Location Aware Secure Multicast Routing Protocol for balancing Energy and Security in Wireless Sensor Network

[1]D. Bhanu, [2]Dr. N. Mohana Sundaram and [3]Dr. R. Santhosh

[1]Research Scholar, [2]Professor and Head, [3]Associate Professor,
Department of Computer Science and Engineering, Faculty of Engineering
Karpagam Academy of Higher Education, Coimbatore

Abstract
Data authentication and Energy Efficiency is one of the major tasks data transmissions in Wireless Sensor Networks. In existing schemes, there was no analysis or steps made for balancing data integrity and energy consumption of clusters in the network. In this research work, Query based Location Aware Secure Multicast Routing for Wireless Sensor Network is proposed to attain energy efficiency and security. There are three modules involved here. In first module, network model and system overview is introduced to attain more network lifetime. In second module, advanced encryption standard and RC6 algorithm was introduced to provide authentication and data integrity. In third phase, efficient energy routes are established and demonstrated to illustrate network reliability. The proposed protocol is simulated with network simulator tool to analyze the network performance metrics.

Keywords:
Network model, system overview, efficient energy routing, encryption and decryption scheme.

1. Introduction

Wireless Sensor Network consists of sensor nodes where it may located in static or dynamic mode. Installation of base station may be required if it goes for high security. In such cases, the base station may not be installed to work in ad hoc fashion. Energy efficiency is one of the important factors to be considered and needs to be improved in the presence of misbehaving nodes. To avoid misbehaving nodes, there is a need of intrusion detection system or secure routing. From the observation, there is a need of certain protocol to achieve balancing between energy and security. In the proposed work, security scheme is added in the mesh based multicast routing to improve the network lifetime and to provide data authentication. The concept of advanced encryption standard and RC6 algorithm are adopted to provide data authentication and integrity..

Manuscript received November 5, 2024
Manuscript revised November 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.11.14

2. Literature Review

Qiong Shi et.al [1] developed an Information based data authentication protocol for sensor networks to protect the data from the attackers in the presence of misbehaving nodes. Here the concept of trust based reputation model was introduced to isolate attackers using trust threshold vector. The probability of attackers was estimated and reduced by means of secure routing. To identify the shortest path to sink node, the Dijkstra algorithm was adopted to reduce the overhead and improve the packet delivery rate. Two metrics were calculated i.e. remaining energy and hop count to provide reliability of network and to increase the network lifetime using the concept of global optimization.

Sathiya and Nandhakumar [2] proposed an Optimized multipath routing with secure data communication and energy consumption model. For security, the cryptographic techniques i.e. private and public key cryptography were implemented. The main reason for using cryptographic techniques was to attain high resilience to attackers and to provide reliable transmission of packets from end to end. The power consumption was reduced using the energy model. The paths are found and data was transmitted with secure routes. The source node initiated the route discovery process and packets were secured to reduce the packet loss.

Kashif Naseer Qureshi et.al [3] introduced the concept of Cluster based dynamic energy aware routing protocol to improve energy efficiency. The energy resources were managed effectively using gateway clustering. The cluster was formed and loads were reduced on Cluster Head (CH) to reduce energy consumption. The heads were chosen and located on efficient geographical position which is located with nearby position of centroid area to improve coverage. The gateway node was the key to reduce the load balancing and energy conservation.

Abhishek Jain et.al [4] introduced the intrusion detection mechanism using trust vector model. The trust based system architecture was developed to handle outside

attackers with the help of risk analysis module. The cluster group was formed using data aggregation module and identification of right nodes was done with trust model. The attackers were identified and data transmission may be permitted or blocked based on the intruders using intrusion detection module.

Obaidat et.al [5] introduced the new energy based security protocol for heterogeneous sensor networks to provide reliability and scalability of links. The following parameters were used i.e. node energy, link quality and distance between nodes. The next hop in the route was determined to reach packets at sink node quickly. The total load was estimated using energy conservation model. The dynamic trust factor was calculated to ensure secure data communication to isolate the misbehaving nodes.

Lata et.al [6] developed domain routing algorithms using secure routing to route the packets in multi-hop manner and increase the energy efficiency. The nodes were searched using special node algorithm to attain the maximum energy. The packets were transferred between two domains. If any node acts as misbehaving node, then the route will be isolated from the network. The selective random routes forward the data packets and the attackers may not able to hack the information.

Imrana banu and Murali [7] introduced the secure routing protocol to isolate the misbehaving nodes from the network. The intrusion detection and prevention scheme was used in conjunction with energy efficient protocol. The network topology was constructed by the base station with path forming messages. Sensor nodes were tracked by the check node to route data packets to nearby station. The route may be changed randomly to enhance the energy using intrusion detection model.

Zare and Soltanaghaei [8] explored a multipath routing protocol using optimized system to choose the best route from many routes to forward the packets effectively. The best route was acting as primary routes to balance the load from source to sink node. The metrics used for selecting best route were signal to noise ratio, link expiry time and energy metric. The best routes where chosen with highest rank to provide continuous data transmission and energy efficiency.

Arzoo Miglani et.al [9] introduced the concept of trust vector approach integrated with energy aware routing that consists of trust based routing module and trust management module. The trust value of nodes and CH were estimated for choosing best routes and cluster head using trust management module. The individual node estimates direct trust and recommendation node computes the indirect trust value. The original LEACH was modified by trust based routing. The modules involved in the trust aware framework were advertising, clustering, scheduling and steady state routing. The node with more packet dropping rate and least energy was considered as malicious nodes.

Selvi et.al [10] introduced a secure routing approach with trust mechanism to provide efficient data transmission in sensor networks. The malicious nodes were detected using trust score evaluation model. The malicious nodes were identified based on temporal constraints to choose the best route using decision tree algorithm. The effective communication was provided with trust enhanced energy efficient model.

Sutagundar and Manvi [11] explored the multipath routing using location identity for sensor networks based on agent route discovery process based on position of nodes in the network region. The global positioning system module was included to obtain accurate location information of sensor nodes. Localization of sensor nodes was perfectly adopted but failed to balance the energy consumption during high network density.

Chi Trung Ngo and Hoon Oh [12] proposed the location based path detection metric from multipath fading in vehicular ad hoc networks. There were two sets of link quality prediction i.e. existing link quality and enhanced link quality which is reserved for future purposes. The existing link quality was obtained based on packet delivery rate and expected transmission value. The reserved future link quality was done based on future geographical position and predicted packet forwarding distance of ad hoc nodes.

Banerjee and Ghosh [13] introduced a weight based energy efficient multicast routing based on energy drain ratio. The routes were stabled and protected from the attackers. The energy drain rate was not changed in the multicast routes based on current session except the new route. The rediscovery of routes were avoided due to high control message cost. The multipath routes were assigned with weights for entire multicast session.

Xiang Wang et.al [14] explored query based location aware geographic routing protocol to improve the network lifetime. The monitoring area was divided into clusters to reduce the communication overhead. The distance between cluster member and grid center was measured from residual energy and nearby adjacent cluster heads. The next hop routes were chosen based on residual energy and distance between the cluster members.

Vinoth and Omkumar [15] proposed the location aware directional flooding algorithm to increase the energy efficiency. The data loss and latency were reduced due to decision based routing and sleep nodes. The reliability and

latency was improved using flooding mechanism to improve network performance.

Pavani and Rao [16] developed a Cluster based Authenticated Routing Protocol using adaptive particle swarm optimisation (PSO) to find data integrity of sensor nodes. The energy consumption was reduced to improve the network lifetime. Hexagonal sensor network architecture was developed to improve energy efficiency and secure routing and verification.

The paper is organized into 5 phases. First phase total deals with introduction of sensor networks. Second phase analyses the existing schemes and found laggings. Third phase deals with the proposed work and fourth discusses the simulation results. The last phase concludes the work.

3. QLAMSR Network Model

The network model is configured between clusters and gateway node. Gateway node is the path way to allow the exchange of data and control packets based on authentication. The following rules are adopted in the network model. Nodes are either static or mobile based on authentication. The position of CH is flexible and setup inside or outside the sensing area.

Location aware multicast routing

The sensor nodes are deployed in 2D deployment with energy level. The distance between sensor nodes was computed based on received signal strength. Network is represented as M = m_1, m_2, … mk. The distance $d_{l,m.}$ The sensor deployment is adopted to reduce the energy consumption. R indicates the transmission range of coverage area. During the packet transmission, distance between two nodes is estimated. The location of node can be determined based on relative geographical information. Once the distance is estimated, packet will be delivered by matching its row and column address. If it is matched, the subnet address will be ascertained and packets will be delivered to the corresponding cluster member. The received packets with row and column address of secondary CH, then the packets will be immediately delivered to the CH with the matched row and column address. The proposed network environment contains several sensor nodes with different sensing capability and multiple destination nodes. If any event is detected by cluster members, it will be sent to an anchor node and the collected information will be forwarded to CH. Both anchor node and destination node are kept as static. The transmission power is reconfigured by the sensor node during deployment phase. In a cluster region, some cluster members are deployed with Geographic Positioning System (GPS) and rest of the cluster members utilize localization algorithm i.e. trilaeration method [15] to find the location.CH can find the accurate location of cluster members in the region with GPS module that reduces the system cost. The accurate location and motion of individual cluster members can be achieved within threshold accuracy using GPS. If the channel is idle in transmission, sink node is ready to receive the packets forwarded by source node. Slot based scheduling is formed to improve the energy efficiency. Potential node becomes the stable node to relay the packet to the sink node via intermediate nodes. The receiving node sends the beacon message once upon receiving the packets from the source node. The zone ID will be allocated to forward the packets quickly. Only one copy of packet is routed to source node.

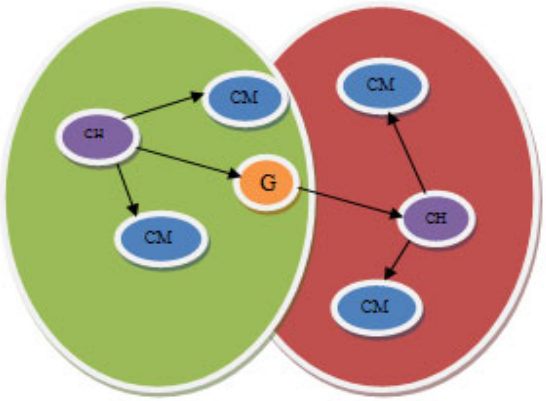

Figure 1. Cluster based Location aware multicast routing

The routing approach is derived as follows.

1. The distance is calculated between source and destination node and perform the mapping process of addresses. The calculation outcome is stored in the packet header.
2. The neighbor node forwards the packets to a node which is located nearby to the destination node. The distance between the co-located node to nearby node of destination node and corresponding sink node is estimated. The distance measured between nearby neighbor node and destination node is forwarded to CH.

3. If a packet moves one hop from its location towards any direction, node decrements 1 in the packet header.
4. Steps 1-3 will be followed until route discovery complete.
5. The energy consumption is reduced by controlling the exchange of control packets. The routing table is not followed to improve the resource usage efficiency. The network burdening is reduced with effective routing.

The location aware multicast routing in the cluster region is illustrated in Figure 1. In this cluster formation, energy routes are established from cluster head to cluster members. The cluster heads can communicate through only gateway nodes.

Data encryption and decryption phase

In this phase, message block is classified into two sub-blocks. The Advanced Encryption Standard (AES) is used to encrypt first sub block and the second one is encrypted using RC-6 algorithm. The message block consists of 256 bits. It is categorized into two parts i.e. p_l[0 to N/2-1] , p_m[N/2-1 to N-1]. The first sub-block is generated by the key K using AES with a block size of 256 bits and length L_k,m.

$$p_l = \sum_{l=0}^{l=\frac{n}{2}-1} A_l \quad 0 \le l \le n/2-1 \tag{1}$$

$$C_l = e_{AES}\left(K_l, A_l\right) \tag{2}$$

where C_l represents the input of ciphers with trusted key and e_{AES} is the AES encryption function. Remaining block of message is encrypted using RC6 algorithm. The security level of message is increased without consuming more execution time using RC6 algorithm. The RC6 algorithm performs better than RC4 in terms of encryption and decryption. Using AES and RC6, two cipher texts are created. The reverse process of encryption is the decryption phase. In this phase, the original plaintext or message will be recovered.

$$p_m = \sum_{k=\frac{n}{2}-1}^{k=n-1} A_l \quad n/2-1 \le l \le n-1 \tag{3}$$

$$C_m = e_{RC6}\left(K_k, A_k\right) \tag{4}$$

$$P_m = D_{RC6}\left(K_f, C_m\right) \tag{5}$$

Identification of shortest path: *Dijkstra algorithm* is used for finding shortest path between two nodes based on minimum hop count. The CHs are communicated and data is transmitted through multi-hop paths. Cluster Head and cluster members are communicated through single hop fashion.

The dijkstra algorithm is an existing algorithm to mitigate the issues in the longer path. In an improved dijkstra algorithm, routing is discovered with fitness value from residual energy, degree of node and distance between source to sink node. Node's behavior is determined based on node intensity and brightness of link. In shortest path finding algorithm, each hop represents the data forwarding path between CH and cluster members.

Algorithm 1: Finding best node

1. Start
2. Destination node broadcasts the hello_message.
3. For all sensor nodes
4. Update the location of sensor node with velocity
5. Map the next location with the closed neighbors
6. Determine the fitness of node
7. Update the best node to CH
8. If iteration = high ? then
9. Pbest node
10. Else
11. Increment best nodes
12. End

Estimation of route energy efficiency through Channel capacity

In this phase, route energy efficiency is estimated from the link efficiency and channel capacity. The channel capacity using Shannon's theorem is given as,

$$C_k = B\log_2(1+SNR) \quad (6)$$

where C_k is the capacity of discrete valued channel k, B is the bit rate of a channel and SNR means signal to noise ratio. The total energy spent for data transmission is E_t. The energy E_k spent for bit transmission per distance d is estimated as,

$$E_k = E_t \times d \quad (7)$$

The efficiency of link (L_e) is estimated as,

$$L_e = \frac{C_k}{E_k} \quad (8)$$

The Route efficiency (R_e) is computed from the link efficiency and it is given as,

$$R_e = Min\{L_{e1}, L_{e2}, ...L_{em}\} \quad (9)$$

Residual Energy ratio (RE_r) is measured between CH and destination cluster member. Let the residual energy of neighbor cluster members is represented as *RN(1), RN(2), ... RN(m)*. The low and high residual energy is represented as R_{low} and R_{high}

$$RE_{low} = Low(RN(1), RN(2), ...RN(m)) \quad (10)$$

$$RE_{high} = High(RN(1), RN(2), ...RN(m)) \quad (11)$$

$$RE_r = \frac{RE_{low}}{RE_{high}} \quad (12)$$

The cluster head maintains the Residual energy ratio throughout the entire route maintenance process.

QLAMSR packet format

Cluster head ID	Energy route ID	Cluster member ID	Encrypted and decrypted code	CRC
2	2	2	4	4

Figure 2. Packet format of QLAMSR

Figure 2 illustrates the packet format of QLAMSR. The first field is the cluster head ID and energy route ID and cluster member ID occupies the 2 byte field. For encryption and decryption, 4 byte field is used and CRC is used for error detection and correction.

4. Simulation Setup

The proposed protocol QLAMSR is simulated using open source tool i.e. NS (2.34). In the simulation setup, 100 nodes are deployed in the coverage area 1000 x 1000 sq.m. Mobility model used for simulation is Random Way Point. Language used is Tool Command Language (TCL). Table 1 shows the simulation settings of proposed protocol.

Table 1. QLAMSR protocol settings

No. of sensor nodes	100 nodes
Routing protocol	LEACH
Coverage area	1000 x 1000 sq.m
Mobility model	Random Way Point
Traffic	Poisson
MAC	IEEE 802.15.4
Frequency band	2.4 GHz
Packet rate	5 packets/sec

Simulation Parameters:

End to end delay: The delay measured from source to destination node during packet transmission.

Network lifetime: It is the lifetime of network where it consumes minimum energy after packet transmission.

Detection ratio: It is the ratio of detected misbehaving nodes to total number of cluster members.

Encryption time: It is the time for encrypting the data packets before reception.

Link reliability ratio: It is the ratio of reliable links to total number of links present for transmission.

The proposed protocol QLAMSR is compared with previous schemes DEESR [5], WEEM [13] and LEDMPR [11]. Table 2 shows the comparative analysis of Proposed and Existing schemes with data taken from simulation analysis.

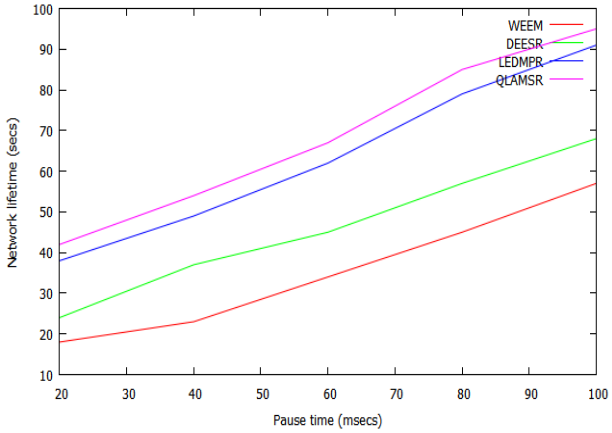

Figure 3. Network lifetime Vs Pause time

Figure 3 illustrates the network lifetime comparison of existing and proposed schemes. It is seen that QLAMSR produces more network lifetime than existing schemes. It is because of selection of reliable route to deliver packets while consuming less energy.

because of selection of reliable route to deliver packets while consuming less energy.

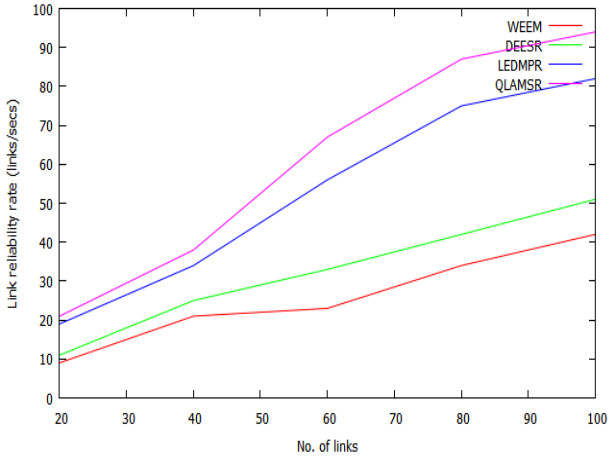

Figure 4. Link reliability rate Vs No. of links

Figure 4 presents the link reliability rate comparison of proposed and existing schemes while varying number of links from 20 to 100. From the results, it is seen that QLAMSR attains more reliability rate than existing schemes.

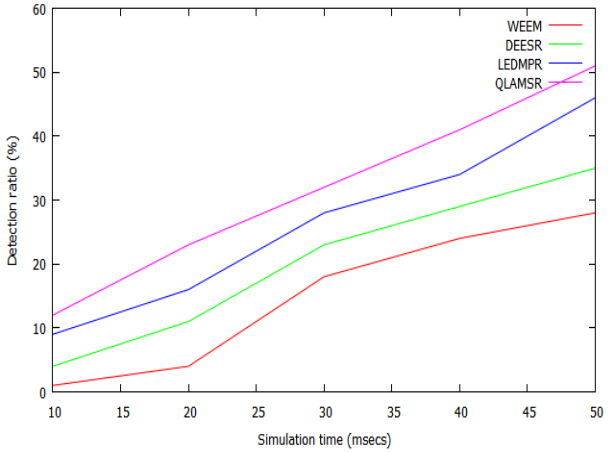

Figure 5. Detection ratio Vs Simulation time

Figure 5 illustrates the performance of detection ratio for QLAMSR, LEDMPR, DEESR and WEEM. Detection ratio of QLAMSR is better than existing schemes.

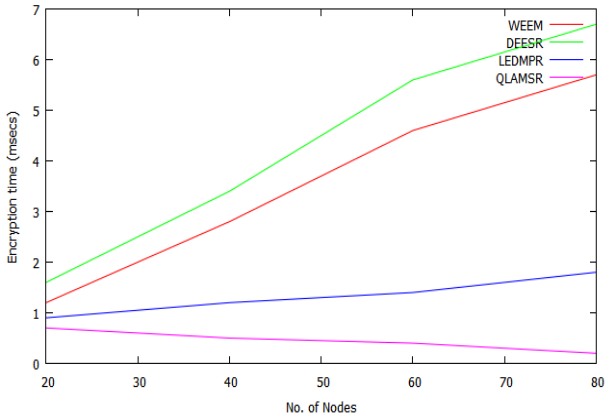

Figure 6. Encryption time Vs No. of Nodes

Figure 6 illustrates the performance of encryption time of QLAMSR while varying the number of nodes from 20 to 80. The proposed protocol achieves less time for encrypting data before transmission.

Figure 7 illustrates the performance of delay while varying the mobility from 20 to 100 bps. From the results, it is seen the delay of QLAMSR is low compared to existing schemes.

Figure 8 shows the performance of location accuracy ratio while varying nodes in x axis from 10 to 100. QLAMSR produces high accuracy ratio than existing schemes. Table 2 shows comparative analysis of proposed and existing schemes.

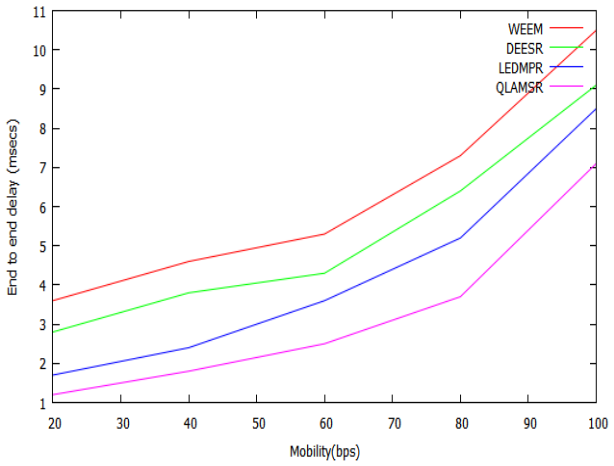

Figure 7. End to end delay Vs Mobility

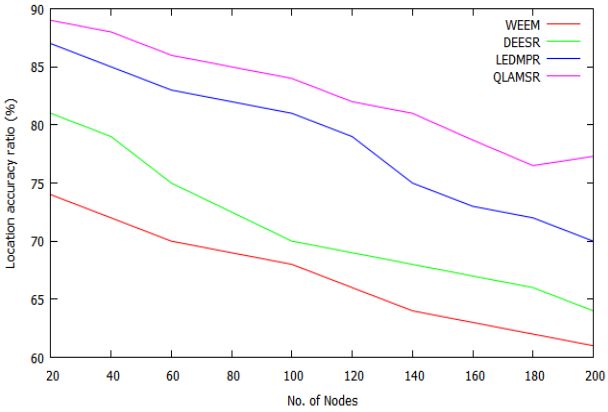

Figure 8. Location Accuracy Ratio Vs No. of Nodes

Table 1. Comparative Analysis

Performance Metrics	WEEM	DEESR	LEDMPR	QLAMSR
Network lifetime (Secs)	18-57	24-68	38-91	42-95
Detection ratio (%)	1-28	4-35	9-46	12-51
Encryption time (msecs)	1.2-5.7	1.6-6.7	0.9-1.8	1.1-0.8
Link reliability rate (links/sec)	9-42	11-51	19-82	21-94
End to end delay (msecs)	3.6-10.5	2.8-9.1	1.7-8.5	1.2-7.1
Location accuracy ratio (%)	74-61	81-64	87-70	89-77

5. Conclusion

In WSN, efficient energy routing with security constraints is the biggest task. In this research work, secure cluster based efficient energy routing is introduced for enhancing network lifetime while consuming less energy during data transmission process. The routes are selected based on energy conservation rate and packets are secured by enhancing encryption and decryption scheme. Based on the results, QLAMSR achieves less end to end delay, more network lifetime, high link reliability rate, low encryption tine and more detection ratio than existing schemes like EATAS and DEESR.

References

[1] Zheng and Lipeng Song, "Information-Aware Secure Routing in Wireless Sensor Networks", Sensors, vol.165, **(2020)**, pp.1-21.

[2] Sathiya and Nandhakumar, "An Optimized Multipath Routing for Secure Communication of Wireless Sensor Network", International Journal of Advanced Research and Technology, vol.8, no.3, **(2020)**, pp.1-6.

[3] Kashif Naseer Qureshi, Muhammad Umair Bashir, Jaime Lloret and Antonio Leon, "Optimized Cluster-Based Dynamic Energy-Aware Routing Protocol for Wireless Sensor Networks in Agriculture Precision", Journal of Sensors, **(2020)**, pp.1-19.

[4] Abhishek Jain, Vishal Jain and Khushboo Tripathi, "Trust based Intrusion Detection System Architecture for WSN", International Journal of Recent Technology and Engineering, vol.8, no.6, **(2020)**, pp.700-703,

[5] Mohammad S. Obaidat, Sanjay K. Dhurandher, Deepank Gupta, Nidhi Gupta and Anupriya Asthana, "DEESR: Dynamic Energy Efficient and Secure Routing Protocol for Wireless Sensor Networks in Urban Environments", Journal of Information Processing Systems, vol.6, no.3, **(2010)**, pp.269-294.

[6] Lata B T , Jansi P K R, Shaila K, D N Sujatha, Tejaswi V, Venugopal K R and L M Patnaik, "Secure Routing using Multiple Domains for Wireless Sensor Networks", International Journal of Computer Trends and Technology, vol.13, no. 3, **(2014)**, pp.103-112.

[7] K. Imrana Banu and G.Murali, "Controlling Residual Energy of WSN with Secure Routing Protocol", International Journal of Science and Research, vol.5, no.8, **(2015)**, pp.154-156.

[8] Meysam Zare and Mohammadreza Soltanaghaei, "A Gray System Theory Based Multi-Path Routing Method for Improving Network Lifetime in Internet of Things Systems", Preprints, **(2020)**, pp.1-28.

[9] Arzoo Miglani, Tarunpreet Bhatia, Gaurav Sharma and Gulshan Shrivastava, "An Energy Efficient and Trust Aware Framework For Secure Routing in LEACH for Wireless Sensor Networks", Scalable Computing: Practice and Experience, vol.18, no.3, **(2017)**, pp.207-218.

[10] Selvi, Thangaramya, Sannasi Ganapathy, Kulothungan, Khannah Nehemiah and Kannan, "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks", Wireless Personal Communications, DOI: 10.1007/s11277-019-06155-x, **(2019)**, pp. 1-16.

[11] Sutagundar and Manvi, "Location aware event driven multipath routing in Wireless Sensor Networks: Agent based approach", Egypt Information Journal, vol.14, **(2013)**, pp.55-65.

[12] Chi Trung Ngo and Hoon Oh, "A Link Quality Prediction Metric for Location based Routing Protocols under Shadowing and Fading Effects in Vehicular Ad Hoc Networks", Procedia Computer Science, vol. 34, **(2014)**, pp.565 – 570.

[13] Anuradha Banerjee and Subhankar Ghosh, "Weight-based Energy-efficient Multicasting (WEEM) in Mobile Ad Hoc Networks", Procedia Computer Science, vol.152, **(2019)**, pp.291–300.

[14] Xing Wang, Xuejun Liu, Meizhen Wang, Yunfeng Nie and Yuxia Bian, "Energy-Efficient Spatial Query-Centric Geographic Routing Protocol in Wireless Sensor Networks", Sensors, vol.19, **(2019)**, pp.1-23.

[15] Vinoth and Omkumar, "Location Aware Directional Flooding Algorithm for improving Energy Efficiency in MANET", International Journal of Innovative Technology and Exploring Engineering, vol.8, no.5, **(2019)**, pp.363-367.

[16] Movva Pavani and Polipalli Trinatha Rao, "Adaptive PSO with optimized firefly algorithms for secure cluster-based routing in wireless sensor networks", IET Wireless Sensor Systems, vol.9, issue 5, **(2019),** pp.274-283.