Self-Management of Wireless Base Stations

Kai Zimmermann, Lars Eggert, Simon Schütz and Marcus Brunner
NEC Europe Ltd., Network Laboratories, Kurfürstenanlage 36, 69115 Heidelberg, Germany
kai.zimmermann@rrz-raisdorf.de, {eggert|schuetz|brunner}@netlab.nec.de

***Abstract*— This paper presents an autonomous, self-organizing and decentralized configuration and management system for a group of base stations in wireless networks. Compared to existing systems, where a central node computes and disseminates management information, the system's decentralized operation improves reliability by eliminating central points of failure and can decrease convergence times for large installations by enabling localized reconfiguration. A second novel feature is the integration of external, third-party input into the distributed configuration algorithm, improving the quality of the configuration result and convergence times. The paper briefly describes the decentralized management approach and presents experimental results that illustrate the system's performance and scalability properties.**

I. Introduction and Motivation

The Internet has included wireless links almost since its beginning. Satellite-based communication [5], early radio networks such as ALOHANET [1] or packet radio networks [10] provided connectivity without wires in the early Internet. However, these systems were not available or affordable by many users and consequently not very prevalent.

Wireless local area networks (WLANs) based on the IEEE 802.11 family of standards [8] started to provide mass-market wireless connectivity ten years ago and are still becoming increasingly more popular. Today, third-generation cellular networks are becoming a second alternative for wireless access across longer distances. In the future, other wireless access technologies, such as WiMax, various ultra-wideband technologies or future-generation cellular networks [11], will provide even more users with a variety of different wireless access technologies. Wireless connectivity is becoming ubiquitous.

Providing wireless connectivity to a larger geographic area requires deployment of multiple base stations, each of which covers a fraction of the total region. This is independent of the specific network technology used to provide this connectivity. The most popular deployment method is access networks that extend a wired core network by a single wireless hop. Deployment of multi-hop wireless access networks is also possible, but less popular due to the intrinsic complexities of this approach, for example, self-interference when forwarding across wireless links.

Once deployed, a group of wireless base stations requires continuous management to provide a uniform service environment, recover from faults or maximize overall performance. Manual management of each base station is only possible for very small groups. As the group of deployed base stations grows, automated management becomes a necessity.

Very few wireless network technologies include adequate management mechanisms. Even if they do, these systems typically only focus on physical or link-specific characteristics and do not manage higher-layer properties. For example, WLAN networks do not include any management functions. Each base station provides an area of wireless coverage that is completely isolated from its neighbors and manages it independently.

Existing approaches to managing WLAN access networks that consist of multiple base stations are primarily centralized. A central master system periodically computes a global configuration for the whole network based on available information. It pushes this configuration out to the individual base stations in a piecemeal fashion or they pull their respective configurations in from the master. A centralized approach has several disadvantages. First, it creates a central point of failure.Second, a central master limits scalability due to processing and communication overheads, especially in environments that require frequent configuration changes. Third, it complicates the system by introducing additional infrastructure, *i.e.*, the central master.

This paper presents a decentralized approach for management of a group of collaborating base stations. The individual base stations aggregate and share network information. They implement a distributed algorithm that computes a local configuration at each base station based on the shared information such that the overall network-wide configuration is consistent. Although the current prototype described in this paper focuses on managing a WLAN access network, the general mechanism is applicable to other wireless and wired access technologies.

A decentralized approach is inherently more resilient to failure. As each base station computes a local configuration based on exchanging information with its neighbors, it can react locally to changes in its local environment without involving a central master node. Furthermore, a decentralized system allows a group of base stations affected by a local change in their environment to react locally. This can improve scalability, convergence time and communication overhead.

II. Related Work

Two different paradigms exist in managing wireless networks. Centralized systems use a single master device to configure a group of base stations or a small group of cooperating master devices for very large networks. The second approach is decentralized. Here, the individual base stations are autonomous entities that collaborate as peers to arrive at a consistent, system-wide configuration. This section describes existing approaches in both areas and briefly outlines a third, hybrid approach.

Several companies provide centralized management solutions for groups of wireless base stations [3] [4]. The majority of these systems implement link-layer "wireless switches" that connect base stations that act as wireless bridges to a switched wired network. The link-layer switch implements the management component. This centralized, link-layer approach offers traffic and channel management, policy, bandwidth and access control. Additionally, this solution provides intrinsic roaming, because the management device can handle client movement at the link layer.

Centralized link-layer solutions also have drawbacks. Link-layer broadcast domains cannot arbitrarily grow due to the

scalability issues associated with broadcast traffic. Additionally, the topology of the wired network may not allow direct connection of the management system to the base stations. Centralized network-layer solutions address this shortcoming.

Decentralized management solutions are popular to configure mobile *ad hoc* networks. These management systems typically focus on the challenging task of enabling peer-to-peer communication in highly dynamic, mobile environments [2] [9]. In contrast, the decentralized solution presented in this paper focuses on configuring a stationary wireless access network for mobile clients, with the goal of improving efficiency and performance.

In addition to centralized and decentralized approaches, hybrid approaches exist [15] as well. These systems push some functionality from a central system into the base stations, which are therefore slightly more complex than the simple wireless bridges of centralized approaches. Although hybrid systems offer minor scalability increases, they do not completely address the drawbacks of centralized systems.

III. Decentralized Base Station Management

This section briefly describes the decentralized solution for wireless network management, including assumptions, the basic idea, security issues and several example applications. A more detailed description of the system and prototype implementation is available at [17] and [16].

A base station in the decentralized management system has to fulfill several requirements. Each base station is a full-fledged IP router for its IP subnet and can operate stand-alone. It needs at least two network interfaces: one to provide wireless services to its clients and a second interface (wired or wireless) for up-link connectivity. Additional wireless interfaces, when present, can be used as dedicated channel scanning interfaces, provide multi-homed up-link connectivity or offer additional client connectivity on different channels or link protocols.

A. Basic Operation

Although each base station is able to operate in a stand-alone fashion, integrated management of a group of base stations that provide connectivity to a geographic region requires collaboration. This collaboration occurs through periodic information exchange across the *up-link interfaces*.The information managed by each base stations falls into three categories:

Private information is only relevant to one specific base station, which consequently never disseminates it and is thus not discussed further in this paper.

Local information is of interest to *neighboring* base stations that are in radio range of one another and hence need to coordinate how they provide wireless connectivity to their coverage area. Local information includes channel use and utilization, current transmission power and number of associated clients, among others. Local information is disseminated to direct neighbors only.

Global information is management information that needs to be consistent throughout the entire wireless network. It includes, for example, security parameters, wireless protocol, ESSID, etc. The management system disseminates global information throughout the system through *epidemic* replication [6], i.e. a base station *periodically* disseminates information to its direct neighbors, which will further disseminate it to their respective neighbors in the next period. Note that this process requires transactional semantics to protect against inconsistencies.The current system implements a very simple method of guaranteeing global consistency based on the election of a central locking service. Future revisions will replace this method with a more scalable variant.

When the network view changes – either because of a locally monitored change in the environment or reception of new information from a peer base station – the configuration may be adapted and the resulting configuration gets propagated with the next periodic information exchange.

B. Base Station Bootstrap

After powering on, a base station configures its IP connectivity [12] and performs a wireless channel scan to detect other base stations in its immediate neighborhood. If no neighbors are detected, it switches to a default configuration.

Otherwise, it attempts to determine the neighbors' up-link IP addresses to initiate a management information exchange. Therefore, it issues *resolution requests* for the neighbors' MAC addresses seen during the channel scan. When receiving a resolution request, base stations reply with the IP addresses of their up-link interfaces.

At present, two different resolution mechanisms are implemented. First, a base station can attempt to briefly become a *client* of its neighbor and issues the resolution request over the wireless network, which is problematic when neighbors secure their wireless network and cannot support parallel resolution of multiple neighbors. Second, a base station can broad- or multicast resolution requests over the up-link network, which may be problematic on routed networks. Future revisions of this work will investigate additional resolution mechanisms and their specific trade-offs.

As a last step, a base stations starts to exchange local and global information with its neighbors and derives its own configuration from gathered information.

C. Management System Functionality

The current management system specifically targets WLAN access networks. It coordinates radio properties, such as channel use or transmission power, among a group of neighboring base stations. It also implements system-wide functions, such as load balancing. By exchanging utilization information, neighboring base stations can distribute client load by raising or lowering transmission power or link speeds. Overloaded base stations, for example, can push clients at the edge of their range onto other base stations by lowering their transmission power.

A second example of a system-wide management function is self-protection through the detection of *rogue* access points. Rogue access points are base stations located within radio range of the managed WLAN access network do not belong to it. They are potential security threats, because they may attempt to spoof clients into associating with them instead of the actual access network and then intercept their traffic. The current management system detects rogue access points and disseminates their presence throughout the system, preventing any legitimate base station from communicating with these nodes.

A third system function provides a means to obtain a global view of the system, *i.e.*, retrieve local information from all participating base stations of the system, for logging, administrative and monitoring purposes. The decentralized measurement system can support this functionality without the need of an explicit logging function. Instead, a *virtual*

neighbor can disseminate its ID throughout the system and thus appear in each base station's neighbor list. The virtual neighbor will then receive the local information that is disseminated by each base station as if it was simultaneously in radio range of all base stations. The virtual neighbor can aggregate and export this system-wide information for a variety of uses.

Additional functions like coverage hole detection and closing, location tracking, management of access control, intrusion detection or even automated software updates may be integrated into the management system in the future.

D. Security Considerations

A decentralized management system must fulfill several security objectives. First, it must protect sensitive information against unauthorized access. Second, it must protect the distributed configuration algorithm from attacks. Third, it must prevent management functionality to be abused as an attack tool, *e.g.*, for flooding attacks. These security aspects are similar to those found in *ad hoc* networks [13].

The prototype uses pre-installed X.509 certificates in combination with two-way authentication addresses all these security objectives. Traffic encryption protects sensitive information while digital signatures allow verification of the authenticity of management communication, protects the operation of the distributed algorithm and consequently mitigates the use of management functions for attacks.

Installation of base station certificates and the corresponding authority certificates still requires one-time manual configuration of base stations. However, methods for semi-automated certificate configuration – such as physically connecting to a mobile certification authority that auto-installs required certificates on first boot – can significantly shorten the configuration process. However, the specifics of such approaches are outside the scope of this paper.

E. Integration of External Information

An inherent problem of the approach taken are *hidden neighbors*, i.e. base stations that have overlapping coverage areas but are outside of one another's radio range (see Figure 1). Hidden neighbors should exchange local information, but fail to detect each other's presence during the channel scan. Consequently, their configurations will not be coordinated, potentially leading to an inconsistent overall network configuration.

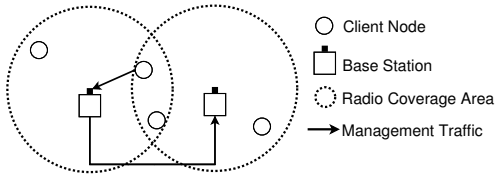

Fig. 1. Integration of information from external nodes.

Integrating *external information* into the configuration process can improve the detection of hidden neighbors. *External information* does not originate at collaborating base stations, but from some external probe node. This paper assumes that probe nodes are user-operated clients of the WLAN access network, but they could also be specialized nodes under control of the WLAN operator [7].

If probe nodes notify base station about which other base stations are within their own radio range, the management system can recognize hidden neighbors when probe nodes enter an overlap area. However, the inclusion of external information also has drawbacks. First, it requires additional software to be present on probe nodes. Second, the system must carefully verify the trustworthiness of external information before acting on it.

External information can improve the self-healing and self-optimization functions of a decentralized management system in other ways. It enables detection of interferences or holes in coverage, can identify rogue access points outside the range of the base stations themselves, aid location tracking. Passive mobile clients – *i.e.*, users-carried devices – can already significantly support the management system. Active clients – *e.g.*, self-propelled robots under control of the management system – are even more useful, because the system can use them to obtain targeted information.

After evaluation of the general scalability and performance characteristics of a prototype implementation, the next section briefly assesses the benefit that external information has on system operation.

IV. Evaluation

The current system prototype is a Perl daemon that is capable of operating on physical hardware, *i.e.*, a Linux PC equipped with IEEE 802.11a/b/g WLAN interfaces. However, an analysis of the scalability properties using physical devices is impractical as it would require a large number base stations. Therefore, the prototype offers a simulation mode, where multiple instances of the same code execute on a single PC inside a simulated topology. The measurements in this paper are based on this simulation mode.

The remainder of this section evaluates different aspects of the prototype implementation. Sections IV-A and IV-B evaluate the performance with regard to an initial startup of a set of base stations and with regard to changing global information, respectively. Section IV-C analyzes the management traffic generated during initial startup. The benefit of including external information is evaluated in section IV-D.

A. Initial Self-Organization Time

The first set of experiments investigates the convergence time of a group of base stations if all start up within a few seconds of one another, *i.e.* the time of the initial self-organization, such as after a power failure. Mobile client nodes are not present. The experiment was repeated 50 times and the results show the calculated mean value and standard deviations. Each repetition uses a randomly generated, connected base station topology, *i.e.* the aggregate coverage area of the base station group is not geographically partitioned and the corresponding graph of neighbor relationships is connected. This is arguably a common deployment case.The number of base stations is a parameter of the experiment and varies from 1 to 100 in increments of 10, with two additional group sizes of 5 and 15 to investigate behavior for small groups.

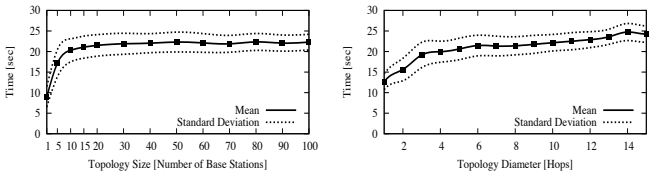

Fig. 2. Initial self-organization time of a group of base stations by topology size (left) and diameter (right).

The left graph of Figure 2 shows the results of the experiment. For smaller groups of 1-20 base stations, the mean initial self-organization time quickly increases to approximately 20 seconds. For larger groups of 20-100 base stations, the mean initial self-organization time remains between 20 and 25 seconds, thus indicating only a minor increase in self-organization time with respect to a growing number of base stations. Self-organization time remains nearly constant for groups of 50-100 base stations.

The right graph in Figure 2 shows the same results by topology diameter instead of topology size. The diameter is the distance between two nodes in the topology that are furthest from one another. After an initial ramp-up for small topologies, self-organization time appears to grow linearly with the topology diameter. This result seems to indicate that the system scales well with a growing number of base stations. The worst-case increase of the diameter – for a linear topology – is also linear with the number of the base stations; the best case – a full mesh – is logarithmic. Based on the specific topology of the neighbor graph, the actual increase will consequently be somewhere in between.

One observation is that self-organization times are already relatively long, even for smaller topology sizes. This is because the bootstrap process influences self-organization times. A base station first performs an initial, random 0-10 second de-synchronization delay before initiating its channel scan to detect and contact its neighbors. The channel scan takes approximately 2 seconds and following a base station has to communicate with its neighbors.Therefore, the bootstrap process for a single base station may already take around 10 seconds.

Note that the current prototype implements a scanning mechanism that can only detect neighbors already offering client connectivity, *i.e.*, being infrastructure mode. A future revision may extend this behavior to detect neighbors that are themselves still channel scanning. With such a mechanism, the de-synchronization delay can be significantly reduced, further reducing initial convergence times.

B. Convergence Time After Changes to Global Information

This section evaluates the system performance when global information changes. The evaluation scenario uses randomly generated topologies for each repetition as in the previous section and the system is already self-configured into a consistent state. Then, a randomly chosen base station introduces a modification to global information, *e.g.*, an administrator logged on and changed the ESSID to be used. The experiments measure the propagation time until the change has been disseminated to all base stations. Again, the number of base stations is a parameter of the experiment and varies from 1 to 100 in increments of 10, with two additional group sizes of 5 and 15 to investigate behavior for small groups. The results show the mean convergence time and standard deviations across 500 repetitions.

The left graph in Figure 3 shows a logarithmically increasing convergence time. This behavior illustrates the scalability properties of the epidemic dissemination mechanism. To evaluate the influence of topology diameter on the convergence time, the right graph in Figure 3 shows the same results by topology diameter. Similar to the results for initial self-configuration time, the convergence time for a change to global information grows linearly with the topology diameter. As before, this seems to indicate that the system scales well with larger groups of base stations.

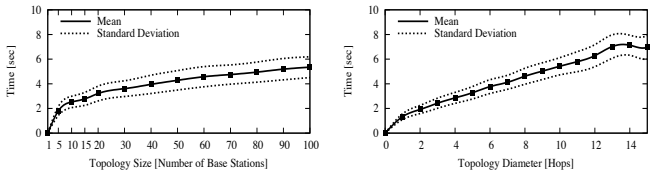

Fig. 3. System convergence time after a change to the global configuration information, by topology size (left) and diameter (right).

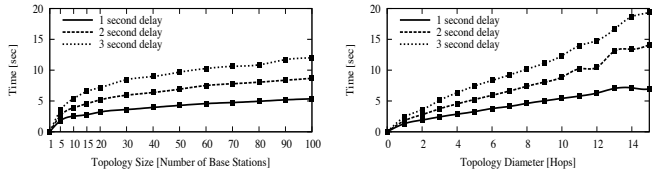

Fig. 4. Impact of different forwarding delays on convergence times for changes to global information, by topology size (left) and diameter (right).

With an epidemic dissemination mechanism, each base station informs its neighbors about changes in fixed, periodic intervals. The measurements above use a default period of 1 second between successive messages.Shorter periods result in faster convergence times, but increase load on the network. Longer periods further reduce load on the network, but lead to longer convergence times. Figure 4 illustrates this effect.

C. Management Traffic

Whereas the previous sections evaluated the convergence times of different system operations, this section investigates the amount of management traffic injected into the network.

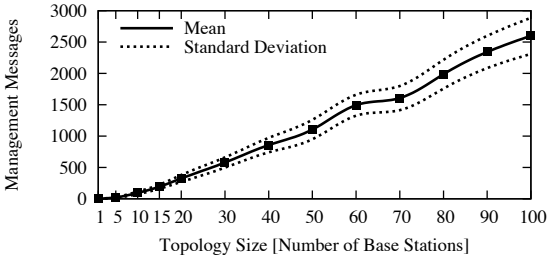

Fig. 5. Management traffic to perform initial self-organization.

Figure 5 shows the number of management information exchanges during the initial configuration for different topology sizes. The results indicate that the amount of management traffic grows linearly with the topology size. For topologies with 100 base stations, the mean approaches 2500 management messages – each base station contacts 25 others on average. Although this seems high, note that these messages are distributed over the duration of the self-organization period, which is usually longer than 20 seconds.

D. Quantitative Benefit of Integrating External Information

A key part of the self-management system is the integration of external information. A quantitative evaluation of the benefits of this technique is difficult. This section presents one preliminary case to illustrate the benefits of including external information by investigating how many "hidden neighbor" relationships can be detected if an increasing number of clients reports to the measurement system. (As before, hidden

neighbors are base stations with overlapping coverage areas that are not directly in range of one another.)

This experiment generates 100 random topologies with 100 base stations. Although the coverage areas of these networks are all continuous, the neighbor relationship graphs are *not* connected, due to the presence of hidden neighbors. In each topology, 500 clients are distributed randomly. The experiment measures the level of connectedness of the neighborhood graph if a given percentage of randomly chosen clients report neighborhood information to the management system. The results present the mean percentages and are shown in Figure 6. This analysis allows to investigate how many clients need to provide input such that the overall management system shows significant benefits.

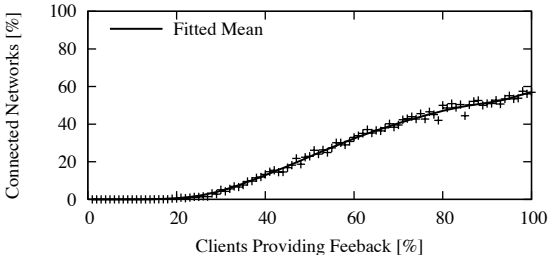

Fig. 6. Benefits of integrating external information.

Figure 6 shows that if 20% of the clients report back to the management system, the first benefits become apparent – some hidden neighbors are eliminated. With an increasing percentage of clients that report to the system, the connectivity percentage increases linearly. In the best case, when all clients report back to the management system, around 50% of hidden neighbors are detected and eliminated.

At first, this result seems low. However, note that only clients within an overlapping coverage area can provide fresh information to the management system. Additionally, the clients in this scenario did not move and can therefore only provide information for a single position within the coverage area. The results are expected to be significantly better with mobile clients over a longer period of time. Still, this result shows that integrating external information improves overall management system operation.

V. Conclusion and Future work

This paper introduced and motivated a distributed approach for wireless base station management and configuration and compared it to existing and mostly centralized solutions. One novel feature of the presented system is the integration of external information into the distributed management process to improve the quality of the configuration result. The paper outlined the current system and prototype implementation and presented a scalability analysis with regard to system startup, network state modification and management traffic. Results indicate that the presented solution scales well with large numbers of base stations. Integration of external information can significantly reduce management partitioning in case that base stations have overlapping coverage areas but are not in radio range to each other.

Improvement and extension of the current prototype is ongoing. Additional management functionalities will be developed, implemented and evaluated. The central locking mechanism to provide transactional semantics for global information will be replaced by a more scalable variant. Additionally, a more detailed scalability analysis for larger networks and additional system operations is currently being planned.

Although the current base station configuration system specifically targets WLAN networks, the general idea of decentralized management certainly applies to other wireless and wired networks. The current system provides a decentralized management "middleware" on top of generic methods for information dissemination that can be adapted to other network technologies in the future.

Acknowledgment

This document is a byproduct of the *Ambient Networks* project, partially funded by the European Commission under its Sixth Framework Program. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the *Ambient Networks* project or the European Commission.

References

[1] N. Abramson. Development of the ALOHANET. *IEEE Transactions on Information Theory*, Vol. 31, No. 2, March 1985, pp. 119-123.

[2] Advanced Cybernetics Group and Meshdynamics. Why Structured Mesh is Different. *White Paper*, 2004.

[3] Airespace Corporation. Putting the Air Space to Work. *White Paper*, October 2003.

[4] Aruba Wireless Networks. Getting a Grip on Wireless LANs. *White Paper*, January 2003.

[5] V. Cerf. Packet Satellite Radio Reference Sources. *RFC 829*, November 1982.

[6] A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart and D. Terry. Epidemic algorithms for replicated database maintenance. Proc. *6th Annual ACM Symposium on Principles of Distributed Computing*, Vancouver, British Columbia, Canada, 1987, pp. 1-12.

[7] S. Felis, J. Quittek and L. Eggert. Measurement-Based Wireless LAN Troubleshooting. Proc. *First Workshop on Wireless Network Measurements (WiNMee 2005)*, Riva del Garda, Trentino, Italy, April 3, 2005.

[8] IEEE-SA Standards Board. ANSI/IEEE Standard 802.11. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *ANSI/IEEE Standard*, 1999.

[9] L. Ji, J. Agre, T. Iwao and N.Fujino. On Providing Secure and Portable Wireless Data Networking Services: Architecture and Data Forwarding Mechanisms. Proc. *International Conference on Mobile Computing and Ubiquitous Networking (ICMU 2004)*, January 2004.

[10] J. Jubin and J.D. Tornow. The DARPA Packet Radio Network Protocols. *Proceedings of the IEEE*, Vol. 75, No. 1, January 1987, pp. 21-32.

[11] N. Niebert, M. Prytz, A. Schieder, L. Eggert, F. Pittmann, N. Papadoglou and C. Prehofer. Ambient Networks: a Framework for Future Wireless Internetworking. To appear: Proc. *IEEE 61st Semiannual Vehicular Technology Conference (VTC 2005 Spring)*, Stockholm, Sweden, May 30 - June 1, 2005.

[12] J. Silva Tobella, M. Stiemerling and M. Brunner. Towards Self-Configuration of IPv6 Networks. *Proc. Poster Session of IEEE/IFIP Network Operations and Management Symposium (NOMS'04)*, Seoul, Korea, 2004.

[13] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. Proc. *7th International Workshop on Security Protocols*, Cambridge, UK, April 1999, In *Lecture Notes in Computer Science (LNCS)*, Vol. 1796, Springer Verlag, Heidelberg, Germany, pp. 172-182.

[14] A. Tanenbaum and M. van Steen. Distributed Systems, Principles and Paradigms. Prentice Hall Inc., NJ, USA, 2002.

[15] Trapeze Networks. Defining An Integrated Access Point. *White Paper*, 2004.

[16] K. Zimmermann. An Autonomic Approach for Self-Organising Access Points. *M.S. Thesis*, University of Ulm, Germany, April 2005.

[17] K. Zimmermann, L. Eggert and M. Brunnner. Self-Management of Wireless Base Stations. Invited paper, *Proc. IEEE Workshop on Management Issues and Challenges in Mobile Computing (MICMC 2005)*, Nice, France, May 14, 2005.