Improving Packet Delivery Ratio in Wireless Sensor Network with Multi Factor Strategies

Venkateswara Rao M[1]
Research Scholar
Department of Computer Science and Engineering
KoneruLakshmaiah Education Foundation
Vaddeswaram, Andhra Pradesh, India

Srinivas Malladi[2]
Professor
Department of Computer Science and Engineering
KoneruLakshmaiah Education Foundation
Vaddeswaram, Andhra Pradesh, India

***Abstract*—In the design of wireless sensor network (WSN), packet delivery ratio is an import parameter to be maximized. In existing schemes, a secure zone-based routing protocol was implemented for life time improvement in WSNs. In multi - hop communication, a new routing criterion was formulated for packet transmission. Security against message tampering, dropping and flooding attacks was incorporated in the routing metric. The approach skipped risky zones as a whole from routing and chooses alternative path to route a packet in secured manner with less energy consumption. Though energy conservation and attack resilience are achieved, congestion in WSN is increased and because of it packet delivery ratio is diminished. To address this problem, we propose a solution to improve the packet delivery ratio with a multi factor strategies involving routing, differentiation of flows, flow-based congestion control with retransmission and redundant packet coding. Detailed analysis and simulations are undertaken to evaluate the efficiency of the contemplated work compared to the existing solutions.**

Keywords—Multi factor strategies; novel routing metric; packet coding; packet delivery ratio

I. Introduction

Wireless sensor network is the collection of sensor nodes which has the capability of wireless data communication. Sensor nodes sense the environment variables depending on the application requirements and send them to sink either directly or through multi hop transmission.

A. Motivation

WSN is being increasingly used in many applications like Military ,precision farming, industrial safety, smart home etc. which needs reliable and high speed data transmission . It is required to design WSN applications by considering the requirements like more packet delivery ratio, life time and security.

B. Earlier Research Work

In earlier works [1], a zone-based sensor network is designed with the consideration of life time and security. The sensor network is secured against message tampering, dropping and flooding attacks. WSN Life time is increased by optimizing the power usage and packet routing. The network is split to zones and each zone is assigned a score. This score is calculated depending on past security lapses and present residual energy in that zone. A zone with higher score is preferred for routing. In zone based attack resilient routing the network life span and attack resilient capability are improved. But data packets are lost due to higher congestion in WSN. The solution in this work minimizes the packet delivery ratio owing to a significant raise in total numbers hops and node overhead in the network.

The major focus of earlier solutions [1,5,6] is finding the optimal route for data transmission .The identified gaps in the previous works are lower packet delivery ratio, less network life time ,lower throughput. These gaps are addressed in the proposed multi factored approach.

C. Proposed Work

Multi factored Secure Routing approach is proposed to improve packet delivery ratio in WSN by addressing the draw backs related to energy efficient attack resilient routing.

In the proposed Multifactor approach, packet delivery ratio is improved by selecting energy efficient route, Differentiation of flows in the network and flow based congestion control and Redundancy & Retransmission management,

The entire WSN is divided in to zones. Energy efficient path from source to sink is selected depending on the preference score calculated at each neighboring zone. The preference score (PS) is measured depending on security score, energy score and reliability score available in the zone. The zone heads are sorted depending on the distance from sink node. Among the neighbouring head nodes, the node whose PS value above threshold T_1 is selected to send data packet.

In the differentiation of flows Packet flow is split into two categories of high and low priority in the network. At each routing hop, the flow of packets is controlled differently for the packets based on high and low priorities. Packets with high priority are transmitted and low priority packets are buffered during network congestion period.

The low priority packets are buffered to reduce network congestion. This allows for reliable transmission of packets. When a node receives a Packet Forward Success (PFS) message, it calculates the Round Trip Time (RTT). When RTT is above the configured threshold, data flow rate is reduced, when RTT is below the configured threshold, data flow rate is increased.

In Redundancy and Retransmission management data content sent from source is divided into n packets using Reed Solomon erasure coding approach. Even if some packets are lost during transmission, the whole message is reconstructed at the destination without retransmission.

Packet delivery ratio is increased by introducing a weighted routing metric with the consideration of various factors. The goal is to increase the packet delivery ratio applying multiple factors like flow management, retransmission control and weighted routing metric to zone based sensor network.

In the following, Section II presents the related review for proposed solution. Section III elaborates the proposed Multi Factored Strategy, Section IV presents salient features in proposed solution, Results related to proposed schemes are given in Section V. Lastly, section VI explores the conclusions and future scope of the proposed solution.

II. Related Work

An opportunistic routing scheme is presented in [2] to increase the packet delivery ratio in WSN. Relay nodes are selected based on minimization of retransmission. Due to the reduction of retransmission, the overall throughput of the network is increased and thereby reducing the packet loss. Security is not considered for end to end delivery .An opportunistic routing scheme similar to [2] is proposed in [3] with the aim of increasing the reliability and reducing the latency. The best relay satisfying the QoS criteria is selected based on reliability and time guarantee. Less network life time is the limitation for this work. Authors in [4] proposed a distributed multi path algorithm with the goal of higher packet reliability. The path selection is adapted to network changes and failures. With the availability of multiple base stations and routing on multiple paths to these stations, fidelity of packet is improved in this work. Nevertheless, the major limitations are increased network overhead and reduced throughput. An optimal energy efficient routing protocol is formulated in [7].improved Packet delivery ratio and Network Life time is addressed in this solution. A stateless position-dependent routing technique is formulated in [8].Stateless routing is realized using greedy perimeter routing. Geographic routing along with greedy data transmission is able to increase the packet delivery time. Detection of malicious nodes in sensor network is explored in [9, 10]. Network life time is increased by enhanced energy efficient clustering of sensor network in [11]. LEACH algorithm is improved to select the best cluster head to enhance the lifespan of the network. Throughput is less in this work. Ant colony-based routing algorithm is proposed in [12] with the goal of higher packet delivery ratio. The ant colony algorithm uses the fitness function optimized based on communication distance, transmission direction and current residual energy. Packet delivery ratio is increased using opportunistic multipath routing in [13]. Similar to it, in [14] A multi path routing algorithm is formulated to increase packet reliability by forwarding on multiple paths. The solution also uses aggregation to diminish the number of efficient transmissions in WSN.Packet prioritization and optimized back-off MAC protocol is proposed in [15]. Due to reduction of collision in the optimized back-off MAC protocol, packet reliability is improved. The optimized back off MAC works by assigning back off time depending on the packet priorities.A virtual node concept is introduced in [16] to enhance the QoS in WSN based on clustering technique. The scheduling is realized using TDMA in this network. High priority is assigned to certain designated nodes. During higher traffic load, the packets from these designed nodes are given more importance in routing so that latency for those packets is reduced. A stateless opportunistic routing protocol is defined in [17] with the objective of enhancing the packet reliability. Forwarding area for packet is adapted dynamically depending on the density of the sensor nodes, so that reliability is increased. Increased overhead is not addressed. Compressive sensing is used to reduce the packet overhead in [18]. Compressive sensing improves the network utilization and packet delivery ratio. Compressive sensing also minimizes the power usage in WSN.Packet reliability is increased using energy aware Quality of Service (QoS) transmission protocol depending on various parameters in [19]. Energy consumption is reduced by optimal positioning of nodes in [20]. Packet low delivery ratio is limitation in this work. Clustering based energy minimization strategies are explored in [23, 28, 21]. Attack resilient routing in wireless sensor network in discussed in [22, 24, 25, 26, 27].

III. Proposed Multi Factored Strategy

The architectural representation of proposed multi factored approach is depicted in Fig. 1. The architecture represents four important concepts to achieve more packet delivery ratio and life span.

- Selection of energy efficient routing path.
- Redundancy and Retransmission management.
- Differentiation of flows in the network.
- Flow based congestion control.

A. Packet Routing

The Whole area of WSN is split into zones of N×N size. With one hop routing, any node in the zone will connect to any other node. Node close to centre of the zone that can observe all packet transmissions is selected as zone head. The information of nodes within each zone is present in the sink. Three distinct scores, security score, energy score and reliability score are attained in each zone. The value of the scores varies from 0 to 10. The zone with high score is recommended for routing when compared with zone having lower score. The zone scores are calculated based on fuzzy function using the following input variables.

- Packet traversing count (PTC).
- Packet traversing failure count (PTFC).
- Tampered incidence count (TIC).
- No tampered count (NTC).

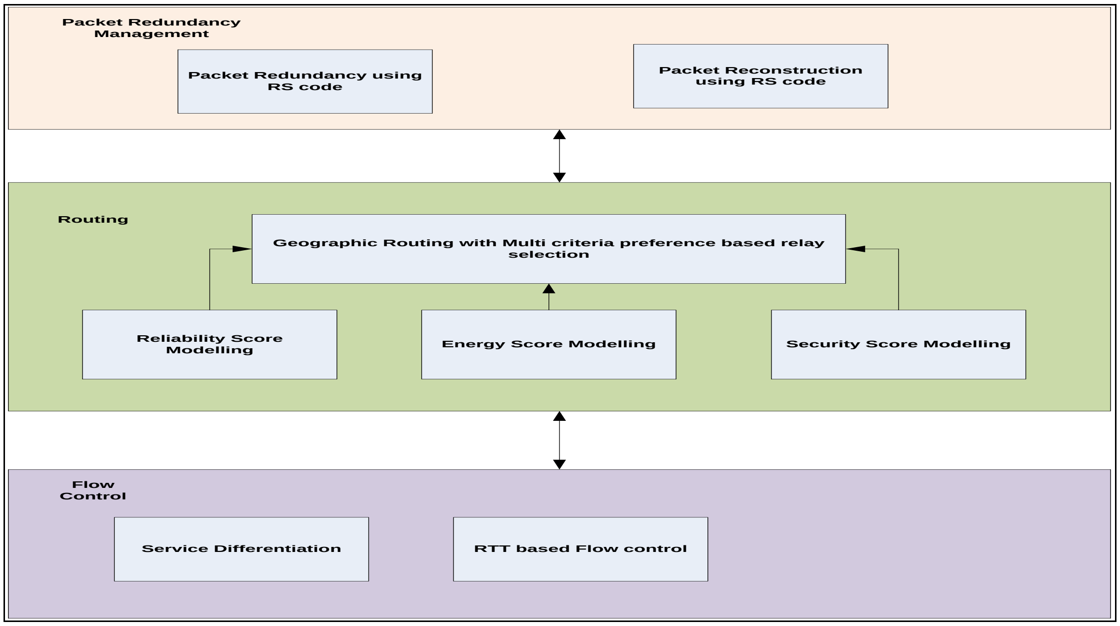

Fig. 1. Architecture of Secure Routing based on Multi Factored Approach.

These scores are detailed in [1] and the counters are kept at sink node. But these counters are kept at zone head in the proposed solution. The fuzzy function for calculating the security score (SS) of the zone is shown in (1).

$$SS = \mu_1 * Q(PTC) + \mu_2 * Q(PTFC) + \mu_3 * Q(TIC) + \mu_4 * Q(NTC) \quad (1)$$

Where

$Q(x)$: The fuzzification kernel of input x.

The de-fuzzification score is measured by using center of gravity formula as shown in (2).

$$Score = \frac{\int \mu_{\bar{D}r}(x).xdx}{\int \mu_{\bar{D}r}(x).dx} \quad (2)$$

Where x = {PTC, PTFC, TIC, NTC}.

The path security score SS_p (3) is measured as.

$$SS_P = \frac{\sum_{i=1}^{N} SS_i}{N} \quad (3)$$

Where SS_i is the zone security score. There are N zones in the path.

The energy score (ES) of a zone is measured as in (4).

$$ES = \frac{10*(E - TPC * E_c)}{E} \quad (4)$$

Where E is the node's initial energy and E_c is the energy utilized for packet transmission at node. TPC is the total packets transmitted.

The path energy score ES_P is calculated using (5).

$$ES_p = \prod_{\min of\ all\ N} ES_i \quad (5)$$

Where ES_i is the energy score of the path.

Rather than the revised AODV based routing addressed in [1] ,the packets are transmitted using a geographical routing through preference score-dependent path selection. Past packet forward statistics are used to calculate the reliability score for the zone. Packet forward success message is sent by each node with successful forward for packet to immediate hop. Whenever this message is received, packet forward success counter (PFS) is incremented. Periodically, the reliability score (6) is measured as.

$$R_t = \alpha \times R_{t-1} + (1 - \alpha)\frac{PFS}{TPC} \quad (6)$$

With $R_0 = 0$ and α is constant.

Initially the data packet is sent from the source node to the zone head. The head of zone sends a packet containing hello message to other neighbouring heads. The heads of zones receiving 'HELLO' message calculate the preference score and send back a 'HELLO_RES' as response to 'HELLO'. The preference score (PS) is measured (7) as the sum of weighted values of security score, energy score and reliability score.

$$PS = w_1 * SS_p + w_2 * ES_p + w_3 * R_t \quad (7)$$

With $w_1 + w_2 + w_3 = 1$ and $w_3 > w_2 > w_1$

The zone accepting 'HELLO_RES' , selects the zone head with highest PS score as relay hop and route the DATA packet to that zone head.

After the reception of HELLO_RES by zone head, the K nearest neighbour heads are sorted depending on the distance from sink node. Among K neighbouring head nodes, the node whose PS value above threshold T_1 is selected to send data packet. Data packet is forwarded to all K neighbour nodes, if none of the neighbour has PS values aboveT_1. This process is repeated at every hop until data packet received by the sink node.

Before applying fuzzy function on the input variables PTC, PTFC, TIC, NTC , these variables must converted from numerical to categorical values of Low (L), Medium (M) and High (H) using the transformation functions . Transformation function for the input variable PTC is shown in the Fig. 2.

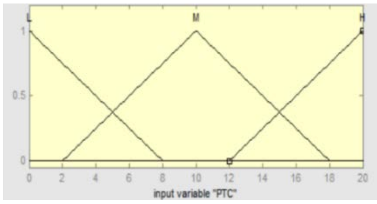

Fig. 2. PTC Transformation Function.

Transformation function for the input variable PTFC is shown in the Fig. 3.

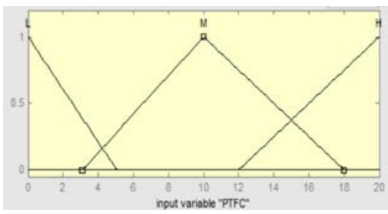

Fig. 3. PTFC Transformation Function.

Transformation function for the input variable TIC is shown in the Fig. 4.

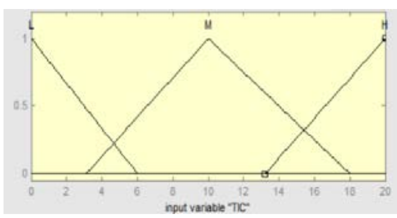

Fig. 4. TIC Transformation Function.

Transformation function for the input variable NTC is shown in the Fig. 5.

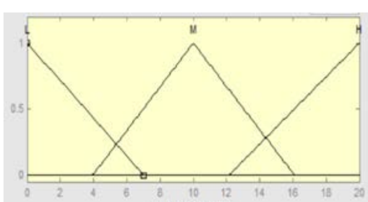

Fig. 5. NTC Transformation Function.

The output variable of preference score is converted from numerical to categorical value using the transfer function given in Fig. 6.

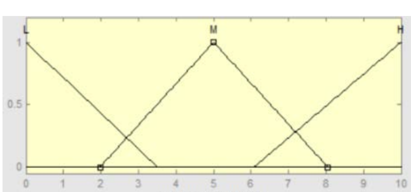

Fig. 6. Preference Score Transformation Function.

The input variables PTC, PTFC, TIC and NTC are mapped with output variable of preference score using fuzzy rule base.

B. Flow Differentiation and Congestion Control

Packet flow is split into two categories of high and low priority in the network. At each routing hop, the flow of packets is controlled differently for the packets based on high and low priorities. Packets with high priority are transmitted and low priority packets are buffered during network congestion period. Due to buffering of low priority packets, network congestion reduces. This allows for reliable transmission of packets. The round trip time (RTT) is calculated, when a node receives a packet forward success response .Based on probability delay, RTT (8) is measured as below.

$$RTT = \begin{cases} \sum_{i=0}^{\infty} f_i(a).f_i(b)\ , x = 0 \\ \sum_{i=0}^{\infty} f_i(a).f_{2x+i}(b) + \sum_{i=0}^{\infty} f_i(b).f_{2x+i}(a), x > 0 \end{cases} \quad (8)$$

Where: a is forward path.

b is backward path.

f is the probability mass function..

Adaptive flow control for the packets is shown in Fig. 7.

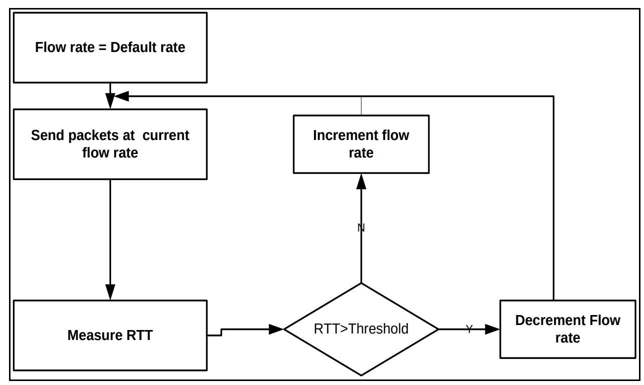

Fig. 7. Flow of Packets.

The flow rate is initially set to the default value and data flow control at each node begins with this value [Fig. 7]. Based on the reception of packet forward success message, round trip delay is calculated. Data Flow rate is decreased when RTT is above configured threshold and increased when RTT is below configured threshold.

C. Redundant Packet Coding

The message content sent from source is divided into n packets using erasure coding (n,k) .Only k of n packets are sufficient for reconstructing the entire message content. The source node sends n packets of the message and if k out of n packets is received at sink, the message can be reconstructed without any necessity for retransmission. This work uses Reed Solomon erasure coding. Use of Reed Solomon code has following advantages.

- The reed Solomon transformed contents are encrypted and secure.
- Retransmission can be avoided to reconstruct the entire message with lesser number of packets.

IV. Salient Features in Proposed Solution

The proposed multi factor strategy has following salient features:

- Packet delivery ratio and network life span are less in earlier works [1],[5],[6] which are addressed in the proposed solution using multi factored approach.
- Risky areas in the network are quantified using scores and routing is adapted to skip those risky areas.
- Packet flow is differentiated and flow is managed to reduce the congestion in the network. Flow management is dynamic to congestion in the network.
- Retransmission is avoided in the network due to erasure coding.
- Attack resiliency is assured with proactive routing in secure paths.

V. Results

The proposed multi factored strategy is simulated in NS2 platform. The simulation parameters used for testing the proposed solution is given in TABLE I.

The performance of the proposed work approach is simulated and evaluated by comparing with the following solutions.

- Secure Energy Efficient Routing is contemplated in [1].
- Optimal Energy Efficient Routing is formulated in [5].
- Secure Localized Routing is defined and implemented in [6].

Performance evaluation parameters considered for comparison are: packet delivery ratio, packet delay, node overhead, network life time and throughput.

Packet delivery ratio (9) measures the ratio of successfully received packets at sink to the total number of packets sent by the sources. It is calculated as

$$PDR = \frac{number\ of\ packets\ recived\ at\ sink}{total\ number\ of\ packets\ sent} \quad (9)$$

The results of packet delivery ratio against number of nodes are given in Table II and Fig. 8.

The packet delivery ratio of the proposed solution is 6.95% more Compared to [1], 14.6% more compared to [5] and 16.51% more compared to [6].

The results of average delay against number of nodes are given in Table III and Fig. 9.

Compared to [1], average delay is lower by 15.38% in the proposed solution, 24.13% lower compared to [5], 37.14% lower compared to [6]. The delay is lower in the proposed solution due to reduction in number of hops in the geographic routing strategy adopted in the proposed work.

The result of network overhead against number of nodes is shown in Table IV and Fig. 10.

TABLE I. Simulation Parameters

Criterion	**Value(s)**
No. of Nodes	50 - 250
Communication range(m)	100
Simulation expanse(m^2)	1000 × 1000
Allocation of Priority (%)	20
Disposition of sensor Node	Random
Time of Simulation	30
Queue size of Interface	50
Medium Access Control(MAC)	802.11

TABLE II. Comparison of Packet Delivery Ratio

No.of Nodes	**Proposed Multi Factored Approach**	**Secure Energy Efficient Routing[1]**	**Optimal Energy Efficient Routing[5]**	**Secure Localized Routing[6]**
50	93	87	82	81
100	92	86	81.5	79.5
150	91	85.2	79.22	78
200	90.5	84	78	76.9
250	89	83.2	76.8	75.1

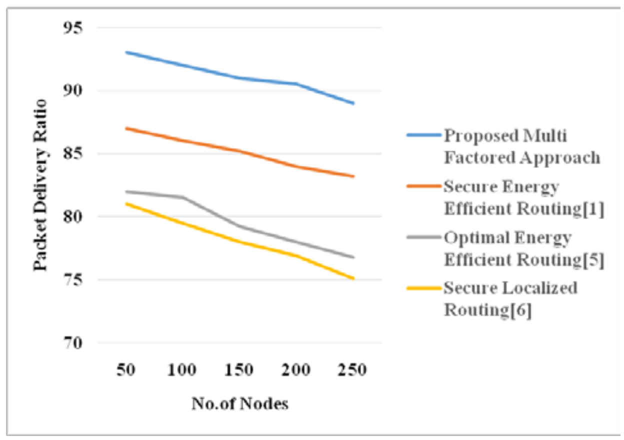

Fig. 8. Packet Delivery Ratio.

TABLE III. Comparison of Delay

No.of Nodes	**Proposed Multi Factored Approach**	**Secure Energy Efficient Routing[1]**	**Optimal Energy Efficient Routing[5]**	**Secure Localized Routing[6]**
50	15	18	21	24
100	14	16	18	22
150	13	15	17	21
200	12	15	16	20
250	12	14	15	18

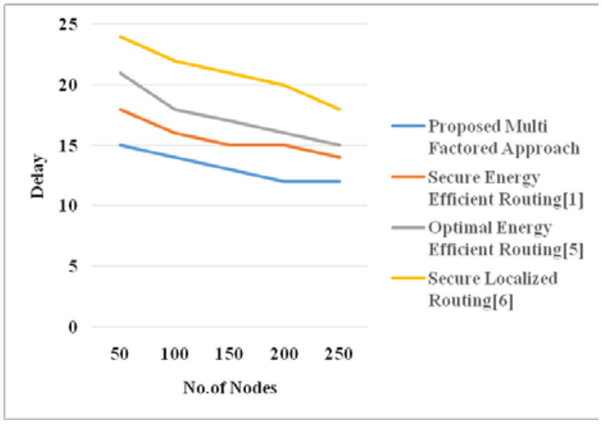

Fig. 9. Delay Comparison.

TABLE IV. ANALYSIS OF OVERHEAD

No.of Nodes	Proposed Multi Factored Approach	Secure Energy Efficient Routing[1]	Optimal Energy Efficient Routing[5]	Secure Localized Routing[6]
50	72	80	82	85
100	85	92	93	97
150	89	97	100	106
200	94	104	108	116
250	97	116	118	127

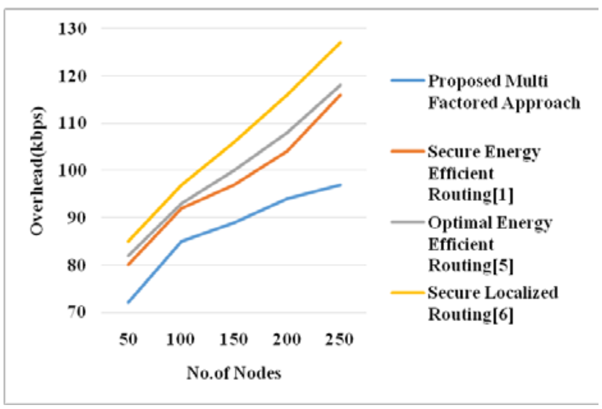

Fig. 10. Analysis of Overhead.

Compared to [1], overhead is lower by 10.63% in proposed solution, 12.77% lower than [5] and 17.7% lower than [6]. Adaptive multi path propagation and geographic routing has reduced the network overhead in proposed solution.

The result of life time against number of nodes is given in Fig.11 and Table V.

Compared to [1], life time is higher by 19.4% in the proposed solution, 72.7% more compared to [5] and 102.1% more compared to [6]. Due to the minimization of number of hops and retransmissions, energy consumption is reduced and this has increased the life span in the proposed work.

The results of network throughput for different rate of packet generation are given in Table VI and Fig. 12.

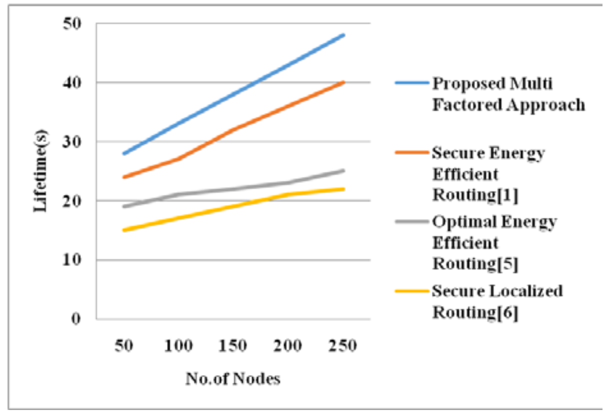

Fig. 11. Life Time Comparison.

TABLE V. LIFE TIME COMPARISON

No.of Nodes	Proposed Multi Factored Approach	Secure Energy Efficient Routing[1]	Optimal Energy Efficient Routing[5]	Secure Localized Routing[6]
50	28	24	19	15
100	33	27	21	17
150	38	32	22	19
200	43	36	23	21
250	48	40	25	22

TABLE VI. THROUGHPUT COMPARISON

Total Sending Rate (kbps)	Proposed Multi Factored Approach	Secure Energy Efficient Routing[1]	Optimal Energy Efficient Routing[5]	Secure Localized Routing[6]
100	92	84	83	81
150	140	136	129	125
200	181	173	167	160
250	224	208	201	195
300	267	251	242	238

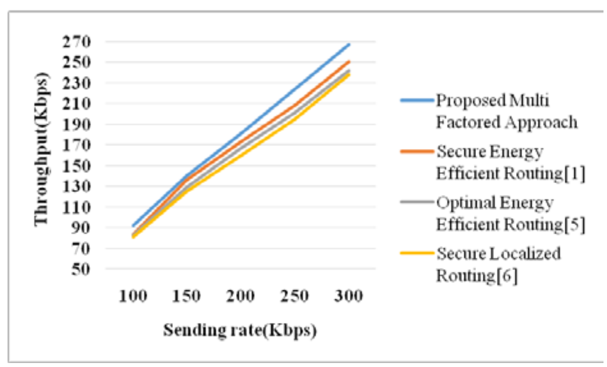

Fig. 12. Throughput Comparison.

The proposed solution has higher throughout in terms of 6.1% more than [1], 9.97% more than [5] and 13.14% more than [6].

The split ratio between high and low priority packet is set to 70:30 and throughput is measured for varied rate of packets from source. The comparison is given in Table VII and Fig. 13.

TABLE VII. COMPARISON OF THROUGHPUT ON 70:30 SPLIT

Total Sending rate (kbps)	Proposed Multi Factored Approach	Secure Energy Efficient Routing[1]	Optimal Energy Efficient Routing[5]	Secure Localized Routing[6]
100	65	52	50	47
150	100	83	82	79
200	130	100	96	90
250	160	120	117	110
300	195	160	157	147

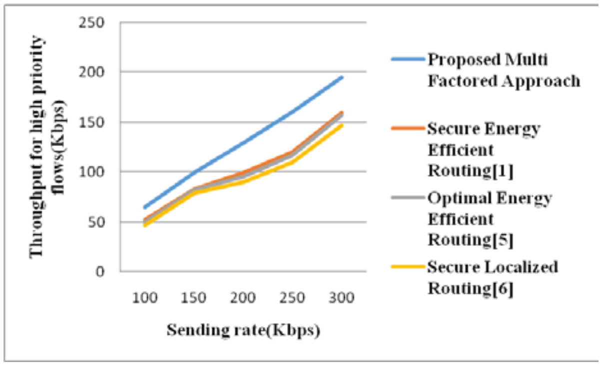

Fig. 13. Throughput Comparison on 70:30 Split.

The proposed solution has higher throughput in terms of 9.97% greater than [1], 29.48% greater compared to [5] and 47.42% greater compared to [6].

VI. CONCLUSION AND FUTURE SCOPE

A multi factored strategy with the objective of providing increased packet delivery ratio in zone-based sensor network is proposed in this work. Geographic routing is adapted with relay selection based on a preference score. Adaptive multi path propagation, flow differentiation and congestion control, redundancy coding are the multi factored strategies proposed in this work. Redundancy in the coding has reduced the number of retransmissions in the network. Flow differentiation and flow control has reduced the congestion in the WSN. Preference score is calculated based on energy availability, security and reliability of the nodes and use of it in routing has increased the packet reliability. Due to multi factored strategy, the packet delivery ratio improved by 6.95% in the proposed work, life time improved by 19.4% and delay reduced by 15.38% compared to the existing works. These results are very much useful for further research in the areas of Military applications, Environmental monitoring etc. In the further enhancement, the proposed solution can be improved to reduce the average energy consumption of nodes within the zone in order to improve packet delivery ratio.

REFERENCES

[1] Venkateswara Rao M and Srinivas Malladi, “Secure Energy Efficient Attack Resilient Routing Technique for Zone based Wireless Sensor Network” International Journal of Advanced Computer Science and Applications (IJACSA), 11(12), 2020. http://dx.doi.org/10.14569/IJACSA.2020.0111267.

[2] Hasnain, Muhammad, Mazhar Hussain Malik, and Mehmet Emin Aydin. "An adaptive opportunistic routing scheme for reliable data delivery in WSNs." Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018.

[3] Chen, Aiguo, et al. "RTGOR: Reliability and Timeliness Guaranteed Opportunistic Routing in wireless sensor networks." EURASIP Journal on Wireless Communications and Networking 2018.1 (2018): 86.

[4] Velasquez-Villada, Carlos, and YezidDonoso. "Multipath routing network management protocol for resilient and energy efficient wireless sensor networks." Procedia Computer Science 17 (2013): 387-394.

[5] Khamayseh, Yaser M., Shadi A. Aljawarneh, and Alaa Ebrahim Asaad. "Ensuring survivability against Black Hole Attacks in MANETS for preserving energy efficiency." Sustainable Computing: Informatics and Systems 18 (2018): 90-100.

[6] Poongodi, Thangamuthu, and M. Karthikeyan. "Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks." Wireless Personal Communications 90.2 (2016): 1039-1050.

[7] Prasad, A. Y., and Balakrishna Rayanki. "A generic algorithmic protocol approaches to improve network life time and energy efficient using combined genetic algorithm with simulated annealing in MANET." International Journal of Intelligent Unmanned Systems (2019).

[8] Yan Sun, Junpeng Guo, "Speed Up Greedy Perimeter Stateless Routing Protocol for Wireless Sensor Networks (SU-GPSR)", IEEE,2017.

[9] Vamshi krishna, H., & Swain, G. “Identification and avoidance of malicious nodes by using certificate revocation method.” International Journal of EngineeringandTechnology(UAE), 7(4.7 Special Issue 7) (2018)., 152-156.

[10] Kalaipriyan, T., et al. "Monkey King Algorithm for Solving Minimum Energy Broadcast in Wireless Sensor Network." Advances and Applications in Mathematical Sciences 17.1 (2017): 129-145.

[11] Prasad, A. Y., and R. Balakrishna. "Implementation of optimal solution for network lifetime and energy consumption metrics using improved energy efficient LEACH protocol in MANET." Telkomnika 17.4 (2019): 1758-1766.

[12] Sun, Yongjun, Wenxin Dong, and Yahuan Chen. "An improved routing algorithm based on ant colony optimization in wireless sensor networks." IEEE communications Letters 21.6 (2017): 1317-1320.

[13] Kim, Sangdae, et al. "Opportunistic Multipath Routing in Long-Hop Wireless Sensor Networks." Sensors 19.19 (2019): 4072.

[14] Dong, Mianxiong, Kaoru Ota, and Anfeng Liu. "RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks." IEEE Internet of Things Journal 3.4 (2016): 511-519.

[15] Onwuegbuzie, Innocent Uzougbo, et al. "Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach." PloS one 15.8 (2020): e0237154.

[16] Almobaideen, Wesam, Mohammad Qatawneh, and OriebAbuAlghanam. "Virtual node schedule for supporting QoS in wireless sensor network." 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). IEEE, 2019.

[17] Ghoreyshi, Seyed Mohammad, Alireza Shahrabi, and TuleenBoutaleb. "A stateless opportunistic routing protocol for underwater sensor networks." Wireless Communications and Mobile Computing 2018 (2018).

[18] Li, Yimei, and Yao Liang. "Compressed sensing in multi-hop large-scale wireless sensor networks based on routing topology tomography." IEEE Access 6 (2018): 27637-27650.

[19] Monowar, Muhammad Mostafa. "An Energy-aware Multi-constrained Localized QoS Routing for Industrial Wireless Sensor Networks." Adhoc& Sensor Wireless Networks 36 (2017).

[20] Yan, Ziwei, et al. "Energy-efficient node positioning in optical wireless sensor networks." Optik 178 (2019): 461-466.

[21] Karthikeyan, T., V. Brindha, and P. Manimegalai. "Investigation on Maximizing Packet Delivery Rate in WSN Using Cluster Approach." Wireless Personal Communications 103.4 (2018): 3025-3039.

[22] Chowdary, Krishna, and K. V. V. Satyanarayana. "Malicious Node Detection and Reconstruction of Network in Sensor Actor Network." Journal of Theoretical & Applied Information Technology 95.3 (2017).

[23] Mallikarjuna Rao, Y., M. V. Subramanyam, and K. Satya Prasad. "Cluster-based mobility management algorithms for wireless mesh networks." International Journal of Communication Systems 31.11 (2018): e3595.

[24] Kadiravan, G., Pothula Sujatha, and J. Amudhavel. "A State of Art Approaches on Energy Efficient Routing Protocols in Mobile Wireless Sensor Networks." IIOAB Journal 8.2 (2017): 234-238. www. https://www.iioab.org/.

[25] Chowdary ,K., & Satyanarayana, K. V. V. "A novel secured data transmission and authentication technique against malicious attacks in WSNs." Journal of Advanced Research in Dynamical and Control Systems, (Special Issue -18) (2017), 161-173.

[26] Arage Chetan, S., & Satyanarayana, K. V. V. "Novel routing protocol for secure data transmission in wireless ad hoc networks." International Journal of Innovative Technology and Exploring Engineering, 8(4S2) (2019)., 101-108.

[27] Manjunath, B. E., and P. V. Rao. "Trends of Recent Secure Communication System and its Effectiveness in Wireless Sensor Network." Journal of Innovation in Electronics and Communication Engineering 6.2 (2016): 46-52.

[28] Gummadi, Annapurna, and K. Raghava Rao. "EECLA: Clustering And Localization Techniques To Improve Energy Efficient Routing In Wireless Sensor Networks." Journal of Theoretical & Applied Information Technology 96.1 (2018).