Paper

IPv6 in Wireless Networks – Selected Issues

Sławomir Kukliński[a], Paweł Radziszewski[b] and Jacek Wytrębowicz[b]

[a] *Institute of Telecommunication, Warsaw University of Technology, Warsaw, Poland*
[b] *Institute of Computer Science, Warsaw University of Technology, Warsaw, Poland*

Abstract—The article presents issues concerning the construction of autonomous wireless networks based on the IPv6 protocol. Prospects of implementation of IPv6 in wireless networks and IPv6 features and mechanisms important in such applications are discussed. Research directions related to the use of IPv6 in wireless networks are also outlined. Then the selected concepts are described, arising in the course of the EFIPSANS (Exposing the Features in IP Version Six Protocols that can be Exploited/Extended for the Purposes of Designing/Building Autonomic Networks and Services) project, during studies on the autonomy of nodes and routing configuration for wireless networks. Concepts presented here apply to wireless ad hoc mesh networks. Discussed is their nature and aspects related to auto-configuration and autonomously operating routing. In particular, there is a Wireless Autonomic Routing Framework (WARF) architecture presented.

Keywords—extension headers, IPv6, WiFi, wireless mesh networks.

1. Introduction

Techniques for creating wireless networks for data transmission are as old and complex as those dedicated to wired ones. Observing the development of wireless networks over the past 40 years, two seemingly contradictory trends can be found: high specialization towards a particular application and uniformity in order to open for application software and to connect globally available subnets to the network. This is an apparent contradiction, because the first goal is achieved by choosing and developing the layer 2 protocols, while the second objective is achieved by applying the higher layers of TCP/IP protocol stack. Today many different types of wireless networks are used, such as:

– mobile communication networks, like CDMA2000, EDGE, UMTS and LTE;

– private radio networks built using TETRA and GSM-R technologies;

– broadband access networks exploiting WiMAX (IEEE 802.16) and WiFi (IEEE 802.11) technologies;

– nomadic and mobile ad hoc networks relying on WiFi;

– sensor networks exploiting ZigBee (IEEE 802.15.4) technology.

They differ not only in layer 2 protocols. Their diversity is derived from the application requirements, geographical coverage, number and mobility of nodes. The prevalence of their deployments is also driven by economic factors (including the history of the development of local economies) and cultural aspects, resulting from the degree of education of local communities.

Most of today's wireless networks use the IPv4 protocol, adopted as a mandatory standard in 1981 (RFC 791). Its widespread use was 10 years later, when first web servers and web browsers appeared. IPv6 was adopted as a standard in 1998 (RFC 1883) and its global availability is possible only since February 2008, when IANA launched IPv6 DNS servers in the Internet backbone. The number of devices using IPv4 is huge and difficult to assess because of the countless number of private networks and the widespread use of NAT. It is difficult to expect that, in a short term, users of these devices decide for their replacement or reconfiguration in order to move to IPv6. It is also probable that, despite the many advantages of IPv6, majority of the current IPv4 users will not want to change, assessing that their network infrastructure meets their needs. On the other hand, the pool of free IPv4 addresses is running out. On the basis of automatically updated statistics (IPv4 address report[1]) it can be concluded that (at the time of writing this publication):

– number of IANA- and RIR-alocated public IPv4 addresses is 3 098 000 000;

– number of public IPv4 addresses observed in core routers' BGP tables is 2 236 000 000;

– exhaustion of free IANA-allocatable address pool will happen on July 19th 2011;

– exhaustion of free RIR-allocatable address pool will happen on March 25th 2012.

At present we see that the global Internet is single, supported parallelly by two protocols: IPv4 and IPv6. Therefore, we can be sure that due to the depletion of free IPv4 addresses, new installations of Internet access networks will be based on IPv6. However, the rate of the existing networks modification will result from the emergence of new applications and network services, which functionality will depend on the version of the IP protocol.

IPv6 compared to IPv4 has several advantages, as it formed on the basis of experience of the operation of IPv4 networks. The benefits of deploying IPv6 are discussed in many publications, e.g., [1], [2], [3], [4]. What is worth

[1] www.potaroo.net/tools/ipv4/index.html

to emphasize, this protocol is pro-developmental in terms of ease of creating new technical solutions and new-quality applications. It is possible to increase the globalization of remote data collecting and control, in relation to the massive amount of terminal equipment. This also applies to the access to devices operating in wireless networks.

There also several books written on the use of IPv6 in wireless networks, e.g., [5], [6]. In summary, it can be concluded that the IPv6 features important for the provisioning of services in wireless networks, are:

- The size of the address space, important for operators servicing millions of subscribers.
- Powerful mobility, which allows nodes to move between subnets without breaking the existing session. Mobile IPv6 is more efficient than Mobile IPv4. With Mobile IPv6 a number of enhancements is related, such as hierarchical management of nodes mobility (RFC 5380), subnet mobility within the Internet (RFC 3963), rapid transfer of nodes between access routers (RFC 5568) using layer 2 mechanisms (e.g., WiFi roaming, WiMax), routing optimization (RFC 4866), possibility of take-over of the responsibility for the signaling associated with the node mobility (RFC 5213) by the network.
- Auto-configuration features are enhanced (detection of neighbors and routers, announcing the network prefix).
- The use of header compression potentially makes IPv6 more efficient than IPv4 – which is particularly important in sensor networks.
- IPv6 offers higher level of security compared to IPv4, because
  - a mandatory implementation of IPsec provides more options for securing networks and applications - without the constraints imposed by NAT servers;
  - there is defined a proposal of a standard for securing, with IPsec and IKEv21, the signaling between mobile nodes and home agents (RFC 4877);
  - it is possible to use the Secure Neighbor Discovery Protocol (SEND, RFC 3971), which improves the safety of nodes auto-configuration – which is particularly important in the radio interfaces;
  - SEND protocol increases the security of neighbors discovery process. It's most important mechanisms are certification paths for routers authentication, and cryptographically generated addresses (RFC 3972) to verify the sender.
- There is possible interoperability of devices in IPv6 and IPv4 subnets and tunneling of IPv6 traffic in IPv4 subnets.

Noteworthy is an interesting study [7] of the use of IPv6 in the satellite communication, commonly used in military applications and for multimedia content distribution (e.g., IPTV). Features typical in satellite communications, such as broadcast and multicast, mobility and global reachability, are well supported by IPv6.

Today, ongoing research related to wireless networks and IPv6 protocol addresses a number of very different issues. Deserve a mention works on:

- communication between devices with low power consumption, led by 6lowpan Working Group (IETF);
- optimization of Mobile IPv6 solutions, led by MobOpts Working Group (IETF);
- communication between cars, and cars and road infrastructure in order to increase road safety (Geonet Project, 7th Framework Programme);
- autonomy of the nodes and networks within the aforementioned project EFIPSANS.

Issues that were analyzed in the EFIPSANS project were: ISO/OSI crosslayer cooperation to improve the performance of a wireless network [8], multipath routing, which can increase performance and reliability of the network [9], [10], mechanisms that can force node users to a cooperation in order to optimize the utilization of network resources [11], [12]. The result of the work is the WARF architecture, presented later in this article, designed to support autonomous routing in wireless mesh networks. In the last section there is a concept of a new IPv6 extension header presented, which is a solution for an efficient transport of auto-configuration and routing messages within the wireless network.

2. Routing in Wireless Mesh Networks

Our interest focuses on wireless ad hoc networks, built on the basis of a popular IEEE 802.11 standard. The popularity is due to the extremely low equipment prices and very attractive operating parameters [13], such as working in unlicensed radio bands, high resistance to interferences, high transmission rates. Ad hoc networks are a hot topic of research for over 10 years. Approximately 120 routing protocols for such networks were proposed, but prior to the publication of the IEEE 802.11 standard in 1997, existed only 6 of them. Most of these proposals were published in the conference materials, 30 of them were proposed IETF standards, 2 of them are active IETF proposals and 4 have become the IETF standards. Furthermore, there are 4 patented proprietary protocols offered in commercial solutions. The multiplicity of these protocols demonstrates the conflicting requirements of different applications of such networks. Mobile ad hoc networks are the subject of multiple present scientific conferences, such as *Ubi-Islands, International Conference on Ad Hoc Networks, In-*

ternational Conference on Cognitive Radio Oriented Wireless Networks and Communications, ICST Conference on Access Network, International Conference of Wireless Networks, IEEE Symposium on Personal, Indoor and Mobile Radio Communications.

A variation of ad hoc networks with relatively low topology variability is a wireless mesh networks (WMN). WMNs can be created as residential area networks, interim solutions for servicing events, etc. They assume so-called nomadic nature of users, namely the lack of mobility while using the network. WMNs are typically created using nodes with IEEE 802.11 radio interfaces. Despite years of research, deployment rates of such networks are still very low. A cause is that not all the problems associated with such networks have been solved. There were too many routing protocols developed, each of which has beneficial properties only in a specific network scenario: some protocols work efficiently in networks with low or high density of nodes, while the other ones are dedicated to networks with low or high topology changes dynamics. Unfortunately, in many WMN applications it is difficult to assume the characteristics of network environment. The problem of selecting an appropriate network protocol is further reinforced by the ambiguous evaluation of the effectiveness of metrics used by the routing protocols (usually they are part of the routing protocols). A number of metrics specific to the WMNs (including ETX, ETT, Airtime [14]) had been developed, initial implementations, however, have not confirmed the benefits of certain metrics, indicated by simulations [15].

One of the problems of present WMN solutions is the lack of information exchange between different network layers. Such an approach significantly and adversely affects the network behavior. A glaring example is the use of routing protocols, which choose a path with the least number of intermediate nodes (hop-count metric). In practice, it appeared that a path formed in this way chooses the longest network spans and therefore the ones characterized by the lowest SNR, and consequently low bitrate (bitrate adaptation to the link quality is part of the IEEE 802.11 standard) and the high probability of packet loss (packet loss rate parameter) [16]. Using information from the physical layer would reject low-quality links in such a case. It is worth noting that the use of information from different layers (cross-layer) is a classical approach used in mobile communication systems (GSM/UMTS/LTE). In IP networks such an approach is still not popular. Another problem of 802.11 mesh networks is that all nodes of the network use the same radio channel. This leads to poor network performance due to the formation of relatively large ‘areas of interference’, where only one node can transmit at the same time.

Furthermore, in most WMNs network management is still centralized, inadequate to the possibility of spontaneous division of the network into two disjoint networks or a combination of two disjoint networks into one. WMNs require specific network management solutions with special focus on auto-configuration (including IP address allocation). WMN networks are usually created not by the operators with relevant experience, but by small companies or the network users themselves. So an important requirement is to incorporate the advanced autonomous management functions into them; manual management should be kept to a minimum.

3. Auto-configuration in Wireless Mesh Networks

Wireless networks, because of their usually higher topology variability, can much more benefit from the auto-configuration features than wired networks. Therefore, IPv6 can be preferred over IPv4, having more support for auto-configuration.

There are two kinds of auto-configuration in IPv6:

- stateful – similar to that known from IPv4, using DHCPv6 servers;
- stateless – that does not require the use of such servers (RFC 2462).

A particular attention deserves the stateless auto-configuration, occurring in IPv4 only in a rudimentary form – dynamic configuration of IPv4 link-local addresses (RFC 3927) and automatic private IP addressing and allocating for communication purposes local addresses from the range 169.254.0.0/16. The most important mechanisms for stateless auto-configuration of IPv6 are: link-local addressing, automatically generated interface IDs, neighbor discovery, duplicate address detection, router discovery and prefix announcement.

IPv6 defines several validity ranges of the addresses, from which the most important are global and link-local addresses. Global addresses are equivalent to public IPv4 addresses and can be used across the public Internet. Link-local address is valid and must be unique only in the “link”, understood as a layer 3 network. IPv6 allocates prefix FE80::/10 for this purpose. These addresses allow for communication between devices within the same network, without having any knowledge of their location in the surrounding networks, and so the network prefix. They can be defined manually, but most are generated automatically, from layer 2 addresses, using the EUI-64 (extended unique identifier) schema. This allows for an easy connectivity setup between devices attached to the same network.

As IPv6 does not define a broadcast address, it is impossible to use well-known IPv4 ARP. It is replaced by the neighbor discovery mechanism, supported by duplicate addresses detection, which are part of the ICMPv6 protocol.

IPv6 allows the end device that use the ICMPv6 protocol for an automatic detection of the default router and the announcement of the network prefix. In conjunction with the automatic generation of the interface ID it allows to automatically configure a full IPv6 address (64-bit network prefix and 64-bit interface identifier), which provides communication between different networks.

The research in the EFIPSANS project has defined new mechanisms to support auto-configuration of wireless networks – the use of several radio interfaces, automatic allocation of radio channels and multi-path routing. For transport of auto-configuration messages IPv6 mechanism of the extension headers is used. It allows to attach control messages to user traffic packets, which is especially advantageous in radio networks with multiple access to a shared medium, due to lack of efficiency losses as a result of additional packets competing for access to the transmission channel.

4. WARF Architecture

The above-mentioned problems associated with WMNs show that a new, open and comprehensive approach to such networks is necessary. It should:

- provide a distributed, autonomous management mechanisms;
- facilitate exchange of information between the layers of the network stack;
- support simultaneous use of different routing protocols (multi-protocol approach);
- allow for the multipath routing;
- ensure the determination of routing metrics in a routing protocol-independent way;
- allow the creation of networks using nodes with multiple radio interfaces.

Above requirements are met by the wireless autonomic routing framework (WARF) architecture, developed by the authors of this article in the aforementioned EFIPSANS project. The main idea of the WARF approach is to create an open environment for WMNs, supporting the above-mentioned, advanced mechanisms, allowing for a relatively easy replacement of algorithms responsible for each specific functionality. WARF is component architecture, allowing for flexibility in the implementation of various routing protocols, routing metrics and radio resource management mechanisms. The use of multiple radio interfaces enables the dynamic resource (radio channels) management mechanism. It must be, however, supported by an appropriate control protocol.

The WARF architecture defines basic building blocks responsible for realization of specific functions. Control messages exchange is performed by the IPv6 protocol, which offers significant benefits like large address space, mobility support and automatic protocol configuration, with additional features called WARF extensions. Thanks to the unified approach to control messages transport it is possible to interpret different messages by all WARF network nodes. One of the mechanisms used for the unified message transport mechanism is IPv6 WARF extension header. The presented mechanisms contribute to higher level of autonomy of the management of such networks, increasing their productivity and reliability, as well as facilitating implementation. WARF extensions can be also used to encapsulate control messages of existing routing protocols such as AODV or AOMDV.

WARF architecture decomposition into functional blocks results from a comparative analysis of ad hoc networks/WMNs routing protocols and the specifics of new, described above, routing and resource management mechanisms. The proposed decomposition is consistent with the autonomous model proposed by IBM [17]. In this model stands out: a part collecting information about the status of the module or a network node (a sensory part), a decision component (which in fact contains a control algorithm and a knowledge base) and actuators. Due to the impact of the decision on the status of the network and feedback information obtained from sensors, we are dealing with a system with feedback, with all the consequences of it – among others the possibility of a delayed action or unstable operation of a node, subnet or a whole network.

WARF architecture is similar to the decomposition proposed by [18]. It consists of four main blocks, divided further into modules (see Fig. 1):

- Resource Maintenance (RSM),
- Route Maintenance (RTM),
- Data Forwarding (DF),
- Policy Control (PC).

Resource Maintenance block contains a Resource State Information (RSI) and a Resource Control (RC) modules.

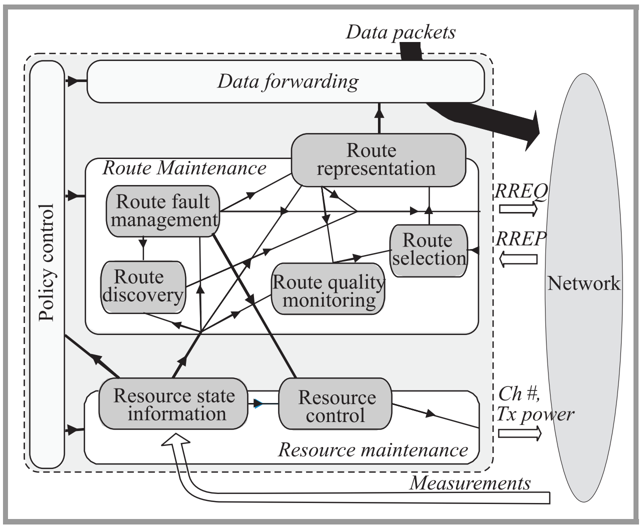


Fig. 1. WARF architecture: Route Maintenance block consists of 4 modules: route discovery, route selection, route representation and route fault detection.

The RSI module is responsible for radio resources (channels, radio links) monitoring – it monitors and spreads all the information related to the resources state. This may include parameters of different network layers, including SNR/SNIR, BER, FER, PLR, node load level, etc.

Table 1
WARF architecture signalling messages

Category	Message	Parameters
Radio resource control	Channel quality report (CHQREPORT)	Number of radio channels Channel ID SNR Channel load Reporting node IPv6 address
	Number of interfaces report (INTFREPORT)	Number of interfaces Interface ID Channel ID, TX power Rporting node IPv6 address
	Set signalling channel (SETSIGHCH)	Channel ID, TX power Requesting node IPv6 address Target node IPv6 address
Route control	Path metric (PATHMETRIC)	Packet error rate, bit error rate Retransmission count Delay, delay variance Bit rate Announcing node IPv6 address Destination network IPv6 address and mask
Legacy routing protocol support (AODV)	IPv6 route request (PREQ) Route reply (RREP) Route error (RERR) Route reply acknowledgment (PREP-ACK)	Parameters analog to the ones from the original AODV protocol, adopted for transporting IPv6 address information instead of IPv4

This module monitors both used and available resources. This is important because of the adaptability of link parameters to propagation conditions. All these operations are performed in real time. RSI may perform measurements aggregation before further information transfer. This module supports also calculations of routing metrics.

Resource control module is responsible for radio resource configuration. The algorithm controlling its operation uses the RSI module information (quality of links and their load) and on this basis decides whether to change the configuration of resources. Reconfiguration may be due to a congestion in the selected routes or a damage to the links. To change the configuration of a radio channel a three-way handshake protocol is used, and signalling messages are have form of IPv6 WARF extension headers.

These modules work together to create a routing table, which is the main output product of this block. They use the resource configuration and state information in order to obtain information about the quality of paths (metrics). All external information of this block use the same IPv6 WARF extension, regardless of the algorithm (routing protocol) used. When in this block classic protocols are used, signalling messages are simply encapsulated. WARF messages of this block are classic routing protocols messages, such as RouteREQest (RREQ), RouteRESPonse (RRESP), RouteERRor (RERR).

Data forwarding block uses a routing table to forward packets. It selects the paths based on metrics. In the WARF architecture it is assumed that this block can support multipath routing and QoS mechanisms, but these operations require no additional WARF control messages. There is also no support of flows at the signalling level. Such support, however, can be built in.

Policy Control block controls all other blocks and modules. WARF is architecture with elements of autonomous administration and a number of parameters of this architecture are subject to self-regulation. Nevertheless, it has been decided to leave some degree of freedom, allowing the network operator to create different policies or change the network profile. The policy control block provides such mechanisms.

5. IPv6 WARF Extension Header

In the described approach, it is proposed to use IPv6 protocol extension headers (RFC 2460) as a channel for transporting WARF architecture signalling messages. WARF-aware nodes can attach these messages as an additional extension header, of the hop-by-hop option category, to user data packets. Header of this category is being analyzed by all the nodes along the packet path. Such an approach has an important advantage: it does not generate additional packets, what decreases demand for computing power in communicating nodes and, what is especially important in wireless networks, does not load the transmission channel with the process of the medium access competition.

Signalling messages, encapsulated in IPv6 extension header are forwarded between nodes. There is proposed a hop-by-

hop header, with number from the range 32-63. It's leading bits (001) mean "skip the header when you not recognize it" (assuring compatibility with non-WARF-aware nodes) and "a header can change along the path".
Structure of the proposed header fulfills the RFC 2460 requirements. One header can transport multiple messages. Messages are grouped into three categories: radio resource control, routing control and support for the legacy routing protocol (e.g., AODV). Their list is presented in Table 1.
One should be aware of two potential disadvantages of sending messages via extension headers:

- It increases data packets length; it can excess the MTU value for the given network.
- When no user data is sent for some time, an unacceptable delay in the signalling messages delivery can occur.

Countermeasures to these shortcomings are easy to design. It is proposed to use for the control messages transport only short packets (e.g., TCP acknowledgement messages or UDP voice packets). Moreover, it is possible to implement an integrated, intelligent transport, which, depending on the occurrence and character of the user data and signal message urgency, selects for it's transport one of three channels: extension header, ICMP packet or zero-payload packet.

6. Conclusions

The use of IPv6 in the Internet is now a reality. We are observing a rapid development of dedicated IPv6 extensions for mobile applications and wireless networks. The essential features of IPv6 and its extensions in support of the construction and operation of wireless networks are mechanisms for mobility, auto-configuration and security.
Presented in this article some results of studies carried out in the EFIPSANS project show that deployment of a new extension header can effectively support the operation of wireless mesh ad hoc networks. In particular, it can improve routing mechanisms.
Although theoretical work on the operation of ad hoc mesh networks is being carried for several years, their widespread use is limited. The reason for this is twofold: lack of applications due to lack of universality of such networks and lack of universality due to lack of autonomy of routing configuration. Routing algorithms and their parameters should be selected to the specifics of the installation and use. This requirement can be met through the deployment of WARF architecture.
We think that the proposed IPv6 extension header could become a factor facilitating construction of flexible routing architecture for wireless ad hoc networks and consequently make them more efficient and effective in supporting a variety of applications. Although IPv6 is not being implemented in existing networks as quickly as expected, we are convinced that in a few years it will be widely used. A steady increase in the number of applications and services that require a constant visibility of each node in a network can be observed. For such applications and services a direct visibility of the nodes, node independence and continuity of network access are key features. As IPv6 better than IPv4 meets these objectives, it is deployed in new networks and will, with some delay, appear in the existing ones.

References

[1] R. Desmeules, "Cisco self-study: implementing Cisco IPv6 networks (IPV6)". *Ciscopress*, 2003.

[2] S. Hagen, *IPv6 Essentials*. O'Reilly, 2006.

[3] K. Siil, *IPv6 Mandates: Choosing a Transition Strategy, Preparing Transition Plans, and Executing the Migration of a Network to IPv6*. Wiley, 2008.

[4] M. Blanchet, *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*. Wiley, 2006.

[5] H. Soliman, *Mobile IPv6: Mobility in a Wireless Internet*. Addison-Wesley Professional, 2004.

[6] R. S. Koodli, Ch. E. Perkins, *Mobile Inter-networking with IPv6: Concepts, Principles and Practices*. Wiley, 2007.

[7] D. Minoli, *Satellite Systems Engineering in an IPv6 Environment*. Auerbach Publications, 2009.

[8] R. Ramdhany, G. Coulson, "Manetkit: a framework for MANET routing protocols", Lancaster University UK, 2010 [Online]. Available: http://www.comp.lancs.ac.uk/≈geoff/Publications/WWASN2008.pdf

[9] M. K. Marina, S. R. Das, "On-demand multipath distance vector routing in ad hoc network", in *Proc. ICNP 2001*, Riverside, USA, 2001, pp. 14–23.

[10] S.-J. Lee, M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", in *Proc. IEEE Int. Conf. Commun. ICC'01*, Helsinki, Finland, 2001, vol. 10, pp. 3201–3205.

[11] P. Michiardi, R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in *Proc. Commun. Multim. Sec. Conf.* Portoroz, Slovenia, 2002, pp. 107–121.

[12] S. Buchegger, J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes fairness in dynamic ad hoc networks", in *Proc. MobiHoc'02*, Lausanne, Switzerland, 2002, pp. 80–91.

[13] E. Perahia, R. Stacey, *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n*. Cambridge University Press, 2008.

[14] R. Baumann, S. Heimlicher, M. Strasser, A. Weibel, "A survey on routing metrics", TIK Report 262, *ETH* Zürich, Feb. 2006.

[15] H. Ştefãnescu, M. Skrocki, S. Kukliński, "AAODV routing protocol: the impact of the routing metric on the performance of wireless mesh networks", in *Proc. 6th Int. Conf. Wirel. Mob. Commun.*, Valencia, Spain, 2010.

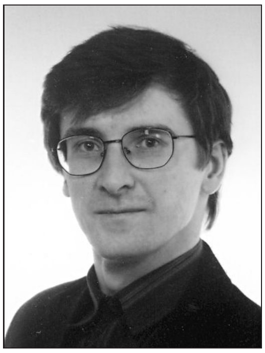
[16] D. Passos, D. V. Teixeira, D. C. Muchaluat-Saade, L. C. S. Magalhães, C. V. N. Albuquerque, "Mesh network performance measurements", in *Proc. 5th Int. Inform. Telecommun. Technol. Symp.*, Cuiabá, Brazil, 2006.

[17] IBM, "Autonomic Computing White Paper: An architectural blueprint for autonomic computing", 4th edition, June 2006 [Online]. Available: http://www-01.ibm.com/software/tivoli/autonomic/pdfs/AC_Blueprint_White_Paper_4th.pdf

[18] I-J. Wang, J. Hopkins, Ch. Liu, T. Saadawi, "Component-based analysis and design of routing protocols for mobile ad hoc networks", 2005 [Online]. Available: http://handle.dtic.mil/100.2/ADA431954

Sławomir Kukliński received Ph.D. degree in telecommunications from Warsaw University of Technology, Institute of Telecommunications in 1994 and since then he is a Professor. He has 25 years long experience in telecommunications – he started from radar systems, switched to distributed algorithms for signal processing (including neural networks) and from 10 years he is working on mobile and wireless systems. At WUT he is a lecturer of mobile systems. In 2003 he joined the Orange Labs Poland. In Orange Labs Poland he is involved in projects related to autonomic management and VANET (car-to-car communications). He was recently involved in FP6 MIDAS project working on context aware routing. Since 2008 he is involved in FP7 project EFIPSANS. In 2008 he has started another project, AUTONET (Autonomic, Wireless Networks) that has been ordered and is financed by Polish Ministry of Science and Higher Education. From January 2008 till July 2010 he was involved in FP7 project 4WARD. He published more than 40 papers, and he also was the member of TPC of many conferences and served as a reviewer to many conferences and journals.

e-mail: kuklinski@tele.pw.edu.pl
Institute of Telecommunication
Faculty of Electronics
and Information Technology
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland



Paweł Radziszewski received M.Sc. (1993) in computer science from the Faculty of Electronics and Information Technology, Warsaw University of Technology. Since that he works at the Institute of Computer Science, WUT. His research interests include: computer networks (especially network protocols and network steganography), software engineering and computer graphics. He is member of Computer Graphics Laboratory. He is an author or a co-author of 10 papers. Since 1993 he has been working as a software developer for TecMath GmbH (Germany), Softwired A.G. (Switzerland), Arkatronik (Poland) and Air Force Institute of Technology (Poland). Since 2003 he has been working as an instructor at the Cisco Regional Academy at International Telecommunication Union Internet Training Centre, WUT. In years 2007–2008 he was involved in the TrustMAS project concerning steganographic routing. Since 2008 he is involved in FP7 project EFIPSANS.

e-mail: p.radziszewski@ii.pw.edu.pl
Institute of Computer Science
Faculty of Electronics
and Information Technology
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Jacek Wytrębowicz is an assistant professor at Warsaw University of Technology, where he gives lectures on computer networks. He is co-author of 4 books and author or co-author of 35 papers in technical journals and conference proceedings. When he worked at Warsaw Heating Utility, he led a project of a Metropolitan Area Network. During this time the company built 50 km of fiber infrastructure inside heat distribution ducts. Working at TEL-ENERGO S.A. (today named EXATEL S.A.) a countrywide telecom operator, he managed the IT department and was responsible for development of business and operational support systems. He is a specialist in Internet protocols and triple play services. As a consultant he wrote technical analysis and telecommunication strategies for municipal authorities and utility companies from Warsaw and Torun. He has a Ph.D. in Computer and Network Science from l'Ecole Nationale Supérieure des Télécommunications Paris and M.Sc. in Computer Science from Warsaw University of Technology.

e-mail: j.wytrebowicz@ii.pw.edu.pl
Institute of Computer Science
Faculty of Electronics
and Information Technology
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland