Router Selfishness in Community Wireless Mesh Networks: Cross-Layer Benefits and Harms

Krzysztof Gierlowski
Faculty of Electronics, Telecomm. and Informatics
Gdansk University of Technology
Gdansk, Poland
e-mail: krzysztof.gierlowski@eti.pg.gda.pl

Jerzy Konorski
Faculty of Electronics, Telecomm. and Informatics
Gdansk University of Technology
Gdansk, Poland
e-mail: jekon@eti.pg.gda.pl

Abstract—In community wireless mesh (CWM) networks following the IEEE 802.11s standard, wireless nodes combine the functionality of a client application host and a transit packet router. Not being subjected to tight administrative control, CWM nodes may act selfishly by refusing to forward transit packets along (selected) established routes or to participate in the route creation process. Unlike in a mobile ad hoc network (MANET), a CWM node is typically connected to mains electricity, hence unconcerned about energy expenditure; the only rational (as distinct from malicious) motivation behind selfish behavior is then to prevent the incoming transit traffic from competing with the source traffic and thereby achieve a higher source throughput. We examine through simulation the benefits and harms of selfish behavior with a cross-layer view and relate them to the router density, selfish routers’ location and details of their behavior. We find many conclusions and intuitions valid for MANET environments incorrect for CWMs.

Keywords—mesh networks, selfish behavior, cross-layer view

I. INTRODUCTION

In community wireless mesh (CWM) networks following the IEEE 802.11s standard [1], wireless nodes combine the functionality of a client application host and a transit packet forwarder. Not being subjected to tight administrative control, CWM nodes may act selfishly by refusing to forward transit packets along (selected) established routes or to participate in the route creation process. The situation resembles that in mobile ad hoc networks (MANETs) [2], where, in anticipation of sufficiently many selfish nodes disrupting the network connectivity, detection schemes are deployed, usually based on watchdog monitored transmissions from neighboring nodes. Subsequent punishment of misbehaving nodes may involve refusal to forward their source packets by other nodes. These schemes are costly and not always reliable [3]. In this paper we dare to ask whether, in some CWM communication scenarios at least, they are necessary at all. Indeed, a CWM node is typically connected to mains electricity, hence unconcerned about energy expenditure; the only rational (as distinct from malicious) motivation behind selfish behavior is then to prevent the incoming transit traffic from competing with the source traffic and thereby achieve a higher source throughput. However, cross-layer considerations suggest that the benefits of this are not obvious. Dropping transit packets does not prevent their transmission from neighbor nodes, which interferes in the MAC layer with transmissions of source packets; on the other hand, not letting a route pass through increases the traffic on nearby alternate routes with similar consequences. We examine through simulation the benefits and harms of selfish behavior with a cross-layer view, in particular relate them to the node density, selfish nodes’ location and behavior details.

In Section II we outline the peculiarities of IEEE 802.11s mesh networks, pointing out those affecting possible motivations of selfish nodes. Section III reports a comparison of available simulation tools to explain the choice of the experimentation method. In Section IV we analyze a number of simulation scenarios in which one or more selfish nodes co-exists with a collection of well-behaving ones, and a selfish node’s strategy consists in actions either in the network- or MAC-layer. Section V concludes the paper.

II. IEEE 802.11S-BASED WIRELESS MESH NETWORK

The emerging new IEEE 802.11s standard [1] describes a particular class of mesh networks [4] (distinct type of multi-hop wireless systems) to which we refer as CWMS. Among the salient characteristics of CWMS are:

• High bandwidth and Quality of Service requirements—the standard describes a broadband network system able to support most modern applications executing in real time.

• Limited node mobility—most nodes can be considered stationary or nomadic; mobility support is not crucial, as it will ordinarily be handled by external mechanisms (e.g., handover in mobile IP or multiple-AP access networks).

• Unlimited node resources—most commonly being powerful desktop/laptop computers, mesh nodes almost never feel constrained by their processing power or memory; also, energy conservation is not a priority for mesh nodes, as they are either permanently connected to mains electricity or have a long-life battery backup.

• Dedicated internetworking devices—it is expected that most traffic in CWMS will be constituted by inter-network flows, so dedicated nodes called mesh portals are made responsible for efficient data transfer between a CWM and outside communication systems.

• Possible presence of centralized network-wide mechanisms—optional parts of the IEEE 802.11s standard assign selected nodes the role of a coordinator (e.g., in the case of tree-based routing to designated mesh portals).
• Dynamically changing node behavior—mesh nodes should be able to quickly adapt to fast-varying traffic conditions in order to utilize network resources economically.

In our experiments we took the above IEEE 802.11s CWM characteristics into consideration when creating network models and traffic patterns for testing. For the sake of clarity, a single-channel network was assumed despite the fact that IEEE 802.11s standard draft allows for multichannel mesh structures. The underlying mechanisms, however, are as yet optional and largely remain unproven.

III. TEST ENVIRONMENT

The most appropriate way to observe mesh node behavior would be to create a testbed environment. This would allow to account for all factors relevant to real-world vendor-specific systems. Unfortunately, the tests that need to be conducted in relation to selfish behavior require a significant number of nodes and a limited-connectivity topology. Such a testbed would be quite difficult to assemble, mainly because of the need to provide nodes with strictly prescribed propagation characteristics to obtain a desired connectivity map.

Well-known methods to perform this task (such as node placement, transmission power control, directional antennas, coaxial cable connections, white noise jamming etc.) are either unreliable or costly, and usually fail to provide a flexibility necessary for testing diverse scenarios.

Faced with the above difficulties we confined ourselves to simulation. Because of the nature of our main question (whether in the real world selfish behavior of a mesh node is beneficial in terms of source throughput), our main concern was high modeling accuracy of PHY- and MAC-layer mechanisms and characteristics. As candidate simulation tools we considered NS-2 [5], JavaSim [6], OMNet++[7] and OPNet [8]. NS-2 was eliminated at an early stage due to significant errors in simulation models relevant to the present research.

An can be seen, the JavaSim environment, despite its modern programming flavor, regrettably lacks a network model library, documentation and analytic support characteristic of OMNet++ and OPNet. The remaining two choices are similar in most respects, but OPNet provides a much richer model library, fit to support even performance planning of real-world systems, and as such allows for highly realistic modeling of our test environment.

It was thus decided to conduct the experiments using the OPNet environment that provides high simulation detail in the PHY and MAC layers.

IV. SIMULATION SCENARIOS

We have created a simulation model of a multihop CWM based on IEEE 802.11g-capable nodes, all working in the same frequency channel within the 2.4 GHz band and with a uniform static unicast transfer rate of 54 Mb/s. Each node has one IEEE 802.11g interface utilizing a 1 mW transmitter and receiver with a −95 dBm sensitivity. These parameters are consistent with the capabilities of real-world WiFi hardware except that the transmitter power had to be significantly reduced in order to produce a multihop topology. In our scenario this amounts to creation of direct wireless links between neighboring nodes, with sporadic cases of moderate quality (significant frame error rate) wireless links across longer distances. To provide route discovery for the network layer, the well-known Dynamic Source Routing (DSR) [9] protocol utilizing HOP metric has been chosen, which tends to provide stable paths in a static environment.

In the following experiments we took advantage of the fact that the most traffic in broadband wireless mesh installations is inter-network. It is forwarded to and from external communication systems by a number of mesh portals, each of which is typically connected to more than one external system. The traffic has therefore many sources scattered all over the mesh topology, but flows towards a limited number of mesh portal nodes. This observation leads to more predictable traffic paths which are expected to make simulation results easier to understand.

We consider a basic network setup of 31 nodes forming a 'multipath' three nodes wide, with a physical span of about 1500 m (Fig. 1); this setup will be modified in successive simulation scenarios. Only adjacent node pairs are assumed within the transmission range of each other. Nodes labeled with the letter S (for source) on the center line of the 'multipath' (comprising 11 nodes) generate a stream of UDP datagrams directed to the leftmost node marked with a distinctive icon and labeled with the letter D (for destination). In such a topology, traffic from the S nodes tends to be forwarded along the center line of nodes constituting the shortest route. At the same time, backup routes are available should any local problems arise, such as node failure or misbehavior, or unacceptable propagation characteristics on certain links.

The data field of each IP datagram has a size of 8 kb, which requires fragmentation at the link layer (as is typical for most real-world IP traffic), yet is small enough to avoid excessive performance degradation due to repeated retransmission in the network layer. The latter can occur in the case of poor wireless link quality, but can also arise when routing IP datagram around selfish nodes, as explained below.

The single selfish node, labeled E (for egoist), adopts a selfish strategy designed to shirk from relaying transit traffic. The strategy consists in unconditional refusal to forward DSR route request (RREQ) messages generated by any other nodes. Such a strategy is more effective than dropping transit traffic along an established route, as the node is considered off-route by all other nodes, hence need not handle incoming traffic. Nevertheless, node E generates its own RREQ messages and replies to RREQ messages addressed to it according to standard, thereby remaining capable of sending and receiving traffic for which it is the source or destination node. This somewhat simplistic model has been devised to illustrate and analyze the effects of mesh node selfishness without being sidetracked by the subtleties of more cunning strategies and the complexity of the network setup.
A. Scenario 1

We first locate the selfish node E as in Fig. 1 i.e., on the shortest route and in a high node density area of the network, where backup paths are available in the immediate neighborhood. Note that node E is located several hops from the destination node D—such a placement allows meaningful assessment of both the impact of node E upon the transit traffic from other source nodes and the gains in source throughput it will obtain by behaving selfishly; note that node E’s source traffic in this case must traverse multiple hops.

The network in this scenario is assumed to operate under saturation load in that the amount of traffic generated by the source nodes S suffices to constantly maintain nonempty send buffers at all nodes on the route.

Fig. 2 compares node E’s instantaneous source throughput (number of successfully transmitted IP datagrams divided by the small observation interval length) to what node E would achieve behaving cooperatively (i.e., correctly participating in DSR routing). Surprisingly, the extra bandwidth gained by refusing to relay transit traffic does not seem to help—in fact, node E’s selfish behavior backfires since it results in the creation of alternate routes passing through the neighboring nodes which therefore carry more transit traffic. As these nodes are located in node E’s interference range, they restrict node E’s access to the transmission medium, preventing any gain in its source throughput. On the contrary, the interference from neighboring nodes actually degrades node E’s source throughput by up to 50% in our scenario. One concludes that a cross-layer view of the effect of selfish behavior might differ significantly from a network-layer one.

Different results are obtained in the case of relatively low network load, here modeled by having only three of the S nodes generate source traffic. In this case, the network traffic is not enough to keep transmit buffers nonempty at all times—there are times when some nodes do not have data to send. As can be seen in Fig. 3, the reduced network load makes selfish behavior in the above described form beneficial in terms of source throughput, due to relatively lower MAC-layer contention overhead from neighboring nodes. In this case, node E’s selfish behavior almost doubles the number of IP datagrams it is able to transmit successfully. Thus we can state another somewhat unorthodox conclusion contrary to the prevailing intuition that selfish behavior generally pays more when the currently available resources are scarce: in our scenario, the less congested alternate routes cause less MAC-layer interference and so make room for a higher node E’s source throughput. Again, this enriched view stems from cross-layer considerations.

B. Scenario 2

In this scenario, depicted in Fig. 4, we have moved the S nodes into the upper line of nodes, as we did node E. Thus, node E is again placed on the most probable shortest route from the S nodes to destination, but this time node E is surrounded by a low node density network area (has fewer neighboring nodes).

Simulation results for the saturation network load scenario are shown in Fig. 5. While they are qualitatively similar to those in Fig. 2, one notices a higher number of node E’s transmitted IP datagrams in the case of both selfish and non-selfish behavior, on account of the lower interference of the few neighboring nodes supposed to handle alternate traffic.

Figure 2. Node E’s source throughput in scenario 1, high network load.

Figure 3. Node E’s source throughput in scenario 1, low network load.

Figure 4. Network setup in scenario 2—selfish node in a low node density network area.

Figure 5. Node E’s source throughput in scenario 2, high network load.
A closer look reveals that the difference between the plots in Fig. 2 and Fig. 5 i.e., between the high and moderate node density around node E, is much smaller (in fact almost none) in the case of node E’s selfish behavior than in the case of non-selfish behavior. In the former case, the heavy alternate traffic interferes with node E’s and it is of little importance whether that traffic is split among two alternate routes in the setup of Fig. 1, or concentrates on one in Fig. 4. In the latter case, the prevailing effect is the reduced amount of interference from the relatively light alternate traffic in Fig. 4, flowing on just one side of node E.

![Figure 6](image6.png)

For a moderate network load (only three of the five source nodes are active), we observe that the non-selfishly behaving node E's achieves a higher number of transmitted IP datagrams than in the case of high surrounding node density—Fig. 6. This is again due to reduced MAC-layer interference. On the other hand, selfish behavior brings no gains here, unlike in the former scenario (Fig. 3); apparently, the fact that now all the alternate traffic uses one route instead of two implies more MAC-layer interference and neutralizes the effect of shedding transit traffic.

C. Scenario 3

In this scenario, depicted in Fig. 7, node E is located in the immediate neighborhood of the destination node D (which in a real CWM would be a mesh portal handling inter-network traffic).

![Figure 7](image7.png)

When behaving non-selfishly, node E node achieves a relatively high source throughput compared to the previous scenarios—Fig. 8. This results from the short (single-hop) route to destination, producing traffic conditions characteristic of a sparse network even though the node density around node E is in fact high. On the other hand, node E’s selfish behavior in this scenario produces the lowest source throughput of all observed before, comparable with the dense network scenario. This could have been expected since the alternate traffic flows now do not compete with each other as much as they did when they had more hops to go to reach node D; hence, node E’s neighbor nodes are more active.

![Figure 8](image8.png)

It turns out that that deactivation of two of the S nodes does not yield a better performance for a selfish node E, as was observed previously—Fig. 9. This stems from the routes converging in the immediate vicinity of node D, which therefore still experiences high-load traffic conditions.

Apart from the latter effect, one can conclude that the placement of node E on the shortest route seems to have little impact on its achieved source throughput; in contrast, node density around node E does make a difference.

![Figure 9](image9.png)

D. Scenario 4

Having tested the impact of a single selfish node, we now extend our simulation scenario to cover multiple selfish nodes. To this end, the network setup was extended by six additional nodes in order to ensure that transit traffic to node D will always have an alternate route. The extended network setup is presented in Fig. 10.

![Figure 10](image10.png)
We have chosen a group of nodes (labeled e) as possibly selfish and run a number of scenarios, each time designating a different subset of the group to use the above described selfish strategy. Node E was assumed to always employ the selfish strategy. As before, we measured node E's instantaneous source throughput (the number of successfully transmitted 8 kb IP datagrams that this node was able to send to the destination node D, divided by the observation time).

Fig. 11 presents the results for all possible subsets of the e nodes behaving selfishly. The distinctive top curve in the figure indicates an all-cooperative scenario where none of the e or E nodes behaves selfishly i.e., all cooperate in DSR routing. Our experiment shows that for no possible locations of the fellow selfish nodes does node E's source throughput exceed that in the all-cooperative scenario. Moreover, in the presence of other selfish nodes, node E's source throughput tends to become highly unstable.

A number of similar experiments show that the presence of other selfish nodes cause momentary surges in node E's source throughput that match—but rarely exceed—that in the all-cooperative scenario; however, the long-run average always remains below all-cooperative. Interestingly, our conclusion implies that even a collusion of several selfish nodes is not much of a worry, since the alternate traffic, as long as it has a way to reach node D, will block node E's traffic nearer node D. This good news is of course due to the peculiar sink-like traffic pattern characteristic of CWMs.

E. Scenario 5

Having analyzed results of simple, but strongly selfish behavior of not participating in DSR routing, we now extend our experiments to an example selfish strategy based on a modification of MAC-layer mechanism parameters. A simple modification of the IEEE 802.11 Distributed Coordination Function (DCF) parameters governing the backoff mechanism [1], namely the minimum contention window $CW_{\text{min}}$ and the maximum contention window $CW_{\text{max}}$, was chosen as the implementation of a selfish MAC-layer attack. In its most aggressive form it has both these values set to 0 i.e., the backoff mechanism is disengaged altogether. Such a backoff attack has been extensively studied before, though mostly in single-hop (WLAN) topologies [10], [11]. However, in a multihop topology, a backoff attack may easily backfire as it prevents the immediate downstream node from passing node E's traffic towards destination. The network setup in Fig. 12 was deliberately chosen to emphasize this point.

To retain communication with node D, node E has to occasionally grant medium access to the neighbor nodes. We assume that it does so by occasionally applying standard $CW_{\text{min}}$ and $CW_{\text{max}}$ values. Thus some of the transit traffic from the right-hand side neighbor will reach node E, which then has a choice of forwarding or dropping it. Apart from this "sophisticated" backoff attack, node E exhibits cooperative layer 3 behavior i.e., participates in DSR routing. Satura tion source traffic at node E is assumed.

As can be seen from Fig. 13, dropping transit traffic combined with the above "sophisticated" backoff attack generally favors node E's source traffic in terms of volume and stability, although standard forwarding may perform better at times due to fewer retransmissions from node E's right-hand side neighbor. Clearly observable changes of node E's throughput can be attributed to a group dropping of data frames from nodes' buffers due to excessive number of retransmissions in heavily loaded network. Such occurrence temporarily reduces intensity of transit traffic, allowing node E to archive temporary boost of its throughput. In our test setup, this effect has been consistent during multiple simulation runs.

This preliminary study shows that MAC-layer selfish attacks are potentially beneficial, especially because the unlimited energy resources of a CWM node justify the increased frame transmission rate with the backoff mechanism disengaged.

Tests in more complex network setups show that topology has little impact on the above results, as the attack only affects traffic streams forwarded through the E node and its immediate neighborhood. Moreover, with protocols and metrics discussed in this paper, the attack does not result in data
patch change, until node E limits transit traffic in such degree, that the patch is considered broken. A new patch is selected than and the scenario gets very similar to already discussed case of node E not participating in routing process – there is however a brief instability phase, between choosing a route thorough node E and its change to an alternate one.

V. CONCLUSION

We have studied the effects of selfish node behavior in community wireless mesh networks (CWMs). Node selfishness is assumed to manifest itself primarily as refusal to forward RREQ message of DSR routing, hence avoiding handling transit traffic; MAC-layer attacks consisting in disengaging the backoff mechanism was also considered. Cross-layer insight, taking account of MAC-layer interference resulting from alternate routing, suggest that the benefits of selfish behavior are not obvious if a node's energy consumption is not a primary consideration. This stands in contrast with MANETs, where selfishness is always justified and has to be coped with using costly reputation schemes. A number of specific conclusions have been drawn, linking the benefits from node selfishness to the node location relative to the destination, node density around the selfish node, traffic load, the nature of selfish attacks, as well as the presence and location of other selfish nodes.

Future research should take a more systematic approach to cross-layer effects of node selfishness and extend the present study to various CWM topologies and perhaps more sophisticated node attacks, combining selfishness in more than one layer. Scenarios where selfishness did pay, notably moderate network load and MAC-layer attacks, deserve particular attention. The fact that in a realistic scenario 4, collusion among selfish nodes turned out pointless encourages further investigation to establish the presence or absence of incentives for collusion in more general settings.

ACKNOWLEDGMENT

Effort sponsored by the Air Force Office of Scientific Research, Air Force Material Command, USAF, Grant FA8655-08-1-3018, supported in part by the Ministry of Science and Higher Education, Poland, Grant PBZ-MNiSW-02/II/2007

REFERENCES