 7: Appling for K-NN for each node

Step 8: To transfer Data for secure multi-hop routing

Step 9: Generates multi keys

Step 10: Transmitted to cluster head

Step 11: Calculating for Data packets from zone

Step 12: Procedure route maintenance

Step 13: Active the route and data transfer

Step 14: Calculating energy threshold

Step 15: Threshold level is higher than the Threshold level to announce re-election for cluster head in particular cluster

Step 16: Time out in packet receiving to cluster head re-adjusts data forwarders.

K-nearest neighbors (k-NN) algorithm, the nodes inside each zone is organized into various clusters. All the clusters are arranged in a hierarchical form to accomplish a subsequent data routing. The relationship between the energy consumption and reliable data forwarding, and to propose a secure multi-hop routing approach in an energy efficient manner against malicious threats and multi key it gives a lightweight solution based on the XOR secret sharing scheme in constrained sensor nodes. In addition, it does not impose additional computational overheads on the network. In the third component, route maintenance is performed to identify faulty links in the constructed routing paths and decrease the chances of route breakages and re-transmissions. In such a case, the proposed protocol re-adjusts the forwarders based on the quantifiable measurement and may lead to improved network lifetime with enhanced route reliability.

B. CLUSTERS FORMATION

Cluster based solutions have been presented by the research community for the improvement of network scalability, network lifetime, and communication overheads. However, these solutions are overlooked in security perspective, as open media are full of network threats and malicious activities. In the cluster formation process, the selection of cluster head is the leading part as it has to perform various other activities rather than its local information gathering. Energy aware and secure multi-hop routing (ESMR) protocol by using the XOR based secret sharing scheme to provide energy efficiency and reliable forwarding via secure inter-mediate nodes against data threats.

The ESMR protocol segments network nodes into inner and outer zones is the main contribution in comparison with other protocols based on distance. In addition, each zone is further decomposed into different clusters using the nearest neighborhood locality. The rationale behind such nodes segmentation is to provide energy efficiency and improved network communication with minimal delay.Secondly, to cope with security and data privacy among resource constraints sensor nodes

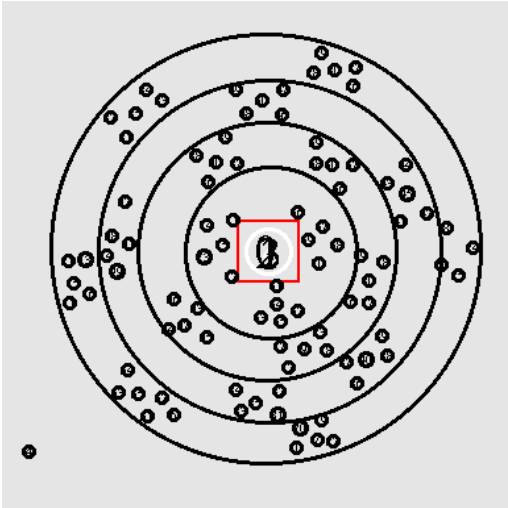

Figure 2

Moreover, the XOR encryption is easier to implement and requires less computational power in the limited resources of sensor nodes. In the end, the route maintenance scheme is accomplished to minimize the routing interruption based on quantitative analysis of the network nodes.

C. SECURE ROUTING PROTOCOL

Energy-aware and secure multi-hop routing (ESMR) protocol based on secret sharing scheme for restricted WSNs is discussed in this section. The details of all its components are to be discussed in the following subsections. The network nodes are decomposed into inner and outer zones based on the distance factor in the first component.

Further, by using k-nearest neighbors (k-NN) algorithm, the nodes inside each zone are organized into various clusters. All the clusters are arranged in a hierarchical form to accomplish a subsequent data routing. In the second component, the main aim is to balance the relationship between the energy consumption and reliable data forwarding, and to propose a secure multi-hop routing approach in an energy efficient manner against malicious threats. It gives a lightweight solution based on the XOR secret sharing scheme in constrained sensor nodes. In addition, it does not impose additional computational overheads on the network. In the third component, route maintenance is performed to identify faulty links in the constructed routing paths and decrease the chances of route breakages and re-transmissions. In such a case, the proposed protocol re-adjusts the forwarders based on the quantifiable measurement and may lead to improved network lifetime with enhanced route reliability.

D. REGION BASED ZONES CONSTRUCTION

Nodes are dispersed randomly to coverage the monitoring square sized area. After the deployment, all nodes are fixed with unique identities.. In the beginning, the BS sends its identity and position information in the sensor field using a multi-hop manner. All nodes received the information of BS via their next-hop and store it in their routing tables. The routing tables of nodes are update based on their neighbor conditions. To send data towards the BS directly the inner zone requires less transmission. However, outer zones make use of their upper zones as intermediates for the transmission of sensory information in an energy efficient manner. Subsequently, the constructed zones are further decomposed into numerous clusters based on the lightweight and simple k-nearest neighbors (k-NN) algorithm.

The K-NN technique is used to group the nearest neighbors into a particular cluster by using the distance function with low computation cost. The value of K is defined by using square root of the number of nodes in a particular zone. When each zone is decomposed into different clusters, then each cluster is given a unique identity to distinguish it from other clusters. Moreover, to decreasethe network cost, a node which is closer to centroid is appointed as an initial cluster head inside each cluster.

E. ROUTE MAINTENANCE

The component of route maintenance is carried out to lessening the chances of route damages and re-forwarding. If the ESMR feels that a cluster head in the upper zone is not suitable for further data forwarding, then it initiates the discovery of alternate routing path. Mainly, the route maintenance process is called in the subsequent conditions.

i. Firstly, whenever in the upper zone the energy resource of the cluster head is less than the specified threshold, the effected cluster head simply quits the data for-warding process and within a particular boundary re-announces the election process. Afterwards, a node that is nearer to the centroid is elected as a new cluster head and updates its status.

ii. Secondly, the performance of the established link between cluster heads $L_{i,j}$are also evaluated based on the packet delay variation (PDV) parameter. The PDV gives an absolute value, which is the difference between two consecutive packets belonging to the same communication link if packet α is transmitted and it covers t_0 time to cross the network, and packet β is transmitted and that covers t_1 time to cross the network, the PDV can be computed by the following equation [22].

$$PDV = |t_0(\alpha) - t_1(\beta)|$$

F. MULTI-KEY GENERATION

All acknowledgment packets to be digitally signed before verified and send out by ACK. However, we fully understand the extra resources that are required with the introduction of digital signature in WSNs. To address this concern, we implemented both the schemes (encryption and decryption schemes). Multiple key generation technique replaces the random keys generated in ESMR (Energy aware secure and multi hop routing) protocol. Hence multi key generation is secure when compared to random key generation.

ENCRYPTION PROCESS:

Step 1: Set the number

Step 2: Set dummy symbol

Step 3: Symbol table and dummy symbol table combine to symbol table with dummy (STWD)

Step 4: Set rotated symbol and rotate data table with dummy

Step 5: Transpose the symbol table after rotation

Step 6: Shift the symbol table after transposition

Step 7: Complement the symbol table after shift

Step 8: Packed control byte table

Step 9: Shift the control byte table

Step 10: After complement combine symbol table and control byte to get cipher text (CT)

The encryption key can be made public and provide the decryption key. That (the public/private key cryptography) is held only by the party wishing to receive encrypted messages. Anyone cannot use the public key for others public keys and to encrypt a message, only for recipient can decrypt it. The relationship between the public/private key pair permits a general rule in mathematical relationship: for one slot of the pair message encrypted with one key can be successfully decrypted with that key's counterpart. If the message is encrypt with the public key means for slot by slot that can decrypt only with the private. The converse is also true.

DECRYPTION PROCESS:

Step 1: Get the cipher text (CT)

Step 2: Separate cipher text into control byte after separation (CBAS) and symbol table after separation (STAS)

Step 3: Shift control byte after separation

Step 4: Pack control byte after shift

Step 5: Complement symbol table after separation

Step 6: Shift symbol table after complement

Step 7: Transpose the symbol table after shift

Step 8: Rotate symbol table after transposition

Step 9: Get plaintext (PT)

V. PERFORMANCE AND RESULT

A. NETWORK LIFETIME

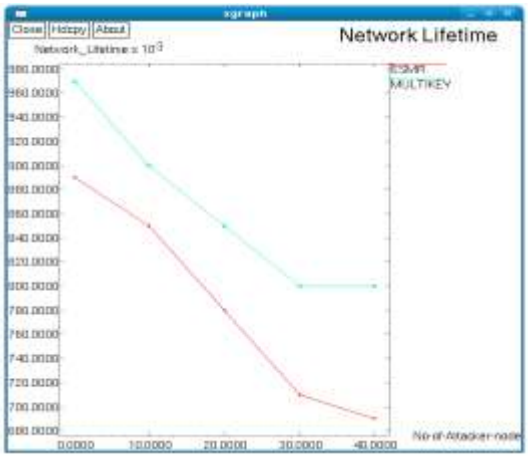

Figure 3

Figure 3 illustrates the performance of the proposed ESMR protocol with multiple key generation technique in comparison with ESMR protocol with random keys in terms of network lifetime. That multi key generation increases the performance of network lifetime when compared to ESMR. Because Multi key generation focuses on both energy efficiency and reliability of the network nodes.

B. NETWORK THROUGHPUT

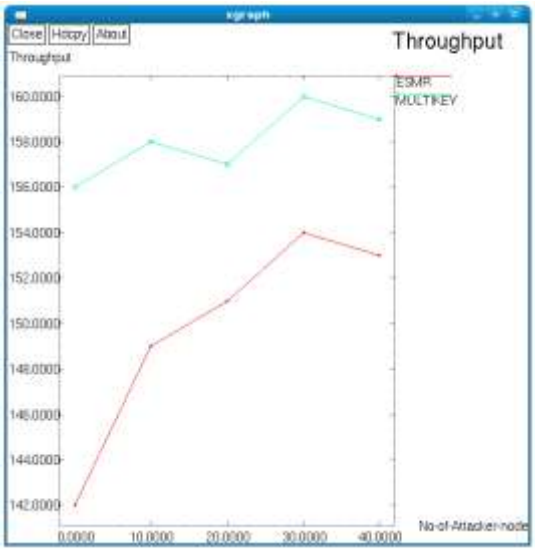

Figure 4

Figure 4 illustrates the performance of the proposed ESMR protocol with multiple key generation technique in comparison with ESMR protocol with random keys in terms of network throughput. Multi key generation increases the performance of network throughput when compared to ESMR protocol. This is due to the fact that Multi key has an energy efficient and robust cluster management along with the incorporation of multi-hop security.

C. ENERGY CONSUMPTION

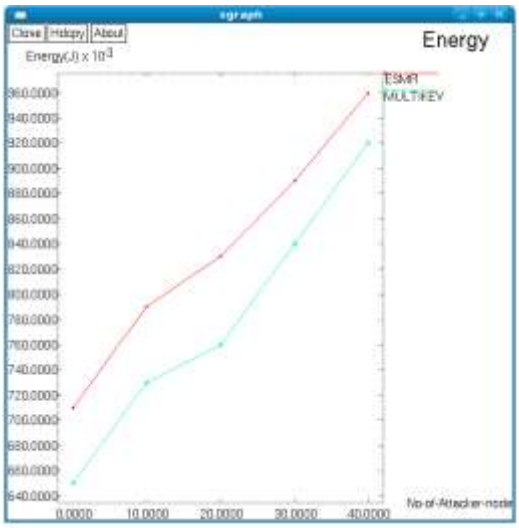

Figure 5

Figure 5 illustrates the performance of the proposed ESMR protocol with multiple key generation technique in comparison with ESMR protocol with random keys in terms of Energy Consumption. That Multi key improves the energy consumption than ESMR due to the formation of cluster heads based on the nearest neighborhood scheme. ESMR outperforms Fr-AODV and TSRF due to the composition of routing paths by incorporating reliable and energy sufficient nodes.

D. AVERAGE END TO END DELAY

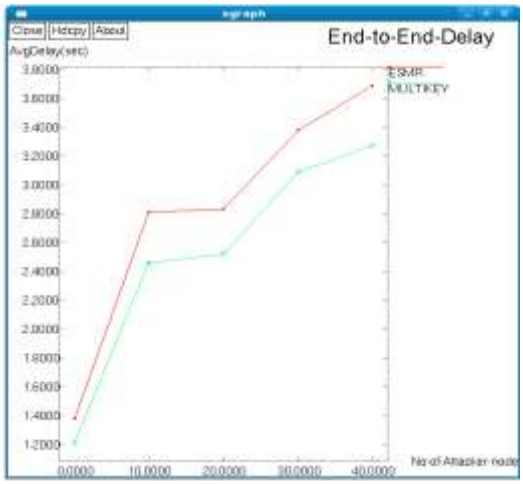

Figure 6

Figure 6 illustrates the performance of the proposed ESMR protocol with multiple key generation technique in comparison with ESMR protocol with random keys in terms of Average end to end delay. Multi key generation improves the end to end delay when compared to ESMR. The longer distance routing paths are more prone to re-transmissions and lead to more end to end delay.

E. CONTROL OVERHEAD

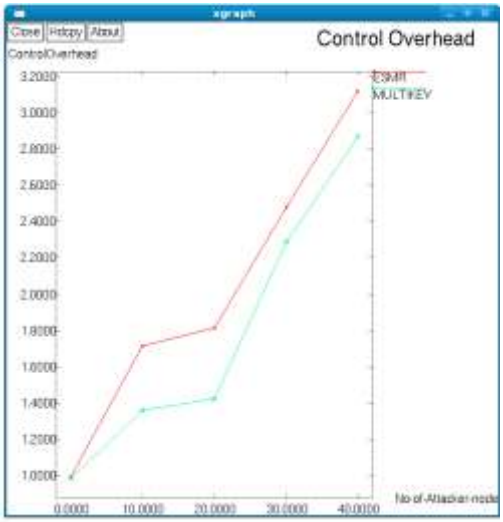

Figure 7

Figure 7 illustrates the performance of the proposed ESMR protocol with multiple key generation technique in comparison with ESMR protocol with random keys in terms of Control overhead. Control overhead gives a vital influence on the evaluation of any data forwarding protocol, as the increase in the control overhead may lead to decreasing energy efficiency and delivery outcomes. Thus Multi key generation improves the performance of control overhead when compared with ESMR.

VI.CONCLUSION

The energy efficiency of an aspirant route is critically dependent on the packet error rate of the fundamental links; because the nodes are directly affect the energy wasted in re-transmissions. The analysis of the interaction between the error rates, number of hops, and transmission power levels make known several key results.In Wireless Sensor Network energy is the most precious resource is to obtain the better results. We have seen various issues in in that energy efficient protocols, so we implement this ESMR protocol with multiple key is generated to overcome this issues. Focus on optimizing the algorithm for efficient energy utilization among all the nodes and for improving the network lifetime.

REFERENCES

[1] Longteng Yi, XiaojunTong , Zhu Wang, Miao Zhang, Honghong Zhu, And Jing Liu “A Novel Block Encryption Algorithm Based On Chaotic S-Box For Wireless Sensor Network “ IEEE Access Volume: 7 2019.

[2] Zahid Ullah, Imran Ahmed, Tamleek Ali, Naveed Ahmad , FahimNiaz, And Yue Cao “Robust and Efficient Energy Harvested-Aware Routing Protocol With Clustering Approach in Body Area Networks” IEEE Access Volume: 72019.

[3] Jiawei Tan, Wei Liu, Tian Wang, Shaobo Zhang, Anfeng Liu, Mande Xie Ming Ma, Ming Zhao “An Efficient Information Maximization based Adaptive Congestion Control Scheme in Wireless Sensor Network” IEEE Access Volume:7 2019.

[4] Tayyab Khan, Karan Singh, Le HoangSon, Mohamed Abdel-Basset, Hoang Viet Long, SatyaP.Singh,ManishaManjul “ANoveland Comprehensive Trust Estimation Clustering Based Approach for Large Scale Wireless Sensor Networks” IEEE Access Volume: 7 2019.

[5] Xiao Luo, Yanru Chen, Miao Li, QianLuo, Kang Xue, Shijia Liu, AndLiangyinCheCREDND: “A Novel Secure Neighbor Discovery Algorithm for WormholeAttack” IEEE Access Volume: 7 2019

[6] Anwar Ghani , Syed Husnain A. Naqvi, Muhammad U. Ilyas, Muhammad Khurram Khan, And Ali Hassan “Energy Efficiency in Multipath Rayleigh Faded Wireless Sensor Networks Using CollaborativeCommunication”IEEEAccessVolume:72019

[7] Zahid Ullah, Imran Ahmed, Tamleek Ali, Naveed Ahmad , FahimNiaz, And Yue Cao “Robust and Efficient Energy Harvested-Aware Routing Protocol With Clustering Approach in Body Area Networks” IEEE Access Volume: 72019.

[8] Jiawei Tan, Wei Liu, Tian Wang, Shaobo Zhang, Anfeng Liu, Mande Xie Ming Ma, Ming Zhao “An Efficient Information Maximization based Adaptive Congestion Control Scheme in Wireless Sensor Network” IEEE Access Volume:7 2019.

[9] Majid Alotaibi "Security to wireless sensor networks against malicious attacks using Hamming residue method" EURASIPJournalon Wireless Communications and Networking 2019.

[10] Feng Tian , Xin Chen, Shidong Liu, Kun Wang, Xu Yuan And Zhen Yang "On Full Duplex Scheduling for Energy Efficiency Maximization in Multi-Hop Wireless Networks" IEEE Access Volume 62018.

[11] Yuxin Liu, Kaoru Ota, KuanZhang,Ming Ma, NaixueXiong, Anfeng Liu, And Jun Long "QTSAC: An Energy-Efficient MAC Protocol for Delay Minimization in Wireless Sensor Networks" IEEE Access Special section on the Internetofenergy:architectures,cybersecurity, and applications (part II) Volume 62018.

[12] Weidang Lu, Shanzhen Fang, Su Hu, Xin Liu, Bo Li, Zhenyu Na, And Yi Gong "Energy Efficiency Optimization for OFDM Based 5G Wireless Networks With Simultaneous Wireless Information and Power Transfer" IEEE Access Special Section On New Waveform Design Volume 62018.

[13] Muhammad Tahir,FazlullahKhan,SyedRoohullahJan,Izaz Ahmad Khan,Nazim Azim "Inter-Relationship Between Energy Efficient Routing and Secure Communication in WSN" International Journal of Emerging Technology in Computer Science & Electronics(IJETCSE) ISSN: 0976-1353 Volume 21 Issue 2 – APRIL 2016.

[14] KorhanCengizAnd Tamer Dag "Energy AwareMulti-HopRoutingProtocolforWSNs" IEEE Access Volume 62018.

[15] Jingjing Yan, Mengchu Zhou, And Zhijun Ding, "Recent Advances in Energy-Efficient Routing Protocols for Wireless Sensor Networks: A Review" IEEE Access Volume: 42016.

[16] Nami Susan Kurian "Energy Efficiency And Security Based Multihop Heterogeneous Trusted Third Party Protocol In Wsn" International Research Journal ofEngineering and Technology Volume: 05 Issue: 10 | Oct 2018.

[17] Hana Rhim, Karim Tamine, RymaAbassi, Damien Sauveron and SihemGuemara "A multi-hop graph-base approach for an energy-e cient routing protocol in wireless sensor networks" Human Centric Computing and Information Science2018.

[18] MovvaPavani And PolipalliTrinatha Rao "Novel Two-Fold Data Aggregation and MAC Scheduling to Support Energy Efficient Routing in Wireless Sensor Network" IEEE Access Volume 62018.

[19] DanyangQin,SongxiangYang,ShuangJia, Yan Zhang, Jingya Ma, And QunDing"Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network" IEEE Access Volume 5 2017.

[20] Zhiqiang Liu, Bin Liu, And Chang Wen Chen "Buffer-Aware Resource Allocation Scheme With Energy Efficiency and QoS Effectiveness in Wireless Body Area Networks" IEEE Access Volume 52017.

[21] Palanisamy T, Krishnasamy KN "Bayes Node Energy Polynomial Distribution to ImproveRoutinginWirelessSensorNetwork". PLoS ONE 10(10): e0138932. doi:10.1371/journal. pone.01389322015.

[22] Khalid Haseeb, Naveed Islam, Ahmad Almogren, IkramUd Din, Hisham N. Almajed 2, And NadraGuizani "Secret Sharing-Based Energy-Aware and Multi-Hop Routing Protocol for IoT Based WSNs" IEEE Access Volume 7, 2019.