Secure Energy Efficient Attack Resilient Routing Technique for Zone based Wireless Sensor Network

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

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

Abstract—**Security and Energy efficiency are two key factors to be contemplated in the design of applications based on wireless sensor networks (WSNs). Optimization of energy consumption is obligatory for an increased life time of the network. Without security, attackers can disrupt the entire operation of sensor network by instigating diverse attacks like message tampering, message dropping either in partial or whole and message flooding etc. This work proposes a secure energy efficient attack resilient routing technique for zone based wireless sensor network with proactive detection of malicious zones and mitigation from the attacks. Different from earlier works on detecting each malicious node, this work cleaves the network to zones and allots a probabilistic fuzzy score to model the success ratio of packet propagation through the zone. The routing is adaptive to ongoing residual energy and security risks. A Firm decision cannot be made on the frameworks influencing the life time of the network considering it may influence the operations of network. Experimentation of the proposed solution is done in NS2 and contrasted with the existing solutions to prove the effectiveness of the approach.**

Keywords*—*Energy efficiency; malicious zones; preference score probabilistic fuzzy score; residual energy

I. Introduction

Wireless sensor network is a network of sensor associated with a wireless infrastructure. The sensing nodes senses assorted parameters and propagate it via multi hop to descend in the networks. With expeditious reduction in cost of sensors, WSN is used in numerous applications like precision farming, industrial security, wild life monitoring, etc. Typical WSN consists of nodes connected with wireless infrastructure. Most sensor network deployments are unattended with sensor nodes being powered with batteries.

Due to sensing, listening, processing, transmission and reception of packets, the battery energy [1] is consumed and these processes are not scheduled in optimum manner, the energy depletes at faster rate and node becomes dead. The node failure does not only reduce the sensing coverage area, but also affects the routing. The communication holes created in the network disrupts the multi hop routing and minimizes the network reliability. Due to unattended nature, it is not possible for battery replacement for dead nodes. In this situation prudent use of energy is the best possible way to increase the life time of nodes and the network. Due to Wireless infrastructure, WSNs are prone to various attacks like message drops, message tampering, denial of service through message flooding etc. Detection of these attackers [25] and mitigation from these attacks is essential for reliability of applications using the sensor network. Implementing a higher complexity security algorithm involves higher energy consumption [11] for processing at sensor nodes and this in-turn reduces the life time of the node.

This work proposes an adaptive security enforcement solution with energy efficiency in routing for wireless sensor networks. The routing protocol is designed to be resilient against message drop, message forging and message flooding attacks. The entire network is split to multiple zones and each zone is allocated to two scores i.e. security score and energy score. The security score which models the security available in that zone. The energy score is calculated based on initial energy of the zone. Preference score is calculated using security and energy scores. Based on the preference score the routing is adapted in such way to meet both security and energy consumption requirements of the applications. Fuzzy logic is applied to score the zones probabilistically based on the current packet delivery performances.

Further, the paper is illustrated as follows: The related work is discussed in Section II. Problem definition is elaborated in Section III. The proposed work is described in Section IV. Novelty of proposed work is presented in Section V. Results of the proposed work is depicted in Section VI. Conclusion and future enhancements are discussed in Section VII.

II. Related Work

A routing protocol using inter cluster coordination with a goal of energy efficiency is developed in [1]. Received signal strength (RSS) from base station is used for clustering decision. A selection protocol to choose the cluster coordinators from node to sink is proposed to transmit data. in [2]. Energy consumption is reduced with efficient clustering with Gaussian Elimination algorithm with the goal to increase network life time. QoS based routing protocol for body area networks is proposed in [3]. Delay is calculated for all paths from source to sink and best path satisfying the delay requirements of the application is selected for routing. A multi path optimized routing protocol is proposed in [4]. Multi base stations to reduce route hops and ON-OFF cycles are the two strategies adopted to increase life time. Energy aware routing protocol is proposed in [5]. It is specifically designed for query-based applications. Zonal broadcasting is adopted in this work to reduce the total energy consumption. QOS routing based on multiple constraints in proposed in [6]. The protocol is highly scalable and adaptive to network dynamics. Greedy forwarder selection approach based on energy aware aggregated metric is proposed to select the best hop for routing. Network overhead is reduced in this protocol due to reduction in exchange of control packets. A scalable routing protocol with the goal of increasing network life time is proposed in [7] and [13]. Analytical model is proposed to find the optimum number of clusters based on location of base station and distribution of nodes. Best clusters to route the packets are selected based on current residual energy. Optimal relay node for packet forwarding based on multiple constraints is proposed in [8] to select the efficient relay nodes for packet forwarding. Packets are differentiated based on the priority. Differential path selection for different packet priority is done based on delay and current residual energy. Energy efficient routing is realized using Artificial Neural Network (ANN) in [9]. Next hop is selected using ANN. QOS factors and residual energy is used to train the ANN. Threshold sensitive Energy Efficient sensor Network protocol (TEEN) is proposed in [10]. The protocol works best for time critical applications. The sensing rate is controlled by the applications based on available energy in the network. Frequent data need requirements are satisfied using this protocol. Routing protocol using the concept of directional antenna is proposed in [12] with the goal for achieving energy efficiency. It is built on top of DSR protocol with extensions for power efficient gathering. Genetic algorithm is combined with bacterial foraging optimization to select energy efficient paths for data transmission. But sensors power consumption due to use of the hybrid algorithm is not considered in this work. An approach for reducing the packet transmissions and the energy consumption due to using the spatial and temporal correlation in the data is proposed in [14]. Temporal correlations in the sensor data is found using prediction-based approaches. Data transmission frequency is reduced for sensors with high correlations in their data. Energy efficient multi path routing protocol is proposed in [15]. Multiple paths are found using particle swarm optimization (PSO). The parameters to find efficient path is optimized using neural network. But the network overhead is very high in this approach due to frequent flooding. A heuristic solution is proposed in [16] to detect grayhole attackers. AODV is extended with bait detection schemes to find grayhole attackers. Since attackers are detected during route discovery stage, the network overhead for detection during packet forwarding is avoided. Black holes are detected using cooperative sensing in [17]. Due to the detection of Black holes, there is limitation in network life time and packet delivery ratio. PSO based clustering is proposed in [18]. Cluster heads were selected based on multiple criteria like mobility, energy. The life time of the network improved using fitness function adopted in this approach. Geographic routing protocol is combined with PSO with the goal of increasing life time of sensor networks in [19]. Energy utilization is drastically reduced in this approach. The fitness function for PSO considers inter node distance and nodal power. Security against routing attacks is studied in [20]. The work proposed an algorithm to detect cooperative black hole attacks. The routing protocol is controlled by some designated nodes in the network called security monitoring nodes (SMN). The black holes in the network are detected by the SMN and routing path is prevented from falling to black hole nodes. However, the work did not consider SMN compromise and there is a limitation in average energy of nodes. Packet transmission delay is also more in this works PSO is combined with TORA routing protocol in [21]. The problem of energy efficient route selection is treated as an optimization problems and PSO algorithm searches for the optimal solution for the problem. Load is distributed fairly and life time of network is increased using this solution. In clustering based solutions, the energy of nodes near to sink is depleted fast. This problem is referred as hotspot. Authors in [22] proposed sink mobility-based solution to solve the hotspot problem. Leech clustering protocol is optimized for energy efficiency in [23]. To overcome the demerits of predominant methods and further increase the lifetime of WSNs, a novel improved energy-efficient LEACH (IEE-LEACH) routing protocol is schemed in [23]. Malicious nodes are detected in the network using combination of cooperative bait detection and reverse tracing in [24]. Neighbor based Cluster Location Aware Routing (NCLAR) is modeled to achieve more packet delivery rate with high location accuracy in [25].Implement a framework for detection of malicious nodes in WSN and elimination of Node in actor nodes by creating a topological structure dynamical by adapting a connectivity point of peer to peer and point to point communications is proposed in [26]. A clustering and localization techniques for improving an efficient energy routing method are schemed in [27]. Certificate revocation based malicious attacker detection and prevention is proposed in [28]. Authors in [29] proposed weight-based clustering with a goal of increasing the life time of the network. An optimized trust-based ant colony optimization (TACO) and integrity verification techniques were implemented for wireless node initialization and trust probability computation in [30]. The author in [31] describes the minimum energy broadcast (MEB) problem for increasing the life time of nodes in wireless sensor networks. Secure communication model was proposed in [32] by considering time, energy, and traffic as factors for wireless sensor networks. The clustering of multiple paths in wireless sensor network is depicted in [33] by combinedly finding the membership and the number of clusters using SCAMS (simultaneous clustering and model selection). An efficient Multiple Objective Function (OF) in Routing Protocol for Low Power and Loss Network (RPL) is introduced in [34] for a Wireless Sensor Network in the field of healthcare. The important factors to be considered for OF are Packet Delivery Ratio (PDR) and the power consumption of sensors.

III. Problem Description

Given a wireless sensor network with N nodes and single sink, each node has residual energy of E and there are k attackers distributed across the network. The attacker can be message dropper (black hole and gray hole attack), message tamper and message flooder (Denial of service attack). Based on the current residual energy E, the sensor nodes are configured with the data sensing rate. Multi hop routing is used to forward data from nodes to sink. First node death concept is used to measure the life time of the sensor network. The objective of this work is to have a secured energy efficient route from source to sink resilient against the attacks.

IV. Secure Energy Efficient Attack Resilient Routing

Architecture is given in the Fig. 2 for proposed solution. Every sensor node contains a unique ID and it is preconfigured with Hyperelliptic curve cryptography (HCC) private key and the corresponding public key is kept at sink node. The key pair between the node and sink is unique and it is not available to any other nodes in WSN.

Hyperelliptic curves are generalization of elliptic curves. In these curves, the value of genus is greater than 1. ECC is special case of Hyperelliptic curve with genus value as 1. Compared to ECC, not much work has been done on Hyperelliptic curves. The work so far done in Hyperelliptic curves are only academic domain.

Assume k be a field. The general equation of hyperelliptic curve C with genus g over k

C:y^2+a(x)y=b(x)

Where

a(x) is a polynomial of degree ≤ g over b

b(x) is a monic polynomial of degree 2g+1 over b

As an example, following is a sample HCC function

$C: y^2 = x^5 - 5x^3 - 4x - 1$ over Q genus g=2

The number of nonintersecting simple closed curves that can be drawn on the surface without separating it is known as Genus of a curve. The number of handles is equal to the genus of a curve. The corresponding non intersecting closed curves are shown in Fig. 1.

Due to offline generation and pre-configuration of keys, there is no energy consumption due to processing of key generation and sharing. Every node is also assigned with a secret key sequence and a hash function H which is known only between the node and the sink.

The entire network is divided into $M \times M$ zones. Every zone has zone ID. The zone id is given by the sink for every zone as a number increasing from 1 to M*M.

The size of the zone is set in such a way that nodes in the same zone are within one hop with other nodes in that zone. All the nodes in the zone operate in duty cycle, so that each node in its duty cycle can process the packet for that zone and forward it to next hop. The duty cycle for the nodes is preconfigured after deployment.

$Zone\ size = \ comm.range^2$

Sink keeps the mapping of nodes in the zone. For each zone, sink maintains two scores – Security Score, Energy Score. Both scores are in value of 0 to 10. Security score of 10 means, there are no known attacks in the zone and score of 0 means there is a severe security risk for the zone. Energy score of 10 means that there is a higher residual energy in the zone and score of 0 means the zone is dead. In addition to these scores, sink maintains following counters for each zone

1) Packet traversal count (PTC)
2) Packet traversal failed count (PTFC)
3) Tampering incident count (TIC)
4) No Tampering count (NTC)
5) Total packets passed (TPC)

All these counters are set to 0 initially.

The AODV routing protocol is extended to design the proposed protocol. The RREQ and RREP message is added with additional fields for the extended routing protocol.

RREP and RREQ modifications are represented in Table I and Table II, respectively.

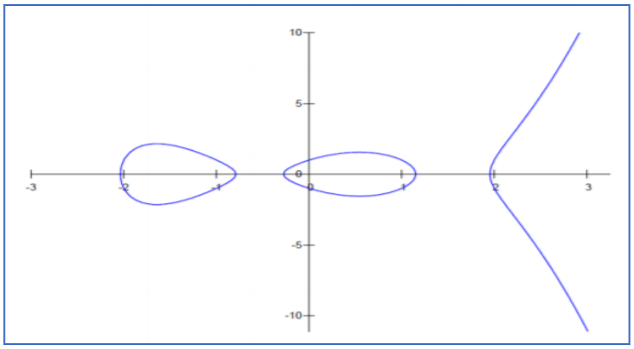


Fig. 1. HCC Curve.

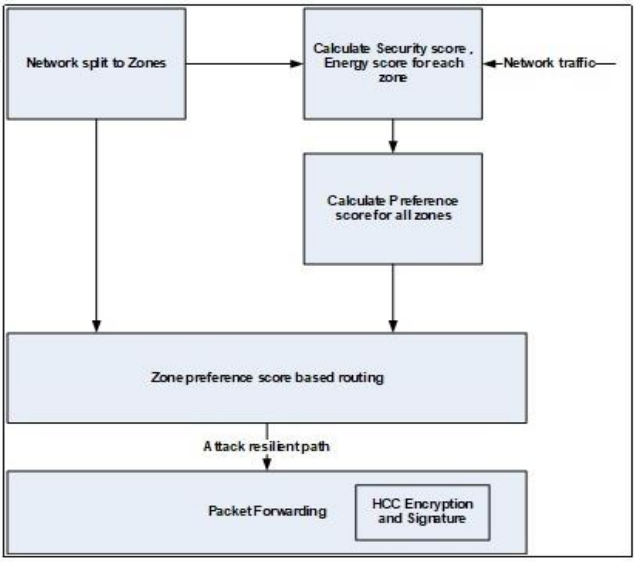

Network split to Zones
Calculate Security score , Energy score for each zone
Network traffic
Calculate Preference score for all zones
Zone preference score based routing
Attack resilient path
Packet Forwarding
HCC Encryption and Signature

Fig. 2. Architecture.

TABLE I. RREQ MODIFICATIONS

Field Name	Detail
Reqkey	Hashed key is added in this field

TABLE II. RREP MODIFICATIONS

Field Name	Detail
Encrypted PS score	Preference score is encrypted and stored
Signature	This signature is used for verification the RREP at the source

When a node wants to route packet, it instigates a RREQ request. The last sent secret key sequence is hashed using H and this hashed sequence is added to the RREQ request. RREQ request reaches the sink through multiple paths. At sink, analysis of each of path is done and a preference score is calculated for each route.

The analysis of path in the RREQ request at the sink node involves following steps:

1) Each node in the path is mapped to the corresponding zone.

2) The security score of the path is the average of the security score of all zones in the path.

3) The energy score of the path is minimum of the energy scores of all zones in the path.

The security score of the path is calculated as

$$SS_P = \frac{\sum_{i=1}^{N} SS_i}{N}$$

Where SS_i is the security score of the zones of N zones in the path.

The energy score of the path is calculated as

$$ES_p = \prod_{\min of\ all\ N} ES_i$$

Where ES_i is the energy score of the path.

A preference score is calculated for the path as weighted function of security score and energy score.

$$PS = w_1 * SS_p + w_2 * ES_p$$

With $w_1 + w_2 = 1$

Sink applies the hash function H on the secret key sequence in the RREQ and uses it to encrypt the preference score using AES encryption function. Also hash of the encrypted preference score and path in the RREP and the key sequence is done using H and this is inserted as signature in the RREP reply and sent. Sink maintains the paths and the preference score generated for a RREQ request from the source in its memory for a certain time period T. We refer this as cache.

Once the source node receives the RREP, it verifies the signature to check if the RREP message was tempered by modifying the path and the preference score. The signature verification is done by generating a signature as below and checking whether the generated signature is similar to the signature in the RREP message.

$$LS = H(\ last\ sent\ secret\ key\ sequence)$$

$$Sig_g = H(encrypted\ PS\ in\ RREP\ |path\ in\ RREP\ |\ LS)$$

$$\begin{cases} Sig_g == Sig\ in\ RREP\ , RREP\ is\ valid \\ Sig_g \neq Sig\ in\ RREP\ , RREP\ is\ invalid \end{cases}$$

The source nodes take the path with highest preference score among valid RREP and use it for routing the packets.

When sink receives the data packets, it finds the path taken for routing from the data packet. If the path is same as the highest preference score path in the Cache, then it increments the PTC count for all zones corresponding to the nodes in the path. If the path is not same, it means that path did not reach the source or the message would have got tampered. In this case, the PTFC count is incremented for all zones corresponding to nodes in that highest preference path and PTC count in incremented for all the zones corresponding to nodes through which the data packet has arrived. All data packets sent from source to sink is signed with the same procedure followed for RREP. At sink the digital signature is verified and if the verification fails, the TIC count is incremented and if the verification succeeds, NTC count is incremented. These counters are increased only once for the data session and not for all the data packets in the session. But TPC count is incremented for all zones corresponding to the nodes in the path every time data packet is received in the sink.

Sink calculates the average rate of data session from a zone and the deviation from the average rate is decided as flooding. The source node from whom data session exceeded the threshold is decided as flooding attacker. To prevent other nodes energy getting exhausted due to processing of flooded packet, sink sends black list packet with the information of flooding node to all the neighbor zones of the flooded node. The neighboring zones drops the packets from black listed flooders. By this way, flooding attack is mitigated in the proposed solution.

The energy score for the zone is calculated based on the TPC count as follows:

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

Where the initial energy of the node is E and the energy consumed for transmission and reception of a packet at node is E_c.

The security score is modelled as fuzzy function of following inputs:

1) Packet traversal count (PTC)

2) Packet traversal failed count (PTFC)

3) Tampering incident count (TIC)

4) No Tampering count (NTC)

These four input variables are fuzzified into three ranges using transfer function. These ranges are represented as Low(L), Medium(M) and High(H) using transform function shown in the following Fig. 3, 4, 5 and 6 for PTC, PTFC, TIC, NTC respectively.

The output variable of security score is also expressed in the form of transform function for values from 0 to 10 in terms of three variables of Low (L), Medium (M) and High (H). The transfer function for the output security score is given in Fig. 7.

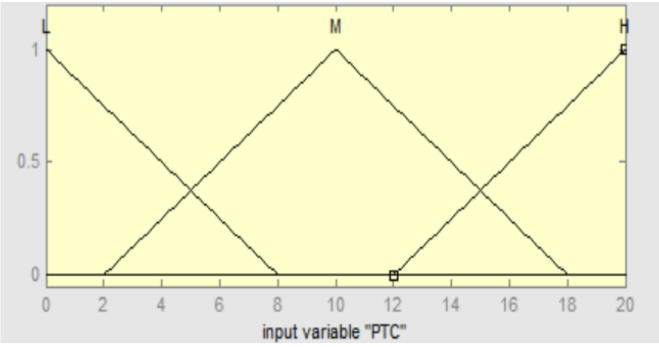


Fig. 3. Fuzzified Transfer Function for PTC.

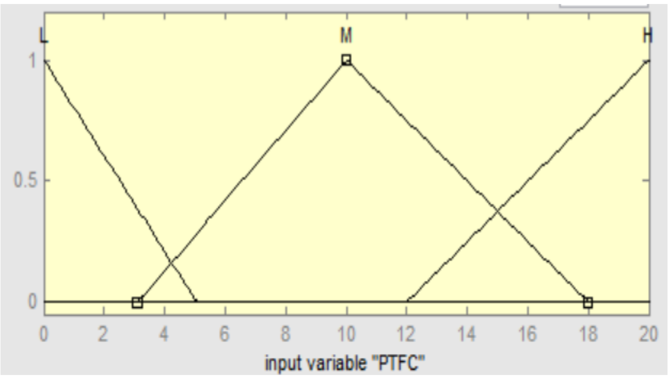


Fig. 4. Fuzzified Transfer Function for PTFC.

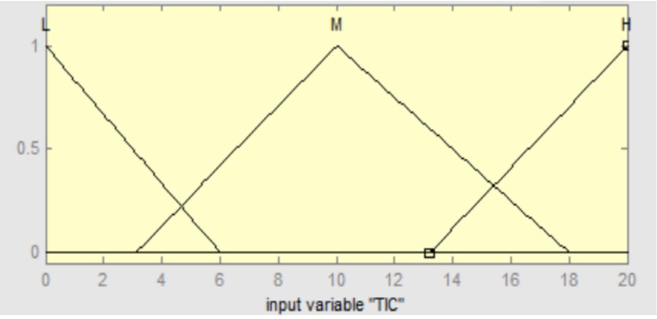


Fig. 5. Fuzzified Transfer Function for TIC.

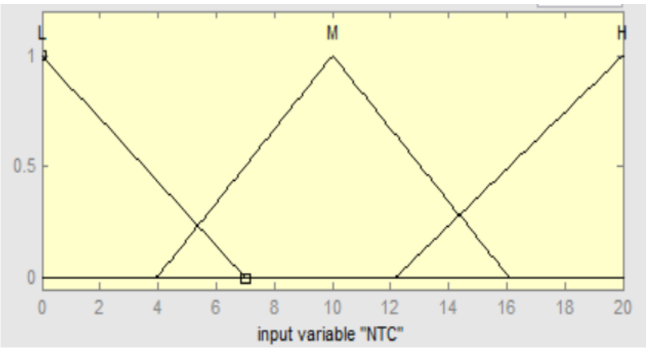


Fig. 6. Fuzzified Transfer Function for NTC.

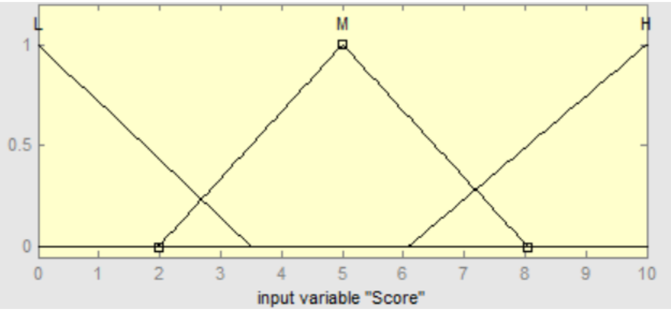


Fig. 7. Fuzzified Transfer Function for Security Score.

Fuzzy rule is designed by mapping the input variables to the output variable for all combinations of inputs. With this fuzzy system a probability fuzzy score for security is calculated from 0 to 10 using the four inputs of PTC, PTFC, TIC and NTC.

The security score calculated using fuzzy function is given as

$$F(score) = \mu_1 * Q(PTC) + \mu_2 * Q(PTFC) + \mu_3 * Q(TIC) + \mu_4 * Q(NTC)$$

Here The fuzzification kernel for input x is Q(x).

The center of gravity method is applied to get defuzzification.

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

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

Compared to other attack detection schemes, in the proposed scheme, we are not detecting the individual attacker. But with presence of attackers in the zone, the security score value goes very low and this zone becomes an unpreferred choice in routing. By this way the routing protocol is resilient against attacks.

The flow chart for secure energy efficient attack resilient routing is shown in Fig. 8.

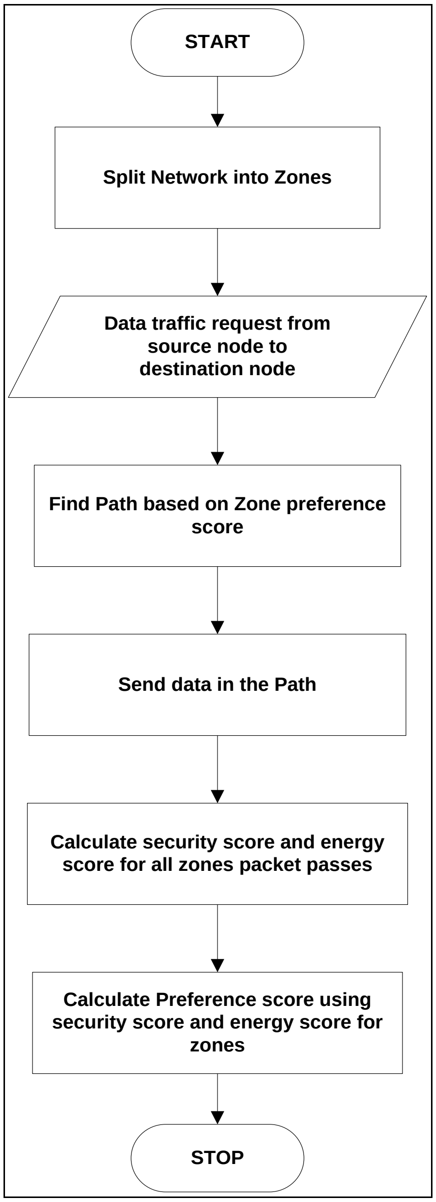

START
Split Network into Zones
Data traffic request from source node to destination node
Find Path based on Zone preference score
Send data in the Path
Calculate security score and energy score for all zones packet passes
Calculate Preference score using security score and energy score for zones
STOP

Fig. 8. Flowchart.

V. Novelty in Proposed Solution

The proposed solution is different from existing solutions is following aspects:

1) Instead of detecting individual attackers, it models the security in terms of zones and moves all the complexity to sink instead of nodes.

2) Paths are adaptively scored based on the security risk and the current residual energy.

3) Multiple attacks of message drop, forging and flooding is considered.

4) Tampering of RREP message contents is also considered.

5) Packet delivery ratio and Life time of the network is improved.

6) Average energy of nodes is increased.

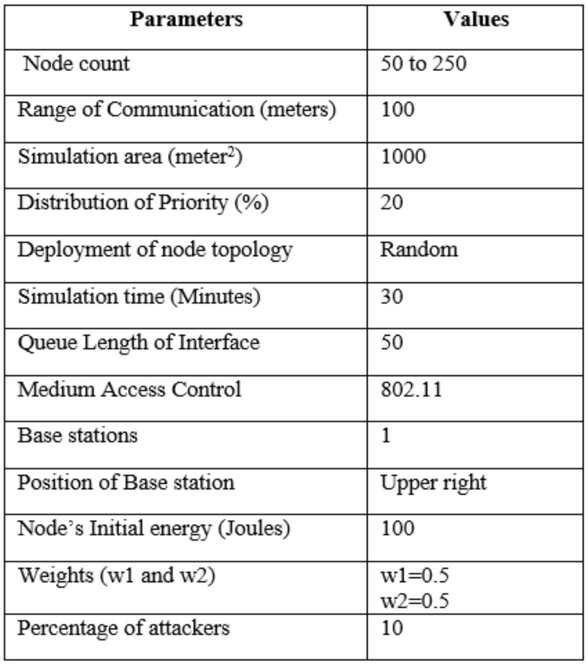
VI. Results

NS2 is used to simulate the proposed solution. The simulation was conducted with following parameters that are shown in Fig. 9.

The proposed solution is compared with solution proposed in [17] for ensuring survivability in contrast to black hole attacks and preserving energy efficiency and solution planned in [20] for localized secure routing architecture in contrast to cooperative black hole attacks. The performance is analyzed in terms of following criterion:

1) Node's Life time.
2) Packet delivery ratio.
3) Node's average energy.
4) End to End delay.
5) Histogram of energy.

Life time is the time at which the energy of the first node goes to 0. The life time is calculated for different number of nodes and is plotted in Fig. 10.



Parameters	Values
Node count	50 to 250
Range of Communication (meters)	100
Simulation area (meter^2)	1000
Distribution of Priority (%)	20
Deployment of node topology	Random
Simulation time (Minutes)	30
Queue Length of Interface	50
Medium Access Control	802.11
Base stations	1
Position of Base station	Upper right
Node's Initial energy (Joules)	100

Weights (w1 and w2)	w1=0.5
	w2=0.5

Percentage of attackers	10

Fig. 9. Simulation Parameters.

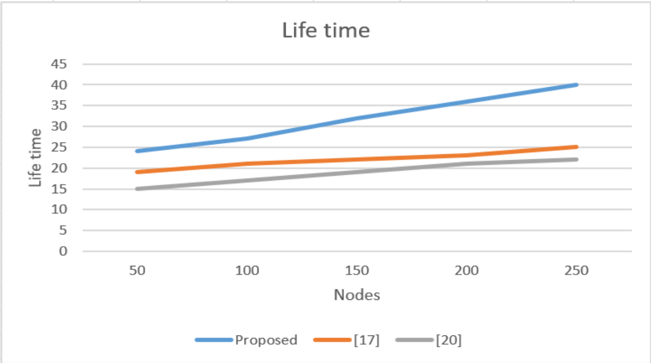


Fig. 10. Life Time Calculation.

The life time is more in the intended solution when compared to [17] and [20]. The life time is more in intended solution is due to because of efficient mitigation of attacks and energy balanced routing path selection. The life time comparison is shown in Table III.

The network packet delivery ratio is measured by changing the number of nodes in the network and the result is given Fig. 11.

The packet delivery ratio is more in the intended method compared to [17] and [20] due to resilient path selection in the proposed protocol. Table IV shows packet delivery ratio.

The packet delivery ratio is determined for different rate of packets and the result is given in Fig. 12.

The packet delivery ratio as shown in Table V, drops as the rate of packet increases, but the drop is very low in the proposed solution compared to [17] and [20]. The reason being the path selection procedure followed in the proposed protocol.

The energy at nodes is averaged at different interval of time and plotted in Fig. 13.

The average energy in the proposed solution (Table VI) is better than [17] and [20] due to well-balanced routing in the proposed solution.

TABLE III. LIFE TIME COMPARISON

No of Nodes	Proposed	[17]	[20]
50	24	19	15
100	27	21	17
150	32	22	19
200	36	23	21
250	40	25	22

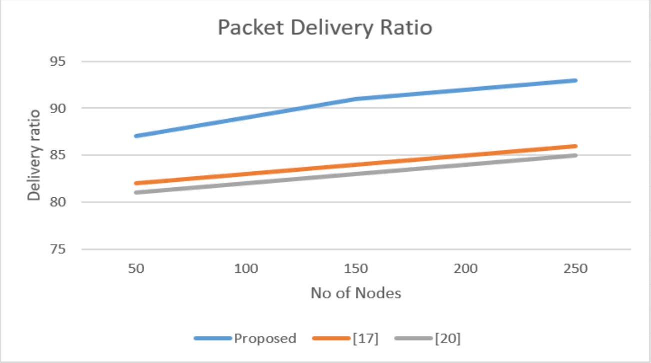


Fig. 11. Packet Delivery Ratio based on no.of Nodes.

TABLE IV. PACKET DELIVERY RATIO COMPARISON

No of Nodes	Proposed	[17]	[20]
50	87.4	82.15	81.5
100	89.3	83.34	82.17
150	91.1	84.56	83.11
200	92.5	85.12	84.32
250	93.3	86.31	85.5

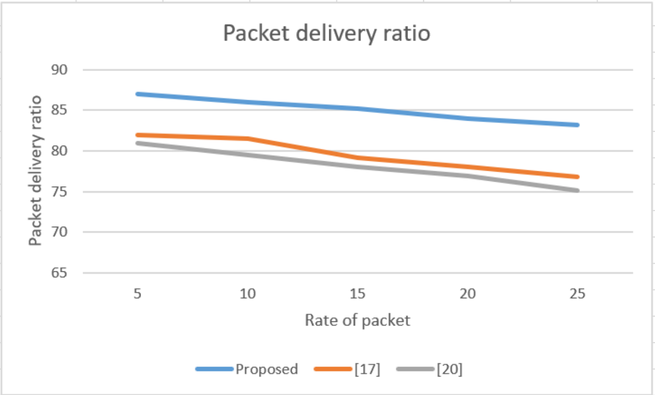


Fig. 12. Packet Delivery Ratio based on Rate of Packets.

TABLE V. PACKET DELIVERY RATIO

No of Nodes	Proposed	[17]	[20]
5	87	82	81
10	86	81.5	79.5
15	85.2	79.12	78
20	84	78	76.9
25	83.2	76.8	75.1

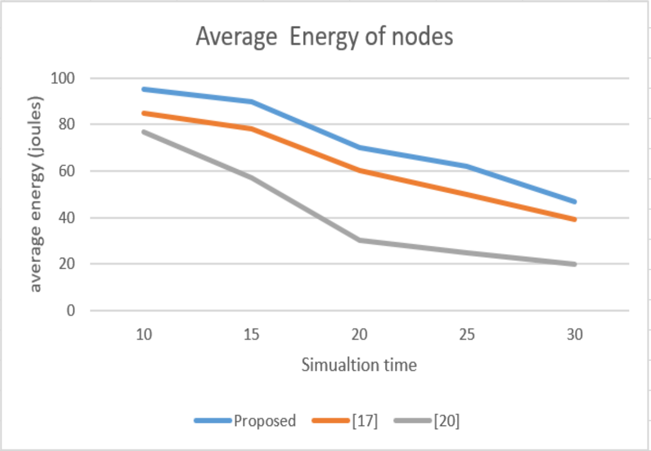


Fig. 13. Average Energy of Nodes.

TABLE VI. AVERAGE ENERGY OF NODES COMPARISON

Simulation time	Proposed	[17]	[20]
10	95	85	77
15	90	78	57
20	70	60	30
25	62	50	25
30	47	39	20

Average end to end delay for packet traversal from node to sink is derived and plotted in Fig. 14.

Due to offloading, all the computations to sink the delay for packet processing is reduced in nodes in the proposed solution compared to [17] and [20]. Delay comparison is represented in Table VII.

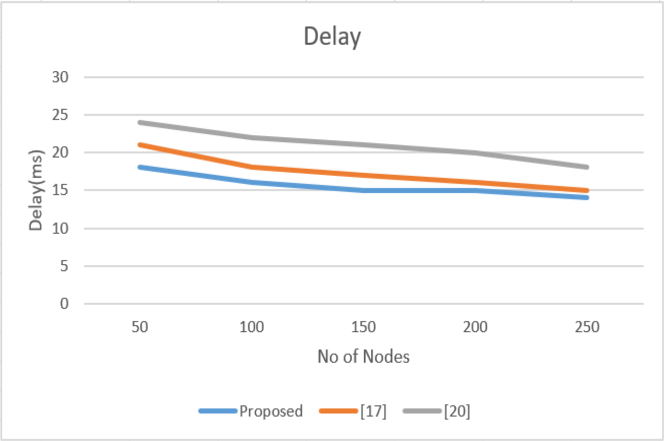


Fig. 14. Delay Comparison.

TABLE VII. DELAY COMPARISON

Simulation Time	Proposed	[17]	[20]
50	18	21	24
100	16	18	22
150	15	17	21
200	15	16	20
250	14	15	18

Histogram of energy is the distribution of nodes depending on their current residual energy. The total energy of 100 joules is split into 5 equal range and the number of nodes whose residual energy falling in the corresponding range is measured and histogram is plotted. The energy histogram gives an indication of how much duration the network will last or how many numbers of nodes are nearing their end of life time. Energy Histogram is shown in Fig. 15.

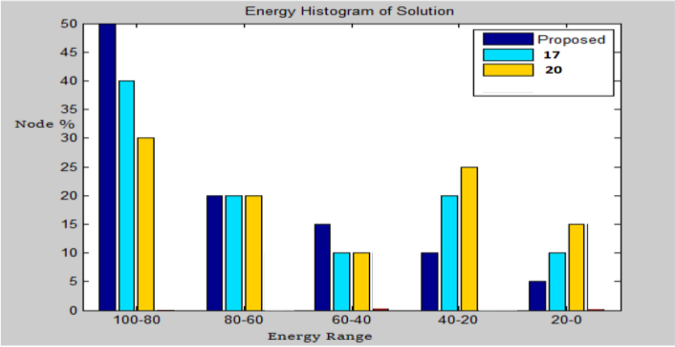


Fig. 15. Energy Histogram.

From the results, it can be seen that nodes with higher energy is available more in intended solution compared to [17] and [20] indicating prolonged life time in the intended solution.

VII. CONCLUSION

In this work, a secured energy efficient attack resilient routing protocol is planned for wireless sensor networks. The routing paths are adaptively scored using a fuzzy function on security and energy consumption. Instead of identifying malicious nodes individually, the proposed solution identified the security risks in a zone and proposed a mitigation mechanism to reduce the probability of routing in those less secure areas. The proposed solution is also able to select the routing path and prolong the life time of the network. The proposed solution can be extended to defend against some more attacks like worm hole as part of future work.

REFERENCES

[1] S. Rani, J. Malhotra, R. Talwar, "EEICCP-Energy Efficient Protocol for Wireless Sensor Networks", Wireless Sensor Network, vol. 5, no. 7, pp. 127-136, 2013.

[2] Nikolidakis, Stefanos A., et al. "Energy efficient routing in wireless sensor networks through balanced clustering." Algorithms 6.1 (2013): 29-42.

[3] Khan, Zahoor A., et al. "A QoS-aware routing protocol for reliability sensitive data in hospital body area networks." Procedia Computer Science 19 (2013): 171-179.

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

[5] Ahvar, Ehsan, et al. "An energy-aware routing protocol for query-based applications in wireless sensor networks." The Scientific World Journal 2014 (2014).

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

[7] Kim, Kyung Tae, and Hee Yong Youn. "An Energy-Efficient and Scalable Routing Protocol for Distributed Wireless Sensor Networks." Adhoc & Sensor Wireless Networks 29 (2015).

[8] Khodabandeh, Hajar, Vahid Ayatollahitafti, and Mohammad Sadeq Taghizadeh. "Link aware and Energy efficient Routing Algorithm in Wireless Body Area Networks." Netw. Protoc. Algorithms 9.1-2 (2017): 126-138.

[9] Mehmood, Amjad, et al. "ELDC: An artificial neural network based energy-efficient and robust routing scheme for pollution monitoring in WSNs." IEEE Transactions on Emerging Topics in Computing (2017).

[10] Manjeshwar, Arati, and Dharma P. Agrawal. "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks." ipdps. Vol. 1. 2001.

[11] Brar, Gurbinder Singh, et al. "Energy efficient direction-based PDORP routing protocol for WSN." IEEE access 4 (2016): 3182-3194.

[12] Gherbi, Chirihane, Zibouda Aliouat, and Mohammed Benmohammed. "Distributed energy efficient adaptive clustering protocol with data gathering for large scale wireless sensor networks." 2015 12th International Symposium on Programming and Systems (ISPS). IEEE, 2015.

[13] Kandukuri, Somasekhar, Nour Murad, and Richard Lorion. "A single-hop clustering and energy efficient protocol for wireless sensor networks." 2015 Radio and Antenna Days of the Indian Ocean (RADIO). IEEE, 2015.

[14] Kandukuri, Somasekhar, et al. "Energy-efficient data aggregation techniques for exploiting spatio-temporal correlations in wireless sensor networks." 2016 Wireless Telecommunications Symposium (WTS). IEEE, 2016.

[15] Robinson, Y. Harold, and M. Rajaram. "Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks." The Scientific World Journal 2015 (2015).

[16] Jhaveri, Rutvij H., and Narendra M. Patel. "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks." Wireless Networks 21.8 (2015): 2781-2798.

[17] 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.

[18] Khatoon, Naghma. "Mobility aware energy efficient clustering for MANET: a bio-inspired approach with particle swarm optimization."

Wireless Communications and Mobile Computing 2017 (2017).

[19] Nallusamy, C., and A. Sabari. "Particle Swarm Based Resource Optimized Geographic Routing for Improved Network Lifetime in MANET." Mobile Networks and Applications 24.2 (2019): 375-385.

[20] 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.

[21] Rajan, C., et al. "Investigation on novel based naturally-inspired swarm intelligence algorithms for optimization problems in mobile ad hoc networks." World Academy of Science, Engineering and Technology International Journal of Mathematical, Computational, Natural and Physical Engineering 9.3 (2015).

[22] 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/

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

[24] 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.

[25] 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.

[26] 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).

[27] 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).

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

[29] 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.

[30] 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.

[31] 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.

[32] Dr. P.V. Rao, Manjunath B E, "Unique Analytical Modelling of Secure Communication in Wireless Sensor Network to Resist Maximum Threats", International Journal of Advanced Computer Science and Applications, (IJACSA) Vol. 10, No. 2, pp 421-427, 2019.

[33] Blanza, F., and L. Materum. "Joint Identification of the Clustering and Cardinality of Wireless Propagation Multipaths." International Journal of Emerging Trends in Engineering Research 7.12 (2019): 762-767.

[34] Al-Shargabi, Bassam, and Mohammed Aleswid. "Performance of RPL in Healthcare Wireless Sensor Network." International Journal of Emerging Trends in Engineering Research 8.3 (2020).