2009

End-to-End Path Stability of Reactive Routing Protocols in IEEE 802.11 Ad Hoc Networks

Daniel R. Franklin
University of Wollongong, danielf@uow.edu.au

Jerry Chun-Ping Wang
University of Wollongong, jerryw@uow.edu.au

Mehran Abolhasan
University of Wollongong, mehran.abolhasan@uts.edu.au

Farzad Safaei
University of Wollongong, farzad@uow.edu.au

End-to-End Path Stability of Reactive Routing Protocols in IEEE 802.11 Ad Hoc Networks

Abstract

Over the years, a considerable research effort has been applied to the design of ad hoc network routing protocols. However, there is still a lack of understanding of the subtle interactions between routing protocols and lower layers in the protocol stack. In this paper, the instability which may arise when reactive routing protocols interact with the IEEE 802.11 MAC protocol is investigated. In particular, several erratic behaviours of the Ad hod On-demand Distance Vector (AODV) routing protocol in a congested IEEE 802.11 ad hoc network are demonstrated. A cross-layer solution is proposed based on an Adaptive Bulk Trigger policy and a Dynamic Window Selection scheme. Simulation studies are presented which show that the proposed solution is effective in alleviating erratic behaviour of AODV and improving the end-to-end path stability.

Keywords

path, reactive, routing, end, ieee, networks, hoc, ad, 802, stability, protocols, 11

Disciplines

Physical Sciences and Mathematics

Publication Details

Wang, J., Abolhasan, M., Franklin, D. R. & Safaei, F. (2009). End-to-End Path Stability of Reactive Routing Protocols in IEEE 802.11 Ad Hoc Networks. 34th Annual IEEE Conference on Local Computer Networks - (LCN 2009) (pp. 499-505). Zurich, Switzerland: IEEE.

End-to-End Path Stability of Reactive Routing Protocols in IEEE 802.11 Ad Hoc Networks

Jerry Chun-Ping Wang, Mehran Abolhasan, Daniel R. Franklin, and Farzad Safaei
Information & Communication Technology Research Institute,
University of Wollongong, Wollongong, NSW 2522, Australia
{jcpw942,mehrana,danielf,farzad}@uow.edu.au

***Abstract*—Over the years, a considerable research effort has been applied to the design of ad hoc network routing protocols. However, there is still a lack of understanding of the subtle interactions between routing protocols and lower layers in the protocol stack. In this paper, the instability which may arise when reactive routing protocols interact with the IEEE 802.11 MAC protocol is investigated. In particular, several erratic behaviours of the Ad hod On-demand Distance Vector (AODV) routing protocol in a congested IEEE 802.11 ad hoc network are demonstrated. A cross-layer solution is proposed based on an Adaptive Bulk Trigger policy and a Dynamic Window Selection scheme. Simulation studies are presented which show that the proposed solution is effective in alleviating erratic behaviour of AODV and improving the end-to-end path stability.**

I. Introduction

The IEEE 802.11 MAC protocol is a data link layer standard for use in wireless networks. In recent years the protocol has been widely adopted in many ad hoc network testbeds and simulations due to the low cost and wide availability of IEEE 802.11 hardware. IEEE 802.11 employs a CSMA/CA mechanism called the distributed coordination function (DCF). As its name implies, DCF is an inherently distributed protocol - however, it was not designed with multi-hop networks in mind. Consequently, when an ad-hoc routing protocol is used on top of IEEE 802.11 DCF, stability and unfairness problems can arise [1]–[6]. One manifestation of this is that the network sporadically experiences large throughput fluctuations over the duration of multi-hop transmissions. Earlier studies attributed the network instability to TCP's congestion control mechanism, which aggressively attempts to estimate congestion levels by exponentially increasing the transmission window size until packet loss occurs [1]–[3]. This has the effect of causing high transient packet loss rates due to link-layer contention.

More recent studies have offered an alternative explanation, and raised the issue of interaction between reactive routing protocols and the underlying MAC protocols [4]–[6]. Ng and Liew demonstrate that the instability problem is not restricted to TCP - it also occurs in UDP traffic [4]. Their work looked at IEEE 802.11 ad hoc networks using the AODV reactive routing protocol, and showed that the large throughput fluctuation is the result of frequent route re-discovery processes triggered by the loss of data packets. The ongoing attempts at data transmission are blocked until the route is recovered, resulting in a sudden drop in throughput. Hence, the problem is redefined as a "*re-routing instability problem*". Other authors re-examined the re-routing instability problem with TCP traffic [5], [6] and confirmed that the excessive data traffic disrupts the routing dynamic of reactive routing protocols, leading to network instability.

Moreover, the interaction between reactive routing and MAC protocols creates potential "*instability loops*" in the network, particularly under high traffic load. Reactive routing protocols rely heavily upon broadcast transmission to collect and distribute routing information. However, the basic 802.11 DCF only offers a minimal service quality for broadcast transmissions, as the stations do not acknowledge received broadcast frames, nor do they have the ability to re-transmit in the event of packet loss [7]. Therefore, when competing against data traffic (which typically is dominated by unicast data), the routing packets are prone to loss [8], [9]. Hence, extended involuntary disconnections occur in the network. In response to these route breakages, reactive routing protocols generate yet more routing (broadcast) packets to flood the network, further exacerbating the problem.

In this paper, the routing pathologies and failures that are likely to occur in reactive routing protocols are explored, using the Ad-hoc On-demand Distance Vector (AODV) reactive routing protocol. Based on these observations, a cross layer solution is proposed to improve the end-to-end path stability. The specific contributions of this paper include:

- A study of AODV routing pathologies in congested ad hoc networks. This extends the work of Ng and Liew's by examining not only a single network flow, but also two concurrent flows with a single common router node (Section III).
- A cross-layer solution that largely avoids the routing instability problem. The proposed solution combines *Adaptive Bulk Trigger* (ABT) - which prevents over-reaction of the reactive routing protocol - with a *Dynamic Window Selection* (DWS) scheme - which offers higher-priority access to the stations with critical routing demands (Section IV).
- A performance evaluation of AODV with and without the proposed solution. The evaluation demonstrates the effectiveness of the proposed solution, which offers

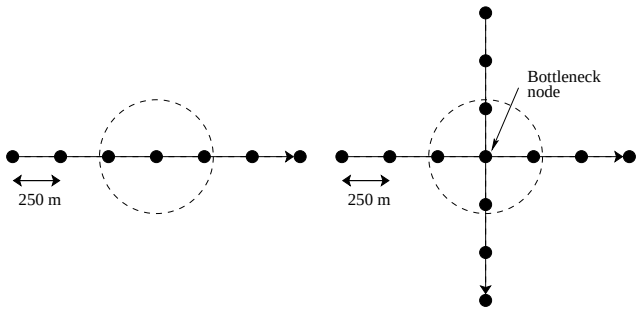
This work is partly supported by the Desert Knowledge CRC (DK-CRC) under the joint DK-CRC / University of Wollongong (UoW) project "Sparse Ad hoc Network for Desert (SAND)".

more stable end-to-end connectivity than the existing approaches (Section V).

Before the ad hoc network instability problems are examined in detail, Section II discusses the simulation environment that will be used throughout this paper.

II. Simulation Environment

The simulations were performed using the Qualnet discrete event network simulator (version 4.0). Each station is equipped with a single 802.11b wireless interface and an omni-directional antenna positioned 1.5 meters above the ground. The RF channel is represented by a *Two-Ray Pathloss* propagation model, and the data bitrate is set at a fixed rate of 11 Mb/s. Under these conditions, each station's maximum transmission range is approximately 280 meters and its carrier sensing range is 500 meters. Qualnet's *MAC_DOT11* library is used as the MAC protocol and the optional RTS/CTS mechanism is disabled[1]. The AODV reactive routing protocol is used to evaluate the routing dynamics. A preconfigured static routing table is also used to provide a baseline performance measurement for evaluation of the reactive routing protocol's performance.



(a) One flow (b) Two flows

Fig. 1. One-flow and two-flow scenarios

The simulations consider several scenarios with one or more identical 6-hop unidirectional traffic flows. For each flow, the network traffic traverses 7 nodes with a hop distance of 250 meters between successive nodes. Figure 1 shows the topology for one-flow and two-flow scenarios. In the one-flow scenario, the network is simply a string topology of 7 nodes. In the two-flow scenario, two 6-hop linear flows share a common central node.

All network traffic flows are constant bit rate (CBR) streams of 1024 byte UDP datagrams. The total offered load is 200 packets per second, equally distributed between the number of flows. According to Qualnet simulation, this aggregated load is sufficient to cause network saturation in a 6-hop network.

III. Routing Pathologies

In this section, the impact of network congestion on a reactive routing protocol is evaluated for one-flow and two-flow scenarios. Figure 2 shows the typical throughput variation seen over a period of 150 seconds in each case. Throughput achieved with AODV is compared to that achieved with simple static routing to demonstrate the instability of the reactive routing protocols.

Table I provides a statistical comparison of the performance of the one-flow and two-flow scenarios averaged over 30 runs, each lasting 900 seconds. The performance of static routing table and AODV is measured using the metrics of throughput, path breakage frequency, mean time between failures (MTBF), mean time to recover (MTTR) and percentage of path availability.

A. One-Flow Scenario

The one-flow scenario demonstrates the impact of network congestion at the source. This type of network congestion occurs when a source generates data at a rate which exceeds the capacity of its network connection. Since the entire network operates at the same bit rate, packets will be dropped at the source and congestion will not be seen elsewhere in the network.

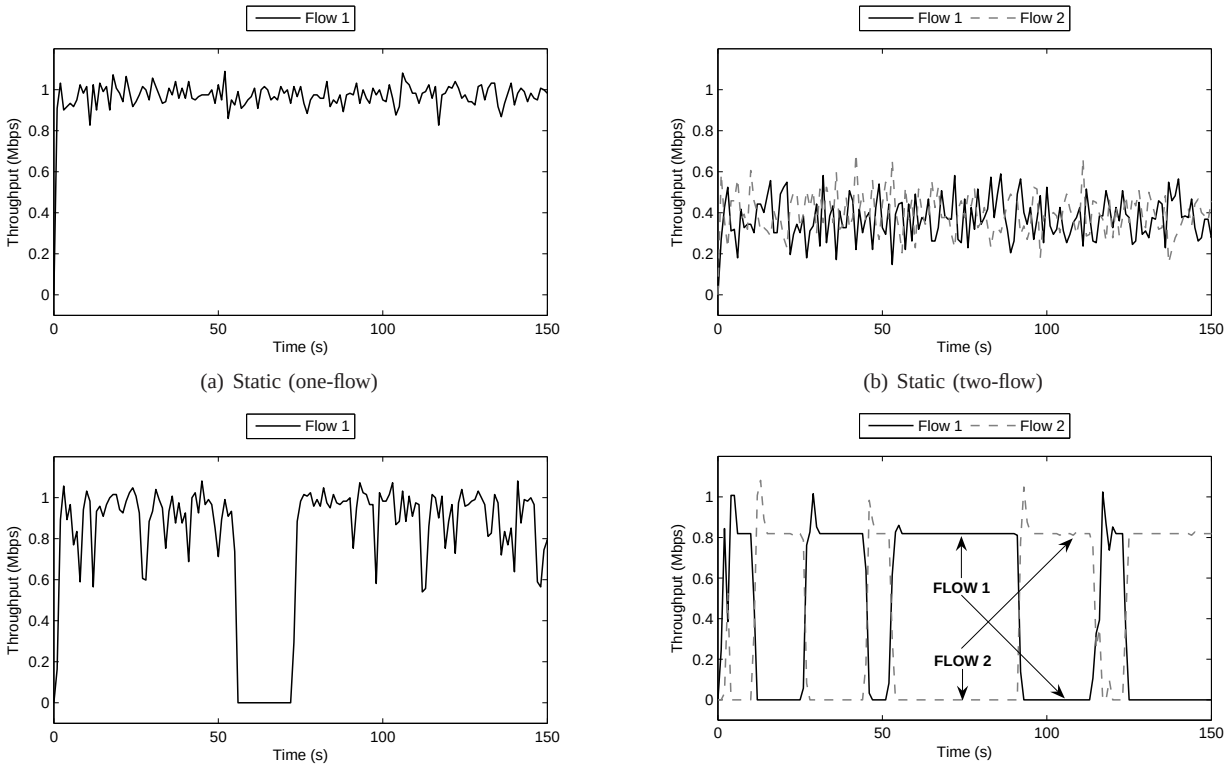
Figure 2(a) shows network throughput using a predefined static route for a single flow. The end-to-end throughput stays approximately constant over the duration of the simulation. The loss of data packets due to network congestion results in small throughput fluctuations only.

By contrast, the throughput of AODV, shown in Figure 2(c), exhibits large fluctuations over the 150 second interval. This is because network congestion results in packet loss, which in turn triggers the route re-discovery process. Since the wireless medium is inherently a shared resource, routing packets are competing against data packets for channel access. However, according to IEEE 802.11 standard, the handling of routing packets at MAC layer has the lowest service quality (since they are broadcast and lack the ability to be retransmitted in the event of packet loss). Hence, the routing packets are more susceptible to packet loss, particularly under saturation conditions [8]

Route discovery can be a costly process as it usually involves (at least partial) flooding of the network. The flooding creates a potential "*Broadcast Storm*" condition, which may adversely affect stations across the network [11]. Moreover, the route maintenance process suspends data transmission until the route is recovered or an alternative route is found - creating an extended network disconnection. This agrees with the results of Ng and Liew [4].

The statistical results presented in Table I show that, as expected, static routing achieves better and more consistent throughput than AODV in one-flow scenario. Since static routing does not undergo route maintenance when a packet is dropped, the end-to-end path remains available and no disconnection will occur during the simulation time. On the other hand, AODV suffers from involuntary disconnections due to network congestion and takes an average of around 9.5 seconds to recover after failure.

[1]The RTS/CTS mechanism is ineffective in ad hoc networks due to large interference range, hence is switched off [10].



(a) Static (one-flow)

(b) Static (two-flow)

(c) AODV (one-flow)

(d) AODV (two-flow)

Fig. 2. Performance of ad hoc routing protocols in one-flow and two-flow scenarios

Routing	1-Flow Scenario					2-Flow Scenario				
	Throughput	Frequency	MTBF	MTTR	Availability	Throughput	Frequency	MTBF	MTTR	Availability
STATIC	0.977 *Mbps*	0.00	900.00*s*	0.00*s*	100.00*%*	0.384 *Mbps*	0.00	900.00*s*	0.00*s*	100.00*%*
AODV	0.822 *Mbps*	4.49	259.56*s*	9.49*s*	96.47*%*	0.417 *Mbps*	35.54	15.39*s*	11.25*s*	57.77*%*

TABLE I
PERFORMANCE OF ONE-FLOW AND TWO-FLOW SCENARIOS AVERAGED OVER 900 SECONDS

B. Two-Flow Scenario

Consider two identical CBR traffic flows, each at half the rate of the single-flow scenario, passing through a common node. In this scenario, congestion occurs at the central bottleneck rather than at the point of ingress as the aggregate incoming traffic exceeds the capacity of the central node's network interface. The performance of static routing in this scenario, shown in Figure 2(b), illustrates that the throughput for both flows is reduced by more than half. In addition, the individual flows experience wider throughput fluctuations due to longer queuing delays at the bottleneck node. Despite the throughput reduction and larger fluctuations, the network still maintains a continuous flow of data, and network capacity is fairly shared between the two flows.

Figure 2(d) and Table I show that the behaviour of AODV would be very different in a two-flow scenario. In particular, routing instability leads to a situation where exclusive control of the channel seems to alternate between the two traffic flows. When one flow dominates, this increases the chance of losing important routing messages for the other flow resulting in its disconnection. The dominant flow then continues for a period of time until it triggers network re-discovery process as a result of packet loss. During this critical moment, the network resource can be taken over by the other flow, forcing the previously dominant flow to become disconnected. Figure 2(d) shows that two network flows take over the network in turn rather than sharing bandwidth with each other.

Further, Table I underlines an interesting and seemingly contradictory result - although throughput is highly variable for each flow when using AODV (i.e. each flow only maintains approximately 57% of route availability), the aggregate throughput is actually *higher* than using a static routing table! This is due to the temporary exclusivity of access while the competing flow attempts to re-establish a path to its sink. The temporary exclusive channel access results in a burst transmission of data packets from a dominant flow, subsequently leading to higher throughput.

Despite the higher average throughput, the sporadic disconnections which occur when AODV is used in the two-flow scenario indicate that this network would be unsuitable for

application-layer protocols which rely on a steady flow of packets (such as VoIP). Furthermore, TCP's congestion control mechanism would perform very poorly in this environment as it would be subject to frequent time-outs and connection resets.

IV. Stability Improvement with Adaptive Bulk Trigger and Dynamic Window Selection

A number of solutions have been proposed to rectify the erratic behaviour of traffic flows over a congested network using AODV, operating at various different network layers. Some studies have shown that by controlling the offered load at the upper layers (i.e. application and transport layers), the erratic behaviour can be greatly alleviated [2], [6], [12]. However, these solutions significantly limit the capacity of the network: exchanging throughput for greater stability.

Another approach, suggested by Ng and Liew, modifies the operation of reactive routing protocol by continuing to use the existing route for data transmission until a new route can be found [4]. While their solution provides substantial improvement on end-to-end stability, it does not prevent AODV from over-reaction due to false link failure declarations. In a busy network with relatively infrequent topology changes (for example, an urban mesh network), AODV is still likely to generate excessive amount of unnecessary control transmissions in the event of packet loss, thereby reducing the efficiency of the network.

Other authors argue that the underlying problem is the interaction between routing and MAC protocols, since apparent link failures are largely a result of network congestion rather than physical link breakages [5], [6]. These failures are frequent but transient, and therefore should be treated differently to longer-term link failures. One way in which this can be achieved is to introduce a bulk trigger (BT) policy, which increases the link failure threshold by allowing small amount of packet losses before announcing link failure. Hence the route re-discovery process only takes place after a certain number of consecutive packet losses.

The drawback of BT policy is that the network assumes a fixed link failure threshold on all stations, whereas the collisions mostly occur at specific nodes (i.e. bottleneck nodes). The choice of link failure threshold is thus a tradeoff between network dynamism and stability. On one hand, if the threshold is too low, it may be insufficient to accommodate the level of network congestion. If the threshold is too high, the network becomes stuck in a static configuration and is unable to react quickly to physical topology changes (e.g. the physical loss or addition of a node). Therefore, given the distributed nature of multi-hop networks, link failure thresholds should be determined by each station based on the local network conditions.

In this paper, two approaches to improving the stability of reactive routing protocols in multi-hop ad hoc networks are presented. The *Adaptive Bulk Trigger* (ABT) improves existing BT policy without specifying a fixed link failure threshold. In addition, the *Dynamic Window Selection* (DWS) scheme enhances ABT policy by assigning higher channel access priority to the stations experiencing consecutive packet losses.

A. Adaptive Bulk Trigger policy

As shown in Figure 2, the erratic routing behaviour observed in AODV is the result of the false link failure declarations triggered by the loss of data packets. In this case, the cost of re-routing is substantial since the same route is repeatedly re-selected from the recovery process - a completely unnecessary process when (as is commonly the case) the nodes are largely static. Hence, the stations should assign higher link thresholds when the same route is constantly being re-selected. If this behaviour is not observed, the threshold should remain low to retain the ability to react quickly to changes in node distribution.

init : $L(i,j), \beta(i,j) \leftarrow 0 \quad i,j \in [1 \ldots n]$
input : Destination Node d
Next Hop Node h

```
1  begin
2      if Transmission is successful then
3          L(d,h) ← 0;
4      else
5          L(d,h) ← L(d,h) + 1;
6          if L(d,h) > β(d,h) then
               // commence re-routing
7              ReportLinkFailure ();
8              β(d,h) ← β(d,h) + 1;
9              L(d,h) ← 0;
10         end
11         if Link(d,h) idle for more than W seconds
           then
12             β(d,h) ← 0
13         end
14     end
15 end
```

Algorithm 1: Adaptive Bulk Trigger (ABT) policy

Algorithm 1 describes the operation of ABT policy. Assume the network contains n stations. The stations keep the record of packet loss count and link failure threshold for each destination and next-hop pair. Let $\beta(d,h)$ be link failure threshold and $L(d,h)$ be the number of consecutive lost packets counted for destination d and next hop h at a given station. The re-routing process is triggered only when the accumulated packet loss count $L(d,h)$ is greater than the threshold $\beta(d,h)$. The lost packet count $L(d,h)$ is reset to zero once the transmission is successful or re-routing process is triggered. It should be noted that the conventional AODV assumes $\beta(d,h) = 0$ for all destination and next-hop pairs, whereas a network with a static routing table can be represented by $\beta(d,h) = \infty$. Thus, ABT policy offers a high degree of flexibility to adjust the dynamics of a reactive routing protocol.

The stations initially assume that the link failure threshold is zero for all destination and next-hop pairs. ABT policy

incrementally assigns the threshold value based on the number of repeated route recoveries. Given that the re-routing process commences when the consecutive packet loss count exceeds the current threshold limit, the routing protocol will increase the threshold value after executing the re-routing process. Thus the threshold continues to rise until an equilibrium is reached, which should still be sufficient to detect real link failures, but not so low as to trigger unnecessary re-routing processes. Otherwise, the route will not be recovered and the threshold value remains low. Finally, the threshold value for a given destination and next-hop pair is reset to zero when the pair becomes inactive for more than W seconds.

B. Dynamic Windows Selection (DWS)

In order to allow all stations to contend for the medium, the IEEE 802.11 Distributed Coordinate Function (DCF) defers a station's access attempt for a random period of time within a bounded interval known as the contention window. Upon each failed attempt, the station doubles its contention window size until the maximum number of retransmissions is exhausted or maximum contention window size (CW_{max}) is reached (at which point the window ceases to grow). The IEEE 802.11 standard specifies a maximum of seven retransmission attempts before dropping a packet. Thus, ABT policy ensures that the station has $7 \cdot \beta(d,h)$ transmission attempts for all destination and next-hop pairs before responding link failure.

Since the contention window size is reset to its initial value (CW_{min}) upon each packet drop, the existing bulk-trigger policy assumes that each data packet delivery is assigned with same priority regardless of current network condition. However, as the consecutive packet loss count $L(d,h)$ approaches to the threshold $\beta(d,h)$, it becomes more critical for a station to successfully deliver the data packets. The underlying MAC protocol should assign higher channel access priority to the stations with larger consecutive packet drop counts $L(d,h)$ to avoid the accumulation of consecutive packet drops as much as possible.

To enable priority access in ABT policy, a Dynamic Window Selection (DWS) scheme is proposed, which assigns channel access priority based on the consecutive packet loss count $L(d,h)$ and threshold value $\beta(d,h)$. In DWS, the channel access priority is refined by adjusting the rate of contention window expansion. Instead of doubling contention window size at each transmission attempts, the rate of contention window expansion is adjusted in accordance with consecutive packet drop count $L(d,h)$. DWS decreases the window expansion rate as the number consecutive packet drop $L(d,h)$ increases. Let CW_i be the size of the contention window at ith attempt, the selection of contention window size can be defined as:

$$CW_{i+1} = \min\left(CW_i \times \left(2 - \frac{L(d,h)}{\beta(d,h)}\right), CW_{max}\right) \quad (1)$$

According to Eq (1), the contention window expansion rate is progressively reduced from binary exponential expansion to zero expansion depending on threshold value $\beta(d,h)$ and $L(d,h)$ (i.e. expansion rate is reducing from a factor of two per iteration to one). For instance, if $\beta(d,h)$ equals to 2, the contention window will initially double its contention at each failed attempt. After first packet drop, the contention window will increase its contention window size by 1.5 times. The window expansion will continue to decrease to the point where the contention window size remains unchanged (i.e. $CW_{i+1} = CW_i$) before reporting link failure at the second consecutive packet drop.

The key effect of incorporating ABT policy and a DWS scheme in reactive routing protocols is that the proposed techniques do not alter the existing routing and MAC operation under non-congested condition. Given that the packets are less likely to drop under non-congested condition, the proposed enhancements remain inactive until network congestion emerges - only taking action and assigning elevated priority to a packet when the previous packet is dropped.

V. Evaluation and Comparisons

To evaluate the stability improvements made by ABT and DWS, simulation results of AODV with and without the proposed schemes are compared. In addition, the comparison also includes the fixed bulk-trigger policy shown in Reference [5], [6] to highlight the effectiveness of the dynamic approach proposed in this paper. Since Section III shows the limitations of only evaluating throughput as a performance metric, this section focuses on other stability metrics. Unless otherwise specified, AODV with ABT and DWS is denoted as *AODV-ABT+DWS*, whereas AODV with fixed bulk-trigger is represented by *AODV-BT* with the corresponding fixed threshold value β.

The evaluation considers a network of 50 stations uniformly distributed across a flat terrain of 1200 m $\times$ 1200 m. The remaining network parameters are as for the configuration described in Section II. The simulation environment ensures that all nodes are able to participate in the network. The network traffic consists of five randomly selected CBR sessions, with each session transferring a stream of 1024 byte UDP datagrams between a randomly source and sink at various data rates. Each simulation lasts 900 seconds and the results are averaged over 30 independent runs for each test case.

A. The Importance of Link Failure Threshold

The average value of the link failure threshold affects the responsiveness of the reactive routing protocol to mobility in the network. According to Ashraf *et al.*, a larger average threshold will cause the network to be much slower to respond to link failures due to node mobility. Therefore, while using a larger threshold size for all nodes will reduce the rate of path breakage due to false link failure declarations, this does not necessarily yield optimal performance [5]. The main objective of our protocol is to keep the *average* threshold at the minimum value necessary to maintain good network stability, while allowing it to automatically increase in areas of severe congestion.

pkt. rate	75	100	125	150	175	200
avg. threshold	0.799	0.819	0.819	0.802	0.801	0.819

TABLE II
THE AVERAGE LINK FAILURE THRESHOLD FOR COMBINED ABT AND DWS STRATEGY

Table II demonstrates that the AODV-ABT+DWS scheme effectively limits the average threshold size on the active paths. Since the dynamic approach only assigns higher threshold value on the congested stations, and idle or less-congested nodes retain the lower threshold value, the average threshold remains low compared to the AODV-BT approach (i.e. $\overline{\beta} < 1$).

B. Mean Time Between Failures

The mean time between failure represents the duration for which a path lasts prior to invalidation. Figure 3 illustrates MTBF plotted against packet generation rate for different variations of AODV. For all AODV variants, the MTBF declines as the packet generation rate and congestion levels increase. The reactive routing protocols then start to initiate route re-discovery after a series of dropped packets.

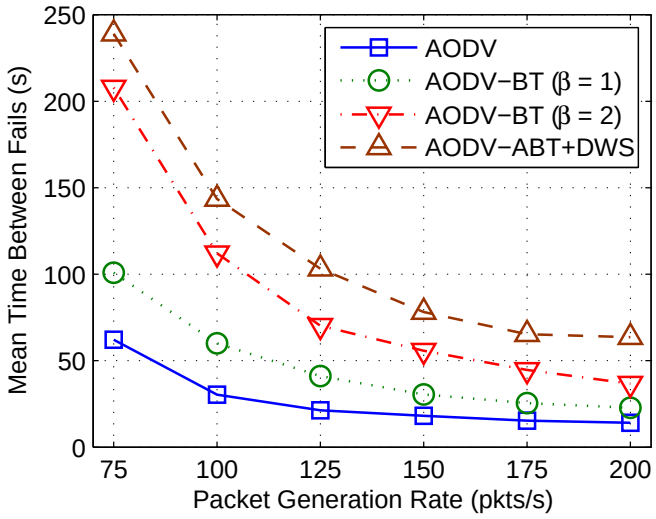


Fig. 3. Mean time between failures vs. aggregated offered load

According to Figure 3, the mean time between failures can be improved in AODV-BT by increasing the β parameter, since this allows congestion-related apparent link failures to be ignored. Once the congestion level deteriorates sufficiently, the average MTBF for AODV-BT becomes quite small for all values of β. However, by contrast, the adaptive scheme allows the stations to dynamically adjust their threshold, strengthening the resistance to false link failure declarations at the most critical (congested) nodes. When compared to AODV and AODV-BT, the proposed AODV-ABT+DWS scheme achieves a significantly improved MTBF over existing approaches - particularly at high levels of congestion.

C. Path Breakage Frequency

The path breakage frequency measures the resistance of a given routing protocol to false link failure declarations. Since the simulation assumes the nodes are stationary and operational for the full duration of the simulation, the only cause of route breakage is network congestion. Under ideal network conditions, the routing protocol should maintain the same path over the entire duration of a packet flow.

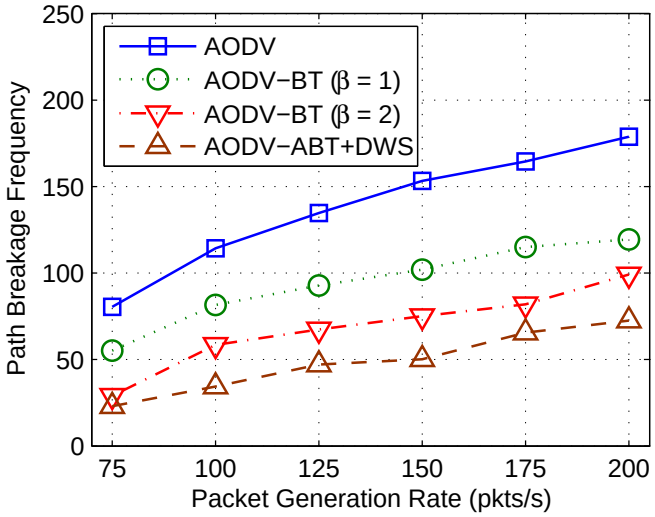


Fig. 4. Average path breakage frequency vs. aggregated offered load

Figure 4 shows the average number of route breakages for different variants of AODV. Classic AODV has highest rate of path breakages among all routing schemes. The results show that the ABT policy successfully reduces the number of false path failures by automatically assigning a higher threshold value where it is required. Moreover, the combined ABT and DWS schemes has shown an outstanding ability to reduce the number of path breakages while maintaining a small average threshold size.

D. Average Path Availability

The average path availability measures the portion of the simulation time that a path is active. As shown in Section III, congestion can reduce the availability of routes, making the end-to-end path unusable for many applications. The impact of network congestion is also shown in Figure 5 where the path availability is diminished as stations generate more packets.

Figure 5 demonstrates that the path availability for AODV deteriorates quickly as the congestion level increases. Path availability is improved for AODV-BT by assigning a higher link failure threshold - for example, AODV-BT with a threshold size of 2 achieves similar level of path availability with AODV-ABT+DWS when the network congestion is low (i.e. 75 pkts/s). This is because the current network threshold size is sufficient to of manage congestion. Once the traffic load increases, however, the performance of AODV-BT starts to deteriorate, whereas AODV-ABT+DWS availability is only mildly reduced.

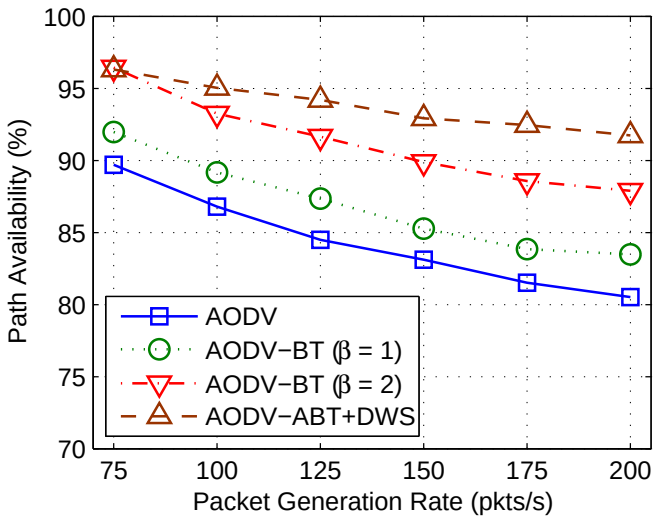


Fig. 5. Path availability

E. Normalised Control Overhead

The route maintenance and discovery process produces a series of control packets propagating across the network. If these operations need to be repeated frequently, a significant fraction of the available network capacity will be consumed by these control packets - introducing yet more packets into an already-congested environment. For networks with low mobility, most of these control messages are not only redundant but actively harmful to other traffic flows. Therefore, it is important to quantify the relationship between the congestion and the number of control packets generated.

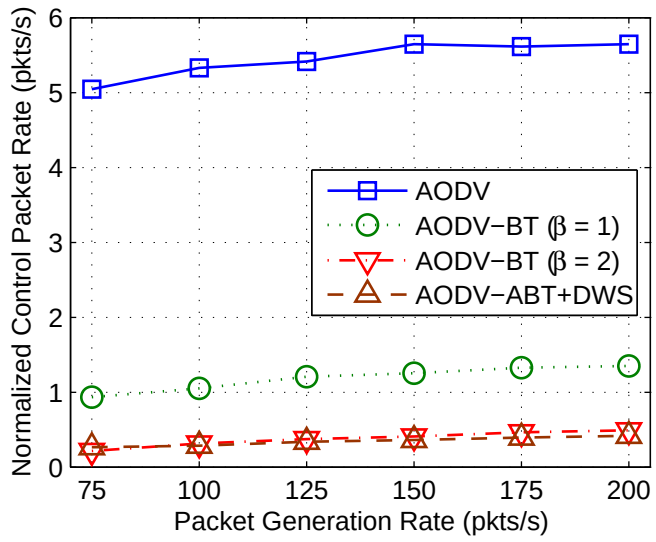


Fig. 6. Control packet rate

Figure 6 shows the rate at which control packets are being generated, averaged over entire the simulation time. The results indicate that standard AODV generates around 5-6 control packets per second over a wide range of traffic levels, increasing slightly with congestion levels. For AODV-BT, the number of control packets is progressively reduced as the threshold value increases. This is because the routing protocol becomes less reactive with a larger threshold. However, the best results are obtained with AODV-ABT+DWS, showing that the algorithm is effective in managing the control packet generation in a congested network.

VI. Conclusion

In this paper, the AODV routing protocol is shown to be unstable and inefficient in highly congested IEEE 802.11 ad hoc networks. It is observed that congestion-driven packet loss will frequently trigger a route re-discovery process in AODV, resulting in large throughput fluctuations and extended disconnections.

A cross-layer solution is presented to rectify the erratic behaviour. In particular, the proposed solution enhances the link-failure tolerability of reactive routing protocols and provides prioritised channel access based on routing demands. Simulations have proven the effectiveness of the proposed solution. Future work will focus on more complex scenarios as well as the introduction of mobility.

References

[1] S. Xu and T. Saadawi, "Does the IEEE 802.11 MAC protocol work well in multihop wireless adhoc networks?" *IEEE Communications Magazine*, vol. 39, pp. 130–137, June 2001.

[2] Z. Fu, H. Luo, P. Zerfos, S. Lu, L. Zhang, and M. Gerla, "The impact of multihop wireless channel on TCP performance," *IEEE Transactions on Mobile Computing*, vol. 4, no. 2, pp. 209–221, March 2005.

[3] E. Hamadani and V. Rakocevic, "A cross layer analysis of TCP instability in multihop ad hoc networks," in *European Wireless (EW2007)*, April 2007.

[4] P. C. Ng and S. C. Liew, "Re-routing instability in IEEE 802.11 multihop ad-hoc networks," in *Proceedings of 29th Annual IEEE International Conference on Local Computer Networks (LCN '04)*, November 2004, pp. 602–609.

[5] U. Ashraf, S. Abdellatif, and G. Juanole, "Efficient route maintenance in wireless mesh networks," in *Proceedings of 3rd International Symposium on Wireless Pervasive Computing (ISWPC 2008)*, May 2008, pp. 712–716.

[6] K. Nahm, A. Helmy, and C. C. J. Kuo, "Cross-layer interaction of TCP and ad hoc routing protocols in multihop IEEE 802.11 networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 458–469, 2008.

[7] IEEE, *IEEE Std. 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*, IEEE std. 802.11-2007 ed., 2007.

[8] J. C.-P. Wang, D. R. Franklin, M. Abolhasan, and F. Safaei, "Characterising the interactions between unicast and broadcast in IEEE 802.11 ad hoc networks," in *Australasian Telecommunications Networking and Application Conference (ATNAC 2008)*, 2008.

[9] R. Oliveira, L. Bernardo, and P. Pinto, "The influence of broadcast traffic on IEEE 802.11 DCF networks," *Computer Communications*, vol. 32, no. 2, pp. 439–452, February 2009.

[10] K. Xu, M. Gerla, and S. Bae, "Effectiveness of RTS/CTS handshake in IEEE 802.11 based ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 107–123, July 2003.

[11] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, "The broadcast storm problem in a mobile ad hoc network," *Wireless Network*, vol. 8, no. 2/3, pp. 153–167, 2002.

[12] P. C. Ng and S. C. Liew, "Throughput analysis of IEEE 802.11 multihop ad hoc networks," *IEEE/ACM Transactions on Networking*, vol. 15, no. 2, pp. 309–322, 2007.