# Bandwidth and Delay Aware Routing Protocol with Scheduling Algorithm for Multi Hop Mobile Ad Hoc Networks

Y. Harold Robinson, E. Golden Julie, S. Balaji



***Abstract*—** The scheduling based routing scheme is presented in this paper to avoid link failure. The main objective of this system is to introduce a cross-layer protocol framework that integrates routing with priority-based traffic management and distributed transmission scheduling. The reservation scheme is based on ID. The presented scheme guarantees that bandwidth reserved time slot is used by another packet in which end-to-end reservation is achieved. The Bandwidth and Delay Aware Routing Protocol with Scheduling Algorithm is presented to allocate channels efficiently. The experimental results show that the presented schemes performed well in various parameters compared to existing methods.

***Keywords*—**Integrated routing, scheduling, MAC layer, IEEE 802.11.

## I. Introduction

RESERVATION setup is used to reserve the time resources in the nodes along a path between a source and destination node. The resource reservation is initiated by the source node. The destination node computes a clear-to-reserve (CTR) message [50]. Transmissions in the real-time path must be protected against interference. If a reservation path breaks and a new one is established, the nodes of the old path should release their reservations [1].

The MANET introduces the framework for integrating with unicast and multicast routing which is based on mesh enclaves. The multicast ad hoc on-demand distance vector protocol preserves a collective tree for every multicast group consisting of receivers and relays [36]. A mesh-activation request has generated by the source node and transmitted by source S to destination D [2]. Energy-based dynamic encryption is used for security purposes [33] in Wireless Communication. Energy Efficiency has been maintained by Virtual Back Bone Path Based Cluster Routing Protocol [42]. The cross layer is introduced to realize maximum throughput. The main contribution of this approach is a joint optimization problem. There are two challenges for achieving maximum throughput [31]:

Harold Robinson Y. is an Associate Professor with the Department of Computer Science and Engineering, SCAD College of Engineering and Technology, India (e-mail: yhrobinphd@gmail.com).

Golden Julie E. is an Assistant Professor, Department of Computer Science and Engineering, Anna University Regional Campus, Tirunelveli, India (e-mail: goldenjuliephd@gmail.com).

Balaji S. is an Associate Professor with the Department of Computer Science and Engineering, Francis Xavier Engineering College, India (e-mail: sbalajiphd@gmail.com).

- Data routing problem at the network layer.
- Power control problem.

These two challenges are achieved by joint optimization problem. A mesh network is the system's capability to competently maintain improved throughput in multicast applications over wireless links [4]. Trustworthy Link Failure Routing Algorithm is used to predict the link failure in MANETs [3].

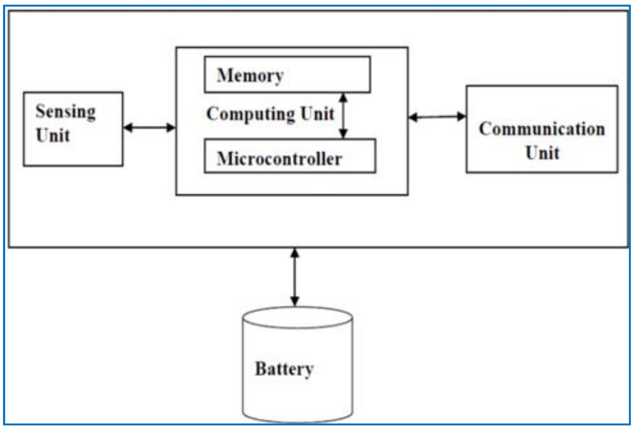


Fig. 1 Architecture of Wireless Sensor Node

The physical layer can be abstracted as a set of elementary capacity graphs. The network coding is used for multicast session [5]. The Fuzzy Enabled Device-to-Device Broadcasting Algorithm is used to transmit the packets from one device to another device [6]. Tree based Opportunistic Routing can be implemented in Mobile Ad hoc Networks to reduce the complexity [27]. Detection of Black Holes can be achieved in MANET Using Collaborative Watchdog with Fuzzy Logic methods [45].

The nonappearance of a packet at the decoder causes a decoding error, which translates into a quality drop that may propagate to subsequent frames. Joint source and channel coding is used to support the new H.264 video coding standard with increased throughput [30]. The joint optimization allows interaction and flexible resource allocation across the network protocol stack [7].The novel algorithm is used to provide loop free routes even while repairing broken links, because this protocol does not require global periodic routing advertisements. The Destination-Sequenced Distance Vector (DSDV) algorithm has been used as a modification of the distance vector routing technique by which wireless mobile nodes collaborate to shape an ad-hoc network [8].Energy-aware Multipath Routing Particle Swarm Optimization algorithm is used to increase the Quality of Service in MANET [9]. The network layers aim at replacing in the classical open system interconnection (OSI) network stack. It may achieve extremely elevated performance in terms of the network performance related to every entity layers; they are not mutually optimized to exploit the overall network performance while minimizing the energy expenditure. The main drawback of this system is a lack of modularity and decreased robustness [58]. The deprived performances for the whole systems will depend on the lack of modularity and reduced robustness [10]. The packet radio network is totally asynchronous and based on completely distributed architecture. The synchronous time frame leads to efficient multimedia support implementation but introduces more complexity and less robustness [12]. A real-time connection is set up using a quick reservation technique. Namely, we imagine that real-time packets reach the specified destination at stable time periods. The first information packet in the multimedia rivulet makes the reservations along the destination. Once the first data packet is accepted on a link, a transmission skylight is reserved at suitable time periods for all the succeeding packets in the association [11].

Extremely Opportunistic Routing (EXOR) [13] is one of the principally in opportunistic routing protocols; it employs the Expected Transmission Count (ETX) as a parameter for intermediate node assortment. Simple Opportunistic Adaptive Routing Protocol (SOAR) [14] employs the ETX parameter for intermediate node assortment. Least-Cost Opportunistic Routing (LCOR) [16] is the other kind of opportunistic routing protocol that employs the Expected Any-Path Transmission (EAX) parameter for intermediate node assortment. In Opportunistic Any-Path Forwarding (OAPF) [17], secured cluster and sleep based energy-efficient sensory data collection with mobile sinks [15], enhanced cluster based key management techniques [18] are used for security related issues in mobile networks, and nodes are educated to pick a preliminary record of candidates with the ETX parameter. Minimum Transmission Selection [19] algorithm generates a specified opportunistic routing protocol using the EAX as a parameter for intermediate node assortment. In contention-based forwarding algorithm [20], the clustering formation can be done using dominant set and trust evaluation methodology [21]. The source node instigates the routing progression by establishing its own special data for delivering data packet. Position based opportunistic routing [22] selects the realizable detachment development during every intermediate node to the destination. Intermediate Node based Routing can be used in the parameters of distance based opportunistic routing [23] and Intermediate node assortment [39]. Additionally, [25], [26] proposed a trust-based methodology for sending data packets from source to their destination in a more consistent approach. For the improved data transmission, the Trust Management approaches can be implemented in several wireless networks [28, [29], [32]. Trust models can be implemented in wireless networks to maintain the Quality of Service [34]-[37], [38]. Conversely, [40] introduced a trust computation methodology for opportunistic using Positive Feedback Messages (PFM). Likewise, [41] and [43] proposed cryptographic methods that detected and isolated black hole attacks in the network nodes in opportunistic routing based networks. Moreover, as assured in [44] and [46], opportunistic routing protocols do better than established routing protocols while it comes to network performance by means of Quality of Service. The methods proposed in [47] and [49] have been used in exceptionally receptive situations such as military related real-time applications for reducing energy consumption and detecting explosions [57] in the area of security awareness in sensor networks. Distributed Self-Healing Protocol is used to transmit data packets in unattended wireless sensor network [51]. Underwater sensor networks are a talented part of wireless sensor networks with the reason of discovering and scrutinizing the world underneath the water's exterior models [52]. Reference [53] indicated that opportunistic routing protocols can be suitable solutions for addressing the capriciousness of such networks. An Encryption Scheme for User-Data Security in Public Networks [54] method has been proposed for User Data based Security problems, Securing Inimitable and Plundering Track for Ad Hoc Network [60] has been implemented for cryptographic issues. As cited in [55] and [56], wireless sensor networks (WSNs) and Internet of Things (IoT) have been used in several real-time scenarios. Opportunistic routing will be implemented in several number of re-broadcast for scheduling algorithm [59]. Security has been maintained by using the opportunistic routing based Secured MAS approach [39] with fuzzy based routing [48]. Clustering can be done using Tree Based Data Fusion Algorithm in WSN [24].

## II. Proposed Scheme

### A. Channel Reservation

Here, the channel is reserved based on their ID. Each node ID is identified while forwarding the packets since those packets encompasses their network node ID. Every frame is a collection of N time slots from slot 0 to slot N - 1. The channel reservation schemes must be carefully designed to provide better QoS guarantee to the mobile users. The reservation is based on ID. Fig. 2 illustrates the data transmission in upstream mode, Fig. 3 illustrates the data transmission in downstream mode and Fig. 4 illustrates the data transmission using bandwidth allocation.

Every single one of the node can access the channel in time ordered sequence. A node x is relaying data packet from source to the destination for transmission.

### B. Channel Reservation

The information needed to verify these conditions are stored in following method.

- Neighbor Lists.
- Ongoing Reservation Lists.
- Reserved Slot List.

If a free slot $slot_c$ is identified, then a node with identifier $Id^x$ transmits a Reservation Request packet to its neighbors and waits for N seconds to collect the replies.

If all the nodes send a reply that Reservation is granted, then the packet is granting the reservation. Then node x considers the slot $slot_c$ as reserved by itself and moves that slot from its list of ongoing reservations to list of reserved slots. Otherwise, node x selects the next free slot in the interval and transmits a new reservation request. This procedure is repeated until a time slot is successfully reserved or all the free slots are allocated. In latter case, nodes wait for mesh announcement period and retry the reservation. Fig. 5 demonstrates the dynamic data transmission using bandwidth allocation.

## III. Scheduling Algorithm

```
Procedure Find_Channel (node, destination, Cost)
    cost_node:=Exp_Tran_Cnt_node,destination
    Cost_Source_node,destination := Empty ;
    while (|Cost_Source_node,destination| < Cost) &&
    (shortest_Path(node, destination)) do
        Optimal_path : = shortest_Path(node, destination)
        Channel :=Find_Neighbour(node, Optimal_path)
    if (Channel := destination) then
            merge(Cost_Source_node,destination, destination)
            cost(destination) :=0
     else
     cost(Channel): = Exp_Tran_Cnt_Channel,destination
     if cost(Channel) < cost(node) then
    merge (Min_Cost_Source_node,destination, Channel)
     end if
     end if
    Remove_Edge(node, Channel);
    Sort_By_Distance_Progress(Cost_Source_node,destination, node,
destination)
    neighbours :=Find_Neighbor(node)
    Eligible_Neighbors := Empty;
    for everyneighbor in neighbors do
     if distance_neighbor,destination<distance_node,destination then
    merge (Available_Neighbors, neighbor)
    end if
    end for
       Sort_By_Distance(Eligible_Neighbors)
    Channel := find_Best_Possible_Neighbor(node)
        Optimal_path : = shortest_Path(node, destination)
        Channel := Find_Neighbour(node, Optimal_path)
End Procedure

Procedure Req_REQ_discovery_phase(Source, Destination)
  If (route_table_seqno < req_src_seqno) then
     route_table_seqno = req_src_seqno
     Acknowledged_hops = ∞
     delete_table(Source)
     insert_reversepath(Source)
  else if(route_table_seqno = rq_src_seq_no) and (Acknowledged
_hops > rq_hop_count) then
     update_reversepath(Source)
  end if
  if (Active_Path(i, S) = UP) then
      if (data_shielded(S)) then
        send_information(S)
      end if
    end if
    if (corrected_destination) then
      dest_seq_num + = 1
      if (established = 0) then
        Num_of_established = 0
        established = 1
        send_Res_RREQ(S)
      end if
    else
      update_Res_REQ(D)
      forward_Res_REQ(D)
    end if

If (route_table_seqno < rrq_dest_seqno) then
  route_table_seqno = rrq_dest_seqno
  Acknowledged_hops = ∞
  delete_table(Destination)
  insert_forwardpath(Destination)
else if (route_table_seqno = rrq_dest_seqno) and (Acknowledged
_hops > r_rq_hopcount) then
  update_ forward _path(S)
     merge(Min_Cost_Source_node,destination, destination)
     min_cost(destination) :=0
         Optimal_path : = shortest_Path(node, destination)
         Channel :=Find_Neighbour(node, Optimal_path)
End if
if (Active_Path (i, Destination) = UP) then
  if (information_buffered(Destination)) then
    information_send (Destination)
  end if
end if
if (i! = Source) then
  update_Res_REQ(Source)
  forward_Res_REQ(Source)
         Optimal_path : = shortest_Path(node, destination)
         Channel :=Find_Neighbour(node, Optimal_path)
end if

Initialize_packet(Destination,Source)
If (information_received = 1) then
  information_received = 0
  start_waiting_timer_val()
else If (NumofCONFIRM < threshold) then
  Num_of_validate + = 1
  information_received = 1
  send_Res_RREQ(S)
  start_waitingtimer()
end if
If (packet_type = Information and destination) then
  data_received = 1
  Num_of_Established = 0
  Established = 0;
         Optimal_active_path : = shortest_Path(node, destination)
         Channel := Find_Neighbour (node, Optimal_path)
End if
End Procedure
```

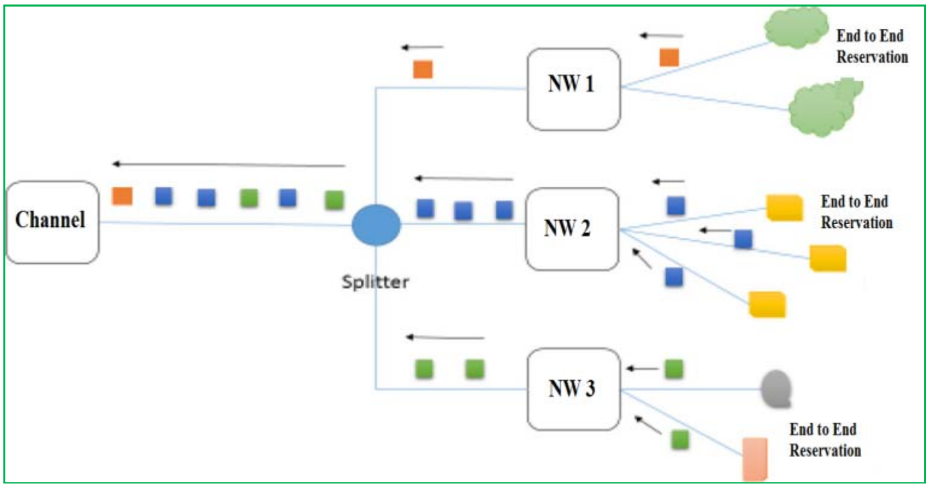


Fig. 2 Data Transmission in Upstream Mode

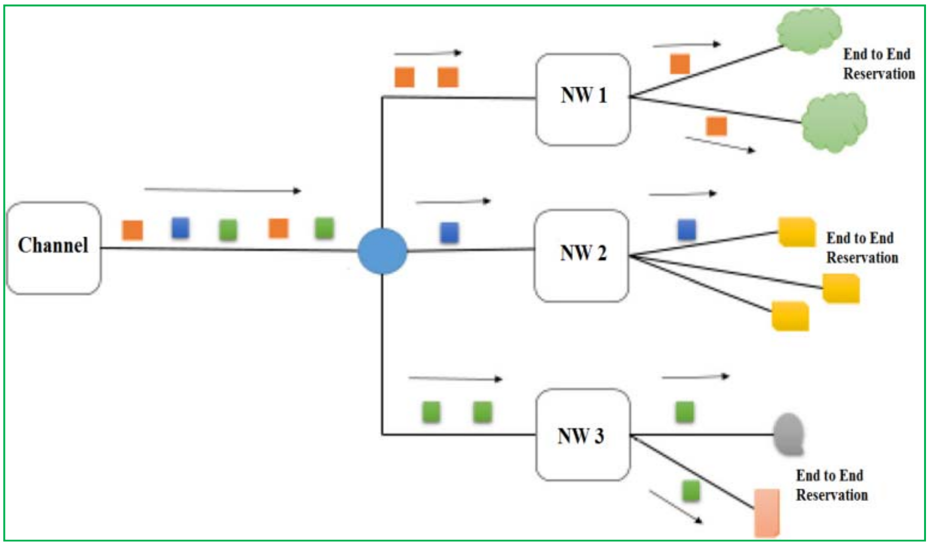


Fig. 3 Data Transmission in Downstream Mode

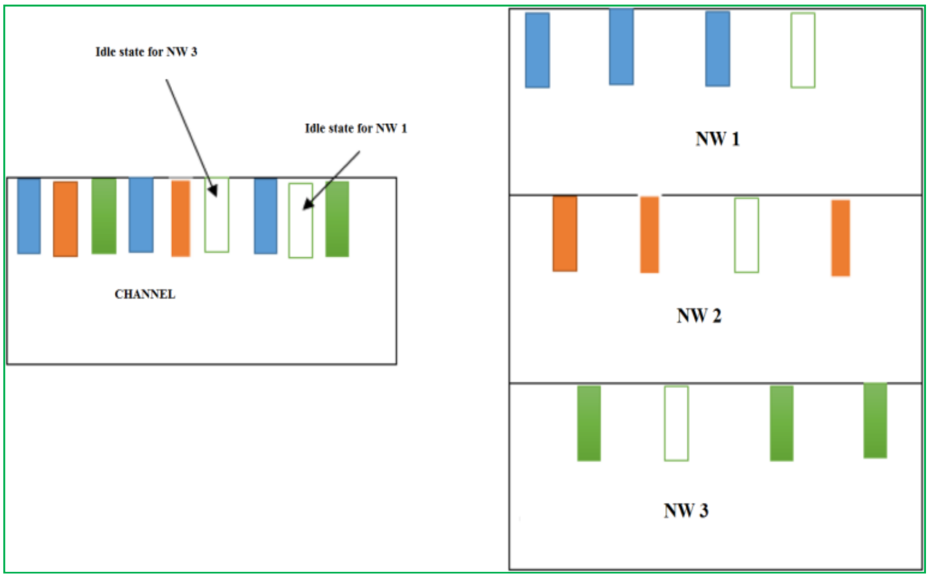


Fig. 4 Static Data Transmission using Bandwidth Allocation

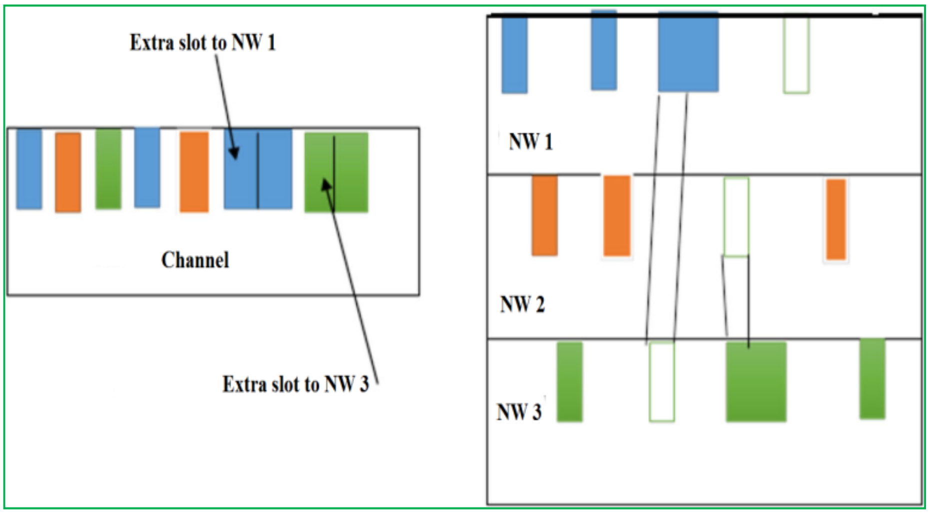


Fig. 5 Dynamic Data Transmission using Bandwidth Allocation

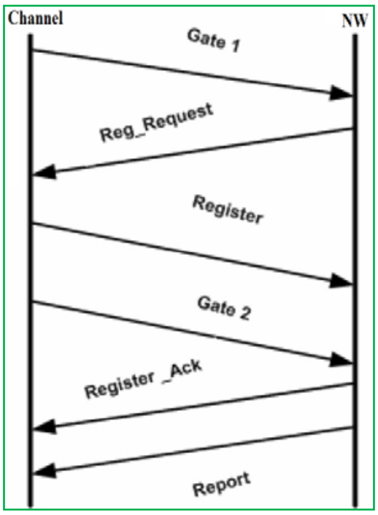


Fig. 6 Register Request format

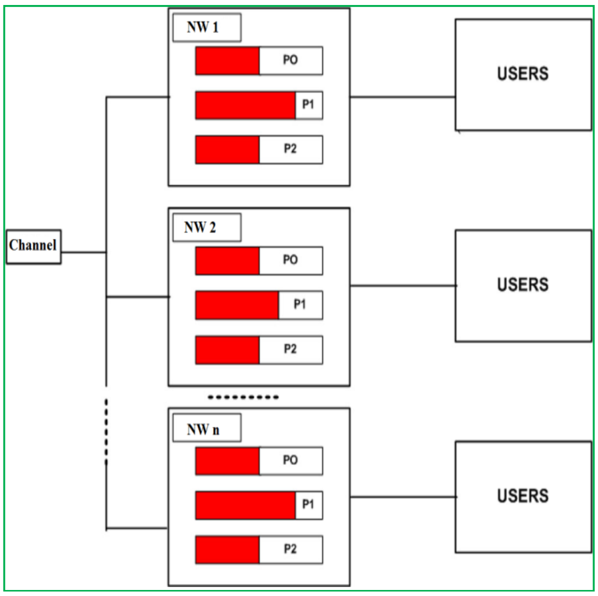


Fig. 7 Scheduling Process

## IV. Bandwidth and Delay Aware Routing Protocol

### A. Network Model

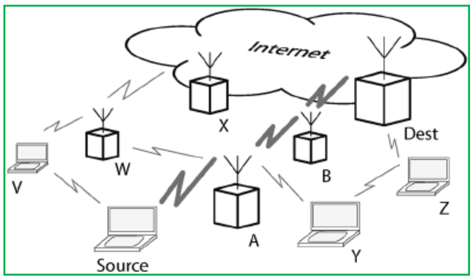


Fig. 8 Network Model

Data_Flow_Matrix can be calculated as

$$DFM_{n\,x\,n+1} = \begin{bmatrix} DT_{10} & \cdots & DT_{1n} \\ \vdots & DT_{ij} & \vdots \\ DT_{n0} & \cdots & DT_{nn} \end{bmatrix} \quad (1)$$

$DT_{ij}$ Denotes the total amount of data transmission from the node i to node j. The network model is illustrated in Fig. 8.

The Main node computes a sequence of queuing model based on the Data_Flow_Matrix$DFM_{n\,x\,n+1}$.

"x" is feasible distance to the core of D ($f\_d\ _{D}^{x}$) is a non increasing function over time that can only be reset by a change of core or by a new sequence number. Feasible distances are used to select a feasible set of next hops.

$$f\_d\ _{D}^{x} = \min\{f\_d\ _{D}^{A}, f\_d\ _{D}^{B}\} \quad (2)$$

The sequence number stored at node x for the core of destination D ($c\_d\ _{D}^{x}$) is a strictly increasing function overtime that can only be reset by a change of core

$$c\_d\ _{D}^{x} = \max\{c\_d\ _{D}^{A}, c\_d\ _{D}^{B}\} \quad (3)$$

A node transmits MAs to inform other nodes about updates in its routing state. These updates can be originated by such time period occurrences as a transform in the group association status (a node joining or leaving a multicast group) that modify the value of $m\_m\ \frac{x}{D}$, or the generation of a new sequence number in the case of the core; or by an external event such as the reception of a neighbor B. Therefore, whenever the core of a destination generates a new MA with a superior sequence quantity, the concluding is distributed beside the enclave advertising the new sequence number and establishing next hop pointers toward the core. The mesh composed of these next hop pointers from a source to the core is called the routing mesh of that source.

The priority function $priority_{xy}$ of $link_{xy}$ as

$$priority_{xy} = \frac{DT_{xy} + DT_{yx}}{|DT_{xy} - DT_{yx}|} \tag{4}$$

A Queue Link Q_L is defined to trace n+1 pairs of the links from the source to the destination links in the network.

$Q\_L_1, Q\_L_2, Q\_L_3, \ldots, Q\_L_q, \ldots, Q\_L_n$ can be combined into a sequence queue as

$$\begin{pmatrix} Q_{L_1} \\ Q_{L_2} \\ Q_{L_3} \\ \vdots \\ Q_{L_q} \\ Q_{L_{q+1}} \\ \vdots \\ Q_{L_n} \end{pmatrix} \tag{5}$$

The queuing scheduling segment establishes the suitable broadcast instructs which stores in a queuing succession. This queuing succession is used in the complex time-slot task segment to allocate appropriate time-slots for every broadcast. In the complex time-slot task segment, there are two situations happened, collision-free and collision detection.

In the collision-free situation, the complex time-slot task segment allocates appropriate time-slots to every $broadcast_{xy}$ according to the queue sequence order. $Q\_L_q$ routes before $Q\_L_{q+1}$ in queue sequence. Each $Q\_L_q$ begins to route at time slot 2k, and $q \leq k \leq n$.

A group of same type of packet distribution $P_{D_{xy}} = \{P_{D_{xy_0}}, P_{D_{xy_1}}, P_{D_{xy_2}}, \ldots\ldots\ldots, P_{D_{xy_s}}, \ldots\ldots\ldots., P_{D_{xy_p}}\}$ is usedto storep+1 packet type distribution from $node_x$ broadcasting to node y, where $P_{D_{xy}}$ s denotes the $s^{th}$ broadcast packet type form x to y and $0 \leq s \leq p$.

A time-slot $W_{S_{xy}}$, which is defined as the x's wake up time-slot between $link_{xy}$. A set of time-slot offset $S_{O_{xy}} = \{S_{O_{xy_0}}, S_{O_{xy_1}}, S_{O_{xy_2}}, \ldots\ldots\ldots, S_{O_{xy_s}}, \ldots\ldots\ldots., S_{O_{xy_p}}\}$ is definedto store q+1 time-slot equalizes from $node_x$ broadcasting to node y, and $0 \leq t \leq q$. The $S_{O_{xy}}$ t denotes the $t^{th}$ time-slot offset broadcast from x to y. $S_{O_{xy}}$ is gathered form $P_{D_{xy}}$ and $P_{D_{yx}}$, which is used to expect the engaged $\text{time-slot}_{offset}$ by $link_{xy}$. For using advance time-slot leasing, master declares every slave $W_{S_{xy}}$ and $S_{O_{xy}}$. Slaves wake up at allocated period $W_{S_{xy}}$ and observe the group of time-slot offset $S_{O_{xy}}$ to broadcast data.

$$S_{O_{yx_t}} = S_{O_{xy_t}} + P_{D_{xy_s}} \tag{6}$$

$$S_{O_{xy_{t+1}}} = S_{O_{yx_t}} + P_{D_{yx_s}} \tag{7}$$

$$W_{S_{yx}} = W_{S_{xy}} + P_{D_{xy_1}} \tag{8}$$

for the period of generating $S_{O_{xy}}$, if master runs out of the $P_{D_{xy}}$ set, $P_{D_{xy_{p+t}}}$ sets to 1 for Acknowledgment reacting.

In the collision detection situation, some occupied time-slots have been allocated over to broadcast probably. Before broadcast, master should notice this situation first. A group of used time-slot U_S = {$U\_S_0$, $U\_S_1$, ..., $U\_S_k$} is defined to store k + 1 used time-slots. Master sums $W_{S_{xy}} + S_{O_{xy}}$ into U_S after allocated time-slots for x. If master assigns time-slots including in U_S to slaves, time-slot collision will occur in the network. Master creates the following formula to verifythe collision position.

$$(W_{S_{xy}} + S_{O_{xy}}) \cap U_S \neq \{\emptyset\} \tag{9}$$

Algorithm

INPUT: $L_i$; $\{m_x\}$
OUTPUT: Q_L (query list); $S_i$ (demandpossibility)
**for** everylatest query, $Q\_L_i(d_j)$ **do**
Use $m_x$ to determine $S_i^*$;
$S_i = 1 - (1 - S_i)(1 - S_i^*)$;
$Q\_L = Q\_L \cup d_j$;
Forward($S_i$);
**end for**
**for** each server transmit time, $L_i$**do**
**if** Q_L = ∅**then**
Ensure the key list, $I_i$;
Download the requireddata_item($S_i$);
**end if**
**if** Q _L = ∅**then**
**if** auncertainty has missed two servertransmit**then**
$S_i = 1$;
**end if**
Forward($S_i$);
**end if**
**end for**
Function transmit($S_i$)
**if** random<$S_i$ **then**
Forward a demand;
Q_L = ∅; $S_i = 0$;
**End if**

Fig. 9 demonstrates the scheduling process, Fig. 10 illustrates the broadcast traffic and send request and Fig. 11 demonstrates the Block Slot.

The reservation path might break during the real-time transmission if the network topology changes. Such changes might occur if nodes switch off or fail or if the channel conditions change. Evidently, the path breaks must be repaired initially, and then only the real-time transmission will continue the process. To initiate a path repair, the node preceding the "hole" in the path must notice the broken link.

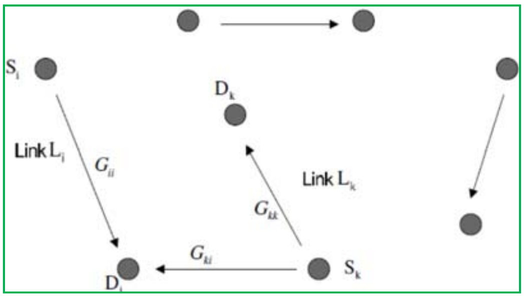


Fig. 9 Scheduling Process

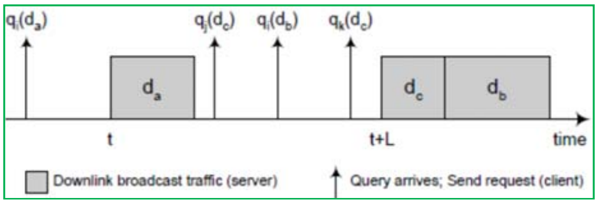


Fig. 10 Broadcast Traffic and send request

Fig. 12 gives an example: Node B switches off and node A detects its link failure to node B. The subsequent path repair is done in two steps: Route repair and reservation repair. First, the MAC layer indicates the link break to the network layer. As in standard DCF, this event triggers the routing protocol to update the route. After the routing protocol has repaired the route between source and destination, the protocol repairs the reservation at the MAC layer.

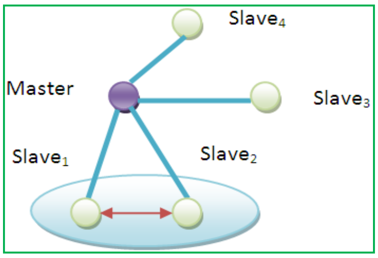


Fig. 11 Block slot

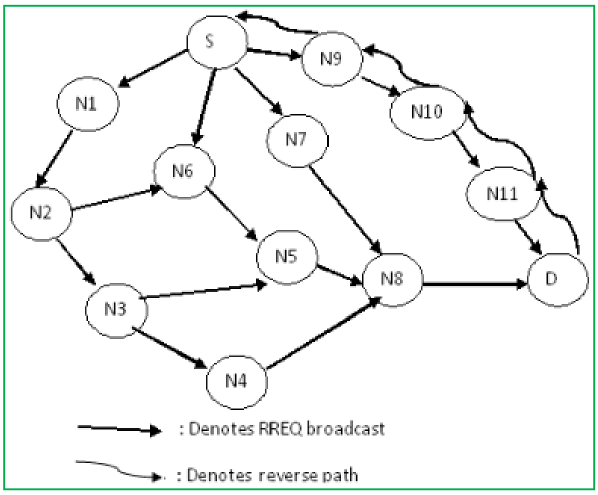


Fig. 12 Link Failure Example

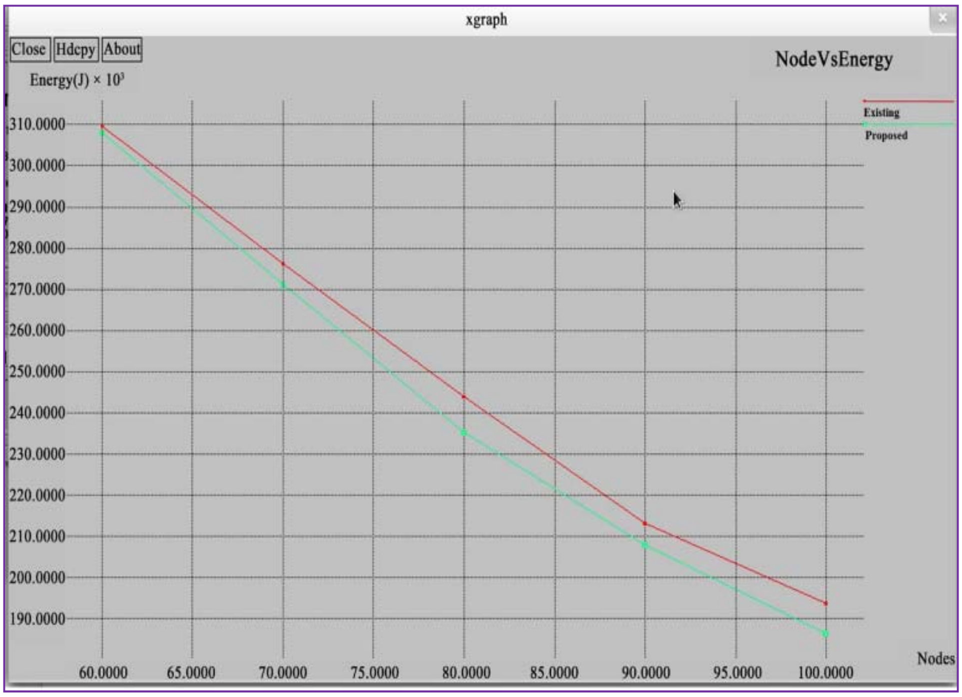


Fig. 13 Energy Consumed

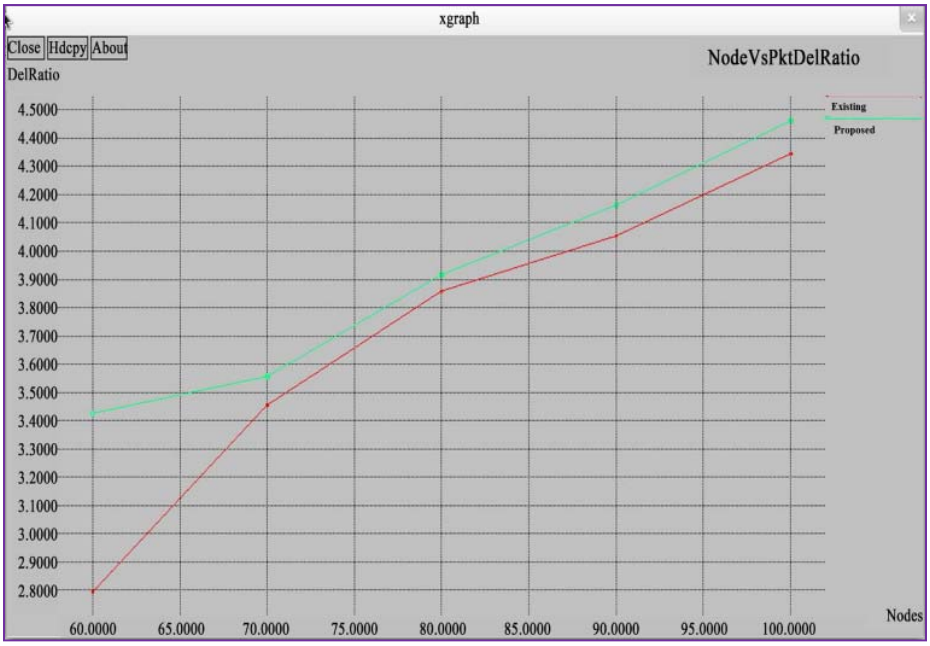


Fig. 14 Packet Delivery Ratio

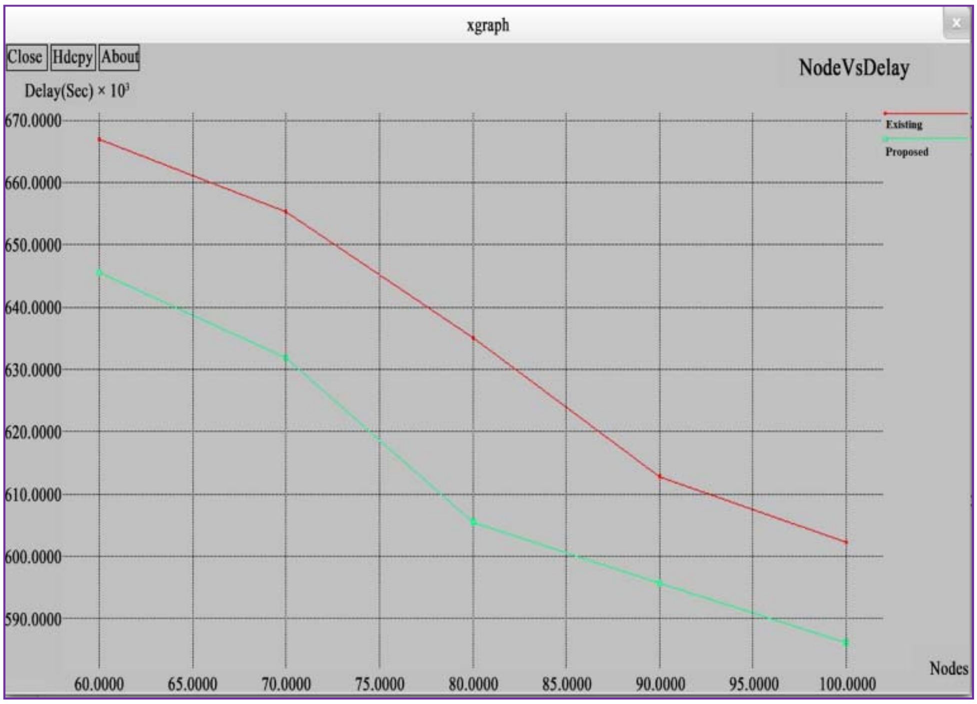


Fig. 15 Delay



## V. Performance Evaluation

This paper presents a Bandwidth and Delay Aware Routing Protocol with Scheduling Algorithm for link failure. Both theoretical and simulation results are given to exhibit the efficiency of the proposed scheme. Fig. 13 demonstrates the Energy Consumed by the proposed method, Fig. 14 illustrates the Packet Delivery Ratio for the proposed method and Fig. 15 denotes the Delay for the presented method.

## VI. Conclusion

This paper presents a link metric based routing scheme for link failure. In multicast routing if any node fails to receive three consecutive acknowledgements from the neighbor then move that node from the neighborhood list and finding the next best-hop to reach their appropriate destination. Both theoretical and simulation results are given to demonstrate the effectiveness of the presented scheme.

## REFERENCES


[1] E. Carlson, C. Prehofer, C. Bettstetter, H. Karl, and A. Wolisz, "A Distributed End-to-End Reservation Protocol for IEEE 802.11-Based Wireless Mesh Networks," *IEEE J. Selected Areas in Comm.,vol. 24, no. 11, pp. 2018-2027, Nov. 2006*.

[2] R. Menchaca-Mendez and J.J. Garcia-Luna-Aceves, "An Interest-Driven Approach to Integrated Unicast and Multicast Routing in MANETs," *Proc. IEEE 16th IEEE Int'l Conf. Network Protocols (ICNP '08), pp. 248-257, Oct. 2008.*

[3] Harold Robinson, Y., & Rajaram, M. (2015). "Trustworthy link failure recovery algorithm for highly dynamic mobile adhoc networks", World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, vol.9, no.2, 233–236.

[4] J. Yuan, Z. Li, W. Yu, and B. Li, "A Cross-Layer Optimization Framework forMultihop Multicast in Wireless Mesh Networks," *IEEE J. Selected Areas in Comm., vol. 24, no. 11, pp. 2092-2103, Nov. 2006.*

[5] Y. Wu, P.A. Chou, Q. Zhang, K. Jain, W. Zhu, and S.-Y. Kung, "Network Planning in Wireless Ad Hoc Networks: A Cross-Layer Approach," *IEEE J. Selected Areas in Comm., vol. 23, no. 1, pp. 136-150, Jan. 2005.*

[6] Harold Robinson, Y., & Rajaram, M. (2016), "A memory aided broadcast mechanism with fuzzy classification on a device-to-device mobile Ad Hoc network", Wireless Personal Communications, 1–23, doi:10.1007/s11277-016-3213-0.

[7] E. Setton, T. Yoo, X. Zhu, A. Goldsmith, and B. Girod, "Crosslayer Design of Ad Hoc Networks for Real-Time Video Streaming," *IEEE Wireless Comm., vol. 12, no. 4, pp. 59-65, Aug. 2005.*

[8] C.E. Perkins and E.M. Royer, "Ad-Hoc On-Demand Distance Vector Routing," *Proc. Second IEEE Workshop Mobile Computing Systems and Apps. (WMCSA '99), pp. 90-100, Feb. 1999.*

[9] Harold Robinson, Y., & Rajaram, M. (2015), "Energy-aware multipath routing scheme based on particle swarm optimization in mobile ad hoc networks", The Scientific World Journal, 1–9. doi:10.1155/2015/284276.

[10] T. Melodia, M.C. Vuran, and D. Pompili, "The State of the Art in Cross-Layer Design for Wireless Sensor Networks," *Proc. EURONGI Workshops Wireless and Mobility, pp. 78-92, 2006.*

[11] C.R. Lin and M. Gerla, "Asynchronous Multimedia Multihop Wireless Networks," *Proc. IEEE INFOCOM, vol. 1, pp. 118-125, Apr. 1997.*

[12] Harold Robinson, Y., & Rajaram, M. (2015), "Establishing pairwise keys using key Predistribution schemes for sensor networks", World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering, 9(2), 608–612.

[13] S. Biswas, R. Morris, Opportunistic routing in multi-hop wireless networks, ACM SIGCOMM Computer Communication Review 34 (1), (2004) 69–74.

[14] E. Rozner, J. Seshadri, Y. Mehta, L. Qiu, Soar: Simple opportunistic adaptive routing protocol for wireless mesh networks, MobileComputing, IEEE Transactions on 8 (12) (2009) 1622–1635.

[15] Balaji, S., Harold Robinson, Y. and Rajaram, M. (2016) SCSBE: Secured Cluster and Sleep Based Energy-Efficient Sensory Data Collection with Mobile Sinks. Circuits and Systems, 7, 1992-2001.http://dx.doi.org/10.4236/cs.2016.78173

[16] H. Dubois-Ferrière, M. Grossglauser, M. Vetterli, Valuable detours: Least-cost anypath routing, Networking, IEEE/ACM Transactions on 19 (2) (2011) 333–346.

[17] Z. Zhong, J. Wang, S. Nelakuditi, G.-H. Lu, On selection of candidates for opportunistic anypath forwarding, ACM SIGMOBILE Mobile Computing and Communications Review 10 (4) (2006) 1–2.

[18] Robinson, Y.H., Balaji, S. and Rajaram, M. (2016) "ECBK: Enhanced Cluster Based Key Management Scheme for Achieving Quality of Service", Circuits and Systems, 7, 2014-2024. http://dx.doi.org/10.4236/cs.2016.78175.

[19] Y. Li, W. Chen, Z.-L. Zhang, Optimal forwarder list selection in opportunistic routing, in: Mobile Adhoc and Sensor Systems, 2009. MASS'09. IEEE 6th International Conference on, IEEE, 2009, pp. 670–675.

[20] H. Füßler, J. Widmer, M. Käsemann, M. Mauve, H. Hartenstein, Contention-based forwarding for mobile ad hoc networks, Ad Hoc Networks 1 (4) (2003) 351–369.

[21] Harold Robinson, Y., Rajaram, M., Golden Julie, E. and Balaji, S. (2016) Dominating Set Algorithm and Trust Evaluation Scheme for Secured Cluster Formation and Data Transferring. World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 10, 388-393.

[22] S. Yang, F. Zhong, C. K. Yeo, B. S. Lee, J. Boleng, Position based opportunistic routing for robust data delivery in MANETs, in: Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE, IEEE, 2009, pp. 1–6.

[23] A. Darehshoorzadeh, L. Cerda-Alabern, Distance progress based opportunistic routing for wireless mesh networks, in: Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, IEEE, 2012, pp. 179–184.

[24] Harold Robinson, Y., Rajaram, M., Golden Julie, E. and Balaji, S. (2016), "Tree Based Data Fusion Clustering Routing Algorithm for Illimitable Network Administration in Wireless Sensor Network", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:10, No:6, pp. 1123 – 1130.

[25] S. Gupta, S. K. Dhurandher, I. Woungang, A. Kumar, M. S. Obaidat, Trust-based security protocol against blackhole attacks in opportunistic networks, in: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013, pp. 724–729.

[26] M. M. Mahmoud, X. Lin, X. Shen, et al., Secure and reliable routingprotocols for heterogeneous multihop wireless networks, Parallel andDistributed Systems, IEEE Transactions on 26(4), (2015) 1140–1153.

[27] Harold Robinson, Y., Rajaram, M., Golden Julie, E. and Balaji, S. (2016), "TBOR: Tree Based Opportunistic Routing for Mobile Ad Hoc Networks", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:10, No:6, pp. 1115 – 1122.

[28] J.-H. Cho, A. Swami, R. Chen, A survey on trust management for mobile ad hoc networks, Communications Surveys & Tutorials, IEEE 13 (4) (2011) 562–583.

[29] H. Yu, Z. Shen, C. Miao, C. Leung, D. Niyato, A survey of trust and reputation management systems in wireless communications, Proceedings of the IEEE 98 (10) (2010) 1755–1772.

[30] Ramalakshmi, S., & Robinson, Y. H. (2014). "ATMPH: Attaining optimal throughput capacity of MANET with power control in heterogeneous network", Programmable Device Circuits and Systems, 6(4), 111–115.

[31] A. Ayyasamy and K. Venkatachalapathy, "Context aware adaptive service based dynamic channel allocation approach for providing an optimal QoS over MANET", *International journal of engineering and technology (IJET)*, vol. 6, no. 3, pp. 1465-1479, jun-jul 2014. ISSN: 0975-4024.

[32] G. Han, J. Jiang, L. Shu, J. Niu, H.-C. Chao, Management and applications of trust in wireless sensor networks: A survey, Journal of Computer and System Sciences 80 (3) (2014) 602–617.

[33] Robinson, Y. H., &Rajeswari, S. R. (2011). "Energy-based dynamic encryption for wireless sensor networks. Wireless Communication", vol.3, no.9, pp. 661–663.

[34] S. Buchegger, J.-Y. Le Boudec, Performance analysis of the confidant protocol, in: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, ACM, 2002, pp. 226–236.

[35] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: Advanced Communications and Multimedia Security, Springer, 2002, pp. 107–121.

[36] Harold Robinson, Y., & Rajaram, M. (2014). "A novel approach to allocate channels dynamically in wireless mesh networks", World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 8, no.10, pp. 1865–1868.

[37] T. Ghosh, N. Pissinou, K. Makki, Towards designing a trusted routing solution in mobile ad hoc networks, Mobile Networks and Applications 10 (6) (2005) 985–995.

[38] A. Boukerche, Y. Ren, R. W. N. Pazzi, An adaptive computational trust model for mobile ad hoc networks, in: Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, ACM, 2009, pp. 191–195.

[39] Golden Julie, E., Tamil Selvi, S., & Harold Robinson, Y. (2014). "Opportunistic routing with secure coded wireless multicast using MAS approach",World Academy of Science, Engineering and Technology,

International Journal of Computer, Electrical, Automation, Control and Information Engineering, vol. 8, no.7, pp. 1247–1250.
[40] N. Li, S. K. Das, A trust-based framework for data forwarding in opportunistic networks, Ad Hoc Networks 11 (4) (2013) 1497–1509.
[41] R. Chen, F. Bao, M. Chang, J.-H. Cho, Dynamic trust management for delay tolerant networks and its application to secure routing, Parallel and Distributed Systems, IEEE Transactions on 25 (5) (2014) 1200– 1210.
[42] Golden Julie, E., Tamil Selvi, S., & Harold Robinson, Y. (2016). “Performance Analysis of Energy Efficient Virtual Back Bone Path Based Cluster Routing Protocol for WSN”, Wireless Personal Communications, Springer, 1–19, DOI 10.1007/s11277-016-3520-5.
[43] S. Gupta, S. K. Dhurandher, I. Woungang, A. Kumar, M. S. Obaidat,Trust-based security protocol against blackhole attacks in opportunisticnetworks, in: 2013 IEEE 9th International Conference on Wireless andMobile Computing, Networking and Communications (WiMob), IEEE,2013, pp. 724–729.
[44] S. Biswas, R. Morris, Exor: opportunistic multi-hop routing for wireless networks, in: ACM SIGCOMM Computer Communication Review, Vol. 35, ACM, 2005, pp. 133–144.
[45] Harold Robinson, Y., Rajaram, M., Golden Julie, E. and Balaji, S. (2016), “Detection of Black Holes in MANET Using Collaborative Watchdog with Fuzzy Logic”, World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:10, No:3, pp. 575 – 581.
[46] Z. Zhao, B. Mosler, T. Braun, Performance evaluation of opportunistic routing protocols: A framework-based approach using omnet++, in: Proceedings of the 7th Latin American Networking Conference, ACM, 2012, pp. 28–35.
[47] I. F. Akyildiz, W. Su, Y. Ankara subramaniam, E. Cayirci, Wirelesssensornetworks: a survey, Computer networks 38 (4) (2002) 393–422.
[48] Golden Julie, E., & Tamil Selvi, S. (2016),“Development of energy efficient clustering protocol in wireless sensor network using neuro-fuzzy approach” The Scientific World Journal, Article ID 5063261, 1–8.
[49] M. P. Đurišic, Z. Tafa, G. Dimic, V. Milutinovic, A survey of military applications of wireless sensor networks, in: Embedded Computing (MECO), 2012 Mediterranean Conference on, IEEE, 2012, pp. 196–199.
[50] Ayyasamy, A., and K. Venkatachalapathy. "Context aware adaptive fuzzy based QoS routing scheme for streaming services over MANETs." Wireless Networks 21.2 (2015): 421-430.
[51] E. Golden Julie, E. Sahaya Rose Vigita, S. Tamil Selvi(2014), “Distributed Self-Healing Protocol for Unattended Wireless Sensor Network”, World Academy of Science, Engineering and Technology, International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:10, pp. 1680 – 1683.
[52] I. F. Akyildiz, D. Pompili, T. Melodia, Underwater acoustic sensor networks: research challenges, Ad hoc networks 3 (3) (2005) 257–279.
[53] L. F. M. Vieira, Performance and trade-offs of opportunistic routing in underwater networks, in: Wireless Communications and Networking Conference (WCNC), 2012 IEEE, IEEE, 2012, pp. 2911–2915.
[54] S. Balaji, M. Rajaram (2014), “EUDIS-An Encryption Scheme for User-Data Security in Public Networks”, World Academy of Science, Engineering and Technology, International Journal of Computer, Information, Systems and Control Engineering Vol:8 No:11, pp. 1825 – 1830.
[55] J.K. Hart, K. Martinez, Environmental sensor networks: A revolution in the earth system science, Earth-Science Reviews 78 (3) (2006) 177–191.
[56] L. Atzori, A. Iera, G. Morabito, The internet of things: A survey, Computer networks 54 (15) (2010) 2787–2805.
[57] G.ArunSamPaul Thomas, R.Karthik Ganesh, A.Kandasamy, S.Balaji, Y.Harold Robinson, (2011) “An Advanced Controlled-Flooding Routing with Group Organization for Delay Tolerant Networks using A-SMART”, Emerging Trends in Electrical and Computer Technology (ICETECT), 978-1-4244-7926-9/11, IEEE.
[58] Ayyasamy, A., and K. Venkatachalapathy. "Increased Throughput for Load based Channel Aware Routing in MANETs with Reusable Paths." International Journal of Computer Applications 40.2 (2012): 20-23.
[59] A. Darehshoorzadeh, R. De Grande, A. Boukerche, Towards a comprehensive model for performance analysis of opportunistic routing in wireless mesh networks, Transactions on Vehicular Technology PP (99) (2015) 1–15.
[60] S. Balaji, M. Rajaram (2016), “SIPTAN: Securing Inimitable and Plundering Track for Ad Hoc Network”, Wireless Personal Communications, Springer, 1-21, DOI 10.1007/s11277-016-3187-y.

**Dr. Y. Harold Robinson** is currently working as an Associate Professor and Head, Department of CSE in SCAD College of engineering and Technology, Tirunelveli. He finished ME degree in Anna University, Chennai. He completed Ph.D. in Anna University Chennai. His research interests are Wireless Networks Mobile Computing, Wireless Sensor Networks. He has published several Research papers in International Journals. He has presented many papers in National and International conferences in Network security, Mobile Computing and Cloud Computing.

**Mrs. E. Golden Julie** received her B.E degree in Computer Science and Engg in 2005 from Anna University Chennai and ME degree in Computer Science and Engineering in 2008 from Anna University Chennai. Currently she is Pursuing her Ph.D. from Anna University Chennai. Presently she is working as assistant professor in Regional centre Anna University, Tirunelveli, India She has published many research papers in various fields. Her research area includes Wireless Sensor Adhoc Networks and Image Processing. She is a member of ISTE.

**Dr. S. Balaji,** completed his Ph.D in Anna University, Chennai and currently working as an Associate Professor in Dept of CSE at Francis Xavier Engineering College, Tirunelveli. His research interests are Wireless Networks Mobile Computing, Network Security with apps, Wireless Sensor Networks, Cloud Computing. He has presented many papers in National and International conferences in network security, Mobile Computing, network security, and Cloud Computing. He has organized and conducted various national and international conferences, International Seminars and National Workshops. And also his methodology of teaching about TCP & UDP is hosted on Wipro Mission 10x portal. He is a life time member of ISTE.