International Journal of Engineering & Technology, 7 (x) (2018) 437-443

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i2.10001
Research paper

Secure and Energy Efficient Routing in Wireless Multihop Clustered Networks Based on RSSI

Jatin Gupta [1] *, Anchal Kathuria [1], Jyotsna Sengupta [2]

[1] Assistant Professor, Chitkara University, Rajpura, India
[2] Professor, Punjabi University, Patiala, India
**Corresponding author E-mail: jatin.gupta@chitkara.edu.in*

Abstract

Today is an era of technology and computing. This technological revolution has created a need for anything and everything to be connected to each other in order to achieve a better communication and utilisation of resources. An isolated computer becomes an information island and may not be able to achieve the optimum use of power and resources. To connect computer systems, there are two options available: one is the installation of LAN (local area networking) cables which may be cumbersome at first but it ensures security and the other one is wireless media. Wireless networking, apart from being simple and efficient, poses serious challenges of security breach by rogue nodes and compromise in performance due to dynamic nature of mobile nodes. Extensive research has been carried out so far and several algorithms and protocols have been formulated to incorporate the location and energy aware characteristics for routing. The technique proposed in this paper considers various factors like energy, distance, vulnerability and battery power while propagating the packet information between the nodes in a sensor networks implementing the heterogeneity in terms of nodes. The ultimate aim is to enhance the longevity of the sensor network while ensuring the security of the network. This is achieved by considering RSSI (Received Signal Strength Indicator) factor in accord with other factors in a multi-hop routing. Extensive simulation results and analysis demonstrate that the proposed technique outperforms other security mechanisms and protocols in the literature in terms of energy awareness, security and routing efficiency.

Keywords: *Vulnerability; RSSI; Multihop; Energy; Security; Cost function.*

1. Introduction

Recent boom in the field of technology has led to the advancements in the field of wireless technology too. Wired media has some limitations which paved the way for the rapid development of wireless networks. Wireless networks are the assortment of sensor nodes scattered physically in an area and deployed randomly to achieve a task [1], [2]. Tremendous developments in the field of micro-electro-mechanical (MEMS) systems and digital electronics has made it possible to manufacture a considerable amount of low cost sensors. The task of these sensors is to sense the data in a sensor field aggregate it and transmit to the base station. The wireless networks suffer from two major flaws which make it different from other cellular networks: Firstly, to address the large number of sensor nodes, IP addressing scheme cannot be applied and due to this, traditional IP based protocols are futile for routing in these networks. Secondly, the performance of wireless networks is often inhibited by the amount of battery power of the sensor nodes, which cuts down the sensor network lifetime and degrades the quality of the network. Several techniques have been devised to reduce the significant consumption of battery power by the sensor nodes in order to minimize overall network wide transmission energy expenditure [3], [4], [5]. In spite of being efficient and hassle-free in terms of connections and wires, the air waves which are the medium of communication in these networks are difficult to contain and the breach in security is also a major issue. Lately, there has been an urgent need of incorporating energy-aware and vulnerability characteristics for routing in wireless networks. Various attacks and security threats can be a major concern in wireless networks [6]. Numerous countermeasures and defence mechanisms are also implemented to deal with these threats [7], [8], and [9]. Routing in wireless sensor networks is a tedious task due to the inherent characteristics of these networks, like dynamic topology, confined computing capability and limited battery power which differ these networks from the other networks. Every now and then, researchers have been trying hard to develop the techniques to achieve the energy-efficiency in wireless sensor networks. In [10], an effective robust routing technique is introduced but it lacks the consideration of energy optimization and susceptibility of the nodes to attacks. Mobility and ad-holism are the key factors that need to be incorporated while designing modern networks as the network devices are evolving immensely in terms of features from desktop systems to smart phones. This evolution has also presented several challenges to sustain such networks in terms of robustness, throughput and energy availability. Since the devices that are to be connected are portable, conserving their battery is a major issue in order to ensure the connectivity of the network for the longest period of time. For such mobile ad-hoc networks (MANET), an energy efficient multi-path routing has been proposed in [11] which aim at conserving the battery of the node and enhancing the QoS and QoE metrics especially for multimedia traffic.

The major objective is to minimize the consumption of battery power and maximize the sensor network life time by introducing an efficient and optimum protocol [12], [13]. Apart from energy awareness routing, spectrum utilization is also a factor that needs to be addressed. These two factors are combined in the routing protocol proposed in [14] for cognitive radio networks (CRNs). It in-

volves the amalgamation of energy aware route selection and spectrum allocation in a cognitive radio networks to improve the throughput and dynamical traffic assignment. Apparently, the heterogeneous clustered wireless networks can act as an ultimate remedy for the limited energy requirements of the sensor networks. It comprises of two different levels of heterogeneity in terms of nodes: simple sensor nodes which are responsible for collecting the data and specialized cluster heads, which receive the data from the nodes, perform significant computation and then relay the aggregated data to the sink. The field in which nodes are deployed is divided into various segments called clusters and each cluster has its own cluster head. In this paper, a new cluster based routing protocol has been proposed which extends the work done in [15], [16]. To incorporate the energy-aware and vulnerability characteristics for routing, it considers RSSI (Received Signal Strength Indicator), among other factors like distance, battery power, energy and vulnerability.

2. Related work

Researchers have been designing several energy efficient protocols that make optimum use of resources and sustain the life of the sensor networks a little longer than usual.

V. Sowmya Devi et.al [11] proposed an energy-efficient routing protocol for mobile ad-hoc networks (MANETs). It aims at optimizing the energy consumption in the multipath routing environment .Particle swarm optimization (PSO) technique and fuzzy optimization are used to find out the next node and clustering is formed such that there are no residual nodes in the system. The technique is considered best for routing multimedia traffic. Simulation results indicate that QoS and QoE metrics are enhanced in the system and data loss is optimized while conserving the energy of the network.

Cognitive Radio networks (CRNs) have offered the solutions to the problem of spectrum under-utilization by exploitation of the unused spectrum by primary users (PUs). The routing technique proposed in [14] assimilates the energy –efficient route selection and spectrum allocation for improving the performance and throughput of the system. It also facilitates effective dynamical traffic assignment in the network.

Amar Kaswan et.al. [17] has proposed two energy-efficient algorithms-RkM and DBRkM with a goal to enhance the lifetime of wireless networks. Wireless networks suffer immensely from the problem of energy exhaustion of those sensor nodes that lie in close proximity to the sink especially when the sink is immobile. This problem is popularly known as hotspot problem [18]. The proposed algorithms exploit the significant contribution of mobile sink in improving the network lifetime. The algorithm introduced in this paper is based on deciding the path of the mobile sink in such a way that balances the trade-off between the data delay and hop-counts in a multi-hop communication. It selects the best possible positions called rendezvous points (RPs) where a mobile sink must visit such that the data collection is efficient and hop count is minimum, It identifies these positions by applying k-means clustering and using a weight function, these positions are minimized to save the energy of the nodes in best possible way. Simulations results depict considerable energy conservation in the network. But it lacks the consideration of data load variability among the sensor nodes in the network.

Ramnik Singh et.al. Introduced a routing protocol based on the adaptive threshold sensitive distributed energy efficient routing protocol [19] that intends to implement the energy-aware routing in the wireless network to prevent the problem of network partitioning that arises due to the energy diminution of nodes. It employs the concept of heterogeneity in the network by deploying three levels of nodes that has different energy levels. At each round of data transmission, cluster heads are chosen in the clusters based on the average energy of all the nodes in the network and the remaining energy of each sensor node. To further minimize the energy consumption, a threshold value is introduced that is compared with the random number generated by each node. This randomization and threshold based calculation are proved to exhibit tremendous increase in the lifespan of the network. Single hop communication between the cluster member and cluster head also conserves the energy to an extent. The threshold T_s can be improved through experiments to increase the accuracy of the results.

Deng et.al [20] devised a protocol (INSENS) that provides intrusion tolerance by making use of an authentication technique called µTesla [21] which is specifically designed for wireless networks. To employ proper security, INSENS uses one-way hash chain (OHC). It also uses the multi-path routing such that identical messages are broken down into several pieces of data and then travel different paths to reach the destination.

In [22], a protocol called SENMA is introduced for the purpose of communication of sensor nodes but the sink in this case, is aerial sink (airplane) which utilises a considerable amount of energy of the sensor nodes. Due to this, the sensor network lifetime may cut down drastically as the nodes may die out soon. The only optimal solution possible in this case is either the quantity of energy needed for the reception of data is enormous or the base station lies in immediacy with the nodes because the receptions happen only at the base station. Another approach which is possible in this scenario is instead of single hop transmission in which data is directly transmitted to the sink, they can relay the data using intermediate nodes so that the nodes may not end up losing their battery power at once. This approach is called 'Minimum-Energy Routing'. But this technique also exhibit limitations like the energy utilised in this system may be greater than the direct transmission. Moreover, the nodes that are close to the base station may require more energy and exhaust their energy soon. This can radically affect the sensor network lifetime [23].

Heinzelman et.al. [23] Introduced a protocol LEACH which employs the concept of clustering in heterogeneous wireless networks for routing. A sensor field is partitioned into clusters and a node is designated as cluster head in each cluster. The task of the cluster head is to aggregate the data from its own cluster propagated by the respective cluster nodes and relaying it to the base station. This protocol performs significantly well in the areas of low activity in terms of event generation. For the situations where data has to be transmitted to long distances, this protocol fails considerably. In addition to this, the cluster heads lack special hardware which may become bottleneck for the cluster.

Subramaniam G.et.al. [24] Proposed an improved version of TUS (Triple umpiring system) by performing energy efficient and secure routing using mine detection. Since the battery life of sensor nodes is very low, the malicious nodes further decrease the sensor network life time. Attempt has been made using this protocol to detect the malicious nodes or erroneous nodes using mine detection algorithm. The CBR (cluster based routing) flow and network size is varied and ESRP-M (energy efficient and secure routing protocol using mine detection) is compared with MMDP (multipath secure routing protocol for flat networks) based on performance metrics like packet delivery ratio and end-to-end delay. The security and the performance turned out to be better in ESRP-M than MMDP. But the inclusion of vulnerability factor of the node is still a major concern in these networks.

In [25], a secure multipath routing protocol is introduced based on the notion of information-theoretic security (ITS) [26]. In this, the multipaths are considered as an optimal rate allocation problem. An attempt is made to prevent the ENs (Eavesdropping node) to decrypt the message between Source node and destination node based on the ITC constraints. In this, we assume that the eavesdropping nodes occur between the multipaths. Further, asymptotic analysis is done to ensure the security in the multipath routing protocol.

In [27], a trust based secure routing protocol is proposed which attempt to identify the suspicious transmission and detecting the malicious nodes by updating the direct and indirect trust values between the nodes. There is an algorithm which is implemented every time the data is routed between two nodes and correspondingly, the trust values are updated which malicious node may find difficult to

resolve. Based on the packet loss which may be incurred due to failure in the updation of trust and weight values, it will be easy to find out the malicious nodes. This protocol employs the concept the vulnerability in the cluster based sensor networks.

The energy-efficient and vulnerability-aware technique which is proposed in this paper extends the quasi-centralized clustering approach discussed in [16]. This technique considers factors like battery power and vulnerability factor to calculate the cost function for every path in the cluster based network. Higher value of cost function indicates that the path consists of critical nodes and is avoided. The striking feature of this approach is it employs single-hop and multi-hop transmission modes periodically depending upon the situation. Simulation results indicate that this technique actually deal with the problems of security and energy constraints in a wireless networks.

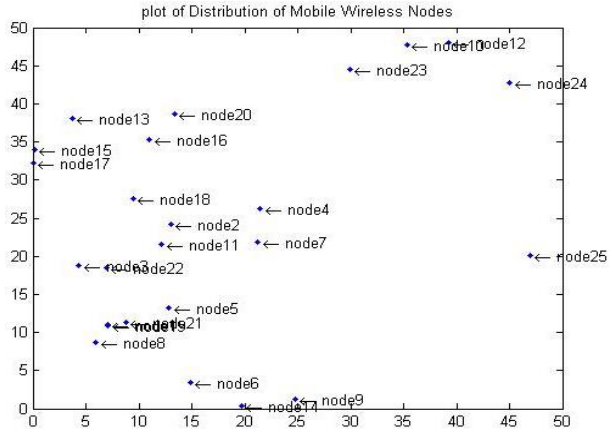

Fig. 1: Plot Showing the Distribution of 25 Nodes in Wireless Network.

3. Problem solution and system model

Following are the postulations of the proposed model for simplification and better understanding of heterogeneous sensor networks. (These assumptions are similar to those in [28]).

- After performing an initial deployment and setup process in the network, all the sensor nodes are capable of communicating with each other and cluster heads are able to track each and every node in their respective clusters.
- We are using a cluster-based approach in this paper, which implicitly states that the task of computation lies with the cluster heads and the sensor nodes in the clusters only relays the data to the corresponding cluster heads.
- The time required for sending and receiving the data is assumed to be same in order to further simplify the energy model and analysis. Also the distance between different nodes in a cluster is not considered to focus more on energy consumption in the network.
- Apart from these, all the sensor nodes consume same amount of energy in sensing and relaying the data to other nodes and cluster heads. In that way, the nodes are considered to be homogeneous.

The network model is shown in Figure 1 in which, 25 nodes are considered and their distribution in the network is shown clearly. Data sensing is done in the network at the instant of triggering of an event and the sensed information is transmitted to control centre through a sink which can be fixed or mobile like an aircraft or a helicopter.

In the network, there are following two types of nodes:

1) Simple sensor nodes which do not have any computation capabilities, they just perform data gathering and relaying tasks.
2) Specialized cluster heads (CHs) which are solely responsible for computation of the data and transmitting to the sink.

An initial set up process is done in the networks in which an ordinary sensor node attaches itself to a particular cluster head after considering the received signal strength (RSSI) factor in addition to other factors. As soon as the sensor node chooses its cluster head and declared itself as a part of a particular cluster, it sends an attachment request to the cluster head and the cluster heads then broadcast the list of the nodes in their respective clusters. After this initial deployment, the sensor nodes sense the data as soon as an event is triggered in the network and then send this data to the corresponding cluster heads and in this way, CHs gather the raw data from the sensor nodes in their cluster process it and then transmit it to the sink.

Since the network is heterogeneous, all nodes are not the same and so is their energy consumption. Some nodes which are closer to the sink tend to utilise more energy than the other nodes due to recurring data transmissions to the sink. These nodes will vulnerably die out of their battery and entire network will collapse. Keeping this in mind, our goal is to enhance the lifetime of the network by minimizing the energy consumption of the critical nodes.

In this paper, our goal is to reduce the energy utilization of the nodes, the critical ones, in particular by taking into consideration various factors like RSSI, vulnerability etc. The secure path is chosen based on these factors as shown in Figure 2 below. The comparison is made between the proposed technique and the previously discussed quasi centralized technique (QCCA) discussed in [16].

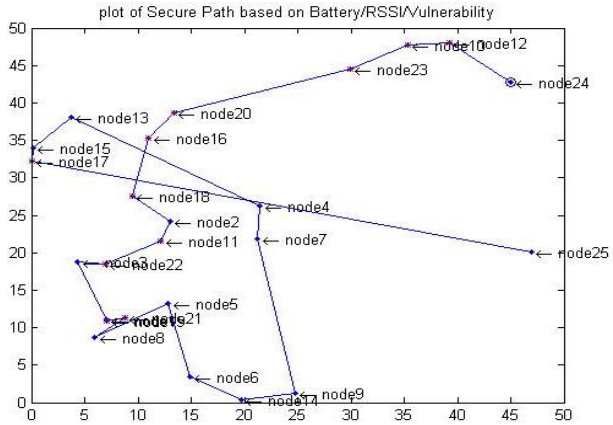

Fig. 1: Plot of Secure Path Based on Battery/RSSI/Vulnerability.

3.1. Proposed work

Various parameters are considered while performing energy and vulnerability-aware routing in the heterogeneous clustered wireless networks. These parameters that are discussed in detail in [15] are briefly discussed below:

3.1.1. Energy factor

The ultimate goal of the wireless networks is maximizing the network lifetime which can be achieved by reducing the energy utilization of each node. Each sensor node maintains the following attribute:

$$E_i = \frac{B_i}{B_i^o} \quad (1)$$

Where B_i is the residual battery power and B^o_i is the initial battery [14]. As the packets are forwarded in the network, the energy of each node is calculated based on the above formula and those paths are avoided in the networks which consist of low energy nodes.

3.1.2 Vulnerability factor

To prolong the longevity of the network, there is a need of vulnerability-aware routing. Vulnerable nodes are those nodes the removal of which has an adverse effect on the overall connectivity of the network. Vulnerability factor is determined to identify secure path. The secure path is the path that contains non-vulnerable nodes. The procedure used to calculate the vulnerability factor of each

node in the network is discussed in [27]. The following formula is used:

$$V_i = \frac{N^i_{before}}{N^i_{after}} * \frac{L^i_{before}+1}{L^i_{after}+1} \quad (2)$$

High value of vulnerability means that the path comprises crucial nodes whose removal may lead to the disconnection of the network. So, we should follow only those paths that have low value of vulnerability.

3.1.3. Received signal strength indicator (RSSI)

RSSI indicates the power level of the signal received in the network. Higher the RSSI value, stronger is the signal. During the initial deployment, this factor is used to deploy the nodes in a cluster. During packet forwarding, this factor is considered among other factors to decide a secure path for routing while sustaining the lifetime of the network. The formula below is used:

$$RSSI=-10n \log10 (d) + A \quad (3)$$

Where n is propagation exponent, d is the distance from the sender and A is the received signal strength at one meter of distance.

3.1.4. Local cost function

It can be calculated using energy factor and vulnerability. The following formula is used:

$$C_i = \frac{V_i}{E_i} \quad (4)$$

Higher value of C_i indicates that the path contains critical nodes. So, those paths are avoided which has higher value of C_i.

3.1.5. Global cost function

Global cost function of a path is calculated based on the local cost function of the individual nodes in that path. It is done to design the routing policy in a manner to select the best possible path from source to destination. Global cost function I_P is determined using the following formula:

$$I_P = min \sum C_i^2 \quad (5)$$

Where C_i is the local cost function of the path. C_i^2 is used instead of C_i to minimise the effect of low energy nodes as discussed in [13], [14]. The efficient routing policy in the network will involve choosing the path with low value of I_P. Higher the value of I_P, more the number of critical nodes in that path. In figures 4, 5 and 6, the algorithm used for calculating the global cost function for finding the secure path. It can be seen that several factors along with RSSI is used for finding the secure path in the network.The notations used to develop the proposed algorithm are shown in figure.4.

Terms	Definition
Prop.	Propagation exponent
$Rec._{sig}$	Received signal strength
n	No. of nodes
B	No of bits
Node_x	x-coordinate of the node
Node_y	y-coordinate of the node
n_d	No.of dead nodes
L_{before}	No. of levels before removing i^{th} node
L_{after}	No of levels after removing i^{th} node
RSSI	Received signal strength indicator
dist	Distance between two nodes
Battery	Current battery power of a node
Initial battery	Initial battery power of the node
$dist_{farth}$	Farthest distance of a node
N_{far}	Node at farthest distance
dist(i)	Distance of i^{th} node
node_x(i)	x-coordinate of i^{th} node
node_y(i)	y-coordinate of i^{th} node
$dist_{avg}$	Average distance of nodes in the network
$dist_{connect}$	Distance between two connected nodes
$N_{connect}$	No. of connected nodes in the network
$dist_{connect}(1)$	Distance of the first connected node
$N_{connect}(1)$	First connected node
N_{temp}	Node at the minimum distance
temp_min_dist	Minimum distance between the nodes
temp_max_RSSI	Maximum RSSI at the minimum distance
Energy_factor	Energy of the nodes
Vulnerabilty_factor	Vulnerability factor of the nodes

Fig. 3: Notations Used in the Algorithm.

Algorithm:
INPUT: Prop., $Rec._{sig}$, n, B, Node_x, Node_y, n_d, L_{before}, L_{after}
OUTPUT: Updated global cost function (I_P) to find the secure path

1) Initialize the values of Prop., $Rec._{sig}$, n, B,Node_x,Node_y, n_d, L_{before}, L_{after}
2) I_P=0 /*Initialization*/
3) For n=1 to 400 do
4) Initial battery=50*array of 1's of size n*n
5) Battery=Initial battery
6) RSSI= array of 0's of size n*n
7) dist= array of 0's of size 1*1
8) distfar=0 /*Initialization*/
9) Nfar=0 /*Initialization*/
10) For i=1 to n do
11) dist(i) = sqrt (node_x(i)^2) + (node_y(i)^2)
12) if distfar<dist(i) then
13) Set distfar= dist(i)
14) Nfar=i
15) end if
16) end for
17) Set distavg= sum of the distance between two nodes divided by no. of nodes
18) distconnect= array of zeros of size n*n
19) Nconnect= array of zeros of size n*n
20) Set Nconnect(1) = Nfar/*initialization*/
21) Set distconnect(1) = distavg /*initialization*/
22) For i=2 to n d
23) Initialize Ntemp, temp_min_dist, temp_max_RSSI.
24) For j=1 to n do
25) Set b=0
26) For k=1 to i-1 do27:
27) if j=Nconnect(k)
28) Set b=1
29) break
30) end if
31) end for
32) if b=0 then
33) dist= sqrt(node_x(Nconnect(i-1))-node_x(j)^2)+(node_y(Nconnect(i-1))-node_y(j)^2)
34) RSSI(i) = -(10*prop*log(dis)+Recsig)
35) if RSSI(i) >temp_max_RSSI then
36) temp_max_RSSI = RSSI(i)
37) temp_min_distance=distance
38) Ntemp=j
39) end if
40) end for

41) end for
42) distconnect(i) =temp_min_dist
43) Nconnect(i)=Ntemp;
44) battery(Nconnect(i-1))=battery(Nconnect(i-1)) -distconnect(i)^2*B*n*100*0.000000001- B*n*50*0.000001
45) battery(Nconnect(i))=battery(Nconnect(i))-B*n*50*0.000001;
46) if battery(Nconnect(i-1))<=0 then
47) Nd(1,n) = Nd(1,n) + 1
48) battery(Nconnect(i-1))=0
49) end if
50) Energy_factor = battery/initial_battery
51) Vulnerability_factor = (n/(n - 1))*((Lbefore+1)/(Lafter+1))
52) Cost_function = Vulnerability_factor/Energy_factor
53) Cost_function2 = Cost_function*Cost_function
54) Global_cost_function = Global_cost_function + Cost_function2
55) end for
56) end for
57) Ip(packets)=global_cost_function

The above pseudo code shown in fig 4, 5 and 6 is implemented in matlab and results are represented graphically as shown in figure 10.

3.2. Packet forwarding

The forwarding of packets in the network is performed exactly as discussed in [16]. The entire procedure is comprised of two steps of operation: set up phase and steady-state phase.

In the set-up phase, in every cluster all the nodes broadcast their I_p values to the nodes which are in close proximity to each other. This process is initiated from a cluster head in the cluster. Every node receives the I_P from their predecessor or up tree nodes and store these I_P values with the corresponding node id in their routing tables. Then the node chooses the lowest I_P value from their tables, insert their own I_P values and transmit it to their neighbours. In this way, the routing tables of all the nodes in the network is flooded with the I_P values of their immediate neighbour nodes which is an important control information required for relaying the data in the network while focussing on energy-aware routing. Initially, the energy and RSSI values of each node is calculated based on their actual distance and average distance between the two nodes and a plot is generated in order to have a clear idea of the network nodes so that the number of dead nodes can be easily calculated as the packets are forwarded in the network. The plot of energy and RSSI versus node number is shown in Figure 5 and 6.

In steady-state phase, the originating node who desires to transmit the data chooses the neighbour node with the lowest I_P value. It sends the data and receives an acknowledgement from the receiving node with their updated I_P value. In this way, the routing tables of each node are updated with the new I_P as the packet forwarding is done and energy of the nodes starts draining out. This increases the I_P value which means the path contains the critical nodes and those paths can be avoided easily. While determining the secure and energy efficient path for routing of each packet as the time progresses, number of dead nodes are found out based on their battery power and RSSI values and those paths can be ignored. Based on this, energy and vulnerability is calculated which updates the global cost function after the transmission of each packet.

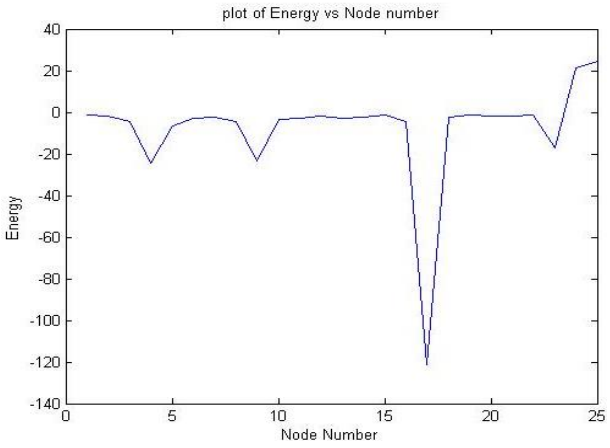

Fig. 4: Plot of Energy vs. Node Number.

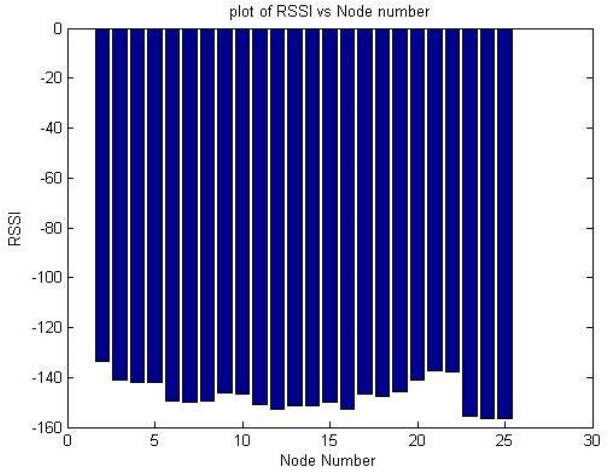

Fig. 5: Plot of RSSI vs. Node Number.

4. Simulation and results

To examine the efficiency of the proposed technique, a network consisting of 100 sensor nodes is generated. The dimension of the sensor field is 0.01km square. In figure 5, energy is plotted against number of nodes. As the sensor nodes start relaying the data in the wireless network, they start dying out of their battery. Initially, there are fewer nodes but as we can see there is a sudden dip in the graph which clearly depicts that most of the nodes in the network die out at the same time. It means that our proposed system manages to keep a considerable amount of nodes alive for quite a long time so that the network is not rendered disconnected. The proposed energy and vulnerability aware routing technique is implemented in this network and the results are critically scrutinised on the basis of global cost value which increases abruptly as the energy of the nodes decreases in the network. In figure 6, RSSI factor is plotted against number of nodes. As the time progresses, there are fewer number of nodes which has low value of RSSI. After a while, there is a clear plunge in the RSSI values of large number of nodes which indicate that substantial no. of nodes die out at once.There are various factors that decide the value of global cost like distance, battery power and vulnerability. We are performing set of experiments in which our proposed technique is compared with the QCCA technique discussed in [14], shown in Figure 7.

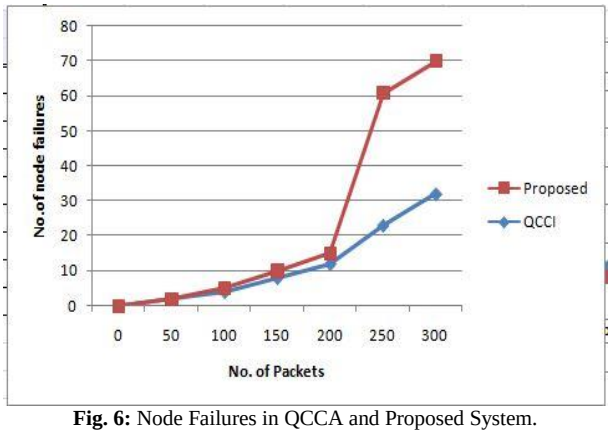

Fig. 6: Node Failures in QCCA and Proposed System.

In the Figure 7, the comparison of quasi centralised cluster based routing technique (QCCA) [14] and our proposed technique is clearly shown. QCCA technique considers two performance metrics E_i and V_i, which play a vital function in deciding the longevity of the network. In the proposed technique, another metric is considered i.e. RSSI in accord with the other factors to calculate the global cost value in the system which is pivotal factor that determines the sustainability of the wireless network. From the Figure 7, it is clearly evident that the rate of node failures is higher in QCCA system than in proposed system. As the time progresses and packets being forwarded in the system, the nodes in the QCCA system start draining out of their battery very quickly. On the other hand, proposed system is able to sustain their nodes alive for a much longer time such that all nodes die out at the exact instant of time.

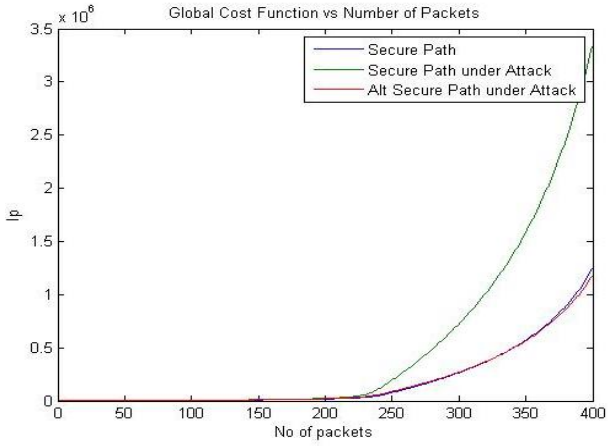

Fig. 7: Choice of Routing Paths Based on Minimum Global Cost Value.

The above Figure exhibits the plot between the global cost function Ip [14] and the number of packets in the proposed system. Based on the vulnerability factor, a secure path is chosen in the network that is less vulnerable to attack. If a secure path is under attack, an alternate secure path is chosen which is much closer to the actual secure path. As evident from the above Figure, in the secure path under attack, the global cost function increases abruptly when no of packets are around 225 or so. It means the nodes die out quickly and the secure path under attack consists of critical nodes, as the value of global cost function increases only when energy of the nodes decreases. The objective is to keep the I_p value minimum to prolong the network lifetime which is achieved successfully in the alternate secure path. On the other hand, QCCA system exhibits abysmal performance in terms of global cost function.

5. Conclusion

This paper presents energy and vulnerability-aware routing technique proposed for heterogeneous cluster based sensor network, which employs two different variety of nodes: cluster heads and ordinary sensory nodes. The proposed technique is energy efficient as it takes various factors into consideration like energy, vulnerability and RSSI. The performance of the technique is evaluated in terms of global cost function and compared it with QCCA technique. It is clearly evident from the rigorous simulation output that the proposed technique outperforms the QCCA technique in fulfilling the objective of enhancing the overall network lifespan. The technique also provides the automatic adaptation of routes when a certain route is under attack. The proposed technique is robust in the sense that it keeps the nodes alive as longer as possible as compared to QCCA technique. Our future work may involve further increasing the network lifetime and implementing security mechanisms in the wireless network.

6. Competing interests

The authors declare that there is no conflict of interests' regarding the publication of this paper

References

[1] D. Estrin, R. Govindan, J. Heidemann, and Satish Kumar. Next Century Challenges: Scalable Coordination in Sensor Networks. In *Proceedings of Mobicom' 99*, 1999.

[2] J. Kulik, W. Rabiner, and H. Balakrishnan. Adaptive Protocols for Information Dissemination in Wireless Sensor Networks. In *Proceedings of Mobicom' 99*, 1999.

[3] W. Mangione-Smith and P.S. Ghang. A Low Power Medium Access Control Protocol for Portable Multi-Media Systems.In *Proceedings 3rd Intl. Workshop on Mobile Multimedia Communications*. Princeton, NJ, Sept 25-27, 1996.

[4] K. M. Sivalingam, M. B. Srivastava and P. Agrawal.Low Power Link and Access Protocols for Wireless Multimedia Networks. In *Proceedings IEEE Vehicular Technology Conference VTC'97*, May 1997.

[5] M. Stemm, P. Gauthier, D. Harada and R. Katz.Reducing Power Consumption of Network Interfaces in Hand-Held Devices. In *Proceedings 3rd Intl. Workshop on Mobile Multimedia Communications*, Sept. 25-27, 1996, Princeton, NJ.

[6] Z. Karakehayov, "Using REWARD to detect team blackhole attacks in wireless sensor networks," in *Proc. Real-World Wireless Sensor-Networks'05*, Jun. 2005.

[7] X. Du and H. H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communication*, vol. 15, no. 4, pp. 60-66, Aug. 2008. https://doi.org/10.1109/MWC.2008.4599222.

[8] V. C. Giruka, M. Singhal, J. Royalty, and S. Varanasi, "Security in wireless sensor networks," *Wireless Communication and Mobile Computing*, vol. 8, no. 1, pp. 1-24, Jan. 2008. https://doi.org/10.1002/wcm.422.

[9] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: attacks and defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74-81, Jan. 2008. https://doi.org/10.1109/MPRV.2008.6.

[10] N. M. Khan, Z. Khalid, G. Ahmed, and M. Yasin. A robust routing strategy for wireless sensor networks.In *Proc. of IEEE International Conference on Electrical Engg. (ICEE)*, pages1 {5, Lahore, Pakistan, April 2007. https://doi.org/10.1109/ICEE.2007.4287337.

[11] Devi, V. S., & Hegde, N. P. (2016). Energy efficient multipath routing protocol for enhancing QoS and QoE in multimedia applications for MANETs. *International Journal of Communication Networks and Information Security*, *8*(3), 158.

[12] J. Chang and L.Tassiulas.Energy conserving routing in wireless adhoc networks.In *Proc. IEEE INFOCOM*, March 2000.

[13] C. Chiasserini, I. Chlamtac, P. Monti, and A. Nucci. Energy efficient design of wireless ad hoc networks.In *Proc. European Wireless*, February 2002. https://doi.org/10.1007/3-540-47906-6_30.

[14] Kamruzzaman, S. M., Fernando, X., & Jaseemuddin, M. (2016). Energy Aware Multipath Routing Protocol for Cognitive Radio Ad Hoc Networks. *International Journal of Communication Networks and Information Security*, *8*(3), 187.

[15] Z. Khalid, G. Ahmed, N. M. Khan, and P. Vigneras real-time energy-aware routing strategy for wireless sensor networks. In *Proc. Asia-Pacific Conference on Communications (APCC)*, Bangkok, Thailand, October 2007.

[16] Khan, Noor M., Ihsan Ali, Zubair Khalid, Ghufran Ahmed, Rodica Ramer, and Alex A. Kavokin. "Quasi centralized clustering approach for an energy-efficient and vulnerability-aware routing in wireless

sensor networks." In *Proceedings of the 1st ACM international workshop on Heterogeneous sensor and actor networks*, pp. 67-72. ACM, 2008 https://doi.org/10.1145/1374699.1374712.

[17] Kaswan A, Nitesh K, Jana PK. Energy efficient path selection for mobile sink and data gathering in wireless sensor networks. AEU-International Journal of Electronics and Communications. 2017 Mar 31; 73:110-8. https://doi.org/10.1016/j.aeue.2016.12.005.

[18] Jaichandran R, Raja JE, et al. Effective strategies and optimal solutions for hotspot problem in wireless sensor networks (WSN). 10th International Conference on Information Sciences Signal Processing and their Applications (ISSPA).IEEE; 2010. p. 389–92.

[19] Singh R, Verma AK. Energy efficient cross layer based adaptive threshold routing protocol for WSN. AEU-International Journal of Electronics and Communications. 2017 Feb 28; 72:166-73. https://doi.org/10.1016/j.aeue.2016.12.001.

[20] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no.2, pp. 216-230, Jan. 2006. https://doi.org/10.1016/j.comcom.2005.05.018.

[21] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: Security protocols for sensor networks," in *Proc. ACM International Conference on Mobile Computing and Networking'01*, Jul. 2001. https://doi.org/10.1145/381677.381696.

[22] G. Mergen, Q. Zhao, and L. Tong. Sensor networks with mobile access: Energy and capacity consideration. *IEEE Transactions on Communications*, 54(11), November 2006. https://doi.org/10.1109/TCOMM.2006.884845.

[23] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. Energy-efficient communication protocol for wsn. In *Proc. 33rd Hawaii International Conference on System Sciences*, 2000.

[24] Subramanian G, Amutha R. Efficient and secure routing protocol for wireless sensor networks using mine detection an extension of triple umpiring system for WSN. In Computing Technology and Information Management (ICCM), 2012 8th International Conference on 2012 Apr 24 (Vol. 1, pp. 141-145).IEEE.

[25] Choi J. Secure multipath routing in wireless multihop networks based on erasure channel modeling. InWireless Advanced (WiAd), 2012 Jun 25 (pp. 6-10). IEEE.

[26] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin,"Wireless information-theoretic security," *IEEE Trans. Inf. Theory* vol.54, no. 6, pp.2515-2534, June 2008. https://doi.org/10.1109/TIT.2008.921908.

[27] Nagarathna, K., Kiran, Y. B., Mallapur, J. D., &, S. (2012, July). Trust based secured routing wireless multimedia sensor networks. In *Computational Intelligence, Communication Systems and Networks (CICSyN), 2012 Fourth International Conference on* (pp. 53-58). IEEE.

[28] Y. Zou and K. Chakrabarty. Energy-aware target localization in wireless sensor networks.In *Proc. First IEEE International Conference on Pervasive Computing and Communications (PerCom'03)*, 2003. https://doi.org/10.1109/PERCOM.2003.1192727.

[29] T. N. Arvanitis, C. C. Constantinou, A. S. Stepanenko,Y. Sun, B. Liu, and K. Baughan. Network visualisation and analysis tool based on logical network abridgment. In *Proc.Military Commun. Conf. (MilCom'05)*, volume 1, pages 106{112, October 2005. https://doi.org/10.1109/MILCOM.2005.1605672.