Making ad hoc networking a reality: problems and solutions

Stefan Bouckaert, Dries Naudts, Ingrid Moerman, and Piet Demeester

Abstract—Despite the fact that many electronic devices are equipped with wireless interfaces and numerous publications on wireless ad hoc and mesh networking exist, these networks are seldom used in everyday life. A possible explanation is the fact that only few of the numerous theoretically promising proposals lead to practical solutions on real systems. Currently, wireless network design is mostly approached from a purely theoretical angle. In this paper, common theoretical assumptions are challenged and disproven, and key problems that are faced when putting theory to practice are determined by experiment. We show how these problems can be mitigated, and motivate why a heterogeneous hierarchical wireless mesh architecture, and a multidisciplinary research approach can help in making wireless ad hoc networking a reality.

Keywords— wireless ad hoc, wireless mesh, experiments, interference, implementation, hierarchical heterogeneous architecture.

1. Introduction

Ad hoc networks have been the subject of international research for over thirty years [1]. Since the initial work on the packet radio network (PRNet) in 1972 [2], computer networks have evolved from small-scale initiatives connecting a few geographically separated sites, into a worldwide broadband communication network. Research interest in wireless packet radio networks initially came from the military. Since the mid-1980s, lots of civil applications for wireless ad hoc networks have been studied, such as emergency communication for public services or communication in disaster areas. In the late 1990s, wireless enabled hardware became cheap and omnipresent, and with the foundation of the MANET (mobile ad hoc networks) Working Group [3], the Internet Engineering Task Force (IETF) started standardization efforts for routing protocols supporting mobile wireless networks.

Countless publications exist covering numerous research topics such as wireless ad hoc, mesh, or sensor networks, studying aspects at all layers of the open system interconnection (OSI) stack. In spite of all these research efforts, wireless ad hoc networks are rarely used in everyday life. How can this contrast be explained, even though lots of scenarios exist that could benefit from ad hoc technology?

In [4], the authors answer this question by suggesting that most ad hoc network design focuses on military or specialized civilian applications, making the solutions impractical for everyday life. This is an important observation, however, this paper addresses other, perhaps more fundamental problems. We feel that a lot of research gets stuck in a cru-

cial phase of development: while there are a massive number of initiatives to design wireless ad hoc solutions, few ideas are implemented on actual systems. Unfortunately, as promising as some ideas may be, they do not always lead to good or practical solutions. Using a purely theoretical top-down approach where implementation is the last step in designing wireless network protocols, architectural decisions are often made which, after months of research, turn out to be impossible to realize because of unforeseen implementation problems.

Wireless research focused on single-interface homogeneous ad hoc networks for a long time. Recently, an evolution in wireless networking research is observed, where researchers start focusing on multiple interface nodes in mesh topologies. Additionally, several aspects of cross-layer research, such as power control, are gaining popularity. While there is a growing awareness within the research community that simulation of protocols might not be sufficient in order to validate the stable operation of wireless networking protocols [5, 6], a lot of assumptions are still made while studying old and new topics in wireless research.

In Section 2 of this paper, we will verify the validity of common assumptions by experiments, and formulate lessons learned during the evaluation of several experimental set-ups and real life implementations using IEEE 802.11 hardware. While some findings may be trivial to people who are familiar with the physical layer of wireless networks, we believe that it is important to show wireless protocol designers the incorrectness of many assumptions, as they can be a major contributor to the slow adoption of ad hoc technology. We are aware of the fact that some problems are vendor specific and that, strictly spoken, it is not the task of people performing research at the higher layers of the OSI stack to actually solve hardware problems. However, we feel that a careful choice of research methodology and network architecture can severely reduce the observed problems. In Section 3, we discuss how heterogeneous hierarchical architectures can help the successful realization of ad hoc networks, and how wireless protocol research can benefit from a close cooperation between research groups working at the physical layer and research groups working at higher network layers.

2. Observations and experiments

When collecting data from test set-ups using any wireless driver, one should always keep in mind that the driver could be causing errors at a node. We have tried, to the extent

possible, to exclude driver-caused errors from the observations below. The observations follow from several real-life experiments and test-beds, using a broad range of hardware. A first test-bed consists of 18 Linux nodes, equipped with D-Link AG520 wireless a/b/g peripherial component interconnect (PCI) cards and external antennas. In addition, a lot of research on mesh networks at our research lab is done using modified 4G meshcubes with up to 4 wireless mini-PCI a/b/g cards per node. Other tests are performed using Linksys WRT54GL wireless routers with modified firmware. All devices can be powered using batteries, allowing to test real mobility.

2.1. Single frequency, single hop networking

Assumption. *In an isolated situation, an IEEE 802.11 wireless link between two nodes will be of better quality if transmission power is increased.*

Observation. Consider a test set-up from Fig. 1, where three identical network nodes, each equipped with a single wireless network interface are stacked on top of each other in a rack. The external antennas are positioned in a triangle, the antennas separated about 1.5 m. Although at some times data can be sent at the theoretical speed limit, results are very unpredictable. Even if a link seems to be stable for a certain period of time, data rates can drop below one third of the stable rate, seemingly without a reason. In addition, links are not always symmetrical: changing the direction of the traffic flow can result in degraded throughput.
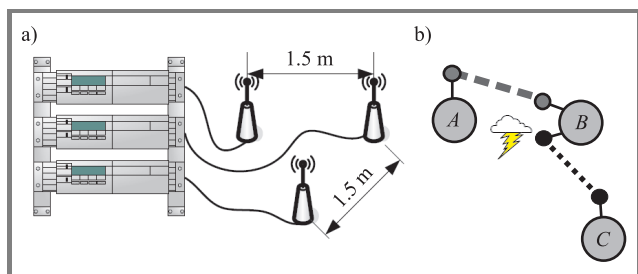

Fig. 1. (a) Test set-up using rack mount devices; (b) simple two-hop test. Node *B* has two wireless interfaces.

In this specific setup, one solution seems to solve most of these problems. *Reducing* the transmit power of the wireless cards results in highly increased stability. In this case, a transmit power of 10 mW gives the best results.

Experiment. When putting single interface meshcubes to test in an RF-shielded box [7], the same observation is made in a controlled environment: reducing power when sender and transmitter are at close distances, increases networking quality.

Placing the antennas relatively close to each other, as in this case, might seem artificial – there are however several situations imaginable where two single interface nodes are placed at comparable distances: e.g., a user can carry a wireless-enabled personal digital assistant (PDA) and a laptop, or, during meetings, there is a high laptop density.

2.2. Multiple frequencies, multihop networking

Assumption. *When configuring the different wireless interfaces of a multi-interface integrated node to theoretically non-overlapping channels, these different links will not interfere. Capacity of a wireless network can be increased dramatically by adding multiple interfaces.*

Observation. Reading through literature, lots of innovative solutions involving wireless networking can be found, and numerous protocols are designed to support systems with multiple network interfaces [8, 9]. Many of these solutions are based on the assumption that multiple theoretically non-interfering channels can be operated simultaneously at a node's different interfaces. This seems obvious when considering theory and simulations. Unfortunately, when these solutions are deployed in a test-bed, it turns out that this assumption is not necessarily true.

When a two-hop path is created using a traditional single-interface approach, the wireless medium has to be shared between two links. The maximum reachable throughput of the total path thus roughly halves because of a single additional hop. Adding a second wireless interface to the middle node and choosing orthogonal frequencies for the first and second link (cf. Fig. 1b) solves this problem, in theory, at the cost of adding a single extra interface. In practice, different results can be observed: even when two interfaces are available at the middle node and a two-hop path is constructed using two theoretically non-overlapping frequencies, the throughput does not rise considerably.

Still, in theory, devices supporting the IEEE 802.11b and IEEE 802.11g (802.11a) standard should be able to use, depending on the region, three (twelve) fully non-overlapping frequencies. Recently, other researchers described the same effects and concluded that wireless nodes with multiple interfaces can suffer severely from self-generated interference between the different interfaces [10, 11].

Experiment. Measurements done at our lab (cf. Fig. 2) show that these effects of self-generated interference can be severely reduced by limiting the transmit power used at the different interfaces and physically separating the antennas of a node. On the other hand, these results also reveal the sad truth that – at least when using off the shelf hardware – a single wireless interface using high transmit power can severely degrade the performance of the other interfaces and surrounding nodes, even when they are set to operate on non-overlapping channels.

When using integrated IEEE 802.11a devices such as the meshcubes in a two-hop test, interference problems are still observed, even when lowering transmit power. The first and second link can be set up separately on orthogonal channels with a goodput of over 30 Mbit/s. However, if both links are used at the same time in a multihop configuration, the goodput drops to about 16 Mbit/s even though the processor of the middle node can handle the packet forwarding.
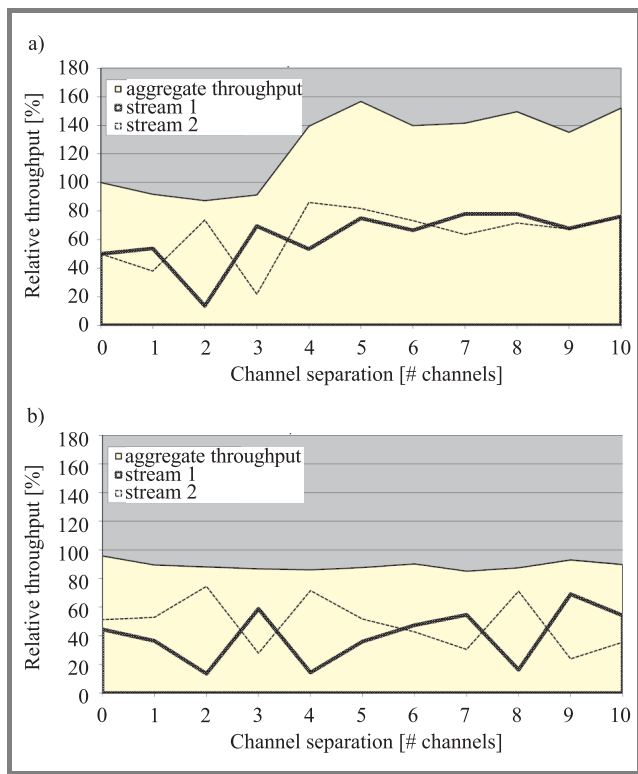
Fig. 2. Throughput measurement. Using two distant groups of two, 1.5 m separated, ethernet-linked WRT54GL routers – representing two nodes with two interfaces each, two connections are set up in parallel. The *Y* axis shows the throughput, relative to the maximum throughput of a single, non-interfered stream. Output power (a) 1 mW and (b) 100 mW.

We have found that in this case, the problem is essentially due to the fact that the meshcubes are densely integrated: it's not only the fact that two mini-PCI cards are located right on top of each other that causes problems, but especially the fact that the distance between the antennas is too small. This is not surprising: the antennas in the integrated devices are located very close to each other. At a frequency of 5 GHz, the wavelength used for transmission is about 6 cm, thus in our integrated devices, up to 4 antennas are separated by less than a single wavelength, resulting in a very unpredictable system. Increasing the distance between two antennas to about 15 cm alleviates this intra-node interference and goodput rises considerably. In [10], the authors conclude that these interference effects can be solved by providing an antenna separation of 35 dB. However, this separation is hard or even impossible to obtain in mobile devices with a small form factor.

Figure 3 shows additional measurements using WRT54GL routers at a transmission power of 1 mW, quantifying the effect of antenna distance on interference between two non-overlapping IEEE 802.11g channels: channel 1 and 11. In scenario of Fig. 3a, two separate user datagram protocol (UDP) streams (starting at 30 Mbit/s, decreasing the bit rate until packet loss is minimal) with a UDP packet size of 1470 bytes are set up, sequential at first, then simultaneous. The graphs show the resultant sum of the average

throughput observed at the receiving interfaces. The individual throughput is not shown on the graph, as bandwidth is equally divided between the two flows. The figure shows that the sum of throughputs is reduced by 16.8% when the flows are set up simultaneously with a distance *d* of 1 m between the antennas. At a distance of 5 cm, throughput is reduced by over 45% compared to non simultaneous transmission. The sum of throughputs reduces both in the sequential and parallel tests when the antenna distance is decreased.
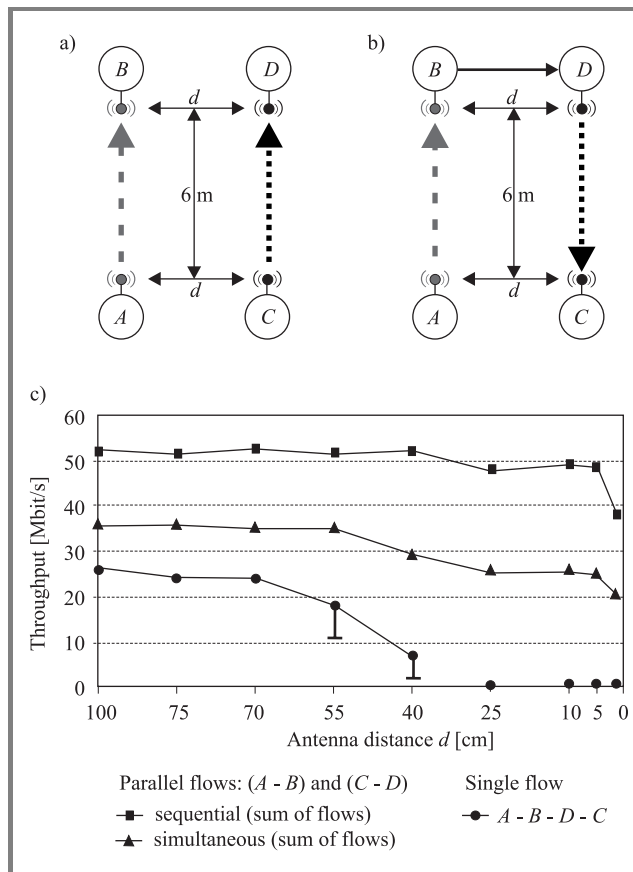

Fig. 3. Two scenarios quantifying the effect of the antenna distance on throughput: (a) parallel flows; (b) single flow. Link *A-B* operates on channel 1, link *C-D* on channel 11; (c) measurements at $d = 1$ cm, 5 cm, 10 cm $+ k \cdot 15$ cm, $k = 0 \dots 6$. Transmission power = 1 mW.

In scenario of Fig. 3b, a single UDP stream with the same characteristics is set up. The test packets are now transferred over wire between interface *B* and *D*, recreating a typical multihop situation where every receiving interface has a sending interface nearby. Looking at the graph with the triangles, a first observation is that the end-to-end throughput is higher than half the aggregate throughput from scenario of Fig. 3a, for antenna distances *d* larger than 55 cm: the single flow is transferred more efficiently than two traffic flows originating separately. However, performance drops faster with the decrease of antenna distance. It is also observed that unlike in the previous situation, throughput is very unstable when the antennas are moved

more closely to each other: moving the antennas slightly can result in a serious performance drop or increase. For this reason, the graph with the triangles shows the maximum values that were obtained from a large amounts of tests. Minimum throughput results are shown with error bars. When the distance between antennas drops below about 40 cm, communication at reasonable throughputs is no longer possible. It is clear that the consequences of interference between neighboring interfaces with nearby antennas are worse in scenario of Fig. 3b than in scenario of Fig. 3a. The receiving interfaces are disturbed by a signal of the nearby transmitter, even though it is sending on a non-overlapping channel, rendering successful reception of the UDP test packets impossible. Note that in both situations, IEEE 802.11 acknowledgement (ACK) messages are sent in the opposite direction of the UDP flows. However, these small packets suffer less from the interference of neighboring interfaces.

This observation raises questions about using multiple interfaces in integrated devices: even if perfect algorithms for using multiple interfaces on devices can be thought of and simulated, it is very likely that the result will not be as expected when deploying them in real integrated systems. We also believe that a test-bed with "full size" computers and wireless PCI cards with external antennas, can not fully represent an integrated end-user device with multiple interfaces.

2.3. Power adaptation

From previous paragraphs, we have learned, that changing power levels can lead to a more reliable link, but increasing transmit power does not necessarily increase communication quality. Furthermore, it was shown that theoretically non-interfering channels will interfere when using off-the-shelf hardware at mid to high transmit power, and that integrated systems with multiple interfaces will suffer from self-generated interference if there is no adequate antenna separation. Consequently, a single device transmitting at a relatively high output power may render all surrounding communication virtually impossible.

Lowering transmission power is often considered as a measure of freedom, in order to decrease interference and thus increase the number of possible simultaneous transmissions in a certain area, or to increase the lifetime of battery powered devices [12]. Our experience shows that when using today's IEEE 802.11 hardware as a base for multi-interface nodes, power adaptation is not a measure of freedom but rather a necessity in order to guarantee network operation. End-user hardware can (and probably will) improve in quality over time, however, we predict that it is very unlikely that in the near future palm-size systems will be able to fully take advantage of using multiple interfaces at relatively high output powers, if the interfaces are tuned to neighboring channels. As frequency regulations only allow a small part of the spectrum to be used for unlicensed civilian WLAN communication, it is not easy to provide the required channel separation. When using only two in-

terfaces, putting one interface in the 2.4 GHz range and the other one in the 5 GHz might turn out effective with some types of hardware, but it is a mere palliative as this solution can currently not be scaled.

2.4. Hardware issues

Assumption. *If an algorithm works on the IEEE 802.11 hardware of vendor A, it will work on the IEEE 802.11 hardware of vendor B.*

A recurring problem faced during tests with hardware from different vendors, is that changing an interface to some specific channels can result in a wireless link of bad quality. As communicating on those channels is possible using hardware from a different vendor, and bad channels stay bad when replacing hardware with an identical spare, the problem is most likely hardware related.

In general, there is a big difference in stability and performance between hardware from different vendors. In Fig. 4,
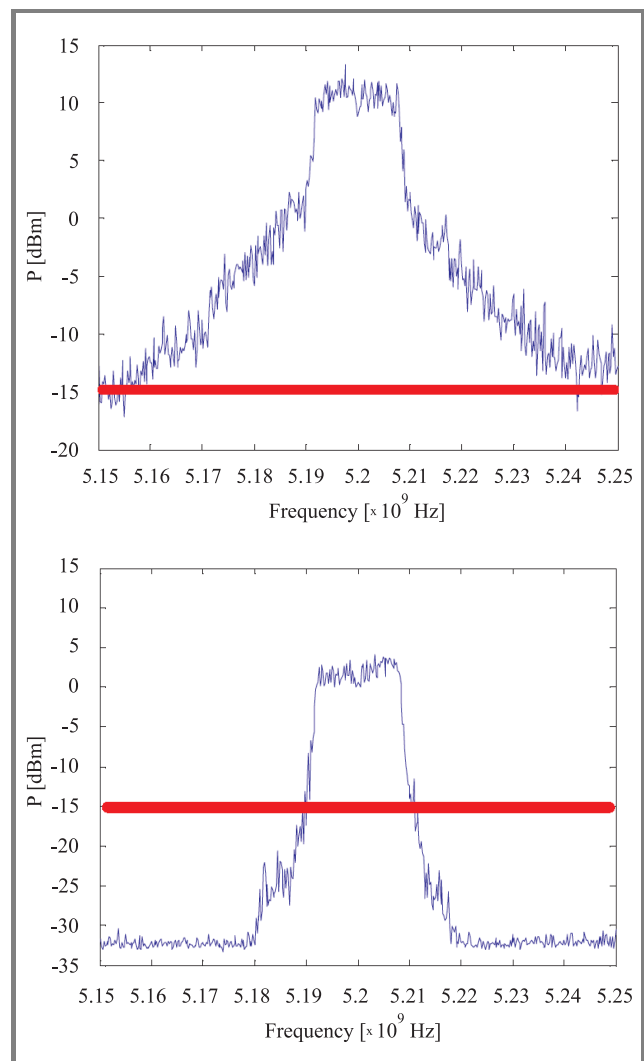

Fig. 4. Spectrum measurements of two different IEEE 802.11a mini-PCI cards operating at same transmission power (15 dBm), both using channel 40.

the spectrum of two mini-PCI cards from different vendors, operated at the same power level and frequency are shown. The figure clearly shows that the second card has a better spectral purity than the first card. Consequently, when building a test-bed with hardware of the first type, test results will be much more pessimistic than test results with hardware from the second vendor, especially when operating at multiple theoretically non-interfering frequencies.

In another test set-up, the maximum throughput of a single non-interfered UDP stream between two identical retail IEEE 802.11 mini-PCI network interfaces, installed at two identical network nodes was measured. The network nodes were separated by 20 m, with a wall in the middle. The same measurements were repeated several times, each time replacing the mini-PCI adapters with hardware from a different vendor. During all tests, the multiband Atheros driver for wifi [13] was used. The performance difference between cards of different vendors can clearly be seen from Fig. 5. Note that the adapters are all about equally expensive.
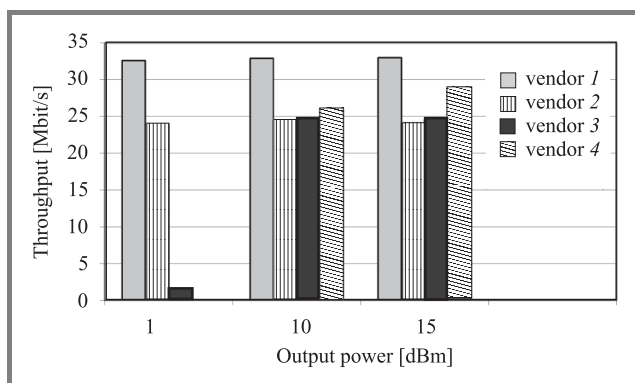

Fig. 5. Throughput measurements on a single unidirectional non-interfered IEEE 802.11a link, using hardware from different vendors, at three discrete power settings.

Although these problems can be solved by replacing faulty hardware with hardware from a different vendor, ad hoc networking protocols will only become successful if a large group of end users can use them instantly without problems, regardless of their choice of vendor. Unfortunately, in a traditional ad hoc network where nodes can join freely, it is wrong to assume that all nodes will react identically to a specific algorithm's action. For example, if a certain algorithm would reduce transmission power of a node to 1 dBm, the algorithm might operate as expected on hardware from vendor *1* or *2*, but fail to work on hardware from vendor *3* or *4*. If the quality of the hardware cannot be guaranteed, control loops should be provided within algorithms to verify whether a certain action has the desired effect. These effects are very hard to model in a simulator and can only be discovered by putting algorithms to test on real-life test-beds.

2.5. A lab environment is not a real environment

Assumption. *If it works in simulation, it will work on a test-bed. If it works on a test-bed, it will work in real life.*

From previous paragraphs, it is clear that designing algorithms and protocols for wireless systems should preferably not be done solely by considering theory or simulations. Creating a wireless test environment in a laboratory is not an easy task. Not only does it require a lot of – sometimes costly – hardware and space, it is also time consuming. On the other hand, creating these test environments and implementing developed algorithms on actual hardware forces the researcher to develop a system close to reality.

However, there is always a risk that the testing environment itself will lose its value as "real test case", as over time wireless systems could be tuned – unintentionally – to work great in the testing environment only. This way, a solution that evaluates positive in a testing environment can at the same time be useless when deployed in an uncontrolled real-life situation. This is a frustrating experience that was witnessed before at our lab: a demonstrator to transmit video over a self-forming and self-recovering multihop mesh/relay network was developed. After the demonstrator had proved to be working perfectly in the lab environment – even when moving the battery fed relay stations through the building – it was taken to a large hangar. Surprisingly, even with relatively short distances between the relaying hardware, and with line of sight communication, link breaks occurred frequently and maximum throughput was low. In this case, the set-up probably suffered from the absence of the waveguide effect described in [14]: there are circumstances where a wireless signal does not degrade as fast when using devices indoor, compared to using them in an open space.

This example, amongst others, shows that a system should not be declared stable based on a single test environment, and certainly not based on simulations. We believe that wireless ad hoc networking protocols and systems will only be used in everyday life if their use is not limited to a specific scenario or environment. However, today, a lot of algorithms are evaluated only in simulators using a very specific test scenario and very simplified propagation models, which are not valid in real-life environment, in particular indoor environments.

3. Solving issues

In the previous section, it was shown how hardware issues hamper successful realization of ad hoc networks. Subsection 3.1 points out which architectural choices can help to reduce the observed hardware problems, and, more specifically, explains why a heterogeneous hierarchical architecture avoids several of the described problems. Finally, Subsection 3.2 discusses how the inheritance of layered network design still impedes the development of algorithms

for wireless networks today, and how a multidisciplinary research approach can help in developing more robust solutions.

3.1. A heterogeneous hierarchical architecture

Section 2 listed many problems that can be observed while bringing wireless ad hoc and mesh networking algorithms to real systems. Some of these problems are vendor related and can be solved by replacing defective hardware. One might argue that it is not the task of networking algorithms to account for these problems. However, it is inherent to the nature of wireless ad hoc networks that low-quality nodes will sooner or later join the network. Wireless systems will always be more unreliable than their wired counterparts, and therefore, algorithms must be able to detect anomalies and react accordingly.

Firstly, because of interference and hardware related issues, the choice for a specific channel has an impact on the wireless link quality. Problems occur at various layers of the protocol stack when wireless links break due to changing channel conditions or failing hardware.

Secondly, transmission power should be chosen wisely: neither too low nor too high. While in a static set-up, transmission power can be set manually by trial and error, there is need for automatic tuning in dynamic environments. Cross-layer protocols might provide a way to implement these control loops.

Thirdly, it was shown that small devices with multiple interfaces suffer from self-generated interference. In order to overcome this problem we should focus our research on an architecture which takes this fact into consideration. An algorithm which presupposes a complete separation between multiple interfaces at end-user nodes will most likely never be able to achieve its claimed results when used in real systems.

In a heterogeneous architecture, devices have distinct capabilities and technologies. In a hierarchical architecture, different nodes can belong to different logical groups, for example, backbone nodes and clients. Heterogeneous hierarchical architectures (Fig. 6) have been described in the past, however, we believe that their true potential has not been discovered yet. In [15], the authors describe a (hybrid) wireless mesh architecture. In a wireless mesh network (WMN), two types of nodes are distinguished: mesh routers and mesh clients. Mesh routers hold superior properties concerning processing power, interfaces, available power and memory, enabling them to perform more complex functions. In addition, they have limited mobility compared to the clients, resulting in a wireless mesh backbone. Mesh routers can be added or removed at any time and act as gateways to other networks such as the Internet. In a *hybrid* WMN, mesh clients can connect to the backbone network either directly, or by using a multi hop path through other clients.

Some benefits of heterogeneous hierarchical networks have been described in the past, such as an increase in coverage,
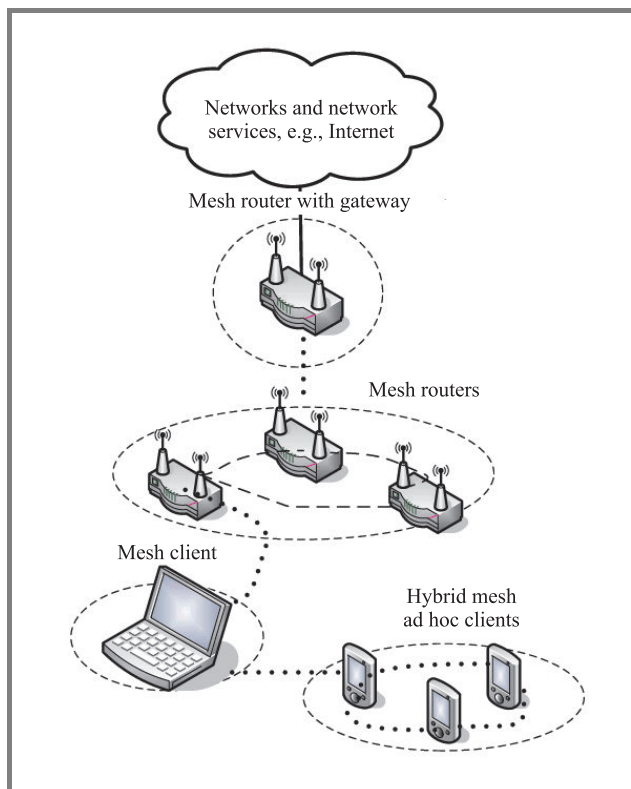

Fig. 6. Heterogeneous hierarchical mesh network, i.e., a hybrid wireless mesh ad hoc network. Clients connect either directly or through another client to a mesh backbone.

or the (theoretical) ease of set-up. However, we believe that there are more reasons why hierarchical heterogeneous architectures can help to realize robust wireless networks, and that a conscientious choice of networking architecture can help certain assumptions that are invalid for homogeneous wireless networks become valid.

Most small and mobile end user devices such as PDAs or smartphones will probably only have a single (high speed) wireless network interface, using the unlicensed bands, enabled at a time, as adding interfaces is suboptimal due to the described interference problems and other limitations such as power and cost. On the other hand, the mesh routers in the backbone can and should have multiple interfaces: they can be bigger in size and antennas can adequately be separated, thereby reducing the interference problems. Additionally, they have an "unlimited" power supply as they are most likely connected to a host system with plenty of power such as a building or a truck.

Faulty hardware may be used within a cooperative wireless network, resulting in decreased performance and satisfaction for the end-users. In a traditional ad hoc network, even if one user invests in high-quality hardware, he can still experience bad performance if the person he is connecting through uses faulty hardware. In a heterogeneous architecture, end users can, e.g., connect to a mesh backbone which is constructed with hardware of better quality. The nodes which are higher in the hierarchy can be more expensive, as less nodes of higher hierarchy are needed.

In a hierarchical network architecture, operators can invest in high quality wireless backbone nodes. In addition to increasing the number of interfaces, more expensive network nodes could also use alternative technologies such as WiMAX. By using more interfaces or better technologies at higher hierarchical layers, wireless networks become more scalable, as throughput and transmission range can increase with every hierarchical level. Ideally, the technologies which are used at a higher layer can operate in other (licensed) frequency ranges, reducing the interference even more.

Changing protocols or interface configuration on all end user devices, constructed by different vendors, is harder to achieve than making changes to a smaller group of devices at a higher hierarchical layer, all the more since it is more likely that wireless devices at a higher hierarchical layer are controlled by a single administrator. For example, multi-interface wireless IEEE 802.11a backbone routers with (proprietary) cross-layer optimizations can easily provide wireless coverage within a building, or at a fair or festival. By adding an extra wireless interface to every backbone router, configured as an IEEE 802.11g access point, end users are able to connect to this backbone with hardware from any vendor, without compromising the quality of the backbone network. If a user has the right hardware and chooses to function as a relaying node and extend the network, he can do this by voluntarily installing the required protocols.

3.2. The need for cooperation

For years, researchers strictly followed a layered approach when designing networking protocols. When adopting a layered network design, different network layers can be optimized separately, and researchers optimizing a certain layer do not need to know the implementation details or exact operation of the adjoining layers.

As a logical consequence of a layered network design, most network research groups historically specialized in either (one of the) upper layers of the network stack, or in the physical layer. The same can be said about wireless research groups in particular, where people developing upper layer protocols, mostly have to rely on simulators to model the behavior of the physical layer. In order to decrease complexity and to ensure a reasonable simulation time, the physical models of these network simulators typically make abstraction of several complex electromagnetic phenomena.

In fixed networks, the layered approach has most certainly contributed to the Internet as we know it today. Inspired by this success, traditional MANET protocol research also followed the layered paradigm. More recently, driven by the continuous search for increased reliability and performance, several authors pointed out how wireless networks can benefit from exchanging parameters between different network layers [16, 17], and researchers started exploring the use of multi-interface nodes and modified physical layers.

The conceptual exploration of new wireless research fields by people originally involved in higher layers only has accelerated so fast, that it is sometimes forgotten that the physical layer models of most of the popular network simulators, such as ns-2 [18], were never designed to model the complex effects that come with these new research topics. For example, the same network simulators are now used to, among other things, simulate the use of multi-interface network nodes or cross-layer parameter exchange. Even if research groups working at the physical layer are aware of the extremely complex interference behavior of multiple antennas placed in each others vicinity, this wisdom seldom makes it to people designing upper layer protocols and architectures, because of the historical separation between research groups.

In our view, and from our experience, a lot of problems which are faced when implementing ad hoc and mesh network protocols cannot be explained solely by studying the upper network layers. The historical layered approach, allowed physical layer and upper layer research groups to work separately. However, as the border between physical layer and upper layers becomes faint at a conceptual level, the need to start or tighten interdisciplinary cooperation between lower and upper layer research groups has never been higher.

4. Conclusion

In this paper, assumptions that are commonly made when researching wireless ad hoc networking protocols were challenged. It was shown that, whether installing a single interface or multiple wireless interfaces at a node, real-life performance is always worse than can be expected from theoretical models or simulations. We raised questions about the usefulness of embedding multiple interfaces of the same type in a palm-size device, and argued that, in contrast to what is believed in many research papers, adjusting transmission power is not a measure of freedom but a necessity. We described how a choice of hardware affects the efficiency of algorithms, and how this influences the stability of wireless networks.

In order to test the robustness of algorithms, testing on one or multiple test-beds is a necessity. However, one must keep in mind that positive test-bed results do not always imply a stable system under all circumstances. Next, we argued that a heterogeneous hierarchical wireless mesh network architecture can help solving the observed problems, by reducing the need for miniaturization and providing incentives for network operators and businesses. Finally, we argued that an effective cooperation between research groups working at physical layer and working at higher protocol layers might help in avoiding many of the described problems. We believe that, if protocols are developed closer to reality, and more realistic architectural choices are made at the start of a design process, the usability of ad hoc and mesh networks can drastically be improved.

Acknowledgements

References

[1] C. E. Perkins, *Ad Hoc Networking*. Boston: Addison-Wesley Longman, 2001.

[2] R. E. Kahn, S. A. Gronemeyer, J. Burchfiel, and R. C. Kunzelman, "Advances in packet ratio technology", *Proc. IEEE*, vol. 66, no. 11, pp. 1468–1496, 1978.

[3] MANET Working Group,
http://www.ietf.org/html.charters/manet-charter.html

[4] R. Bruno, M. Conti, and E. Gregori, "Mesh networks: commodity multihop ad hoc networks", *IEEE Commun. Mag.*, pp. 123–131, March 2005.

[5] C. F. Tschudin, P. Gunningberg, H. Lundgren, and E. Nordström, "Lessons from experimental manet research", *Ad Hoc Netw.*, vol. 3, no. 2, pp. 221–233, 2005.

[6] P. De, A. Raniwala, S. Sharma, and T. Chiueh, "MiNT: a miniaturized network testbed for mobile wireless research", in *INFOCOM 2005, 24th Ann. Joint Conf. IEEE ComSoc., Proc. IEEE*, Miami, USA, 2005, vol. 4, pp. 2731–2742.

[7] Qosmotec. Air interface simulator, http://www.qosmotec.com/

[8] J. Tang, G. Xue, and W. Zhang, "Interference-aware topology control and QoS routing in multi-channel wireless mesh networks", in *Proc. 6th ACM Int. Symp. Mob. Ad Hoc Netw. Comp.*, Urbana-Champaign, USA, 2005, pp. 68–77.

[9] P. Kyasanur and N. H. Vaidya, "Routing and interface assignment in multi-channel multi-interface wireless networks", in *Wirel. Commun. Netw. Conf. 2005*, New Orleans, USA, 2005, vol. 4, pp. 2051–2056.

[10] J. Robinson, K. Papagiannaki, C. Diot, X. Guo, and L. Krishnamurthy, "Experimenting with a multi-radio mesh networking testbed", in *WiNMee 1st Worksh. Wirel. Netw. Measur.*, Riva Del Garda, Italy, 2005.

[11] W. Vandenberghe, K. Lamont, I. Moerman, and P. Demeester, "Connection management over an Ethernet based wireless mesh network", in *WRECOM Wirel. Rur. Emerg. Commun. Conf.*, Rome, Italy, 2007.

[12] E.-S. Jung and N. H. Vaidya, "Power aware routing using power control in ad hoc networks", Tech. Rep., CSL, University of Illinois, Urbana, Febr. 2005.

[13] Multiband Atheros driver for wifi, http://madwifi.org/

[14] D. Lu and D. Rutledge, "Investigation of indoor radio channels from 2.4 GHz to 24 GHz", in *IEEE Anten. Propag. Soc. Int. Symp.*, Columbus, USA, 2003, pp. 134–137.

[15] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey", *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, 2005.

[16] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges", *Ad Hoc Netw.*, vol. 1, no. 1, pp. 13–64, 2003.

[17] C. Verikoukis, L. Alonso, and T. Giamalis, "Cross-layer optimization for wireless systems: a European research key challenge", *Glob. Commun. Newslett.*, pp. 1–3, July 2005.

[18] NS2. The network simulator, http://www.isi.edu/nsnam/ns

Stefan Bouckaert received the Masters degree in electrotechnical engineering from the University of Ghent, Gent, Belgium, in 2005. In August 2005, he joined the INTEC Broadband Communications Networks Group at the same university, where he is currently working as a doctoral researcher. His Ph.D. research includes the design and implementation of a cross-layer framework for wireless mesh networks. His main research interests are in wireless mesh networks and cross-layer optimized dynamic channel selection protocols.
e-mail: Stefan.Bouckaert@intec.ugent.be
IBCN – Department of Information Technology
Ghent University
Gaston Crommenlaan 8 bus 201 – B-9050 Gent, Belgium

Dries Naudts received the Masters degree in computer science from the University of Ghent, Gent, Belgium, in 2001. In April 2005, he joined the INTEC Broadband Communication Networks Group, where he is currently working as a researcher. He is currently involved in the research on broadband mobile and wireless communication. His main research interest are in ad hoc and mesh networking and focuses on the development of routing protocols and monitoring algorithms.
e-mail: Dries.Naudts@intec.ugent.be
IBCN – Department of Information Technology
Ghent University
Gaston Crommenlaan 8 bus 201 – B-9050 Gent, Belgium

Ingrid Moerman received the Masters degree in electrotechnical engineering and the Ph.D. degree from the Ghent University, Gent, Belgium, in 1987 and 1992, respectively. Since 2000, she is a part-time Professor at Ghent University. In 2006 she also joined IBBT, where she is coordinating several interdisciplinary research projects. She is currently involved in the research and education on broadband mobile and wireless communication networks. Her main research interests are: wireless broadband networks for fast moving users, mobile ad hoc networks, interaction between ad hoc and infrastructure networks, personal networks, body area networks, sensor and control networks, wireless mesh networks, fixed

mobile convergence, protocol boosting on wireless links and QoS support.

e-mail: Ingrid.Moerman@intec.ugent.be
IBCN – Department of Information Technology
Ghent University
Gaston Crommenlaan 8 bus 201 – B-9050 Gent, Belgium

Piet Demeester received the Masters degree in electro-technical engineering and the Ph.D. degree from the Ghent University, Gent, Belgium, in 1984 and 1988, respectively. In 1992 he started a new research activity on broadband communication networks resulting in the IBCN-Group (INTEC Broadband Communications Network Research Group). Since 1993 he became Professor at the Ghent University where he is responsible for the research and education on communication networks. The research activities cover various communication networks (IP, ATM, SDH, WDM, access, active, mobile), including network planning, network and service management, telecom software, internetworking, network protocols for QoS support, etc. He is author of more than 300 publications in the area of network design, optimization and management. He is member of the editorial board of several international journals and has been member of several technical program committees (ECOC, OFC, DRCN, ICCCN, IZS).

e-mail: Piet.Demeester@intec.ugent.be
IBCN – Department of Information Technology
Ghent University
Gaston Crommenlaan 8 bus 201 – B-9050 Gent, Belgium