2.2.2.4. IP4 - Self-organized networking

2.2.2.4.1. IP description, goals

The goal of this project is to investigate fundamental mechanisms of networking in self-organized wireless networks. As such, the purpose is to devise appropriate protocols at the MAC, network, and transport layer, which are able to cope with the wireless and mobile characteristics of the network. A second dimension consists in taking into account the characteristics of the device, and in particular to identify solutions that minimize power consumption. A third dimension consists in thwarting possible greedy and malicious behaviors in such networks. By its nature, IP4 is at the core of MICS, as it interfaces with distributed computing, security, technology and, of course, the physical layer.

2.2.2.4.2. Description of research topics

A. Self-organization / cooperation issues at the network layer in multi-hop networks

We are currently studying two aspects of cooperation in wireless multi-hop networks.

A.1. Incentives for packet forwarding in multi-hop networks
Naouel Ben Salem, Mark Felegyhazi, Jean-Pierre Hubaux

In multi-hop networks, nodes need to cooperate to perform the packet forwarding operation. In [MartiGLB:00], Marti et al. propose a *watchdog* mechanism to identify the non-cooperating nodes and a *pathrater* mechanism to exclude them from routing. In [ButtyanH:00], we present a solution based on a virtual currency called *nuglet* but, unlike [MartiGLB:00], it makes the non-cooperative behavior irrational. We assume the existence of a central authority in [BenSalemBHJ:05] and we propose a solution that encourages packet forwarding in hybrid ad hoc networks (i.e., ad hoc networks with an infrastructure support). So far, the need for these mechanisms was not formally justified. Recently, some researchers have shown in [SrinivasanNCR:03] that cooperation may emerge without incentive techniques based on a random connection setup model. In [FelegyhaziBH:03], we propose a model based on game theory and graph theory and we prove that in static ad hoc networks cooperation needs to be encouraged. We extend our contribution in a journal paper [FelegyhaziHB:04b].

References
[MartiGLB:00] S. Marti, T. Giuli, K. Lai and M. Baker. “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”. In Proceedings of *Mobicom*, 2000.
[SrinivasanNCR:03] V. Srinivasan, P. Nuggehalli, C. F. Chiasserini and R. R. Rao, “Cooperation in Wireless Ad Hoc Networks”, In Proceedings of *INFOCOM*, 2003
[ButtyanH:00] Levente Buttyan, Jean-Pierre Hubaux, Enforcing Service Availability in Mobile Ad-Hoc WANs, *IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), Boston, MA, USA, August 2000*
[BenSalemBHJ:05] N. Ben Salem, L. Buttyan, J.P. Hubaux, M. Jakobsson, Node Cooperation in Hybrid Ad hoc Networks, *IEEE Transactions on Mobile Computing (TMC)*
[FelegyhaziBH:03] M. Felegyhazi, L. Buttyan, J. P. Hubaux, Equilibrium Analysis of Packet Forwarding Strategies in Wireless Ad Hoc Networks – the Static Case, *Personal Wireless Communications PWC 2003, Venice, Italy, September 23-25, 2003*
[FelegyhaziHB:04b] Mark Felegyhazi, Jean-Pierre Hubaux and Levente Buttyan, Nash Equilibria of Packet Forwarding Strategies in Wireless Ad Hoc Networks, *IEEE Transactions on Mobile Computing (TMC)*

A.2. Reputation system
Slavisa Sarafijanovic, Jochen Mundinger (Cambridge U.), Jean-Yves Le Boudec

Our alternative, non cryptographic approach to the problem of packet forwarding is a reputation system. Marti, Giuli, Lai and Baker [MartiGLB:00] propose a way of mitigating routing misbehavior in DSR. Dynamic Source Routing [HuJM:03] is a reactive routing protocol for mobile ad-hoc networks. However, reputation systems are vulnerable to liars and robustness has not been analyzed in detail.

With our work [MundigerL:05] [MundigerL:05b], we provide an analysis of a reputation system based on a deviation test. Nodes accept second hand information only if this does not differ too much from their reputation values. We show that the system exhibits a phase transition: In the subcritical regime, it is robust and lying has no effect. In the supercritical regime, lying does have an impact. We compute the critical values via a mean-field approach and use simulations to verify our results. Thus, we obtain conditions for the deviation test to make the reputation system robust and provide guidelines for a good choice of parameters. We have also explored the use of artificial immune systems, a promising technology that has the potential to react to a broad set of possible misbehaviours. We have shown how it is possible to avoid the preliminary phase inherent to such systems [SarafijanovicL:04b].

References
[MartiGLB:00] S. Marti, T.J. Giuli, K. Lai, M. Baker. “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks”. In Proceedings of *Mobicom,* 2000
[HuJM:03] Y. Hu D. Johnson, D. Maltz. “The dynamic source routing protocol for mobile ad hoc networks (dsr)”. http://www.ietf.org/internet-drafts/ draft-ietf-manet-dsr-09.txt, April 2003.
[MundingerL:05b] Jochen Mundinger and Jean-Yves Le Boudec, Analysis of a Reputation System for Mobile Ad-Hoc Networks with Liars, *WiOpt '05, Riva del Garda, 3-7 Apr 05*
[MundingerL:05] Jochen Mundinger, J. Y. Le Boudec, Analysis of a Robust Reputation System for Self-Organized Networks, *European Transactions on Telecommunications (Wiley)*
[SarafijanovicL:04b] Slavisa Sarafijanovic and Jean-Yves Le Boudec, An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering, Danger Signal and Memory Detectors, *ICARIS-2004, 3rd International Conference on Artificial Immune Systems, Catania, Italy, 13-16 September 2004.*

B. Beacon-less routing and ants-inspired routing
Marc Heissenbüttel, Torsten Braun

In position-based routing protocols proposed in the literature (e.g. GFG[1], GPSR [2]) all nodes need to announce their positions by broadcasting hello messages, which has several drawbacks. We developed a stateless routing protocol based on a new routing paradigm where routing decisions are no longer taken at the sender but at the receivers of a packet, which allows the disposal of hello messages. Promising results were obtained by simulations [HeissenbuettelBBW:04a] and real world experiments [HeissenbuettelBRB:05]. The same paradigm was also applied to develop a broadcast protocol for ad-hoc networks [HeissenbuettelBWB:05].

References:
[1] P. Bose, P. Morin, I. Stojmenovic, J. Urrutia, “Routing with guaranteed delivery in ad hoc wireless networks”, in Proceedings of *DIALM*, 1999.
[2] B. Karp, H. T. Kung, “GPSR: Greedy perimeter stateless routing for wireless networks”, in Proceedings of *Mobicom*, 2000
[HeissenbuettelBRB:05] Marc Heissenbuettel, Torsten Braun, Tobias Roth, Thomas Bernoulli, GNU/Linux Implementation of a Position-based Routing Protocol, *IEEE ICPS Workshop on Multihop Ad hoc Networks: from theory to reality (REALMAN), Santorini, 14 July 05*
[HeissenbuettelBWB:05] Marc Heissenbuettel, Torsten Braun, Markus Waelchli, Thomas Bernoulli, Optimized Stateless Broadcasting in Wireless Multi-hop Networks, *2nd IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON 2005), Santa Clara, 26-29 Sep 2005*

C. TCP over ad hoc networks
Ruy de Oliveira, Torsten Braun

We proposed two end-to-end schemes to improve TCP efficiency in ad hoc networks. The first scheme aims to improve the response of TCP to random packet loss. It uses a fuzzy logic mechanism to distinguish between congestion and medium induced errors. In contrast to [LiuS:01], we do not rely on feedback from the network but decide based on packet delay variations within the network [OliveiraB:04b]. The second approach extends the delayed acknowledgement strategy proposed to reduce collisions and to improve bandwidth utilization [JimenezA:03] by a more adaptive mechanism. The receiver monitors the channel condition and adaptively fulfills the sender's minimum need of acknowledgements [OliveiraB:05]. Simulations results also show a lower number of spurious retransmissions and higher energy efficiency.

References
[LiuS:01] J. Liu and S. Singh. "ATCP: TCP for Mobile Ad hoc Networks". Vol. 19, IEEE Journal on Selected Areas in Communications, July 2001.
[JimenezA:03] T. Jimenez and E. Altman. "Novel Delayed ACK Techniques for Improving TCP Performance in Multihop Wireless Networks". In Proceedings of *PWC*, 2003.
[OliveiraB:04b] Ruy de Oliveira, Torsten Braun, A Delay-based Approach Using Fuzzy Logic to Improve TCP Error Detection in Ad Hoc Networks, *IEEE WCNC 2004, Atlanta, 21-25 Mar 04*
[OliveiraB:05] Ruy de Oliveira and Torsten Braun, A Dynamic Adaptive Acknowledment Strategy for TCP over Multihop Wireless Networks, *IEEE Infocom 2005, Miami, 13-17 Mar 05*

D. Group communication in ad hoc networks
Jun Luo, Jean-Pierre Hubaux

Securing ad hoc networks is notoriously challenging, notably due to the lack of an on-line infrastructure. In particular, key management is a problem that has been addressed by many researchers but with limited results [ZhouH:99, LuoKZLZ:05]. Leveraging on our results in group communications [LuoEH:04], we have recently addressed the problem of key management in groups of mobile nodes operating in a disconnected way from the certification authority. Our solution, DICTATE (DIstributed CerTification Authority with probabilisTic frEshness) [LuoH:04] innovates in two aspects: (i) a set of certificate management protocols that allow trading protocol overhead for certificate freshness or the other way around, and (ii) a combination of threshold and identity-based cryptosystems to guarantee the security, availability, and scalability of the certification function.

References
[ZhouH:99] L. Zhou and Z. Haas, "Securing Ad Hoc Networks," in *IEEE Network*, vol. 13, no. 6, pp. 24–30, 1999.
[LuoKZLZ:05] H. Luo, J. Kong, P. Zerfos, S. Lu and L. Zhang, "URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks," To appear in *IEEE/ACM Trans. on Networking*, 2005.
[LuoH:04]Jun Luo and Jean-Pierre Hubaux, NASCENT Network layer service for vicinity ad hoc groups, *The First IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON 2004), Santa Clara, 4-7 Oct 04*
[LuoEH:04] Jun Luo, Patrick Th. Eugster and Jean-Pierre Hubaux, Probabilistic Reliable Multicast in Ad Hoc Networks, *Elsevier Ad Hoc Networks, Volume 2, Issue 4, October 2004*

(Tasks E and F have been phased out.)

G. Power control for ad-hoc networks
Bozidar Radunovic, Jean-Yves Le Boudec

Some MAC protocols [SadeghiKSE:02] are focused on rate adaptation while others [JungV:02], adapt power and keep rates fixed. However, there are no MAC protocols that adapt both rate and power at the same time, and the fundamental issues in this joint adaptation problem are not well

understood. In [RadunovicL:05] we show that, perhaps contrary to intuition, there is a whole class of networks for which power control is not required, or may even be suboptimal. We assume the underlying physical layer allows fine-grained rate adaptation (like in 802.11a/g, HDR/CDMA, UWB). We prove that, when maximizing rates, 0-PMAX is the only possible optimal power control strategy in the linear regime.

References

[SadeghiKSE:02] B. Sadeghi, V. Kanodia, A. Sabharwal and K. E., "Opportunistic media access for multirate ad hoc networks," in *Mobicom*, September 2002.
[JungV:02] E.-S. Jung and N. H. Vaidya, "An energy efficient mac protocol for wireless LANs," in Proceedings of *INFOCOM*, 2002.
[RadunovicL:05] Bozidar Radunovic and Jean-Yves Le Boudec, Rate Adaptation, Power Adaptation and Mutual Exclusion in Variable Rate Wireless Networks, *RAWNET Workshop (Resource Allocation in Wireless Networks) in conjunction with WiOpt 2005, Riva del Garda, 3 Apr 05*

H. Greedy behavior in CSMA/CA protocols

Imad Aad, Mario Cagalj, Maxim Raya, Jean-Pierre Hubaux

We have identified two severe weaknesses in the CSMA/CA protocol of IEEE 802.11.

H.1. DOMINO: detection of greedy behavior in IEEE 802.11 hotspots

The IEEE 802.11 standard for the MAC protocol of WiFi networks contains weaknesses that allow greedy users to obtain higher bandwidth shares at the expense of well-behaving users. This problem was initially mentioned in [KyasanurV:04] and we fully explored its aspects in [RayaHA:04] where we described several cheating techniques. We also designed DOMINO, a system to detect several types of greedy behaviour, that can be easily integrated into Access Points and is compatible with existing equipment. In addition, we implemented one of the cheating techniques, thus demonstrating the severity of the problem, and a prototype of DOMINO.

References

[KyasanurV:04] P. Kyasanur and N. Vaidya. Selfish MAC layer misbehavior in wireless networks. In *IEEE Transactions on Mobile Computing*, April, 2004.
[RayaHA:04] M. Raya, J. P. Hubaux and I. Aad, DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots, *ACM MobiSys 2004, Boston, 6-9 June 2004*

H.2. Smart cheating in CSMA/CA networks

This problem is similar to the previous one, except that here we consider the more general case of several greedy wireless stations located in the same collision domain, while we remove the assumption about the presence of an access point. In [CagaljGAH:05], we use a game-theoretic approach to investigate the problem of efficient coordination between several greedy stations; we focus specifically on IEEE 802.11. We characterize two families of Nash equilibria in a single stage contention game, one of which always results in a network collapse. By applying the model of dynamic games borrowed from game theory, we derive the conditions for the stable and optimal functioning of a population of cheaters. In most of the existing work on selfish behavior on the MAC layer in wireless networks, only Aloha networks were considered [MacKenzieW:03], [AltmanEJ:02].

References

[MacKenzieW:03] A. B. MacKenzie and S. B. Wicker, "Stability of multipacket slotted Aloha with selfish users and perfect information", in Proceedings of INFOCOM, 2003.
[AltmanEJ:02] E. Altman, R. El Azouzi and T. Jiménez, "Slotted Aloha as a stochastic game with partial information", in Proceedings of WiOpt, 2002.
[CagaljGAH:05] Mario Cagalj, Saurabh Ganeriwal, Imad Aad and Jean-Pierre Hubaux, On selfish behavior in CSMA/CA networks, *IEEE INFOCOM 2005, Miami, 13-17 March 05*

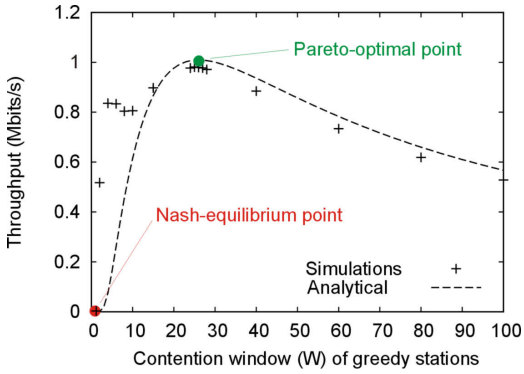

Figure 2.2.2.4.2-1. The aggregate throughput for 10 greedy IEEE 802.11b stations, all of which use the same contention window.

I. Reputation-based Wi-Fi deployment
Naouel Ben Salem, Jean-Pierre Hubaux

Two major hurdles still slow down the wide-scale adoption of Wi-Fi: the lack of a seamless roaming scheme and the variable QoS experienced by the users. Several studies [EfstathiouP:03, ZhangLWT:02] addressed the first problem but none, except ours, addressed both. In Year 3, we devised a solution that (i) allows a mobile node to connect to a foreign Wireless ISP in a secure way while preserving his anonymity and (ii) encourages the WISPs to provide the users with good QoS [BenSalemHJ:04a]. In Year 4, we have further pursued this effort by designing the related security protocols; this work is now part of IP6.

References
[EfstathiouP:03] E. Efstathiou, G. Polyzos. "A Peer-to-Peer Approach to Wireless LAN Roaming". In Proceedings of WMash, 2003.
[ZhangLWT:02] J. Zhang, J. Li, S. Weinstein, and N. Tu. "Virtual Operator Based AAA in Wireless LAN Hot Spots with Ad Hoc Networking Support". In Mobile Computing and Communications Review, vol 6, no 13, 2002.
[BenSalemHJ:04a] Naouel Ben Salem, Jean-Pierre Hubaux, Markus Jakobsson, Fuelling WiFi deployment: A reputation-based solution, *WiOpt 2004 (Cambridge, UK, March 24-26)*

J. DoS resilience in ad hoc networks
Imad Aad, Jean-Pierre Hubaux, Ed Knightly (Rice University)

Research on security in ad hoc networks was so far restrained to an "arms race" (attacks/solutions) [HuPJ:03] or to securing communications techniques (key establishment, secure routing) [HuPJ:02]. The contribution of our work [AadHK:04] is the assessment of DoS impact on multi-hop ad hoc networks. We introduce a class of DoS attacks that we called "protocol-compliant" attacks. These attacks are typically based on IP properties such as packet reordering, dropping and delaying, but in a malicious way. "Protocol-compliance" makes these attacks very hard to diagnose and time consuming. We define the proper set of measurements for DoS effects. We also show how the network gets highly partitioned, typically unfair, and that, counter-intuitively, the system overall throughput may increase.

References
[HuPJ:03] Y.-C. Hu, A. Perrig and D. B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of WiSe, 2003.
[HuPJ:02] Y.-C. Hu, A. Perrig and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Proceedings of Mobicom, 2002.
[AadHK:04] Imad Aad, Jean-Pierre Hubaux and Edward W. Knightly, Denial of Service Resilience in Ad Hoc Networks, *MOBICOM 2004, Philadelphia, 26 Sep - 1 Oct 2004*

K. Joint mobility and routing for lifetime elongation in wireless sensor networks
Jun Luo, Jean-Pierre Hubaux

Although many energy efficient/conserving routing protocols have been proposed for wireless sensor networks, the concentration of data traffic towards a small number of sinks remains a major threat to the *network lifetime*. The solution we propose in [LuoH:05] suggests that the sink be *mobile*; in this way, the nodes located close to it change over time. Data collection protocols can then be optimized by taking both sink mobility and multi-hop routing into account. We perform detailed analytical investigations and corroborate them with simulation results. We show that the obtained improvement in terms of network lifetime is in the order of 500%.

References
[ChakrabartiS:03] A. Chakrabarti, A. Sabharwal, and B. Aazhang, "Using Predictable Observer Mobility for Power Efficient Design of Sensor Networks," in Proceedings of IPSN, 2003.
[KansalSJSE:04] A. Kansal, A. Somasundara, D.D. Jea, M.B. Srivastava, and D. Estrin, "Intelligent Fluid Infrastructure for Embedded Networks," in Proceedings of MobiSys, 2004.
[LuoH:05]Jun Luo and Jean-Pierre Hubaux, Joint Mobility and Routing for Lifetime Elongation in Wireless Sensor Networks, *IEEE INFOCOM 2005, Miami, 13-17 March 05*

L. Key agreement in peer-to-peer wireless networks
Mario Cagalj, Srdan Capkun, Jean-Pierre Hubaux

Two users, each equipped with a personal device capable of communicating over a radio link, get together and want to establish a shared key. Although they can visually recognize each other, we assume that they share no authenticated cryptographic information (e.g., public keys or a shared secret) prior to this meeting. The challenge is the following: *How can the users establish a shared key in a secure way?* In [CagaljCH:05], we present an approach that is based on the Diffie-Hellman key agreement protocol. We propose three techniques: the first is based on visual comparison of short strings, the second on distance bounding, and the third on integrity codes; in each case, the users do not need to enter any password or other data [GehrmannMN:04], nor do they need physical or infra-red connectivity between their devices [StajanoA:99].

References
[GehrmannMN:04] C. Gehrmann, C. Mitchell and K. Nyberg. Manual Authentication for Wireless Devices, 2004. RSA Cryptobytes, Vol. 7, No. 1.
[StajanoA:99] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In Proceedings of the International Workshop on Security Protocols, 1999.
[CagaljCH:05] Mario Cagalj, Srdjan Capkun and Jean-Pierre Hubaux, Key agreement in peer-to-peer wireless networks, *Proceedings of the IEEE (Special Issue on Security and Cryptography),2005*

M. Multi-operator games
Mark Felegyhazi, Jean-Pierre Hubaux

So far, the frequency bands used by cellular operators have been of wireless operators are carefully separated. There has been some initial work addressing the possible coexistence of several network operators in a *shared frequency band* from both the economics [Benkler:04] and the computer science community [HalldorssonHEM:04]. In our paper [FelegyhaziH:05a], we study this situation in detail, assuming that each mobile node can *freely roam* among the various operators. As a major result, we prove that a socially optimal Nash equilibrium exists and that it can be enforced by using punishments. In the scenario of *multi-domain sensor networks*, which was never considered before, we address the problem of cooperative packet forwarding [FelegyhaziBH:05]. We show that the energy saving provides a "natural incentive" for the authorities to cooperate.

References
[Benkler:04] Y. Benkler, "Some Economics of Wireless Communication", In Harvard Journal of Law and Technology, vol 16, no 1, 2004.

[HalldorssonHEM:04] M. Halldorsson, J. Halpern, L. Erran Li, V. Mirrokni, "On spectrum sharing games", In Proceedings of PODC, 2004
[FelegyhaziH:05a] Mark Felegyhazi, Jean-Pierre Hubaux, Wireless operators in shared spectrum
[FelegyhaziBH:05] Mark Felegyhazi, Levente Buttyan and Jean-Pierre Hubaux, Cooperative Packet Forwarding in Multi-Domain Sensor Networks, *IEEE PerSeNS 2005, Hawaii, 12 Mar 2005*

N. Simulation of mobility models

Jean-Yves Le Boudec, Milan Vojnovic (Microsoft), Santashil PalChaudhuri

The simulation of the random waypoint poses a surprising number of challenges, such as speed decay, a change in the distribution of location and speed as the simulation progresses [YoonLN:03], [CampNB:04]. All of these observations are related to the existence of a stationary regime. We show how this is related to Palm Calculus [LeBoudec:04b]. Then we use this tool to define a set of realistic extensions of the random waypoint, which we call "random trip"; it contains as special cases: the random waypoint on convex or non convex domains, random walk with reflection or wrapping, city section, space graph and other models. We give a necessary and sufficient condition for a stationary regime to exist. When this condition is satisfied, we compute the stationary regime and give an algorithm to start a simulation in steady state (perfect simulation). The algorithm does not require the knowledge of geometric constants. For the special case of random waypoint, we provide for the first time a proof and a sufficient and necessary condition of the existence of a stationary regime. Further, we extend its applicability to a broad class of non convex and multi-site examples, and provide a ready-to-use algorithm for perfect simulation. For the special case of random walks with reflection or wrapping, we show that, in the stationary regime, the mobile location is uniformly distributed and is independent of the speed vector, and that there is no speed decay. Our framework provides a rich set of well understood models that can be used to simulate mobile networks with independent node movements. Our perfect sampling is implemented to use with ns-2, and it is freely available to download from http://ica1www.epfl.ch/RandomTrip. [LeBoudecV:05]. We obtained the Infocom Best Paper Award for this latter publication.

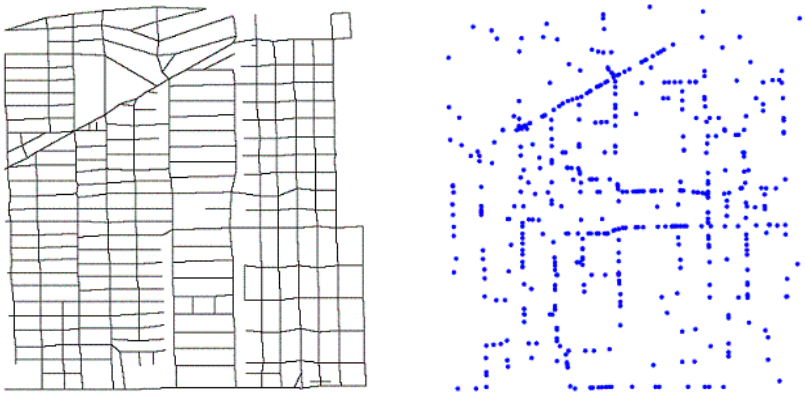

Figure 2.2.2.4.2--2: The random trip model can imitate the movement of mobiles in a city. Left: map from census bureau. Right: stationary distribution of mobiles.

References

[YoonLN:03] J. Yoon, M. Liu and B. Noble. "Sound mobility models". In Proceedings of Mobicom, 2003.
[CampNB:04] T. Camp W. Navidi and N. Bauer. "Improving the accuracy of random waypoint simulations through steady-state initialization". In Proceedings of MS, 2004.
[LeBoudec:04b] Jean-Yves Le Boudec, On the Stationary Distribution of Speed and Location of Random Waypoint, *IEEE Transactions on Mobile Computing*
[LeBoudecV:05] Jean-Yves Le Boudec and Milan Vojnovic, Perfect Simulation and Stationarity of a Class of Mobility Models, *IEEE INFOCOM 2005, Miami, 13-17 March 05*

O. UWB networking
Ruben Merz, Jean-Yves Le Boudec, Jörg Widmer, Bozidar Radunovic

Pulsed Time-Hopping Ultra-Wideband (TH-UWB) is a radio technology that has the potential to satisfy the requirements of very low power systems. However it is sensitive to strong interferers and near-far scenarios. Existing designs [CuomoMBF:02, AugustH:04] use a fixed channel code. In contrast, we base our design on rate control, which allows a radical simplification of the ocerall system. We further take advantage of the nature of pulsed TH-UWB to propose an interference mitigation scheme that alleviates the need for an exclusion scheme. A source is always allowed to send and continuously adapts its channel code (hence its rate) to the interference experienced at the destination. We show by simulation that we achieve a significant increase in network throughput compared to alternative designs [MerzWBR:05].

References
[CuomoMBF:02] F. Cuomo, C. Martello, A. Baiocchi and C. Fabrizio. "Radio resource sharing for ad hoc networking with UWB". IEEE Journal on Selected Areas in Communications, 20(9):1722-1732, December 2002.
[AugustH:04] N. August and D. Ha. "An efficient UWB radio architecture for busy signal MAC protocols". In Proceedings of SECON, 2004.
[MerzWBR:05] Ruben Merz, Joerg Widmer, Jean-Yves Le Boudec, Bozidar Radunovic, A Joint PHY/MAC Architecture for Low-Radiated Power TH-UWB Wireless Ad-Hoc Networks, *Wireless Communications and Mobile Computing Journal, Special Issue on UWB Communications*

2.2.2.4.3. IP highlights

- (C) is a novel proposal for TCP over multi-hop networks which does not require specific cooperation from intermediate nodes.
- (J) is the first paper describing DoS attacks against ad hoc networks, perpetrated at the transport layer; it provides a quantified assessment of the potential damage.
- (K) is the first analytical study of the benefits in terms of power savings induced by a mobile sink
- (L) contains two novel techniques to respond to the fundamental challenge of authentication and secure key establishment over a wireless link
- (N) proves for the first time the stability of the random waypoint.

2.2.2.4.4. Target - actual comparison over the entire term

From the very beginning of MICS, IP4 has promised to deliver novel solutions for the network layer, in order to cope with the challenges raised by future wireless networks. In the initial proposal (written in early 2000), we have mentioned the intention to focus in particular on the topics that were - at that time - considered to be the most crucial for mobile ad hoc networks:
- addressing and location
- packet forwarding
- resource control and management
- interconnection with the Internet.

These initial goals proved to be a powerful source of inspiration and helped us tremendously at thinking about wireless networks independently from legacy systems. During the unfolding of the project, the focus has been adapted, in order to take the evolution of the state-of-the-art into account: in the meantime, mobile ad hoc networks had become very hot in the research community.

As a result, IP4 has been a very productive project (24 journal papers and 57 conference papers published or accepted by June 2005). It has contributed to generate research questions which have then been investigated also by other IPs (e.g., routing techniques in IP1, IP7, and IP9; security protocols in IP6). In some areas, the results have gone beyond our expectations.