Mobile and Ambient Environments of the Future

Research Challenges for Wireless Ad-Hoc and Sensor Networks

Rolland Vida[1], Karoly Farkas[2], Dan Grigoras[3], Utz Roedig[3], Jorge sá Silva[4],
Petia Todorova[5], Andreas Pitsillides[6], Vasos Vassiliou[6], Lars Wolf[7]

[1]Budapest University of Technology and Economics, vida@tmit.bme.hu
[2]ETH Zurich, farkas@tik.ee.ethz.ch
[3]University College Cork, {d.grigoras, utz}@cs.ucc.ie
[4]University of Coimbra, sasilva@dei.uc.pt
[5]Fraunhofer Institute FOKUS, petia.todorova@fokus.fraunhofer.de
[6]University of Cyprus, {andreas.pitsillides, vasosv}@cs.ucy.ac.cy
[7]Technical University Braunschweig, wolf@ibr.cs.tu-bs.de

Abstract – There are two important trends that seem to be the driving forces in the evolution of communication networks. On the one hand, mobility support becomes a "must" for emerging services and technologies. On the other hand, services tend to have a ubiquitous nature, they are based on intelligent devices being embedded in the ambient environment surroundig us. These new trends result in new research challenges as well. In this paper we first present the specificities of wireless ad-hoc and sensor networks, technologies that were developed to support these new requirements. Then, we highlight the most important and most challenging issues that arise from these specificities.

1. Introduction

The traditional wired Internet, with PC users and centralized, server-based services faces today important changes: users tend to be more and more mobile, and services tend to be more and more ubiquitous, making use of the intelligent ambient environment surrounding us. The specific characteristics and research challenges related to wireless ad-hoc and sensor networks came therefore in the focus of the research community.

More and more wireless mobile devices like laptops, PDAs, smart phones, GPS-enabled devices, MP3 players and sensors target various user needs, covering an entire spectrum from daily routine work to entertainment and health care purposes. While any active person usually has at least two different mobile devices (e.g., a PDA and a smart phone), the potential of these devices is not fully exploited. Each mobile device manages specific resources and services and is radio enabled, but its capacity of interacting with other devices is limited. On the other hand, by aggregating all the resources and services, the owner of a set of mobile devices can benefit of a mobile platform with extra computing power and rich in services.

Besides mobility, the ambient nature of the provided services is also an extremely interesting feature that future technologies should definitely support. Ambient networks, either in public or private spaces allow users to be aware of local and

remote services while on the move. Some of these services could be provided by wireless sensor networks, systems that might integrate thousands of low cost, self organizing and self-managing devices to support various kinds of applications.

In the same time, permanent (mobile) access to a large range of services, provided by different devices/platforms is a complex task that requires research at all network layers. Mobility, heterogeneity and the scarcity of resources are some of the main features that need adequate management tools.

The rest of this paper is organized as follows. First, in section 2, we present the specific features of mobile ad-hoc networks. Then, in section 3 we describe the specificities of wireless sensor networks that differentiate them from both the traditional wired systems and the previously described mobile ad-hoc networks. In section 4 we present then some of the research challenges related to these special kinds of networks, challenges that should be in the focus of the research community in the following years.

2. Specificities of Mobile Ad-hoc Networks

Mobile Ad-hoc Networks (MANETs) consist of a group of devices (nodes) that communicate with each other over a wireless channel without any centralized control. This network is typically created in a spontaneous manner. The nodes are expected to cooperate in forwarding data packets from one node to another, thus forming a multi-hop ad-hoc network.

MANETs have some interesting properties that provide for certain application areas. Networks can be setup without deploying and relying upon infrastructure, communication can be cheap, and transmission power can be relatively low if the distances to neighbours are kept short. This makes them of interest for applications in the military area, for conferences & meetings, for leisure time activities, for vehicular & telematics applications, and for networks in circumstances like disaster recovery.

Nodes of a MANET are usually considered to have limited resources available, since they consist of mobile devices that are battery powered and of small physical extensions. For some specific scenarios, however, this is not necessarily the case, e.g., for the special case of a vehicular ad-hoc network where nodes are vehicles like cars or trucks which can have relatively high processing, storage and energy resources. Nevertheless, even in those cases resource efficiency is a major concern (e.g., communication with a parked vehicle must be very seldom; otherwise it will use up the battery).

MANETs differ from other communication networks (e.g. the traditional IP-based wired Internet) regarding several characteristics, features and parameters. In the following we briefly present some of these MANET specificities.

   a) *Dynamic nature of the network*: The mobility of nodes and the behavior as well as interest of users lead to various problems such as changes in the topology of the network, varying link characteristics, network splits due to communication / link failures or node outages (e.g., due to lack of power or user initiated shut-off), nodes newly joining or leaving the network etc. Compared to this, infrastructure-based networks are very stable and predictable.

b) *Sophisticated routing*: The aforementioned network instability makes routing much more difficult because the used routing protocols have to cope with these challenges. Further aspects include the treatment resp. avoidance of selfish nodes, i.e., nodes which do not relay packets from other nodes but want to use the forwarding service offered by them. Additionally, the used methods should able to satisfy the QoS (Quality of Service) requirements of the applications used in these networks, which will comprise real-time applications as well. Yet, QoS provisioning in MANETs is even more difficult than in wired networks because of, among others, arbitrary mobility, unreliable wireless links, signal fading and interference and the used channel access mechanisms.

c) *High security threats*: Ad-hoc communication introduces several challenges with respect to security mainly due to the mobility of the nodes, limited device resources, properties of the wireless channel and the lack of central co-ordination. MANETs are subject to various kinds of attacks. For example, wireless communication links can relatively easily be eavesdropped, known attacks like masquerading, man-in-the-middle, and replaying of messages are more easily carried out than in wireline networks. Moreover, deploying security mechanisms is difficult due to the inherent properties of ad-hoc networks, such as the high dynamics of their topology (due to mobility and joining/vanishing devices), limited resources of end systems, or bandwidth-restricted and possibly asymmetrical communication links. [1]

Due to these characteristics and differences, new protocols and mechanisms are needed for MANETs, and this not only at the network layer. Methods on various layers must be reconsidered in the light of MANETs; e.g., services can and will be provided by nodes in the network, discovering and using them will only be possible if the specific characteristics of MANETs are taken into account.

3. Specificities of Wireless Sensor Networks

Although, in the last years, we witnessed the increase in processing capabilities and in the bit rates of communication systems, we consider that, in a near future, an inversion of trends will occur: the next years will be marked by the conquest of the last resistant redoubts to the Internet phenomenon. However, these new technologic systems will not consist of devices with high processing power, but simply of networks of sensors. The widespread distribution and availability of small-scale sensors, actuators, and embedded processors is transforming the physical world into a computing platform.

Sensor networks consist of a number of battery powered sensor nodes. Each node is endowed with physical sensing abilities (such as temperature, light, humidity, toxic plume, or seismic sensors), limited processing and memory and short-range radio communication. These nodes collectively form a network and forward information gathered on a hop-by-hop basis in order to reach the desired destination. For the purposes of collecting and analyzing the data from the sensor nodes, a base-station or data sink may be the destination.

Although many protocols and algorithms have been proposed for traditional wireless ad-hoc networks, they are not well suited to the unique features and application

requirements of sensor networks. The main differences between sensor networks and ad-hoc networks can be summarized as follows:

- Sensor nodes are limited in power, computational capacity, and memory;
- Sensor nodes are prone to failure;
- The topology of the sensor network changes very frequently, usually not due to mobility, as in MANETs, but because of node failures, sleep scheduling algorithms or controlled changes in transmission power levels ;
- Sensor notes use a broadcast/multicast communication paradigm;
- Sensor nodes are densely deployed.

The positions of sensor nodes do not need to be engineered or predetermined, thus allowing random deployment even in inaccessible terrains. This means that sensor networks algorithms and protocols must possess self-organizing capabilities. Hence, network self-assembly and continuous network self-organization during the lifetime of the network in an efficient, reliable, and scalable manner are crucial for the successful deployment and operation of such networks. Furthermore, sensor networks are directed towards specific scenarios and according information exchange (based on data gathered by sensors) while MANETs are seen as general communication networks.

Decisions in daily life are based on the accuracy and availability of information. Sensor networks can significantly improve the quality of information as well as the ways of gathering it. For example sensor networks can help to get higher fidelity information, acquire information in real time, get hard-to-obtain information and reduce the cost of getting information. Therefore it is assumed that sensor networks will be applied in many different areas in the future. Application areas might be traffic management, environmental supervision, manufacturing, warehouse management, surveillance and security, health care, (bio)medicine or military applications.

Sensor networks differ from traditional wired (e.g., IP-based Internet), but also wireless (e.g., MANETs) communication networks regarding several characteristics, features and parameters. We already highlighted some of these specificities in the previous paragraphs. Let us now detail the most important aspects:

a) *Specific traffic characteristics:* The traffic patterns in the Internet are difficult to predict as they are caused by a variety of applications used by many different users. In a sensor network, traffic is generated by homogeneous sensors monitoring one particular phenomenon. Thus, the expected traffic pattern is clearly restricted by the dynamics of the physical properties of the monitored phenomenon. In the Internet a balanced traffic flow is observed as edge systems (hosts or entire networks) normally send and receive a similar amount of data. In a sensor network, a sink-biased traffic flow is observed. Traffic is generated by the sensors and is directed towards the sink used to analyze sensor data.

b) *Dynamic nature of the network:* The Internet is in many respects a very stable network. Routers have a constant forwarding capacity, links are stable regarding bandwidth and error rates and the topology is not changing frequently. This is different in a wireless sensor network. Routers (forwarding sensor nodes) might have fluctuating forwarding capacities, depending on their current power constraints. Links have a variable bandwidth and error

rate. Additionally the topology is changing frequently, depending on the availability of links between nodes.

c) *Unique network features:* Sensor networks provide features that are unique to this type of networks. Sensor nodes might perform data processing before data is forwarded in the network. A sensor node might for example perform data aggregation - fusing data of several messages into one - on data that is transported. This results in an alternation of the network traffic in a way that is not perceived in the traditional Internet.

d) *Unusual priorities of network parameters*: The utility of a sensor network is characterized by parameters that are not taken into account in the classical Internet. The most prominent example is the parameter power consumption that defines ultimately the lifetime of a sensor network. Therefore, different solutions, such as clustering, data aggregation or adaptive sink mobility [2][3] are specifically developed to increase the energy efficiency of the system. Other specific network parameters can be CPU or memory requirements in the nodes; they need to be minimized in a sensor network to reduce node cost. On the other hand, some parameters that are most important in the Internet play a secondary role in a sensor network. For example, data throughput is important in the Internet; in most sensor networks, small data volumes have to be transported and thus throughput is not the main concern.

e) *Unattended and autonomous operation:* Sensor networks are usually considered to be quickly and/or massively deployed and with minimal initial configuration and ongoing supervision.

The aforementioned differences make it impossible to use existing network strategies directly within wireless sensor networks. Thus, existing methods must be modified to be useful within sensor networks. If a modification is not possible or feasible, new strategies must be explored.

4. Research Challenges

Due to the above mentioned specificities of MANETs and wireless sensor networks, various research challenges have to be addressed ny the research community. In the following we raise several of those which we consider as highly important.

4.1 Mobile Ad-hoc Networks

Realistic scenarios: MANETs are more sensitive to the specific type of application scenario than the traditional Internet due to the highly varying communication characteristics. E.g., depending on the specifics of the Mobile Ad-hoc Network such as its number of nodes, physical extension, mobility model, node speed etc., the choice of a suitable routing scheme can vary substantially. Often, studies of routing protocols are done for relatively large topologies; however, it is unclear whether this will be realistic considering the underlying link layer technologies. Hence, realistic application scenarios should be developed.

Mobility models: Previous work showed that the choice of specific mobility models for network simulations has significant effects on the simulation results. Hence, realistic movement patterns are very important for network simulations, but so far,

simplified models like random waypoint [4] are typically used within the research community. Realistic mobility models depend heavily on the particular application scenario, e.g., the behavior of conference delegates varies significantly from that of vehicles.[14]

Real world applications and measurements: In the past years, the design and development of protocols for MANETs has primarily been based on simulation studies. The use of common tools for these simulations has been very important to enable easy communication and exchange of results between different research groups, not only within Europe but worldwide. An example is the network simulator ns-2 [5]. It is widely accepted as one of the standard tools for wireless network simulation.

Currently, the research community realizes that the performance of protocols developed in the simulator needs to be proven in its real target environment. "Real world implementations" allow performance measurements on real devices which behave far from the assumptions made in the simulators. That means that only the implementation on real hardware (additional to simulations) is able to show the relevance of the developed protocols. The negative side of this is that real world experiments consume a lot of time compared to the produced results. This has to be simplified by constructing implementation and evaluation frameworks which have the power to establish standards for the evaluation of protocols in the real world, similar to simulators like ns-2.

Service provisioning: Network nodes offer certain services to the other nodes in the network. This requires methods for service discovery, service deployment, and service placement. All these strategies depend on the characteristics of the Mobile Ad-hoc Network as well as the resources of the nodes. [12, 13]

Transport protocols: It is well known that standard transport protocols such as TCP have difficulties to deal with the peculiarities of MANETs. Protocols which are capable to cope with the characteristics of these networks are needed, e.g., to address the varying connectivity, or delay issues. [6]

Internet integration: While MANETs provide communication means between nodes in that network, often access to the Internet resp. from the Internet to nodes is wanted. Hence, Internet integration is needed, using some types of gateways [7]. Depending on the particular application scenario, e.g., such as vehicular communication, gateways will be available from time to time only and not permanently; thus, relations to delay- and disruption-tolerant networks exist.

Security: Wireless communication is by definition much more vulnerable to security threats than the traditional wired solution. Any "adversary" that arrives near a wireless access point can disturb the communication, intercept, modify or even drop the packets of an authorized user. There are many approaches to handle these problems. However, some of them proved to be inefficient (e.g., the WEP), others might be too complex, heavyweight solutions for devices with very limited resources (e.g., sensors). Mobility only complicates further the situation. User authorization, authentication and accounting should be managed in a transparent manner, even for handovers between service areas of possibly different providers. Wireless routing solutions should also deal with security concerns. Current routing approaches typically assume a non-hostile environment. However, this is not necessarily the case.

One approach to deal with this is to use a reputation-based system based on personal perceptions and recommendations from neighbors.

4.2 Wireless Sensor Networks

To devise methods and strategies useful for wireless sensor networks and able to deal with the specificities presented in Section 3, different research directions can be pursued. Naturally, due to limited research resources, it has to be decided which research problems should be tackled first.

Small scenarios: Currently, research in sensor networks is focused on large-scale deployments of hundreds or even thousands of tiny sensor nodes communicating in a self-organizing fashion. Nodes are supposed to be able to detect other nodes in their neighborhood, distribute different tasks among each other and build communication topologies. Since energy consumption is among the most relevant concerns, energy-efficient protocols are needed to fulfill the overall task of such a network.

However, we believe that this vision is still a distant prospect. Most of the deployed sensor networks in the real world consist of far fewer than 100 nodes. There are still open problems regarding administration, communication, routing, synchronization, data retrieval, etc. Thus, for the near future, it will be inescapable to concentrate research more on smaller real world networks than on simulations using thousands of nodes.

Real world applications: The design of a sensor network is strongly influenced by the application scenario it has to support. Thus, research should take real application scenarios into account to ensure that solutions are applicable in real-world deployments. Much can be gained if we have generic interfaces to the development of sensor applications. These interfaces will hide different properties, and will support energy and quality of services requirements. However, there is much work to be done in this area.

Energy efficiency: Energy efficiency is a dominant consideration. This is because sensor nodes have only a small and finite source of energy. For these reasons the communication or message passing process must be designed to conserve the limited energy resources of the sensors.

Clustering sensors into groups, so that sensor communicate information only to dedicated nodes, called cluster heads, which are in turn responsible for sending the aggregated information to the processing center may save energy. Additionally, clustering in sensor networks provides scalability and improved robustness. Developing energy efficient clustering algorithms [8] is of high importance, especially for large sensor networks.

The development of an adaptive, energy-efficient MAC layer suitable for the decentralized sensor network environment is also an important aspect. Another approach is to build on the exploitation of redundancy. If the nodes are not specifically positioned there is a higher probability that a sensor with high energy reserves can transmit the sensed data instead of a neighbor with lower leftover power.

Localization: In most of the cases, sensor nodes are developed in an ad hoc manner. Knowing the geographic position of the nodes (localization) is a key enabler for most

sensor networks applications. Moreover, location awareness of nodes may improve routing in terms of communication overhead and therefore power consumption.

Collaborative Signal and Information Processing: Signals detected at physical sensors have inherent uncertainty, and they may contain noise from the environment. Detection, reading estimation, and location estimation are critical parameters. Solutions need to rely on fundamental theories of detection and estimation developed within other disciplines such as signal processing and information theory. These need to take into account the issue of synchronization as well. Sensor malfunction might also generate inaccurate data, and unfortunate sensor placement might bias individual readings.

Performance control: Wireless sensor networks are currently the subject of intense research and many prototype installations are currently investigated. These existing sensor network installations have in common that they are not considered time critical. No immediate action has to be undertaken as a response to the received data.

However, many future application areas of wireless sensor networks such as plant automation and control, traffic management or medical applications require this feature. In such environments, data has to be transported reliably and in time through the sensor network. In other words, performance guarantees regarding a variety of network parameters are required. Due to the lack of appropriate models, components and protocols, it is currently very difficult to construct and operate a wireless sensor network with a controlled performance. Thus, the commercial success of wireless sensor networks in many application areas is unsure unless this particular problem is understood and solved. Therefore, research towards performance control in wireless sensor networks is certainly of great importance.

Topology control: In a dynamic WSN nodes can change location, be removed, or added. A topological change occurs when a node disconnects and connects from/to all or part of its neighbors. In case of clustered networks modification of the cluster structure in the presence of topology changes leads to performance degradations in the network. The research in the area has to focus on maintaining a connected topology while minimizing energy consumption [9].

IP/Sensor network interconnection: Data gathered by a sensor network needs to be accessed through existing network infrastructures. Interworking between sensor networks and the IP-based Internet is required for this purpose. Appropriate strategies for this interconnection are needed. Although many argue that IP(v4) will never have, or even will be able, to be integrated in Sensor Networks, given its limitations, it is important to study and propose new models that extend and optimize IPv6 in Sensor Networks and, thus, to contribute to the Global Information Network. Current projects addressing TCP/IP integration in sensor networks do not explore key aspects of IPv6 functionalities, such as the larger address space, the neighbour discovery mechanism or the mobility support [10]. It is also crucial to solve a major limitation: the TCP/IP protocol stack is too complex for sensors with reduced processing power and leads to prohibitive power consumption. Therefore it is necessary to create lighters TCP/IP stacks, which can be easily portable to microprocessors, based on solutions from the 6LowPAN [11] IETF working group.

Security: Security issues in sensor networks need to be addressed in the future especially if an interconnection between sensor and IP networks is planned.

Furthermore, a single sensor network infrastructure might be used for different tasks at the same time which also requires security measures.

Network organization: Sensor nodes and the services they provide have to be organized within a network after deployment. To do so, methods and algorithms are necessary. One solution could be to assume self-configuring networks, which would be based on mechanisms that allow a sensor network to adapt its behavior to changing user objectives, environment characteristics, communication impairments, or power failures.

Mobility: Sensor networks are usually assumed to be composed by static nodes. However, recent studies proved the importance and the applicability of the mobility support in these networks. There are some studies that consider mobility at MAC Layer. As a future work, it would be also important to consider and study mobility at network layer [10].

5. Conclusions

In this paper we made an attempt to present an overview of the characteristics of mobile ad-hoc networks and wireless sensor networks and outline the research challenges we identify in each for the future. While several issues are similar between mobile ad-hoc networks and wireless sensor networks, they often differ when looking more deeply into their requirements and specifities. We believe that both network technologies can provide for exciting new application areas. In order that this vision becomes true, more research on important challenges is needed.

Acknowledgement

References

[1] Marc Bechler, Hans-Joachim Hof, Daniel Kraft, Frank Pählke, Lars Wolf: *A Cluster-Based Security Architecture for Ad Hoc Networks*, Proceedings of INFOCOM2004 (The 23rd Conference of the IEEE Communications Society), Hongkong, March 2004

[2] Z. Vincze, D. Vass, R. Vida, A. Vidacs, *Adaptive Sink Mobility in Event-driven Sensor Networks*, INC 2006, 6th International Network Conference, Plymouth, UK, July 2006.

[3] Z. Vincze, D. Vass, R. Vida, A. Vidacs, A. Telcs, *Adaptive Sink Mobility in Event-driven Multi-hop Wireless Sensor Networks*, Intersense 2006, First International Conference on Integrated Internet Ad hoc and Sensor Networks, Nice, France, May 2006.

[4] T. Camp, J. Boleng, and V. Davies, *A survey of mobility models for ad hoc network research*, Wireless Communications and Mobile Computing (WCMC) – Special issue on Mobile Ad Hoc Networking: Research, Trends and Applications, vol. 2, no. 5, pp. 483–502, 2002.

[5] Information Sciences Institute ISI, *The Network Simulator ns-2*, http://www.isi.edu/nsnam/ns/

[6] M. Bechler, S. Jaap, L. Wolf: *An Optimized TCP for Internet Access of Vehicular Ad Hoc Networks*, in Proceedings of the IFIP Networking Conference, Waterloo, Canada, May 2005

[7] Marc Bechler, Walter Franz and Lars Wolf: *Mobile Internet Access in FleetNet*, in 13. Fachtagung Kommunikation in Verteilten Systemen (KiVS 2003), Leipzig, February 2003

 [8] L. Tzevelakas, A. Ziviani, M. D. de Amorim, P.Todorova, and I. Stavrakakis, *Towards Potential-Based Clustering for Wireless Sensor Networks*, CONEXT 2005, First International Conference on Emerging Networking Experiments and Technology, Toulouse, October 2005

[9] P.Gober, A. Ziviani, P.Todorova, M. D. de Amorim, Ph. Huenneberg, and S. Fdida, *Topology Control and Localization in Wireless Ad Hoc and Sensor Networks,* Ad Hoc&Sensor Wireless Networks, Vol. 1, pp.01-21, Old City Publishing, Inc. 2005.

 [10] T. Camilo, J. Sá Silva and F. Boavida, *IPv6 in Wireless Sensor Networks, a New Challenge*, First International Workshop on Convergence of Heterogeneous Wireless Networks, Budapest, Hungary, July 2005

[11] IPv6 over Low power WPAN (6lowpan) – IETF Working Group charter http://www1.ietf.org/html.charters/6lowpan-charter.html

[12] Dan Grigoras, Mark Riordan, *Service Driven Mobile Ad Hoc Networks Formation and Management,* Proceedings of ISPDC 2005 July 2005, Lille, France

[13] Laurentiu Petrea, Dan Grigoras, *Mobile Code Platform for Ad-Hoc Networks* , Proceedings of the IEEE INFOCOM 2005, Student Workshop

[14] Patrick McCarthy, Dan Grigoras, *Multipath Associativity Based Routing,* Proceedings of the WONS 2005, St. Moritz, Switzerland.