International Journal of Electrical and Computer Engineering (IJECE)
Vol. 6, No. 5, October 2016, pp. 2322~2330
ISSN: 2088-8708, DOI: 10.11591/ijece.v6i5.11624

Node Cooperation to Avoid Early Congestion Detection Based on Cross-Layer for Wireless Ad Hoc Networks

Abdalrazak Tareq Rahem, Mahamod Ismail, Nor Fadzilah Abdullah, Mohammed Balfaqih
Department of Electrical, Electronics and Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia (UKM), Malaysia

Article Info

Article history:

Received May 16, 2016
Revised Jul 12, 2016
Accepted Jul 29, 2016

Keyword:

Ad hoc wireless
Alternative route
Congestion
Network topology
Routing protocol

ABSTRACT

The resent application of wireless ad hoc networks (WANET) demands a high and reliable data load. The simultaneous transfer of large amounts of data different nearby sources to nearby destinations in a massive network under these circumstances results in the possibility of network congestion. Congestion is an extremely unwanted condition because it creates extra overhead to the already deeply loaded environment, which ultimately leads to resource exhaustion, and can lead to packet drops and retransmission at either the MAC or upper layers. We present a lightweight congestion control and early avoidance congestion control scheme, which can effective control congestion while keeping overhead to a minimum. This scheme is based on the Cross-layer between the MAC and network layers lead to early detection of congestion. With the help of node cooperation the sender node is triggered to find an alternative route based on TMT. This mechanism controls the network resources rather than the data traffic. Detailed performance results show enhancement in the throughput and packet delivery ratio, as well as a reduction in packet drop. Generally, network performance increases.

Corresponding Author:

Abdalrazak Tareq Rahem,
Department of Electrical, Electronics and Systems Engineering,
Faculty of Engineering and Built Environment,
National University of Malaysia (UKM)
Email: abdtareq1@siswa.ukm.edu.my

1. INTRODUCTION

A wireless ad hoc network (WANET) refers to a particular wireless network. Particular networks (ad hoc) aim to obtain specific characteristics, such as dynamic, independent, self-configuring, decentralized, and infrastructure-less. The routing protocol plays an essential role in improving the performance of wireless networks [1]. The main goal of any routing protocol is to determine dynamically the correct route between a source node and a destination node [2]. In the case of control messages, forwarding of large amounts of data from one node to another without the cooperation of each node leads to congestion. Congestion occurs in any midway from a source node to a destination node if massive data packets travel. Consequently, high packet loss and long delay are encountered. This situation leads to the degradation of network performance. Network congestion can be addressed through either traffic control or resource control. However, the situation worsens if resources are increased without considering the congestion type, traffic pattern, and network topology. As shown in Figure 1, congestion occurs in Route 1: 20→ 21→ 22→ 23→ 24→ 25→ 26→ 27→ 28→ 29. Because most routing protocols choose that path without considering the network topology [3]. AODV, DSDV, OLSR, and DSR have no congestion control algorithms. Typically, reducing packet loss involves congestion control. We have used detection methods to preempt congestion. Our proposed routing protocol considers and selects the optimal and most efficient route by reading the network

topology as well as avoids congestion before it occurs. The proposed mechanism was analyzed using a mathematical model and evaluated using a NS-3 simulator.

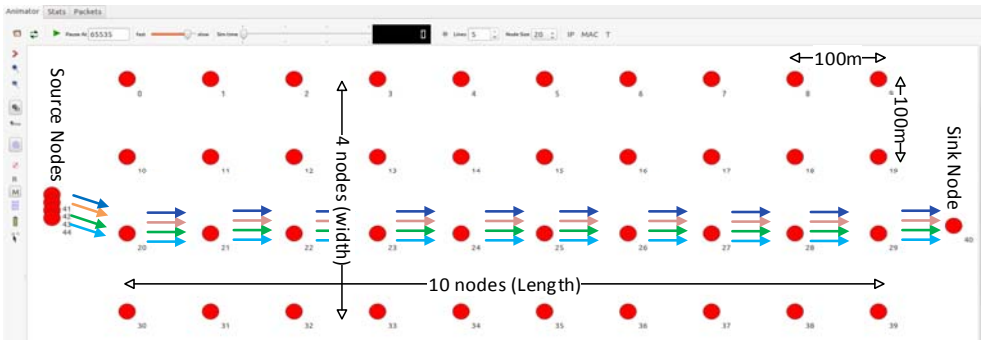

Figure 1. Congestion route

2. RELATED STUDIES

High data loads can easily lead to congestion because of the limited nodes resources available in the wireless ad hoc network. Congestion is a highly undesirable situation because it creates additional overhead to the already heavily loaded environment, which eventually leads to resource depletion. To reduce the delay and buffer overflow produced by network congestion and to enhance performance, congestion must be avoided before it occurs. Congestion detection in wireless ad hoc networks has been studied [4]-[8]. An earlier study [9] introduced a novel cross-layer hybrid metric based on AODV protocol for ad hoc networks based on information obtained from wireless channel conditions in the physical layer, link quality and congestion in MAC layer, and minimum hops in network layer. After checking the route for the existence of congestion in any intermediate node, the new route is initialized. Golnaz Karbaschi [10] addressed a new link-quality and congestion-aware metric for multi-hop wireless routing. The author found that cross layer between routing protocol and MAC layer is helpful in enhancing routing in terms of end-to-end delay and throughput in the judgment of the minimum-hop count metric. Moreover, cross-layer routing is intended to play an essential role in improving the performance of wireless networks. Congestion detection in sensor networks has been studied [6],[7],[11],[12].

A prior study [13] presented a topology-aware resource adaptation (TARA), which is an adaptation strategy for alleviating congestion. The main idea of TARA is the capacity analysis model, which can be used to predict the capacity of different topologies. This model is formulated using a graph-coloring problem. TARA is advantageous because it is distributed, energy efficient, and topology aware. Related works have discussed congestion based on the use of the size of queue to detect the congestion. Situations exist wherein the actual queue size reaches full buffer size, even when the average queue is below the maximum threshold (MAXth). In some cases, packets will be dropped because of overflow [14],[15].

The alternative path selection scheme (DAlPaS), which is an effective scheme that controls congestion while keeping overhead to a minimum, has been represented in the WSN [16]. The operation of this scheme is based on the control of resources instead of the control of the sending rate at the source. Congestion can lead to packet drops and retransmission either at the MAC or upper layers, which are events that exhaust the already limited power of WSNs. Node power exhaustion can result in routing holes in the network, which can render the network unable to accomplish its objective. Several research works on controlling congestion in WSNs have been implemented [16],[17]. The performance of DAlPaS has been evaluated against comparable schemes and showed promising results.

3. PROPOSED SCHEME

This section illustrates the mathematical model including our proposed scheme through two parts. The first part explains how to preemptively detect congestion with the help of MAC and network layer information. This is represented as Step I and Step II in the Figure 2. The second part shows how to discover alternative routes to the destination with the help of the TMT. This is represented as Step III. First, it predicts congestion before it occurs, and combines two different methods to discover the congestion. Two parameters, namely, failure and queue size, from the MAC and network layers, respectively are used. Second, it is

represented by finding the new path based on the topology of the network. The scheme is an organized as in the following steps:

Step I: Checking the network layer to discover the congestion before it occurs (early congestion detection), and sending a warning message only to neighbor's nodes to cooperate and avoid congestion.

Step II: Checking the MAC layer parameters to activate an alternative route finder after receiving such warning message.

Step III: Finding a new path based on the TMT.

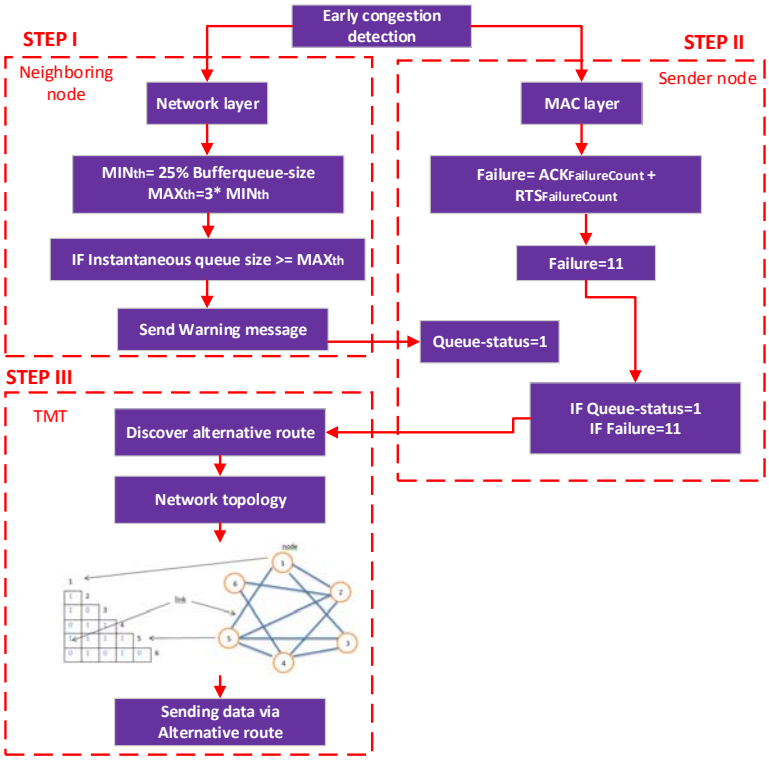

Figure 2. The Proposed Scheme

3.1. Early Congestion Detection

The congestion in wireless ad hoc networks probably occurs in either the MAC or network layers, and there are different ways to detect it. However, the cross two layers in term of checking the parameters are helpful to detect any early congestion before it occurs. To avoid such congestion, it must be predicated first and then, there should be cooperation to find an alternative route. The cross layers are: (a) Network congestion and (b) MAC congestion as following.

Step I: →(a) Network congestion: All nodes have a limited buffer queue size. Therefore, if the received data size is greater than the actual queue size of the node, then, the data will be dropped, which is mainly due to the occurrence of overload congestion. The network layer has parameters to measure the current queue size. Equations 1 and 2 represent the parameters related to network layer to measure such current queue size.

$$Q_{min} = 0.25 \times Buffer_{queue\text{-}size} \quad (1)$$

$$Q_{Threshold} = Q_{max} = 0.75 \times Buffer_{queue\text{-}size} = 3 \times Q_{min} \quad (2)$$

Where Q_{min} denotes to the quarter of actual queue size of node which represents the minimum threshold of the actual queue size. And the $Q_{Threshold}$ denotes to the three quarters of actual queue size that represents the maximum threshold of the actual queue size. $Buffer_{queue\text{-}size}$ represents the actual queue size of node. If the current queue size of the node reaches more or equal $Q_{Threshold}$ then, a warning message is sent to all neighboring nodes This approach is illustrated in STEP I in Figure 2 where it predicts and detects if there is

an imminent congestion crossing with MAC parameters too (STEP II). The queue-status was added to all nodes. By default, queue-status is '0'. For instance, to detect an early congestion of a given link, the instantaneous queue is first checked. Instantaneous queue size refers to the current queue size. If the current queue size is equal or greater than three quarters of the actual queue size, then, a warning message is sent to the neighboring nodes. Every node must cooperate with each other to send this message. If any node receives such warning message, then the queue-status for that particular node will be modified to '1'.

Step II:→(b) MAC congestion: The mobile ad hoc network employs a distributed coordination function (DCF) for a medium access. The DCF is a basic channel access protocol for asynchronous data transmission in the contention period based on a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism. There are two parameters in IEEE 802.11 MAC layer are $ACK_{FailureCount}$ and $RTS_{FailureCount}$. Where, $ACK_{FailureCount}$ denotes the number of Failure to send DATA and obtain ACK, and $RTS_{FailureCount}$ denotes the number of Failure to obtain free media as shown in Figure 3. Retransmission occurs only when an ACK or a CTS frame is not received from the destination node; thus, DATA or RTS frame is not sent.

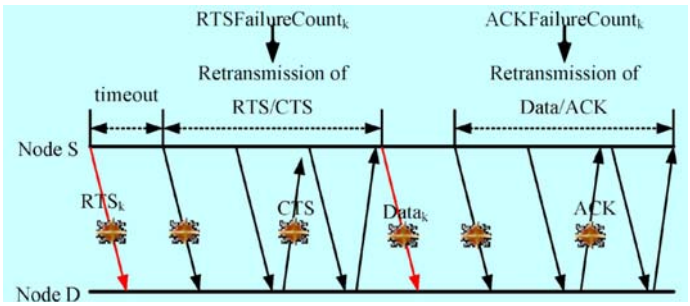

Figure 3. MAC frame retransmission method

Such situation leads to dropping of packets or frames in the network because the data is sent in the RTS/CTS phase to obtain the channel and avoid the hidden/exposed node problem. If the sender does not receive the CTS for a period time, the sender node retransmits an RTS until a CTS and holding channel are obtained. Therefore, the maximum retransmission failures over the node denote the possibilities that the link is possibly and not possibly congestion. Every node uses these two variables to represent the number of retransmissions failure in the MAC layer. The default maximum value of $RTS_{FailureCount}$ is 7 and the default maximum value of $ACK_{FailureCount}$ is 4 as standardization of MAC layer in IEEE 802.11 RTS/CTS [18],[19]. Equation 3 reflects the number of retransmit failure, where $F_{Threshold}$ denotes to the maximum threshold of both DATA and RTS.

$$F_{Threshold} = ACK_{FailureCount} + RTS_{FailureCount} \quad (3)$$

The number of RTS retransmissions refers to the contention level of the link, as well as the estimation of the link quality. If $F_{Threshold}$ occurs '11' times, then either congestion between nodes or some other reasons including interference will occur. Therefore, no guarantee is given that congestion occurs by counting the number of $F_{Threshold}$. Hence, it must be used as an indication of congestion detection with the help from the network layer. In this case, nodes need to cooperate with the queue status in the network layer as previously explained in STEP I (a).This work combined the MAC information with the routing layer protocol to detect this congestion.

To detect such early congestion, Equations 1, and 2 were used to examine the instantaneous queue size and to send warning messages to all neighbor nodes while Equation 3 was used to detect the MAC layer information (Failure). The queue status in the routing table utilizes congestion prediction. As an example, let suppose if a given node checks the queue status condition for the destination node which is'1'. Then, the second step is checking $F_{Threshold}$. If the number of retransmit $F_{Threshold}$ for the MAC layer reaches '11', in this case, the alternative route mechanism must find a new route.

3.2. Alternative Route Determination

Alternative routes should be found to avoid this congestion. Thus the network topology was represented using a Triangular Matrix Table (TMT) to obtain full network topology information [20]. The Figure 4 illustrates an example to show how the TMT is filled from network topology. Here, the triangular

metric dimensions are equal to the number of nodes. Thus, each node inside the network is assigned a number, which may represent the MAC or IP address. The position of the node address is represented on the diagonal of the TMT, as shown in Figure 4.

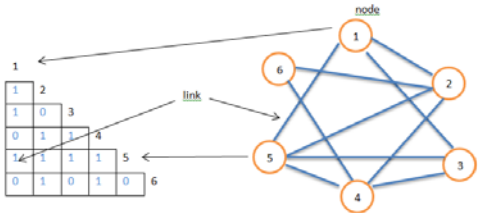

Figure 4. Represent Triangular Matrix Table

Each link between two nodes represents by "1" bit inside TMT. Otherwise, the absence of a link between two nodes will be represented by "0" bit. The position inside the TMT depends on crossing the row node with column node address.

To find the routes from source node to destination, we assumed that the source node is Node 1 and that the destination node is Node 4. Every bit in Column 1 [1, 1, 0, 1, 0] must check. The corresponding connection related to Node is (2, 3, 4, 5, and 6). Because "1" bit in the TMT only represents the links. Therefore, Nodes (2, 3, 5) must check it, if anyone has new link with others. First save (2, 3, 5) in the vector queue. Moreover, the unique function avoids the insertion of any double node number inside the vector queue. Technically, the unique function is the key to ensure loop-free. If the check function does not find the destination node, then the first element from the vector queue checkout, meaning deletion from vector queue, and becomes the next step of the search. Here, the vector queue becomes (3, 5, **4**, 6). At this point, the check function finds the destination node, which is Node 4. The route is 1→ 2, → 4.

Accordingly, if any node in the network probably gets congested, then the process of finding route skips temporary for that node by putting zero bit in the TMT for short time (5 *ms*). For instance, let us assume the network with Node 2 about congestion. Then put "0s" for Node 2 inside TMT for 5 *ms* to avoid this node temporary time. However, Node1 now has this links (3, 5). So likewise previous method (3, 5) push in the queue, then pup 3 and check the connections with Node 3. And the new connections for Node 3 to queue (5,4). Hence, the new alternative route is 1→ 3→ 4. Finally, conclude if the congestion occurs in Node 2, then the route 1→ 3→ 4, and 1→ 5→ 4 become the alternative path.

4. SIMULATION SETUP

The main goal of this simulation is to find alternative paths whenever congestion happens is imminent. Therefore, a scenario was designed to simulate this problem as shown in Figure 1. The source nodes transmit massive data traffic to node 40 by using the CBR data traffic. The source node 41 begins to transmit data traffic to node 40 after 15 seconds. Then, nodes 42, 43, and 44 start sending packets after one, two, and three seconds later, respectively. All node preparations such as WiFi, MAC, AdhocWifiMac, WifiMacQueue, RtsCtsThreshold, DropTailQueue, and DsssRate2Mbps are set according to Table 1. The routing protocols include AODV, OLSR, and DSDV protocols.

Table 1. Simulation parameters

METRICS	VALUE
Application protocol	CBR
Number of nodes	45 nodes
Number of source node	4 nodes
Source node ID	Nodes 41,42,43,44
Number of sink node	1 node
Sink node ID	Node 40
Wi-Fi	802.11b
Packet size	128 Byte
Transmission range	250 m diameter
Bandwidth link	2 Mbps
Simulation time	30, 120 s

5. NETWORK PERFORMANCE

Here, the source nodes are convergent, and near node 20. In these circumstances, all source nodes send packets through one route to sink Node 40. The situation worsens if resources are increased without considering the congestion type, traffic pattern, and network topology. The routing protocol selects one route to send all packets via: Route 1: 20→ 21→ 22→ 23→ 24→ 25→ 26→ 27→ 28→ 29. Technically, when applying standard routing protocols, the routing protocol does not consider congestion as well as the other nodes. However, after applying our scheme, the alternative route works properly as shown in Figure 5. The routing protocol forwards the packets in an efficient path because every node possesses the complete network topology information. Nodes cooperate with each other by sending warning messages, thereby enhancing the overall network performance. The validation of these observed routes was achieved by Wireshark software and NetAnim 105.

Route 1: 41→10→0→1→2→3→4→5→6→7→8→9→19→40.
Route 2: 42→10→11→12→13→14→15→16→17→18→19→40.
Route 3: 43→20→21→22→23→24→25→26→27→28→29→40.
Route 4: 44→30→31→32→33→34→35→36→37→38→39→40.

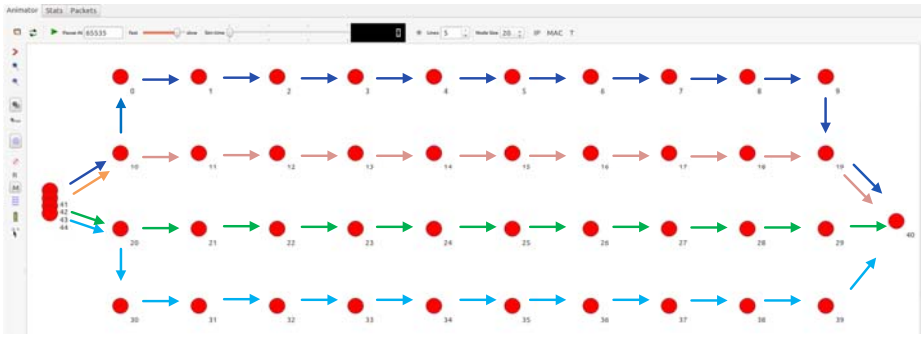

Figure 5. Alternative route

The most important metric that can be used to measure network performance is throughput. Figure 6 shows the throughput with 45 nodes and simulation time of 120 s. The throughput measured for whole network includes four nodes sending data traffic (Node 41 to 44). In addition, one node receives the data traffic, the sink node, node 40. Generally, the throughput is enhanced by 57%, as a result of the reduced packet loss and the new route to the destination. Furthermore, the average packet delivery ratio is enhanced by 57% against AODV protocol, as shown in Figure 7, which also shows the results for the whole network.

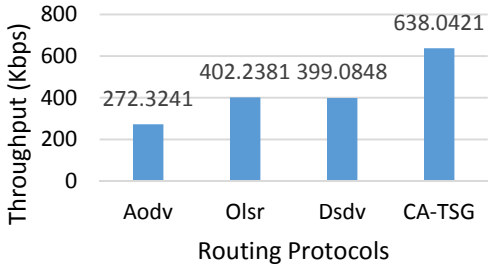

Figure 6. Average Throughput for source nodes

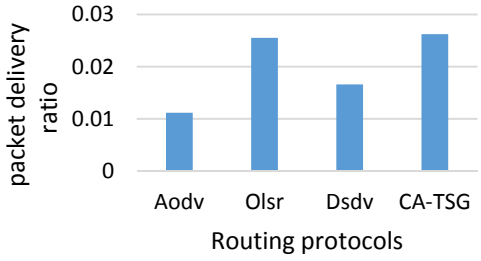

Figure 7. Average Packet Delivery Ratio for source nodes

The standard routing protocols AODV, DSDV, and OLSR forward packets from Nodes (41, 42, 43, and 44) to Node 40. To send any data packets, the MAC layer must send RTS and receive CTS frame to hold media, and then send DATA frame and receive ACK frame. This three-way acknowledgement exhausts the network. Thus, the behavior of routing protocols does not consider the cross-layer between network and MAC layers. Consequently, the throughput appears random for Nodes 41 to 44. In the second scenario, the

same topology has been used, except the simulation time is 30 seconds. It used this scenario to show the behavior of the routing protocol in short periods, especially in the first few seconds. Therefore, the DSDV protocol is not included in the Figures given its long time requirement to discover the network and build routing tables. AODV rapidly discovers the route to the destinations but is not as efficient as the OLSR protocol. The result shows that throughput for proposed protocol is again the best result for the short period of packets sending for 15 seconds, as shown in Figure 8.

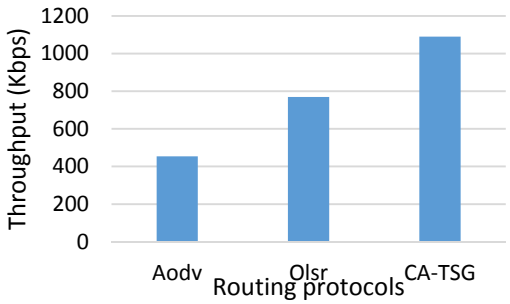

Figure 8. Throughput for average 4 source Nodes

In Figure 9, the throughput for every source node (41, 42, 43, and 44) is listed. Similarly, source nodes 41 and 44 have high throughput in proposed protocol. However, for the AODV and OLSR protocols, only source node 41 has high throughput because of the three-way acknowledgement. Figures 10, 11 show the lost packets, the packet delivery ratio, respectively. Finally, it can be concluded that the throughput has enhanced to 57.319% against AODV protocol. The received packets enhanced to 57.348% against AODV. The packet delivery ratio enhanced to 57.35% against AODV. The packet loss enhanced to 34.96% against OLSR protocol.

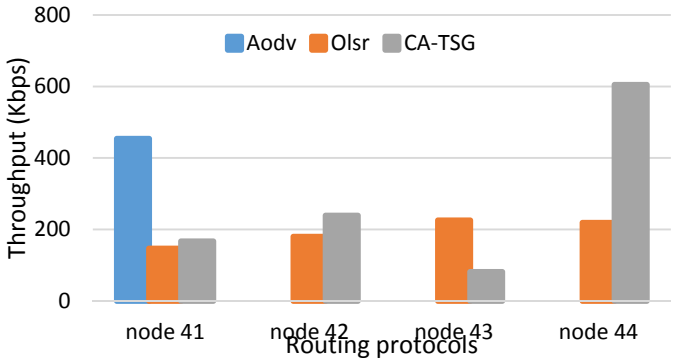

Figure 9. Throughput for source nodes 41 to 44

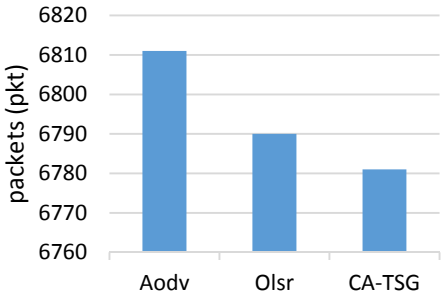

Figure 10. Lost packets for 30 seconds

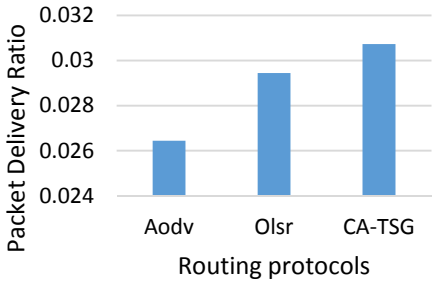

Figure 11. Packet delivery ratio for 30 seconds

6. CONCLUSION

We proposed a new scheme through which early congestion can be avoided based on the information from the MAC and network layers. We applied this scheme to the routing protocol with the help of network topology, and succeeded in obtaining alternative routes from the source to the destination prior to congestion. All nodes must pay attention to the warning message and check the automatic $Failure_{account}$. If the number reaches 11, then the next hop to that node will be avoided. Consequently, every node can recompute a new path from the source to the destination to transfer the data packets. This paper presented an efficient and lightweight congestion control algorithm. The performance characteristics of the network in cases of throughput, lost packets, and packet delivery ratio were generally enhanced. Future efforts may enhance the aspect of power consumption by distributing power throughout the whole network, not by depending on one route alone.

ACKNOWLEDGEMENTS

This work is supported by Ministry of Higher Education Malaysia and ministry of science and learning, under Grant No. LRGS/TD/2011/UKM/ICT/02/02. Also Iraqi board of supreme audit Iraq/Baghdad (Government Body). Authors thanks Iraqi board of supreme audit Iraq/Baghdad (Government Body) which contributed effectively to give us this opportunity for publishing.

REFERENCES

[1] M. I. A. A. R. T. Rahem, *et al.*, "A Comparative and Analysis Study of Vanet Routing Protocols," *Journal of Theoretical and Applied Information Technology,* vol. 66, pp. 691, 2014.
[2] R. N. Devikar, *et al.*, "Issues in Routing Mechanism for Packets Forwarding: A Survey," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 6, pp. 421-430, 2016.
[3] R. Havinal, *et al.*, "EASR: Graph-based Framework for Energy Efficient Smart Routing in MANET using Availability Zones," *International Journal of Electrical and Computer Engineering,* vol. 5, 2015.
[4] C. Cetinkaya, "Multi-channel cooperative MAC protocol for wireless LANs," *Ad Hoc Networks,* vol. 28, pp. 17-37, 2015.
[5] E. G. Villegas, *et al.*, "A novel cheater and jammer detection scheme for IEEE 802.11-based wireless LANs," *Computer Networks,* vol. 86, pp. 40-56, 2015.
[6] S. M. Aghdam, *et al.*, "WCCP: A congestion control protocol for wireless multimedia communication in sensor networks," *Ad Hoc Networks,* vol. 13, Part B, pp. 516-534, 2014.
[7] C. Sergiou, *et al.*, "Congestion control in Wireless Sensor Networks through dynamic alternative path selection," *Computer Networks,* vol. 75, Part A, pp. 226-238, 2014.
[8] A. P. Silva, *et al.*, "A survey on congestion control for delay and disruption tolerant networks," *Ad Hoc Networks,* vol. 25, Part B, pp. 480-494, 2015.
[9] L. Jun, "A cross-layer routing optimization method in Wireless Mesh Network," in *Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference on*, pp. 357-360, 2013.
[10] G. Karbaschi and A. Fladenmuller, "A link-quality and congestion-aware cross layer metric for multi-hop wireless routing," in *Mobile Adhoc and Sensor Systems Conference, IEEE International Conference on*, pp. 7, 655, 2005.
[11] M. Haghpanahi, *et al.*, "Topology control in large-scale wireless sensor networks: Between information source and sink," *Ad Hoc Networks,* vol. 11, pp. 975-990, 2013.
[12] A. Ghaffari, "Congestion control mechanisms in wireless sensor networks: A survey," *Journal of Network and Computer Applications,* vol. 52, pp. 101-115, 2015.
[13] K. Jaewon, *et al.*, "TARA: Topology-Aware Resource Adaptation to Alleviate Congestion in Sensor Networks," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 18, pp. 919-931, 2007.
[14] G. Feng, *et al.*, "Modified RED gateways under bursty traffic," *Communications Letters, IEEE,* vol. 8, pp. 323-325, 2004.
[15] S. Floyd and V. Jacobson, "Random early detection gateways for congestion avoidance," *Networking, IEEE/ACM Transactions on,* vol. 1, pp. 397-413, 1993.
[16] C. Sergiou, *et al.*, "Congestion control in Wireless Sensor Networks through dynamic alternative path selection," *Computer Networks,* vol. 75, pp. 226-238, 2014.
[17] N. J. Hussein, *et al.*, "IR and Multi Scale Retinex image Enhancement for Concealed Weapon Detection," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 1, pp. 399-405, 2016.
[18] L. Jun, "A cross-layer routing optimization method in Wireless Mesh Network," in *IEEE International Conference on Software Engineering and Service Science ICSESS*, pp. 357-360, 2013.
[19] S. S. Kumaran, "Early Congestion Detection and Self Cure Routing in Manet," *Computer Networks and Information Technologies,* pp. 562-567, 2011.
[20] A. A. R. T. Rahem, *et al.*, "A Triangular Matrix Routing Table Representation for Efficient Routing in Manet," *Journal of Theoretical & Applied Information Technology,* vol. 64, 2014.

BIOGRAPHIES OF AUTHORS

Abd Al-razak Tareq Rahem is currently a Ph.D candidate at Universiti Kebangsaan Malaysia (UKM), the Department of Electrical, Electronics and Systems Engineering. He received the B.S Computer Engineering and Information Technology from University of Technology, Baghdad, Iraq, in 2002, and the Master of Technology degree in Information Technology college of Engineering from BVDU, Pune, India, in 2012. His current research interests include wireless networking and mobile ad hoc network. Routing Protocol. Network Performances. He was consulting in DG Pioneer Magazine in Iraq (2005-2008).

Mahamod Ismail is currently a professor in Communications Engineering at the Universiti Kebangsaan Malaysia (UKM). He received the B.Sc. in Electrical and Electronics from University of Strathclyde, U.K. in 1985, the M.Sc. in Communication Engineering and Digital Electronics from UMIST, Manchester U.K. in 1987, and the Ph.D. from University of Bradford, U.K. in 1996. Professor Mahamod is an executive member of Communications/Vehicular Technology Society, IEEE Malaysia chapter. His current research interests include Mobile Communications and Wireless Networking.