Master's Thesis

Kai Zimmermann

An Autonomic Approach for Self-Organising Access Points

Supervisors:

Dr. Marcus Brunner, Dr. Lars Eggert and Dr. Stefan Schmid

NEC Europe Ltd., Network Laboratories

Kurfürsten-Anlage 36, 69115 Heidelberg, Germany

Examiner:

Prof. Dr.-Ing. Franz J. Hauck

University of Ulm, Faculty of Computer Science

James-Franck-Ring, O-27/348, 89069 Ulm, Germany

Eidesstattliche Erklärung

Hiermit versichere ich, die vorliegende Arbeit selbstständig und unter ausschließlicher Verwendung der angegebenen Literatur und Hilfsmittel erstellt zu haben. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

_____

Kai Zimmermann. Heidelberg, den 31.03.2005

Abstract

This thesis presents an automated and decentralised configuration and management system for sets of autonomic base stations in wireless access networks. The system implements self-configuration, self-optimisation, self-healing and self-protection. Compared to existing centralised systems, where a central management device computes and disseminates management information, this system improves reliability by eliminating the central point of failure and can increase performance due to parallel communication and processing. A second novel feature of this approach is the integration of external information into the distributed algorithm, further improving the quality of the configuration result. This thesis describes the proposed approach and its prototype implementation. It also presents a qualitative evaluation and experimental results that illustrate the scalability properties of the system. It finds that the prototype implementation of a self-managed wireless access network scales with large numbers of base stations.

Acknowledgement

Without the encouragement and the help of many people this thesis could not have been completed. I have to thank all the colleagues working at the *Next Generation Internet group* of the NEC Netlabs in Heidelberg/Germany.

I would like to thank my supervisors for all their help, their advice, and the inspiring discussions we had. Especially, I would like to thank **Dr. Lars Eggert** for reading my paper and providing me with technical and linguistic advice. This work could not have been done without his help. Furthermore, I have to thank my examinator **Prof. Dr.-Ing. Franz J. Hauck** from the *University of Ulm* and my manager **Dr. Jürgen Quittek** for their help. I'm also very grateful to my parents for their financial and mental support.

I dedicate this paper to **Manuela Dettling**, who always supported me, gave me advice from a non-technical point of view and listened patiently to all my endless monologues. Thank you for your love and your understanding.

Contents

List of Figures

Chapter 1

Introduction and Motivation

During the last years, the traditional world of networking has changed. Radio networks allow users to become more mobile and flexible. With the success of IEEE-802.11 based radio networks and the third generation cell-phone, participants of today's global network community are used moving freely while they are connected to the *Internet*. Next to the private consumer, more and more enterprises are using wireless access networks to allow their employees improved mobility inside their buildings and at any place where their business occurs. Next to this, it allows enterprises to maintain a flexible and reusable network infrastructure. It is possible to redeploy the equipment if the organisation makes a need for change.

These wireless access technologies have been successful because they allow people to be connected independently of their location. While this radio technology has been growing over the years, the lack of proper management capabilities for these networks became obvious. This thesis contributes to the ongoing research process in the area of wireless access network management.

1.1 Contributions

Very few wireless access network technologies include adequate management mechanisms. Even if they include such mechanisms, these systems typically only focus on physical or link-specific characteristics and they do not manage higher-layer properties. For example, IEEE-802.11-based networks do not include any management functions. Each base station

provides an area of wireless coverage that is completely isolated from its neighbours. The management of each base station is independently of its neighbouring stations.

Existing approaches to managing IEEE-802.11-based access networks that consist of multiple base stations are primarily centralised. A central *master* system periodically computes a global configuration for the whole network based on available information. It then pushes this configuration out to the individual base stations in a piecemeal fashion, or they pull their respective configurations in from the central system.

A centralised approach has several disadvantages. First, the creation of central points of failure make the system unreliable, *e.g.*, if the central management station fails the whole network is not able to deliver its services in an adequate manner. Second, the creation of network and computation bottlenecks by forcing the management operations through one node (the central management station) reduce the system's scalability capabilities, *i.e.*, any decision regarding network expansion is based on the management stations capabilities. Third, it complicates the system, because this approach introduces additional infrastructure, *i.e.*, the central master.

This thesis presents a decentralised approach for management of a set of collaborating base stations. The individual base stations aggregate and share network information in order to implement *self-management* functionality. 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. Each station acts fully *autonomically*, *i.e.*, they manage themselves based on high-level objectives [51]. Although the current prototype described in this thesis focuses on managing an access network based on IEEE-802.11 base stations, the general mechanism is applicable to other wireless access technologies.

Figure 1.1 shows four wired connected base stations and several mobile nodes inside their coverage area. They are not connected to central management station, thus acting autonomic.

A decentralised approach is inherently more resilient to failure. Because each base station

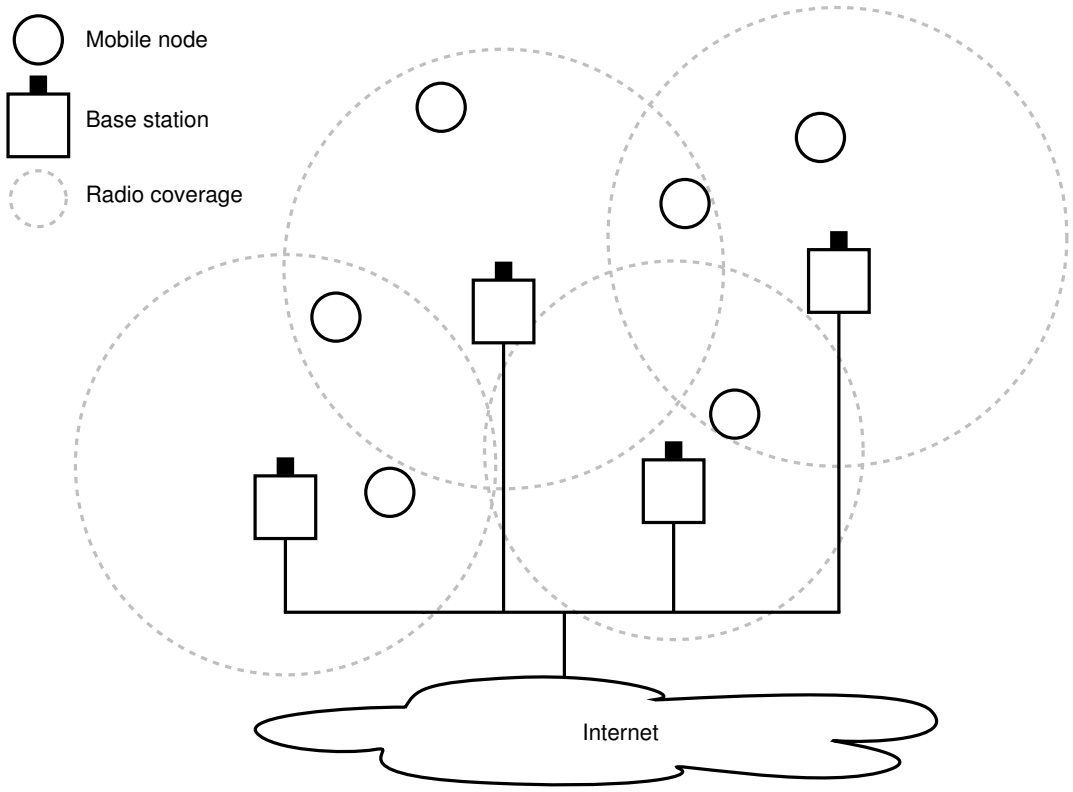

Figure 1.1: A wireless access network without a central management station.

computes a local configuration based on exchanging information with its neighbours, it can react locally to changes in its local environment without involving a central master. Furthermore, a decentralised system allows the group of base stations affected by a local change in their environment to react locally. This can improve scalability, convergence time and communication overhead.

A decentralised approach, however, also introduces challenges, for example, to guarantee convergence, establish system-wide consistency of the configuration, as well as trust issues between otherwise independent nodes or the problem of discovering new system members.

The next section explains the background to this thesis and shows the reason for developing new management capabilities for wireless access networks.

1.2 History and Background

The *Internet* has included wireless links almost since its beginning. Satellite-based communication [28], radio-based networks like ALOHANET [6] or *packet radio networks* [46] provided connectivity without wires in the early *Internet*. However, these systems were not available or affordable by many users and consequently not very prevalent.

The evolution of cellular networks introduced long-distance wireless connectivity for the masses. The first generation of mobile cellular networks was made available in 1983 with the *advanced mobile telephone system* (AMPS)[85]. The second generation (2G) like the *global system for mobile* (GSM) [55] introduced digital multiple access technology, *i.e.*, *time division multiple access* (TDMA) and *code division multiple access* (CDMA). It was developed in the 1980s and was available in 1991. Although the first generation supported primarily voice communication, second generation offered rudimentary data communication like the *short message service* (SMS).

The next step for cellular networks was to provide enhanced data-transport service to allow users to access their *Internet* services through their mobile-phone account. This was introduced with the *general packet radio service* (GPRS) [49] in the 1990s. Additionally GPRS allowed volume-oriented charging.

However, cellular networks still had low bandwidth, *i.e.*, they were not widely used for data transport. Third-generation (3G) cellular networks, *e.g.*, the *universal mobile telecommunications systems* (UMTS), made the execution of mobile applications possible through their higher transport capabilities [47].

Another key technology in the area of mobile communications are *wireless local area networks* (WLANs) based on the IEEE-802.11 family of standards [1]. They started to provide mass-market wireless connectivity ten years ago and are still becoming increasingly more popular. They are a low priced alternative for wireless access on short distances.

In the future, other wireless access technologies, such as WiMax [82], various ultrawideband technologies [60] or future-generation cellular networks [58][5][59], will provide even more users with a variety of different wireless access technologies. More information can be found in [77].

Wireless access networks offer a new kind of mobility. People may roam freely while being connected to a network and they can work at nearly any place they want [38][42], *e.g.*, a test engineer is able to retrieve information from his companies main frame while performing his measurements.

In addition, these networks give users a new kind of flexibility. They can connect whenever they want. The evolution in networking made a whole new industry possible. *Internet service providers* (ISPs) are now able to offer *public hot spots* in places like a municipal park, an airport or a hotel. Furthermore, running a wireless access network instead of a wired one may even be cheaper. There is no need for cable installations that are cost expensive and time consumptive. Historical buildings may not even allow installing a wired infrastructure.

Another movement that came up with wireless LANs are *grassroots community networks*. Volunteers connect together their private wireless infrastructure, offering a free service for all members, even guests.

Additionally, more and more applications and solutions appear on the wireless market. For example, key drivers for wireless LAN adoption are *voice over IP* [42], online games, video streaming and conferencing. Because of these, wireless networking has become more popular and wireless connectivity has 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 method of deploying these base stations is as access networks that extend the wired core network by a single wireless hop. Typical large area wireless access networks are described in [52][74].

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 [30][9].

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

1.3 Wireless Access Networks

This section defines the characteristics of a wireless access network. Furthermore, it introduces the concept of a self-managed wireless access network and lists the characteristics that such an network will have.

1.3.1 Components

A wireless access network contains two groups of nodes. First, the *base stations*, which provide wireless uplink connectivity to a wired network for the second set of nodes, the *mobile nodes*. Furthermore, they may provide services for the mobile nodes, such as authentication mechanisms, address allocation [34], domain name resolution [54] or routing. Note, that *access point* is a synonym for *base stations* in the area of IEEE-802.11 wireless LANs.

Mobile nodes use the *base stations* to connect to each other and to a (wired) network. They are mobile and roam between the base stations of the wireless access network, *i.e.*, detach from the current base station, change location and attach to another base station. Note, that *client* or *wireless client* are synonyms for *mobile nodes* in the area of IEEE-802.11 wireless LANs.

1.3.2 Characteristics

To implement a system outlined in Section 1.1 the first question that has to be answered is what makes wireless access networking different from wired networking and the problems that have to be taken care of, which do not exist in wired *local area networks* (LANs).

First, rapid environment changes, *e.g.*, radio noise, radio interference or signal attenuation [18]. For example, base stations change their radio channels or reduce transmit power in order to avoid interference with other senders.

Second, load changes that come with mobile users. New users may connect to a base station; they may leave or switch from one station to another. The base stations have to react with a load balancing mechanism in order to distribute the mobile nodes over the base stations. Furthermore, they can allocate additional or release unused resources, *e.g.*, processors or network bandwidth, to be able to serve a greater or lesser number of mobile nodes.

Third, security issues that arise with having a wireless access network. Malicious users may interrupt the communication, may catch sensitive information or spoof regular users. Even regular uses may not be trusted. These are problems that do not arise in a typical wired network, *i.e.*, the access to the network is restricted to those who have access to the wire.

Consequently, a management system for a wireless access network must be able to detect and to rapidly adapt those changes and, to be effective, establish the changes on all regarding base stations. In addition, the detection of security threats by the base stations, which have to be taken care of in the same way, *i.e.*, the threat must be reported to all regarded base stations and confronted by them. However, to find a solution for the variety of security threats in wireless access networks is outside the scope of this thesis (for more information see [37]).

1.3.3 Self-Managing Wireless Access Networks

To allow a wireless access network as defined in the sections above to be distributed and *self-managed* it needs *autonomic* base stations. For this kind of base stations, several goals are defined. The stations must implement *self-organisation*, *self-optimisation*, *self-configuration* and in order to implement this they have to be *self-adaptive*. Furthermore, the system should be *self-healing* and *self-protecting* in order to create a high available wireless access network. A further step is a *self-deploying* network as described in [56]. However, this is not targeted by this thesis but may be a target for future work.

Self-Organisation and Self-Optimisation

The self-managed wireless access network must be able to adapt changes detected by its members. This has to be done without external influence, *e.g.*, an administrator or a management station. The self-managed wireless access network continuously seeks for opportunities to improve its own performance and efficiency. If, for example, one base station has a large number of mobile nodes connected to it, it may inform its neighbouring stations about this fact and together, as a whole system, they may decide to readjust transmit power to force the mobile nodes to reconnect and get a more balanced result.

Self-Configuration

When a station starts up it must be able to integrate itself into the wireless access network without depending on a external management entity, e.g.*, a central management station or an administrator.* A self-configuring base station is able to determine its local configuration based on its locally collected information and the information retrieved from other base stations.

Self-Healing and Self-Protection

The self-managed wireless access network has to react to failures, errors and disruptions as fast as possible. The network automatically detects, diagnoses and repairs its components. For example, if a participating station fails, the neighbouring stations extend their radio

transmission power in order to ensure radio coverage. Furthermore, the system has to react on security threats and forced errors from malicious users. This also includes that the system tries to avoid such threads in the first place, *i.e.*, implements authentication and encryption mechanisms.

1.4 Problem Description

As a result of the definition of the capabilities of a *self-managed wireless access network*, the goals for the development of *autonomic base stations* can be described. They define the problems that have to be taken care of to let the vision of a self-managed wireless access network come true.

Each base station is *autonomous*, *i.e.*, has a local copy of management information and a local installation of the management mechanisms, in order to be able to self-configure itself.

To apply a self-organising mechanism that allows further self-optimisation the base stations have to be connected with each other in order to be able to exchange information. That means, they have to *find each other*, have to *contact each other* and *apply authentication* during their self-configuration process.

As mentioned, the network is self-adaptive, thus each base station has to *inform all others about changes in its environment.* Furthermore, the base stations have to *trust the exchanged management information.* and the *information has to be protected against malicious users* in order to ensure confidentiality (self-protection).

Additionally, the self-managed network needs a *communication paradigm that ensures high scalability*, *i.e.*, the exchanged traffic should not rise dramatically with a growing system of participating stations. *A station that cannot find any other suitable participants has to set a default configuration*, *i.e.*, each station must be able to work alone in order to ensure self-configuring capabilities for each individual base station.

Finally, a *base station that detects a failure or error has to solve it locally or, if necessary, inform other stations in order to solve it globally*, to implement a self-healing behaviour.

1.5 Research Objectives

To solve the various tasks that come with the idea of a decentral management mechanism for self-managed wireless access networks and to fulfil the defined targets in order to implement it, the main objectives for this thesis are:

1. Define a protocol that implements *self-configuration* for *autonomic* base stations.
2. Find a *self-adaptive* solution for the base stations behaviour.
3. Find applications that implement *self-protection*, *self-healing* and *self-optimisation* for the *self-managed* wireless access network.
4. Analyse the *scalability* of the proposed management system.

1.6 Thesis Organisation

Chapter 2 describes existing approaches for wireless LAN management and related work in the area of node collected information. Furthermore, it discusses related technologies and algorithms, *e.g.*, epidemic protocols. Chapter 3 presents the decentralised solution that is the key contribution of this thesis and different applications that may run on the proposed management system. Chapter 4 makes a quantitative evaluation of the prototype implementation and a qualitative discussion of the proposed concept. Finally, the conclusion and discussion of future work in Chapter 5.

Chapter 2

Related Work

Related work to the proposed management system exists in several areas. First, existing management solutions for wireless access networks are discussed, analysed and compared to the proposed management system, especially for IEEE-802.11 wireless LANs. Second, wireless LAN analysers are introduced, which are in several areas related to the nodes that provide external information to the proposed management system. Third, the ongoing work in the area of the integration of external information into the management process is described. Fourth, epidemic protocols that are used by the proposed concept for reliable and scalable information distribution are explained.

2.1 Management Solutions for Wireless Access Networks

Two different paradigms exist in managing wireless networks. Centralised systems use a single master device or a small group of cooperating master devices to configure a group of base stations. The second approach is decentralised. 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 describe a third, hybrid approach.

2.1.1 Centralised Management Systems

Several companies provide centralised management solutions for groups of wireless base stations [18][23][24][25][36]. 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 connection is typically based on the *lightweight access point protocol* (LWAPP) [27], which tunnels packets from the mobile nodes to the central management station.

The link-layer switch implements the management component. This centralised, link-layer approach offers traffic and channel management, policy, bandwidth and access control [42]. Additionally, this solution provides intrinsic roaming, because the management device can handle node movement at the link layer. Furthermore, centralised solution vendors promise a reduced *total cost of ownership* (TCO) for the wireless access network [17] compared to existing non-centralised and non-automated solutions.

Centralised 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. Centralised network-layer solutions address this shortcoming, *e.g.*, specialised network *appliances* or software installed on a personal computer [22][14].

Figure 2.1 shows four base stations. Two of them are configured by a wireless switch with link layer access. The other two cannot be access on link layer because of the router, thus a management appliance is used to establish *Internet* layer access to the base stations. An administrator can configure both management devices.

Furthermore, as mentioned in the introduction, a centralised approach has additional drawbacks, *e.g.*, the creation of central points of failure and the creation of network and computing bottlenecks.

Another problem comes with the traffic management. In many central solutions, the wireless traffic goes from the base stations directly to the central management station. However, the IEEE-802.11 standard is only about 45 percent efficient with encoding and encryption overhead, *i.e.*, an IEEE-802.11a/g capable base station actually inserts 54 Mb/s into the wired network that are only 25 Mb/s of actual wired IEEE-802.3 data [80]. These circumstances make the scalability problems that come with the central solution

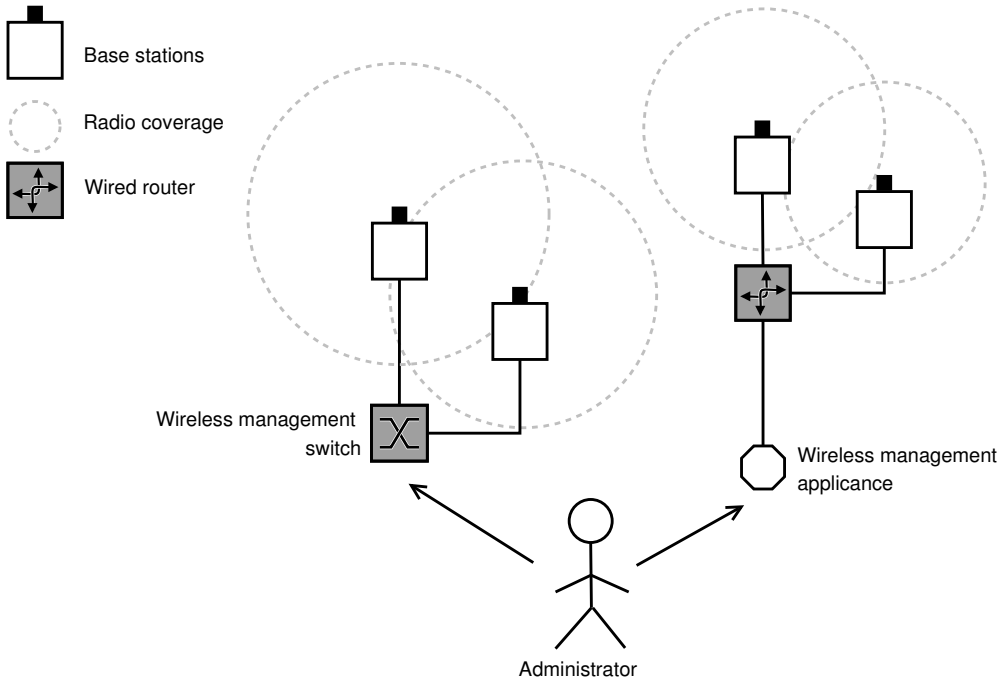

Figure 2.1: Centralised management solutions with both link and Internet layer access to the base stations.

even worse, because the entire overhead of the IEEE-802.11 protocol is tunnelled through the wired network. In the decentral approach, only the payload is inserted into the wired network.

Additionally, the more complicated infrastructure, *i.e.*, the central management station, may make the roll out of the wireless access network more time and cost consumptive.

2.1.2 Distributed Management Systems

Decentralised management solutions are popular to configure mobile *ad hoc* networks (MANET) [30][77]. These management systems typically focus on the challenging task of enabling peer-to-peer communication in highly dynamic, mobile environments [45]. They are widely used in environments were no wireless infrastructure exists at all.

In contrast, the decentralised solution presented in this thesis focuses on configuring a

stationary wireless access network for mobile nodes, with the goal of improving efficiency and performance.

However, because of their nature that each node decides based on its local scope [8] and no central management station exist they are very familiar with the proposed concept. Various research [53][86] is still ongoing in order to find a self-configuring solution for those environments.

The typical *ad hoc* approach uses the same IEEE-802.11 device for providing service to others and its own uplink. Compared to that, [9] introduces up to three radio devices on each *ad hoc* node, one for providing service to clients and two as part of a backbone structure.

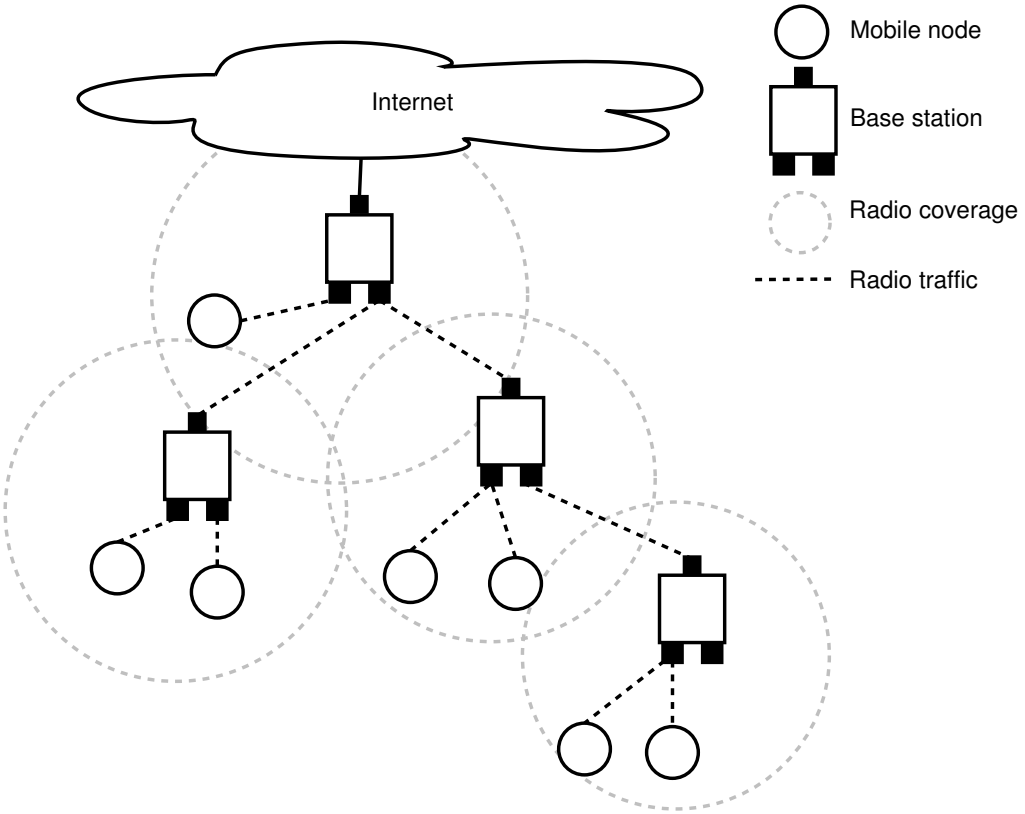

Figure 2.2: Ad hoc mesh with three radio devices at each node.

Figure 2.2 shows four base stations with three radio devices. One to provide uplink

connectivity to the mobile nodes and two to build a backbone network, *i.e.*, one to provide uplink to other base stations and one get uplink from another base station. The usage of three devices reduces interference problems, *i.e.*, different devices are used for different purposes.

Furthermore, the device for the mobile works typically in the IEEE-802.11b/g channel spectrum, the backbone in the IEEE-802.11a spectrum in order to avoid interference between the different devices. The top base station provides the uplink to the wired network.

Such an approach is even more similar to the proposed concept but focuses on using only wireless access technologies. The proposed concept is able to handle both, *i.e.*, the uplink device of each base station can be wired or wireless.

Ad hoc networks are not only used in IEEE-802.11 wireless LANs but also in 802.15 *personal area networks* (PANs), thus have different tasks to solve, *e.g.*, energy management.

2.1.3 Hybrid Management Systems

Besides centralised and decentralised approaches, hybrid approaches exist. [81] pushes functionality from the central system into the base stations, which are therefore slightly more complex than the simple wireless bridges of centralised approaches. The base stations handle all radio specific functions, the central management station handles security control, management and data flow analysis [80].

For example, the central device handles user authentication in order to allow users to access all base stations in the network. On the other side, the base stations perform radio analysis and statistics in order to locate rogue base stations.

[73] introduces *access point agents* which are installed on regular computers, distributed over the system and managing conventional base stations. This approach introduces decentralisation but is based on base stations that already exists an the market.

Although hybrid systems offer minor scalability increases, they do not completely address the drawbacks of centralised systems, *i.e.*, they are still not as scalable as a decentralised system and still have central points of failure.

2.2 Wireless LAN Analysers

Another area in wireless access network management are WLAN analysers. The information that base stations collect by themselves is limited. The usage of specialised scanning probes can improve radio measurements and troubleshooting.

Vendors like Airmagnet, Agilent Technologies [10] or AirDefense [12] provide equipment for radio and security measurements in wireless networks. However, these solutions do not go the whole way. They concentrate on analysing but do not integrate this information into the management system as the proposed approach does.

2.3 Integration of External Information

The integration of external information is used in the proposed concept in order improve the information base of the base stations. Related work exists in that area.

The usage of knowledge collected from the mobile nodes has been described in [71] as a neighbour discovery mechanism. This approach goes into the same direction as the later described *integration of external information* but uses the mobile nodes only for neighbour discovery and not for measurements as part of the *self-management* process. [29] use the mobile nodes to spread information between the base stations but focuses on *quality of service* (QOS) related questions.

[56] is very similar to the proposed concept, they use node collected information as part of the *self-management* process in order to establish a *cellular automata* [70] like mechanism where each base station decides independently. However, in this approach, the base stations do not communicate with each other, thus they can only find a pair-wise state for management information that can be seen by individual stations and mobile nodes,

e.g., radio channel assignment, radio transmission power level assignment or interference level.

2.4 Epidemic Protocols

For scalability reasons the proposed concept uses an epidemic algorithm in order to avoid centralised data repositories and keep the number of messages as low as possible.

Although, these protocols came from the database world [32][65], they are also used in sensor networks [41] and various peer-to-peer systems. The usage of epidemic algorithms in large distributed systems has been discussed in [35][43]; the problems of malicious peers in such systems in [44].

In typical epidemic approaches, the nodes pick their communication partner at random (*anti-entropy*) [75][39][50]. Because they do not rely on a specific topology, *e.g.*, ring or tree, they are very robust in terms of node failure. However, these approaches do not take the benefits of knowing the topology in account.

In the proposed self-managed wireless access network, each station decides based on its neighbourhood in airspace which stations to take for the information exchange. Compared to the idea of *anti-entropy* this has the benefit of being able to piggy-back the epidemic message spread on information that has to be exchanged between neighbours only. However, even if in terms of classical epidemic theory this is not an epidemic algorithm anymore, it comes closer to the original paradigm of human diseases, *i.e.*, objects that are physically nearby get infected.

2.5 Summary

This section has described existing technologies in the area of wireless LAN management; next to this, it introduced WLAN analysers and the usability of the mobile nodes knowledge. In addition, it introduced traditional epidemic protocols and explains the difference to the epidemic approach used in this thesis. The next chapter will discuss the proposed solution for the problem of automated wireless network management.

Chapter 3

Solution

This chapter describes the proposed solution for decentralised wireless access network management. After discussing assumptions that are made by the self-managed base stations, it then describes the basic system's functionality and discusses security aspects. Finally, it introduces different management applications that may run on the basic system.

3.1 Assumptions

A base station in the proposed self-managed wireless access network has to fulfil several requirements. Each base station is a full-fledged *Internet protocol* (IP) [62] router for its delegated IP subnet, able to operate stand-alone. It needs at least two network interfaces; one to provide wireless services to its mobile nodes and a second interface (wired or wireless) for uplink connectivity to the networks behind that base station, *e.g.*, the *Internet*. This interface is used as *management interface* for the information exchange between the self-managing base stations. Additional interfaces, when present, can act as probe interfaces, they can offer additional connectivity for the mobiles nodes on different channels or link protocols or represent different uplink interfaces to different wired of wireless networks.

Figure 3.1 show three base stations. Each of them has one wireless interface to provide uplink functionality to the mobile nodes. Two of the base stations have only one uplink

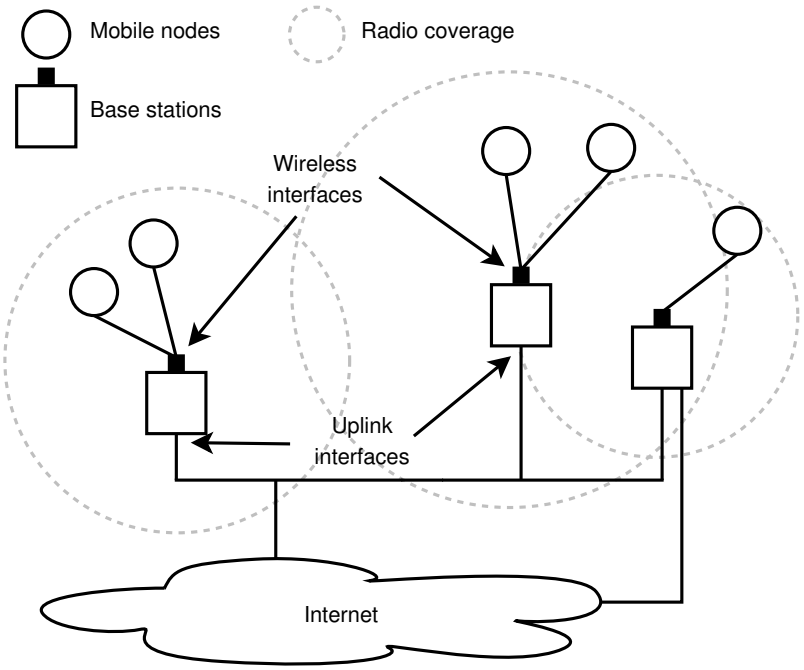

Figure 3.1: Each base station has at least two interfaces.

interface to the *Internet*, which they also use as management interface. The third base station has a second uplink interface in addition to the management interface.

Base stations automatically distribute the available address space among them, configure subnets for the mobile nodes on their wireless interfaces and configure the addressing of their uplink interfaces. In the current prototype, IP auto-configuration occurs through a separate mechanism that was an earlier research effort [76]; the next revision of the prototype implementation will integrate this process.

The current prototype uses *X.509* [7] certificates signed by a common certification authority to establish trust between base stations and to indicate access network membership (self-protection). Consequently, each base station has an individual certificate. This certificate has a second function: a hash of the certificate provides a statistically unique identifier for each base station in current prototype implementation. The prototype uses the *MD5* algorithm [68] for this purpose. Alternatives to a hash are possible, *e.g.*, *medium access control* (MAC) addresses of the wireless or uplink interface or the IP address of

the uplink interface. However, IP addresses may change and the MAC addresses are hardware dependent.

3.2 Basic Concept

The proposed concept is based upon the idea that the management functionality will be entirely distributed, *i.e.*, no central management station exists. This avoids having a central point of failure or bottlenecks in communication and processing. Therefore, each station must implement the management capabilities (*autonomic base stations*) and each station must be able to work stand-alone.

To allow the distributed base stations to interact as one homogeneous wireless access network, information has to be exchanged. Information that is important for the wireless network configuration and management, *e.g.*, radio frequencies, traffic encryption, roaming information etc. The communication paradigm is that each station retrieves information from all its *neighbours*, *i.e.*, stations in radio range.

Based on retrieved and locally collected information, a station is then able to select an appropriate configuration. Compared to a central solution where each station informs a central management station but not other base stations, this neighbourhood approach reflects the plausibility that stations that are close together (in radio range) have often information to exchange that is not important for the entire wireless access network. For example, the stations radio frequency to avoid interference or the amount of connected mobile nodes in order to implement a load balancing mechanism.

Some part of the information that is exchanged between single base stations has to be consistent throughout the entire network (*global information*). This *global* information is spread as part of the continuous information exchange between the neighbours. It is spread throughout the network by *epidemic replication*. Each station only informs its direct neighbours that in turn will then forward it to their neighbours, to float throughout the entire network. Each base station informs its neighbours about changes in periodic intervals. However, information floods need more time to get throughout entire network

but this procedure avoids message storms compared to an approach where each change is immediately forwarded by the base stations.

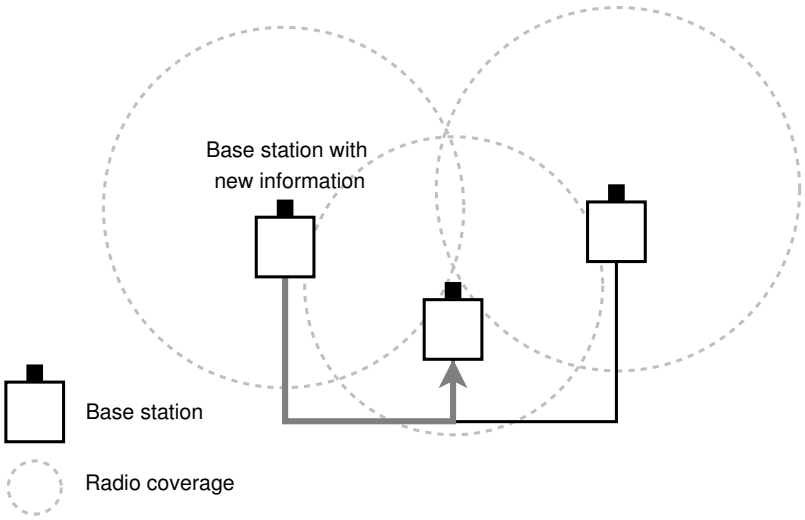

Figure 3.2: Epidemic message spread: A base station only informs its direct neighbours.

Figure 3.2 shows a base station that sends new management information to its neighbour. In Figure 3.3 this neighbour forwards all changes of its information base, including the changes initiated in Figure 3.2, to its own neighbours at its next forward interval. This includes a message back to the originating sender, which is recursive if no other change has happened during the interval. However, this happens only once because for the originating station this is no new information anymore, thus it will not forward the change again.

If a base station wants to initiate management information changes, the epidemic replication avoids that a station has to contact all other stations within the network individually. Additionally, a base station does not even have to know all other base stations within the network but only its own neighbours.

Another concept, which is proposed as part of the concept, is that the base stations get provided with information, but the configuration is done completely autonomously, *i.e.*, no base station can force another station to use or not to use specific information. This reflects several considerations, *i.e.*, no intruder can force the base stations to work in

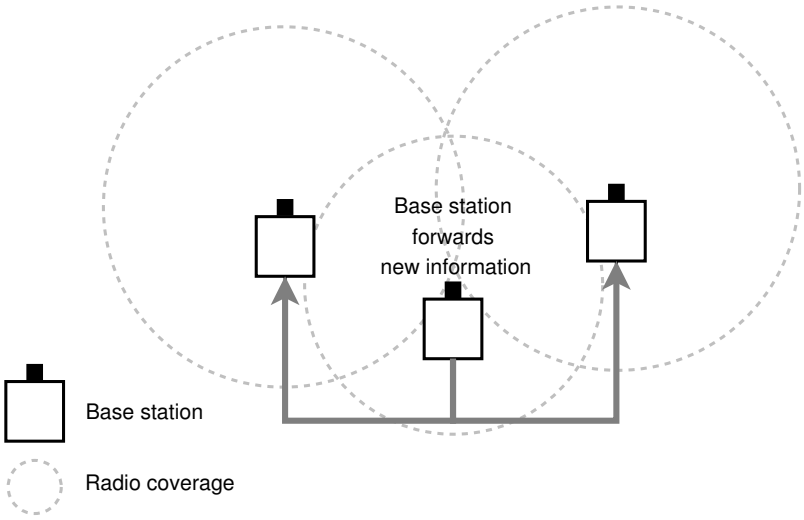

Figure 3.3: Epidemic message spread: The neighbour forwards to its own neighbours.

his meanings and no wrong configured base station can force its configuration to base stations that are in the specifications.

However, if an intruder know how the stations work internally he can always try to force the stations to act in his meanings by providing them with manipulated information. This is the reason why additional security considerations have to be made (Section 3.5).

3.3 Information Categories

The information that each station maintains is partitioned into three different categories. This will allow the base stations to decide how the information has to be processed. First, *private* information is only locally available and is not forwarded to any neighbours, *e.g.*, the position of the *X.509* certificate in the file system, logs or measurement information that waits for analysing.

Second, *public* information is disseminated to direct neighbours, *i.e.*, other base stations within radio range. *Public* information is the base station's current channel, the number of connected nodes, the unique ID or the addresses of the interfaces. This allows a group of neighbours to adapt their configurations in response to local events. A base station

periodically disseminates updates about its local state to its neighbours and likewise receives their updates.

Third, *global* information is spread throughout the whole network by using the epidemic approach, *i.e.*, piggy-backed onto the periodic local information exchanges between neighbours. *Global* information can be the currently used wireless protocol, the wireless network encryption key, the networks ID or a list of unwanted mobile nodes.

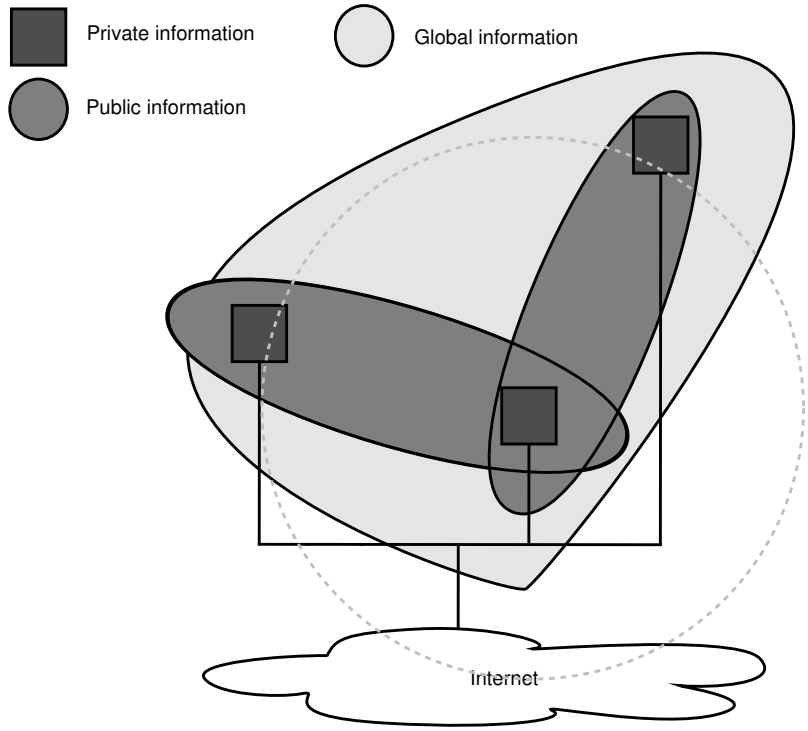

Figure 3.4: Three base stations share different parts of their information.

Figure 3.4 shows three base stations sharing *global* information between all of them and *public* information between subsets of them. *Private* information is not shared.

Each kind of information is handled in a different manner and each station decides how the information is partitioned into the different categories. Based on this decision the information spread is handled. The categorisation process is static, *i.e.*, patterns will be used as basis for the decision. Furthermore, the decision-making process has to be homogeneous throughout the network.

3.4 Functionality

This section will introduce the basic management functionality of the proposed self-managed wireless access network. It starts with the explanation of the self-configuration process, *i.e.*, the integration of new base stations. It then describes the mechanisms that ensure homogeneity for *global* information and finally explains how a central configuration repository could be established in the decentral self-managed wireless access network.

3.4.1 Integration of New Base Stations

When a base station starts up (Figure 3.5), after a brief randomised de-synchronisation delay, it performs a probing phase before configuring itself to provide connectivity to the mobile nodes. The de-synchronisation may be needed if all base stations start at the same time, *e.g.*, after a power failure. This avoids that all base stations are scanning for neighbours in parallel, thus they do not see each other because no one is in *infrastructure mode* [38]. Note, that no scanning is possible in infrastructure mode is typical in IEEE-802.11 WLANs, it may be possible in other wireless access technologies.

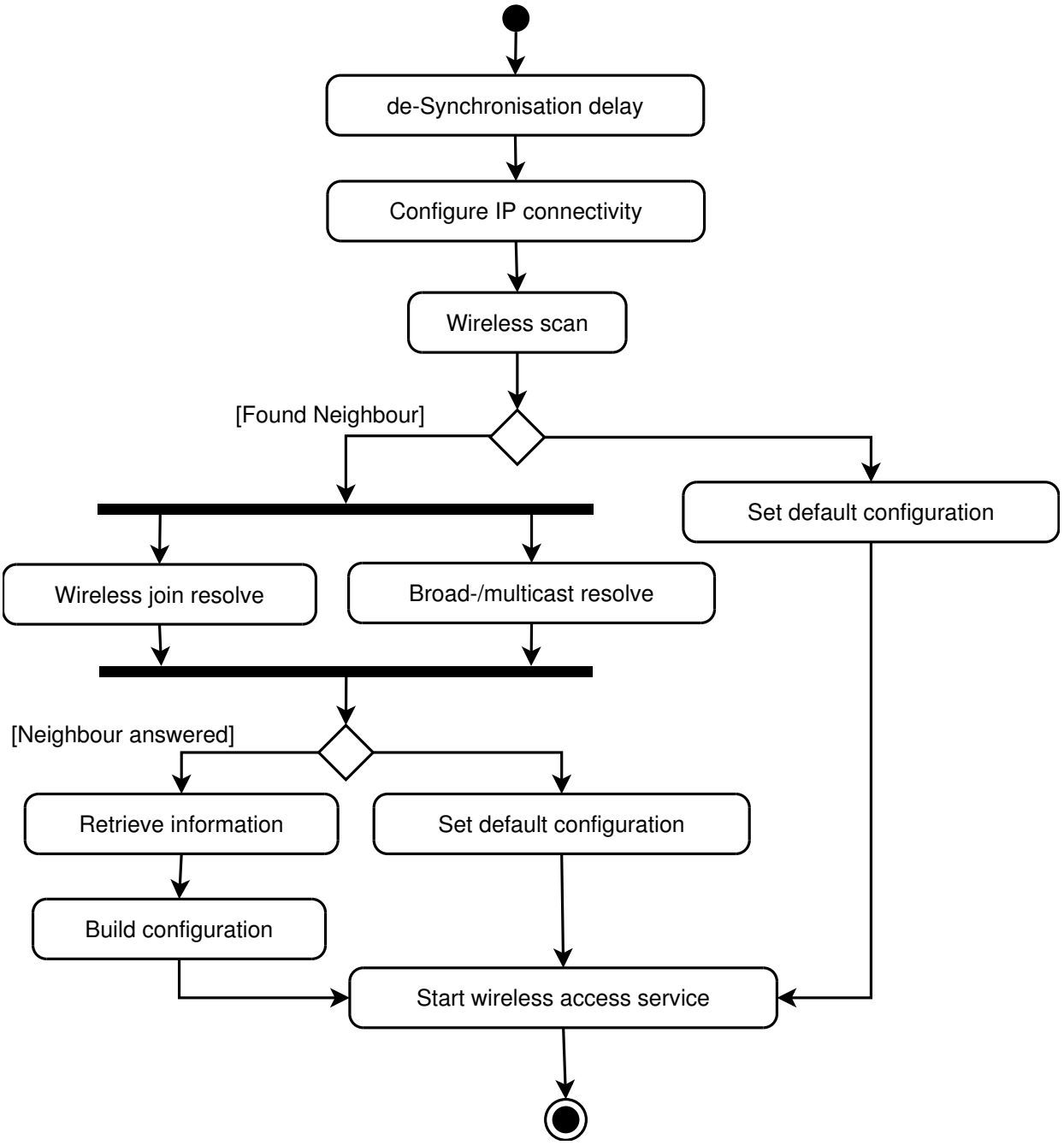

Figure 3.5: Integration of a new base station.

During the first part of the probing phase, the base station auto-configures its IP connectivity, *i.e.*, it obtains a subnet delegation to serve the mobile nodes and configures its uplink interface [76]. In the next step it probes for neighbouring base stations and their specific configuration in order to integrate into the self-managed wireless access network, this is done in several steps.

First, find neighbouring base stations through a wireless scan. In IEEE-802.11 WLANs a station goes to every channel in the channel list and waits for beacons in order extract network management information from them. The beacons are designed to allow the stations to find out everything that is needed to start communication (*basic service set* (BSS)). More information can be found at [38]. If the base station does not see any neighbours during the scanning, it sets a default configuration and starts its service to the mobile nodes.

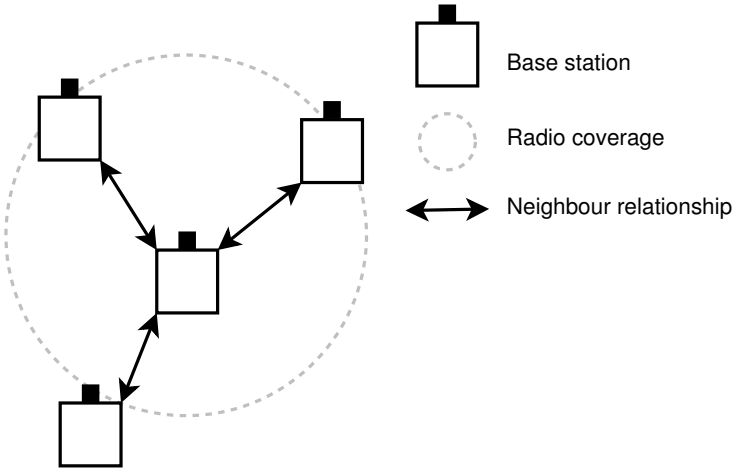

Figure 3.6: Wireless scan shows neighbour relationships.

Figure 3.6 shows four base stations. The station in the centre performs the wireless scan and sees that it is inside the coverage area of three other base stations. As a result, the base station in the centre declares these three as *neighbours*.

Second, resolve *management interface* addresses of neighbours. The base station sends a *resolve request* to the base stations that were found as result of step one. A resolve request

contains the sender's uplink interface address, such that the contacted stations can reply to the new base station through their management interfaces, and all the addresses seen during the wireless scan. In IEEE-802.11 WLANs this is the MAC address of the interface that provides the wireless service.

Two different ways are possible for this mechanism. On one side, the new base station uses the wireless interface to connect to the neighboured stations as a mobile node and sends the resolve request to that station. On the other side, the new station uses its management interfaces to send the resolve request as a broadcast or multicast message. The first method prevents unnecessary broadcast or multicast messages within the network, but it fails if the neighboured base stations have restricted access, *e.g.*, using encryption or link layer filtering. The *resolve request* is sent as *user datagram protocol* (UDP) [61] message, in order to allow broad-/multicasts.

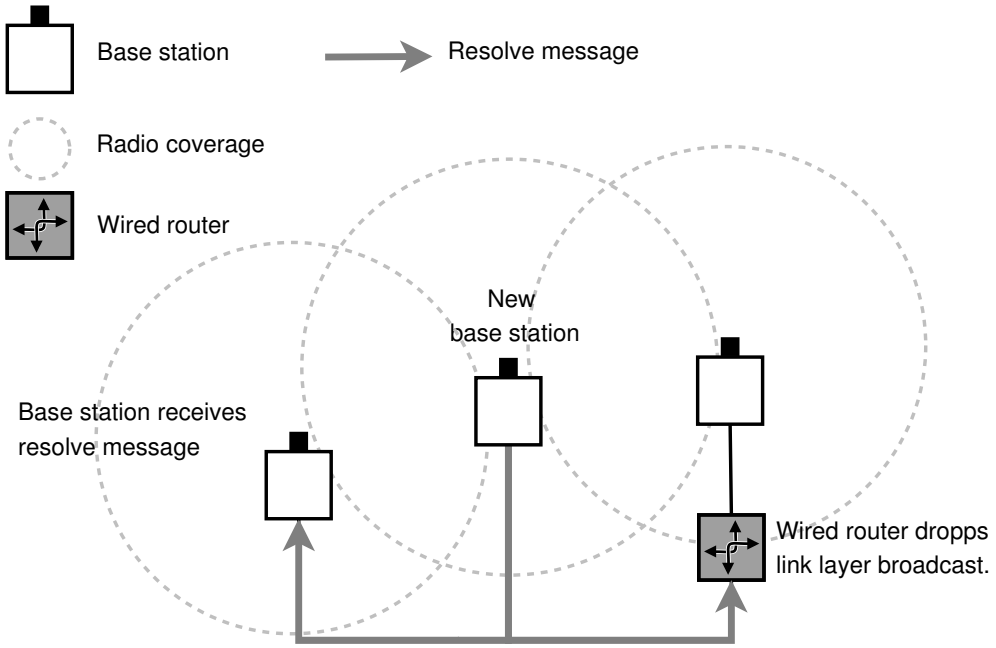

Figure 3.7: Broadcast-based resolution.

Figure 3.7 shows the new base station in the centre, sending the resolve request message as a broadcast over the wired link. The router droops the link layer broadcast message, thus it is not reaching the base station on the right of the figure. Figure 3.8 shows the

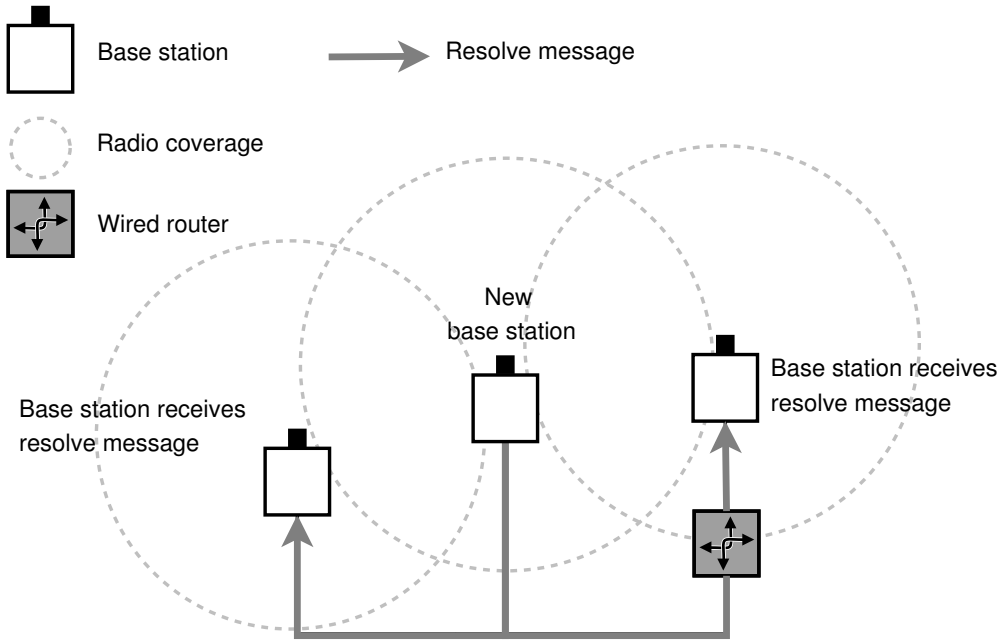

Figure 3.8: Multicast-based resolution.

same situation as a multicast. The router does not drop the message, thus it is received by the base station on the right.

If the base station does not get any answers from its neighbours, it sets a default configuration and starts its service to the mobile nodes.

Third, retrieve configuration information (Section 3.3) from the detected neighbours, through their management interface. The new base station introduced itself the first time to its seen neighbours by sending the resolve request.

If the neighbours decide, to authorise the new station to be part of the network, *i.e.*, is successfully authenticated, they will react on this introduction by informing the new neighbour about their information from the point of introduction on. In the current prototype implementation this authentication is done with an *X.509* certificate (Section 3.5). There are other schemes for decentralised security [84], *e.g.*, chain of trust establishment [48], trust management systems [26][3] or reputation base models [4][31]. However, this thesis introduces a basic system that may be extended in the future.

The information exchange is embedded into *transmission control protocol* (TCP) [63] streams, in order to ensure the reliability of management information exchange. The next step for the new station is to substantiate the introduction by providing the neighbours continuously with *public* and *global* information.

Fourth, create own configuration based on gathered information, *i.e.*, the base station merges information from the different neighbours and information retrieved during its own probing phase together. For example the base station decides which radio channel to take based on the occupied channels seen during probing phase and the information of its neighbours which channels are occupied inside its coverage area.

Once configured, the base station periodically performs scans to detect changes in its environment. Because client connectivity is disrupted during the scan, the base station performs this scan less frequently when it provides uplink connectivity to mobile nodes and more frequently when it does not. It can also use a dedicated probe interface for this purpose, if available. The base station also starts to participate in global and local information exchanges with its peers.

3.4.2 Modification of Network-Wide Information

The application of new *global* configuration settings may take place at any station in the entire network. Two different mechanisms are introduced to ensure that the *global* information is consistent.

First, the *global* information includes two version counters. One for automatic changes done by any base station (*version counter*) and a second one that is increased by any change that is done from a third person, *e.g.*, by an administrator (*admin counter*).

Figure 3.9 shows the mechanism in a activity diagram. When new *global* information comes in, the base station first checks the *admin counter*. If it is higher then the *admin counter* of the local set of *global* information, the new information replaces the local one. Additionally, the same procedure takes place with the *version counter*. However, if a base

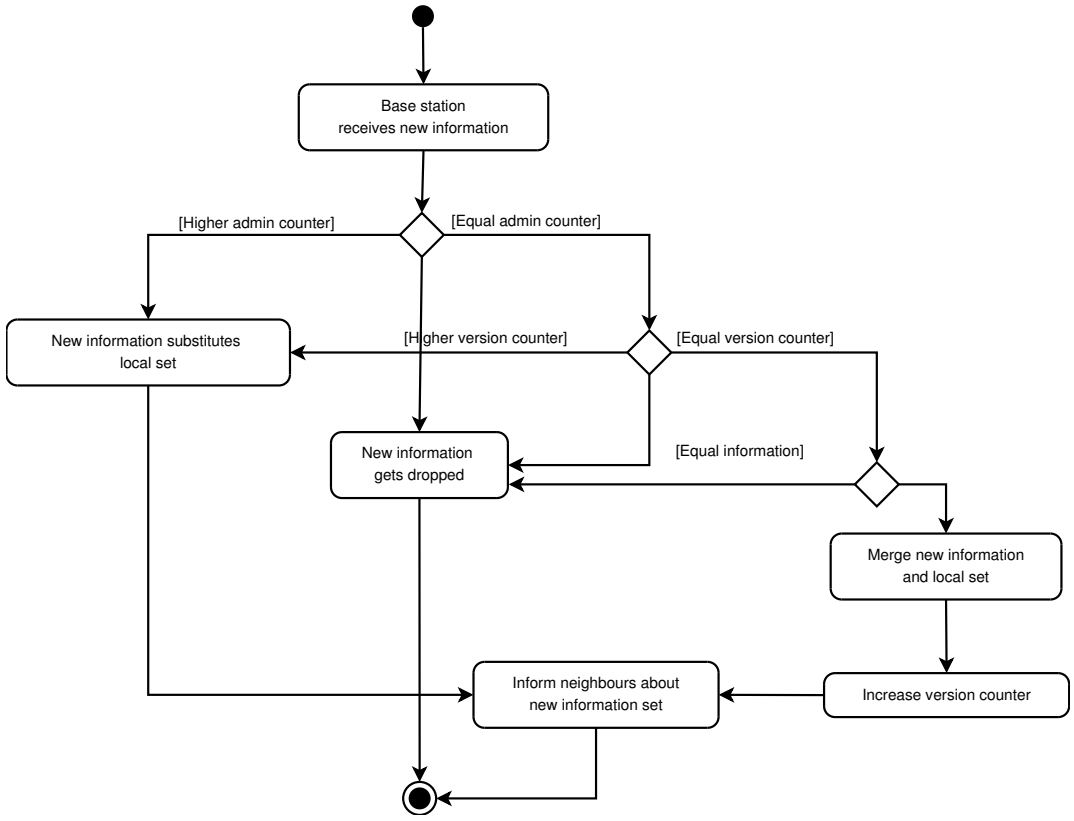

Figure 3.9: Base station handles incoming global information.

station detects different *global* information sets with the same *version counter* and the same *admin counter* it assumes a collision and tries to merge the different sets together.

In the current prototype, this is done by copying the two sets above each other. If one set has more values in a variable they will survive. After the merge, a higher *version counter* will be set. This may happen very often during the networks's convergence time when the base stations start their service. This simple mechanism can be replaced by more advanced approaches in future implementations.

No change should drop away that was made by an administrator. A second mechanism exists for this kind of changes. One base station will provide a global locking service (*mutual exclusion*). The address of this *keeper* is part of the *global* information.

Whenever a base station wants to increment the *admin counter* in order to apply a third

person's change at the *global* information, it has to get a lease from the *keeper*. The lease must hold until the information is spread throughout the network. However, any base station can decide that a new local information is too important to get dropped by any other (merging) station. In this case the station increments the *admin counter* as well, even if this change did not came from a third person.

3.4.3 Network-Wide Information Repository

For some purposes, it is useful to provide a database that stores information about all (or a subset of all) participating entities in a network, *i.e.*, log-daemon functionality. This allows to get information collected at one point in a otherwise entirely distributed concept. An administrator can use the function in order to get information about the current network configuration and state. Another reason may be to have a backup of all information, or a security related reason like having information about breakings into the wireless access network, which cannot be deleted by the intruder who broke in, because the information is out of its reach.

There are two solutions in the concept to solve this task. The first one is the *global neighbourhood* function. Each base station holds a *global* list of addresses for nodes that want to be informed about any change in the *public* and *global* information base of all stations. Thereupon, all stations will not only inform their *direct neighbours* about changes but also these *global neighbours*.

The second solution is to create *virtual neighbours*, *i.e.*, entering a neighbour into a stations neighbour list, even if it is not in radio range. Consequently, this *virtual neighbour* receives all messages that the *direct neighbours* receive. From the stations view, there is no difference between *virtual* or *real* neighbours. This function is more scalable, as a virtual neighbour only retrieves the configuration of a (selected) subset of all stations within the network.

Figure 3.10 shows a base station that provides its regular neighbour and a virtual neighbour with information.

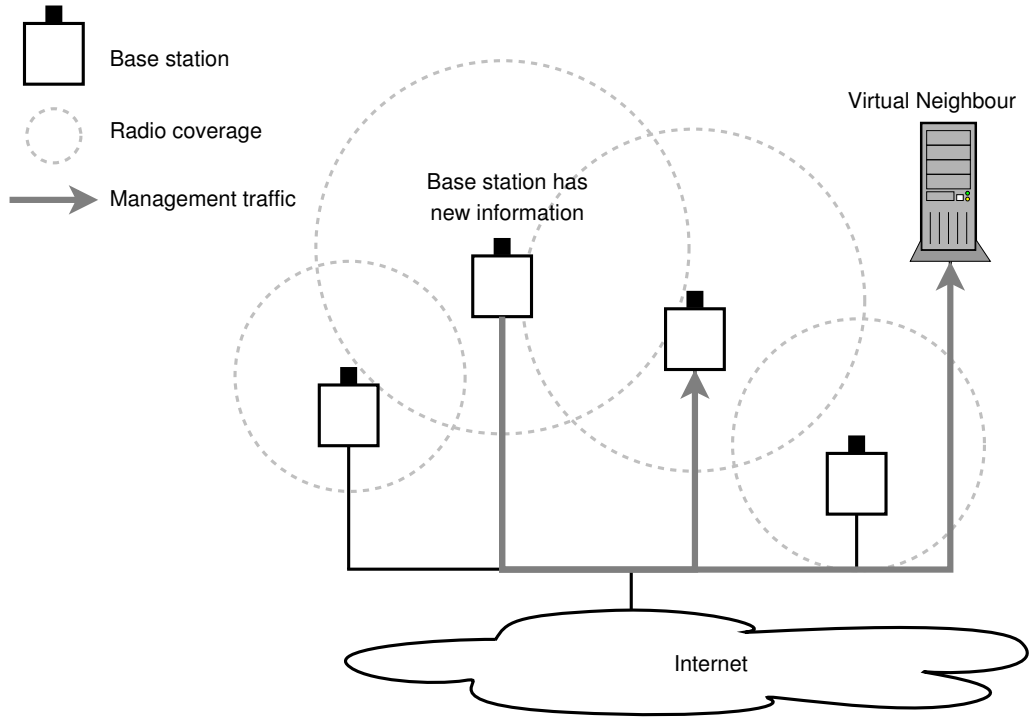

Figure 3.10: Creating centralised databases in a decentral wireless access network.

3.5 Security Considerations

A self-managed wireless access network must fulfil several security objectives. First, it must protect sensitive information, *e.g.*, wireless encryption keys and authentication information for the mobile nodes, against *interception, interruption, modification and fabrication* [75].

Second, it must protect the distributed configuration algorithm from attacks, *i.e.*, the base stations must prevent that an attacker infiltrates the self-managed wireless access network. For example, an attacker tries to declare itself as an official base station in order to be able to manipulate the traffic of the mobile nodes.

Third, it must prevent the management functionality to be used as an attack tool, *e.g.*, for flooding attacks. An attacker broadcasts resolve messages for all known stations and uses a victim's address as the return address. Thus, an attacker only sends one request

and the victim will receive as many answers as the number of stations that received the resolve request (Figure 3.11).

The use of *X.509* [7] certificates and two-way authentication addresses all these security objectives. Traffic encryption protects sensitive information; digital signatures allow verification of the authenticity of management communication and they allow establishing an authorisation mechanism for the integration of new base stations into to the self-managed wireless access network. It will protect the operation of the distributed algorithm and consequently mitigate the use of management functions for attacks.

The current prototype, the encryption of the information exchange is done using the *transport layer security* (TLS) protocol which is *"designed to prevent eavesdropping, tampering, or message forgery"* [33] based on the stations certificates. If a station is able to establish a full *TLS Handshake*, in two-way authentication mode, with a neighbour it can be sure about the authenticity of the neighbour and thereupon authorise the neighbour for information exchange. In addition, the information exchange is encrypted from this point on.

The *resolve request* messages are signed using *secure multipurpose Internet mail extensions* S/MIME [66]. In the current prototype, the implementation of the signing process is reused from the *X-Bone* [78] project. The signature allows each receiving base station to verify the claimed identity of the sender.

The installation of each base station's certificate and the corresponding certification authority's public key in order to allow each base station to verify its neighbours certificates still requires one-time manual configuration of the base stations. However, methods for semi-automated certificate configuration, such as physically connecting to a mobile certification authority that auto-installs the required certificates on first boot, can significantly shorten the configuration process. The specifics of such approaches are outside the scope of this thesis and may be part of future implementations.

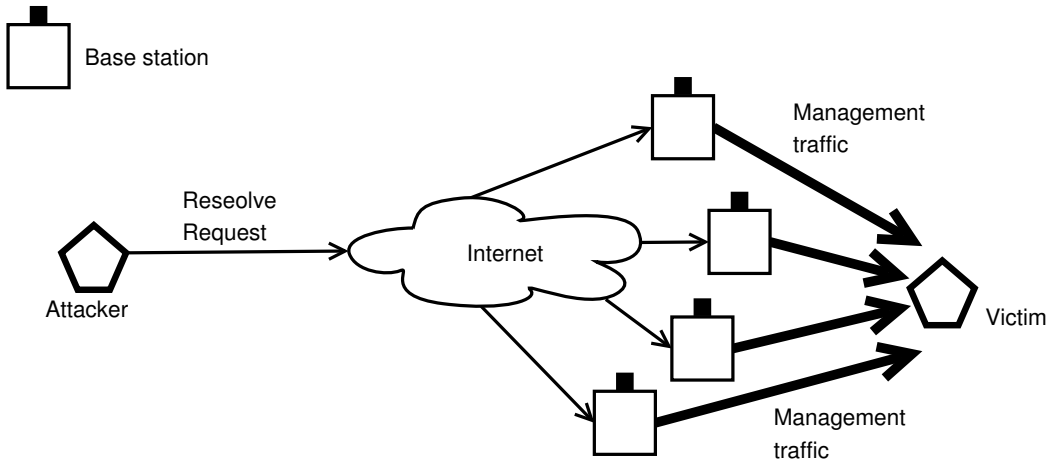

Figure 3.11: Attacker performs a flooding attack by using the resolve mechanism.

3.6 Integration of External Information

One challenge for automated configuration of wireless access networks is base stations with overlapping coverage areas that are unable to detect this occurrence because none is within the area of overlap. Figure 3.12 shows such a situation. These base stations should become neighbours and coordinate their configurations, but fail to detect each other's presence during the probing phase. Consequently, their configurations will not be coordinated, leading to an inconsistent overall network configuration.

One approach to this problem involves manual configuration, forcing the base stations to treat each other as virtual neighbours (Section 3.4.3). Obviously, this approach does not fit with the goal of complete self-management.

Another solution is the integration of *external* information into the configuration process. This external information does not originate at base stations but is contributed by other nodes into the configuration algorithm. This means that a wireless participant that is running inside both coverage areas will inform the two neighbours about their relationship. Figure 3.13 shows a mobile node informing one base station, that will use this information to build a neighbour relationship.

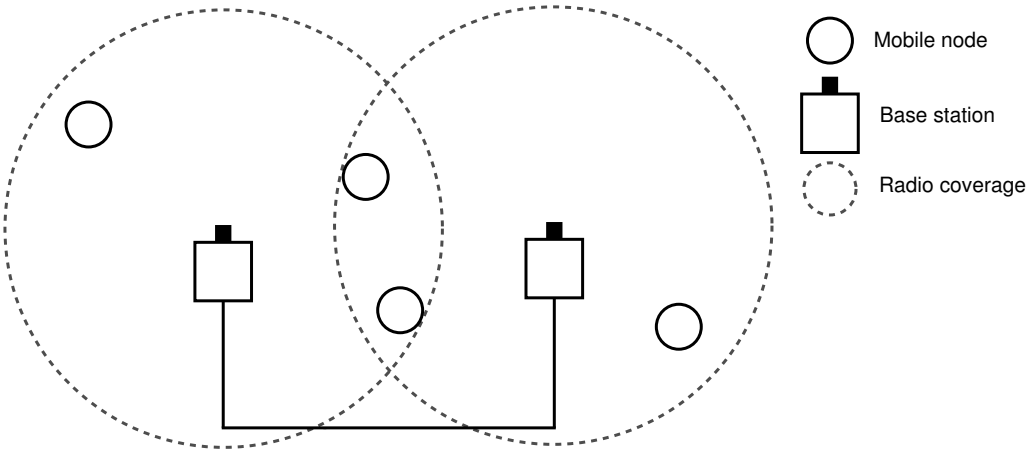

Figure 3.12: Base stations with overlapping coverage areas are unable to detect each other.

That means the use of external information can address the overlap problem. If mobile nodes periodically notify their base station of other mobile nodes and base stations within their radio range, the base stations can update the neighbour relation, eliminating or at least significantly reducing the overlap problem.

There are two possible sources for this external information. First, provide a user-controlled mobile node with software that runs a monitoring functionality (*sniffer*) [83].

However, the integration of external information from user-controlled nodes has several drawbacks. It requires additional software to be present on the mobile nodes, software that has to be installed, administrated and secured, *i.e.*, the base stations must verify the trustworthiness of external information carefully before acting on it. For example, the mobile nodes host machine may be corrupted by a virus, which then changes measurement information in order to corrupt the entire network. Additionally, the mobile nodes may only be guests of the wireless access network for a short period of time, *e.g.*, at airports or hotels.

Another source for external information is to position a monitoring device (*probe*) [83] inside the coverage area of the wireless access network (*measurement node*). For example, an add-on probe connected to a wired connected host or a dedicated probe, designed

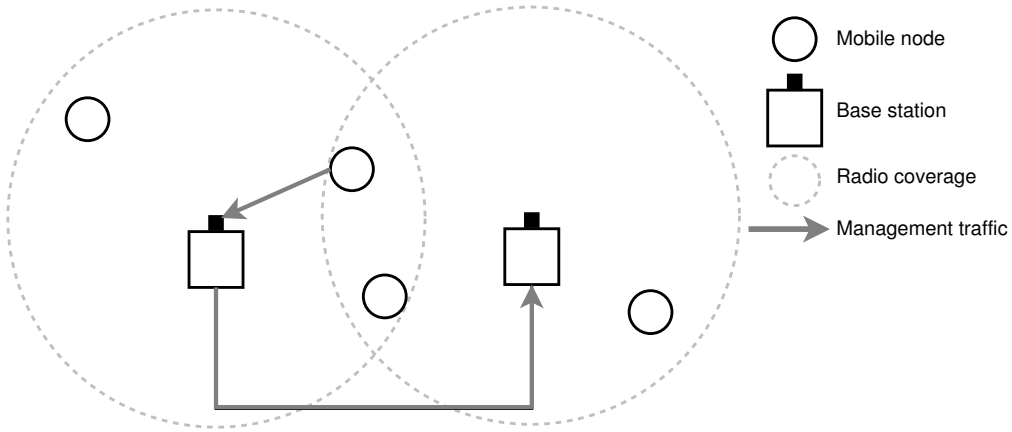

Figure 3.13: Base stations with overlapping coverage areas get informed about their relationship.

exclusively as monitoring device. Those monitoring devices are similar to the concept of wireless analysers, except that they report directly to the base stations and do not go the indirection through the network administrator.

An addition to this statically probe concept uses a robot to position the measurement node. The robot moves through the coverage area of the wireless access network and perform the measurements. The robot can drive on a specified route, can find the way by itself or can be integrated into the network, *i.e.*, the base stations send the robot to any point where they detect a need for immediate measurement, *e.g.*, based on geographic coordinates.

External information can improve the *self-healing* and *self-organisation* functions of a self-managed wireless access network in other ways. It enables detection of interferences, can detect holes in coverage and allow to automatically closing them by helping the base stations to find the right transmission power. In the same way, it helps to reduce to much overlapping in the wireless access network. The measurement node can identify rogue access points, even outside the range of the base stations or it helps with location tracking of nodes. Furthermore, it operates all kinds of logging operations.

However, to be able to perform long-run measurements that may take place while not being connected to a base station, *e.g.*, inside a coverage hole or measuring of multiple

channels, the nodes may have to save the information and transmit it to the next base station they get connected to.

This concept merges the idea of wireless analysers (Section 2.2) with the concept of a wireless management system.

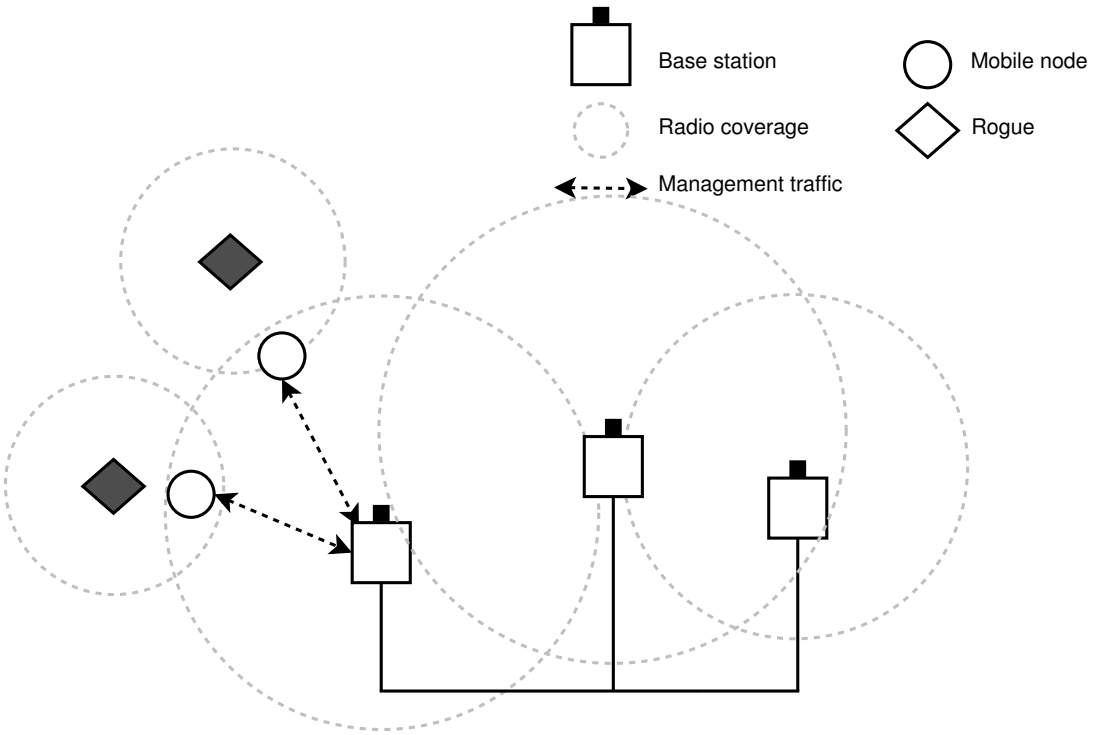

Figure 3.14: Base stations get external information from different wireless participants.

Figure 3.14 shows three regular base stations and two rogue base stations. The base stations are not able to see these rogues on their own during a wireless scan. However, one of the base stations gets informed of the existence of the rogues by the mobile nodes.

3.7 Design Alternatives

This thesis describes a concept that incorporates many individual components (locking, flooding techniques, etc.). Although the initial prototype chooses a particular instantiation for each of those components, it often picks the simplest one. Future versions are

expected to replace some of these with more featureful or scalable variants.

3.7.1 Information Handling

There are alternatives to the epidemic message spread as described in Section 3.2. A simple information spread from one base station to all other is more simple but the improved scalability makes the epidemic approach the better choice, *i.e.*, the motivation for using this *epidemic replication* is that in a growing network at some point the network and computing capabilities of a single base station will come to its limits. This limit may be reached with 10, 100 or 1000 base stations depending on the network connection and computing power of the base stations.

A pull based approach, where each base station informs itself about information changes has the same scalability problems. The third alternative is a central configuration repository with the option of a limited number of replicas distributed over the network [75]. However, such an approach is still more central than the proposed technique.

A fourth alternative is to use an epidemic approach including anti-entropy (Section 2.4). However, such an approach does not meet the fact that a large part of the information exchange has to be done between direct neighbours and that global information can be piggy-backed to this continuous exchange.

An alternative to the pattern based information deviation process is to do this division dynamically, *i.e.*, each base station decides, based on the importance of the information, if it should be kept private or spread to neighbours. Further aspects are taken into account for the decision process, *e.g.*, the urgency of the information in face of the current network or processing load in the wireless access network or the existence of an malicious user (*rogue* [83]) can be kept local until the rogue does not move. The decision process is done only once, *i.e.*, one base station declares a piece of information *global*, which is from this point on spread throughout the wireless access network. An alternative is to redeclare this piece at every station. Each station decides if this information is spread further or not. For example, on information may be only relevant for all stations in one specific building.

To achieve mutual exclusion for changes to *global* information is also possible in different ways. The network's provider may insert other mechanisms, a distributed or token ring algorithm for example [75]. The centralised solution is used for the prototype because it was the easiest to implement. However, future implementations should contain a decentralised solution [39][67][11] in order to fulfil the idea of an entirely decentralised and self-managed wireless access network.

3.7.2 Security

Other security mechanisms than *X.509* certificates in combination with *TLS* and *S/MIME* are possible. For example, the base stations may use a *shared secret* (encryption key) for symmetric encryption in order to authenticate and encrypt the exchanged information and resolve messages. The *advanced encryption algorithm* (AES) [2] solves this task.

However, a shared secret brings always the risk that it may get lost, especially if it is shared between large numbers of entities. For example, if a base station gets lost, the whole network has to change its encryption key because its not secret anymore. In the concept described above, only the certificate of the base station has to be revoked. A list of revoked certificates gets inserted into the *global* information section.

Another mechanism is to use a *key distribution centre* (KDC) in order to allow each pair of stations to have a single key for their information exchange. An example of an protocol using a KDC is the *Needham-Schroeder authentication protocol* [57]. However, such an approach is centralised, needs online presence of the KDC and should be avoided in order to build a fully decentralised self-managed wireless access network.

In addition, systems like *secure overlay networks* (SON) [40] may be a better solution for the future because they are fully distributed and have no need for offline authorities.

3.8 Management Applications

The described concept introduces only a framework that provides a basic service for system management purposes. Different applications may run on it, different algorithms

and logics may be used inside of it and different wireless access technologies may be managed. A middleware [75] that allows management services to act transparently on different wireless access technologies. This allows the concept to be more modular and have a better expandability in the future.

This section will introduce several examples for such management applications. However, this is only a small set of thinkable usage for the proposed self-managed wireless access network.

The middleware provides an interface for several kinds of administrative tasks that are carried out in wireless networks. These tasks can affect either network wide configurations or only direct neighbours. They can also make use of *public* or *global* information that is available at the base stations running the specific administrative application.

The management applications are partitioned into three different categories: *management* related functions and mechanisms, different *accounting* functionailies and *security* features. Each application section follows the same rules: explain the task, explain a solution and describe how the integration of external information helps to solve the task even better. Note, the usage of external information does not make sense in all of the cases.

3.8.1 Management

Management related applications help to provide a better wireless access for the mobile nodes. Better, in this case mean to provide the mobile nodes with a usable, high available and fast wireless access service the same way as keeping the radio transmission power as low as possible in order to reduce the burden for both human users as other radio services.

Channel Selection

A IEEE-802.11b/g wireless LAN has typically 13 different channels (between 2.412 GHz and 2.472 GHz) where each base station can choose from in order to provide its wireless

service. Those 13 channels which are recommended by the *European telecommunications standard institute* (ETSI) are not fully adopted by all European countries (France allows only 4, Spain only 2) and the U.S. and Canada use also only a subset of them [38]. However, for the this section it is assumed that all 13 channels are available.

Even if a base station can choose freely between the 13 channels the chosen channels have to differ by at least five in order to avoid interference with overlapping coverage areas (Figure 3.15).

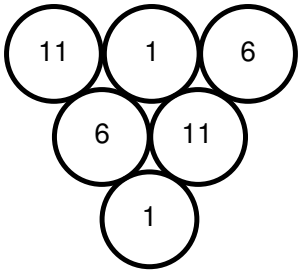

Figure 3.15: Optimal channel selection for IEEE-802.11b/g wireless LANs.

To implement channel selection each autonomic base station informs its neighbours about its own selected channel and the chosen channels of all other seen base stations as part of the *public* information exchange . Note, "seen base stations" does include all existing neighbours, *i.e.*, managed base stations, but it includes also all other base stations that are not self-managed.

That means that each upcoming base station gets informed about all selected channels that have overlapping coverage with it even if it does not see all of them directly as result its own wireless scan (Figure 3.16).

In the next step, it will select a channel with the maximum difference available. For example, a new base station gets informed that it has overlapping coverage with stations that send on channel 1 and 11 it will decide to choose channel 6 in order to avoid interference. However, this simple channel decision process does not involve the transmission power. An improved algorithm takes this into account if interference cannot be avoided, *i.e.*, try to reduce the interference as much as possible.

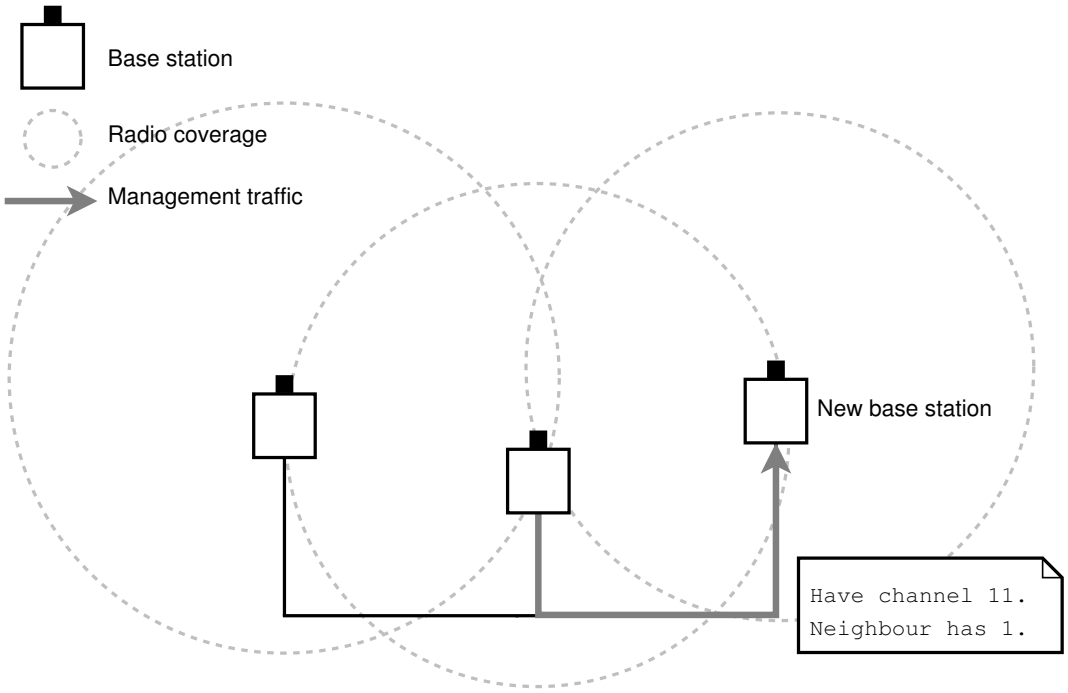

Figure 3.16: Incoming base stations gets informed about selected channels.

To get a channel allocation list with a maximal difference between all stations, each station may decide to change its channel allocation (*self-optimisation*). When in the example above a fourth base station comes up, this station will decide to take a channel between 1 and 6 or 6 and 11. The base station took channel 3 what is a good choice from its point of view, the stations now have a set of different intervals between the chosen channels. Because of the regular information exchange between the neighbours, all of them will become aware of that decision. They will react by re-ordering the channel allocation in order to re-establish a list of chosen channels with even intervals. To avoid that all base stations try to find a new better channel selection at the same a de-synchronisation delay is inserted.

The integration of external information helps the base stations to obtain input about other senders that appeared after their scanning phase and senders that are outside their range. Many of today's wireless LANs attempt to get a maximum coverage with a minimum number of base stations, very few base stations will see each other in order

to establish a neighbour relationship. In such a wireless LAN, only the integration of external information enables automated channel selection.

Coverage Hole Detection and Closing

If a mobile node detects a coverage hole and reports this hole to a base station, an algorithm working on the base stations is used to tell the neighbours to extend their transmission power to close the holes. Such an algorithm tries to hold the transmit power at each base station as low as possible and as high as necessary to avoid holes.

The proposed self-managed concept provides the information to find the holes and the capabilities to close them. It supports this mechanism with having a field for each stations transmit power in the *public* information section and a field with geographic information about coverage holes in the *global* information section. However, such an algorithm relies on the geographic coordinates of the regarding base stations and coverage holes. A satellite navigation system provides this information.

Another solution is to extend the coverage area of each base station as far as possible. This is not always a good solution. For example, it sends (unnecessarily) information in areas that do not need radio coverage. Furthermore, it creates interference for other wireless services or creates to much overlapping fields which will result in interference as described above.

Load Balancing

Load in this terms mean, how much the wireless service of each base station is in usage. Because the mobile nodes that are connected to one base station have to share the stations capabilities, *e.g.*, the stations computing power, wireless-service and uplink device bandwidth, as a result of a growing number of mobile nodes, each node will have less service available.

In order to optimise the base stations capabilities to provide service to the mobile nodes it is not only important to close detected coverage holes but also to distribute the mobile

nodes equally over the serving base stations.

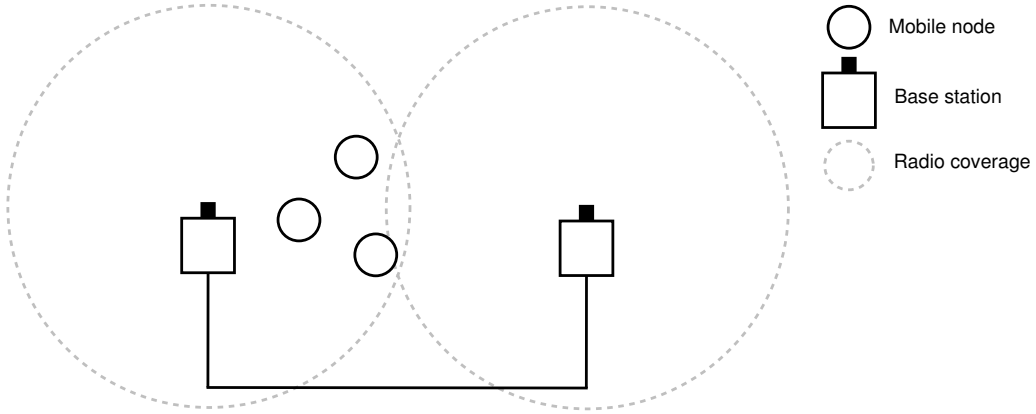

Figure 3.17: Mobile nodes are unequal distributed above the base stations.

If a base station is under high load and its neighbours are not, an algorithm that works on the self-managed base stations, reduces the transmit power of the regarding base station and extend the power of neighbouring stations. This reaction result in mobile nodes changing their base station to get a better connection.

Figure 3.17 shows two base stations and three mobile nodes. All three mobile nodes are in the coverage area of one base station. In Figure 3.18 the base stations change their transmit power in order to force the mobile nodes to switch.

The self-managed base stations provide this algorithm with the needed information by setting a load field in the *public* information section in order to allow each station to find out how much load is on its neighbours, which results into the decision to keep the current transmission power or to low/extend it.

However, such an approach has several drawbacks. To force the mobile nodes in this way also includes that they will lose wireless service until they are reconnected. Even if this is done in the best meaning for the nodes they may not want it. Furthermore, such an algorithm may interfere with the coverage hole closing mechanism described above.

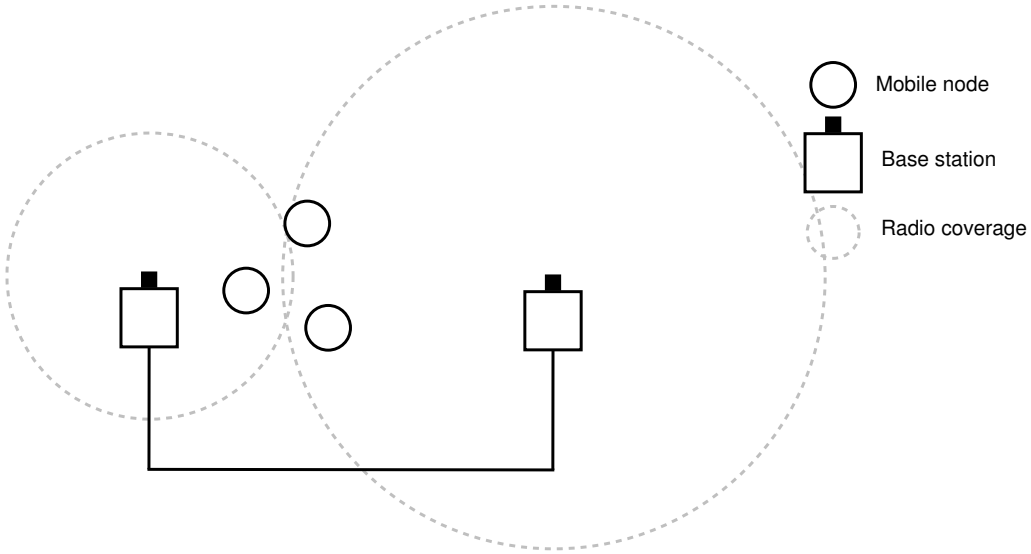

Figure 3.18: The base stations change their transmit power in order to force the mobile nodes to switch.

Software Updates

On a modern base station several software packages have to be installed in order to provide its service, *e.g.*, the operating system, a DHCP [34] server, a firewall, a graphical user interface (GUI) for the administrator and the management software itself.

The middleware helps to keep the stations in a fair state by having a list with references to actual versions of software, including where and how they can be retrieved, in the *global* information section. Such an input is made by a third person, *e.g.*, the network administrator or the base stations vendor.

Each base station may decide to install a new software, if available and the impact on its connected mobile nodes is not to serious. As addition, each software reference is marked with a *level of importance* showing the base station how important the update is. For example, a critical security update is important enough for an base station to install it immediately regardless of how many base stations may loose service. An update that provides only new features may be not important enough and has to wait until a less number of mobile nodes is connected to the base stations.

However, the base stations have to make sure that software updates, especially of the self-management software, does not result in network partition, *i.e.*, the base stations are not able to exchange management information anymore.

Fault Tolerance

When a base station fails to provide its service this has several consequences for the entire wireless access network and for the mobile nodes connected to it. Several arrangements have to be made in order to allow the self-managed wireless access network to be fault tolerant. First, the stations have to find out that they lost a neighbour. Second, the stations have to re-establish a neighbourhood structure that represents the new topology. Third, the stations have to provide service for the mobile nodes that lost service.

The base stations solve this task in the following fashion. Whenever a base station is not able to connect a neighbour, as part of the regular *public* and *global* information exchange, for a longer period of time it may assume the neighbour has failed. In this case it erases the failed station from its neighbour list (*self-cleaning*). The next step for the station is to introduce itself as neighbour to all neighbours of the failed station if they are not already in the stations neighbour list. The last step is to re-run the management applications, *e.g.*, coverage hole detection, load balancing, etc.

The same steps are used if the topology changes are not caused by failure. For example, if a station goes into a sleep mode in order to save power or if a base station changes its position.

3.8.2 Monitoring

Accounting related applications help the network administrator to get better information about what happens inside the wireless access network that is in his responsibility. This information is retrieved directly by the base stations or is based on external information that was collected by the individual stations.

Monitoring on Each Base Station

Possible information to monitor are the interference level, *i.e.*, radio interference from entities that are not part of the self-managed wireless access network like microwaves, the load on the individual base stations, the channel interference between the base stations and the signal strength.

The information gets collected by each individual base station and will be send to its neighbours. Even if a base station fails, the administrator is able to inform himself about what happened before the station failed. However, a *global neighbour* helps to get an overview about what happens in the entire network as described in Section 3.4.3.

External information from user-controlled nodes or specialised measurement nodes [37] helps the administrator even more to deliver a working, full-featured wireless access service by providing him with additional information that is out of the scope of the base stations. For example, a mobile node can analyse link-layer sequence numbers or deducting link congestion based on transmission traces [37].

Location Tracking

The location tracking of wanted or unwanted attendees in a wireless access network helps network administrators in several areas, *e.g.*, to improve the positioning of the base stations in order to establish better coverage or to track down rogue base stations and malicious users.

The concept provides the information about which base station can see which neighbour. In combination with external information, *i.e.*, the mobile nodes report at which position they saw which base station, this information is used to calculate the geographic position of all legitimate and illegitimate (rogue) base stations.

Figure 3.19 shows two base stations that try to locate one mobile with the help of second mobile node. All three of them know that the mobile node is inside their coverage area. That makes it very likely that the geographic position of the mobile node is between them.

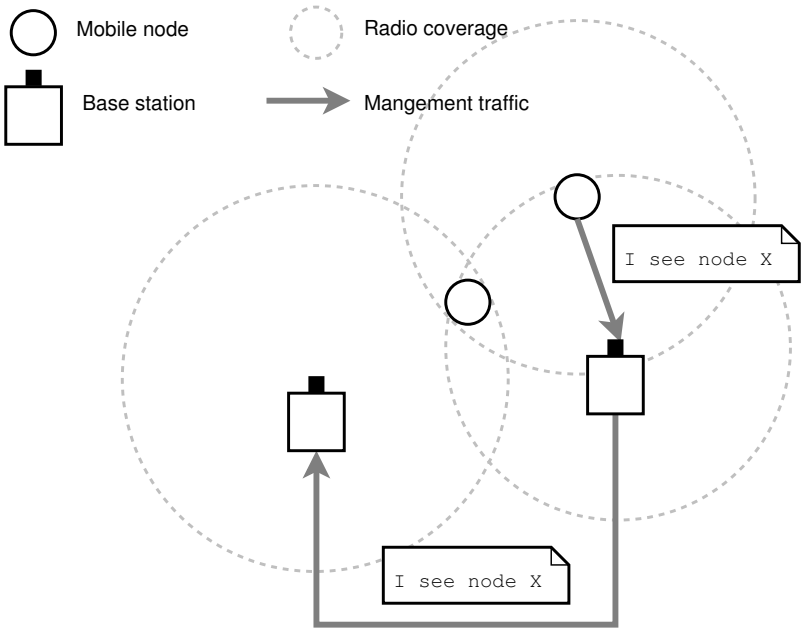

Figure 3.19: Location tracking of a mobile node.

However, the proposed self-management mechanism has all the information needed to solve this task but to discuss an algorithm that is able to provide such services is out of the scope of this thesis, for more information see [16].

3.8.3 Security

One of the most important unresolved problems in today's wireless LANs is the question of security. Even if the network is carefully planned several characteristics of the IEEE-802.11 wireless access networks make security a hard to solve task [72]. Several steps can help to avoid breaking the security, *e.g.*, identify rogue base stations, enable policy enforcement and detect network scans from malicious users.

Because of the amount of security related problems in wireless LANs, security systems and frameworks [13] have become very popular in the past. However, the proposed concept is not meant to solve security issues [19] by itself but it is able to provide security mechanisms its services.

Rogue Detection and Classification

A rogue is a mobile node or base station that runs inside the coverage of the manged wireless access network and either runs in *ad hoc* mode [77][30] or in *infrastructure* mode like a base station [79]. As a result, mobile nodes may connect to this rogue, which is now capable of listening to the mobile node's traffic.

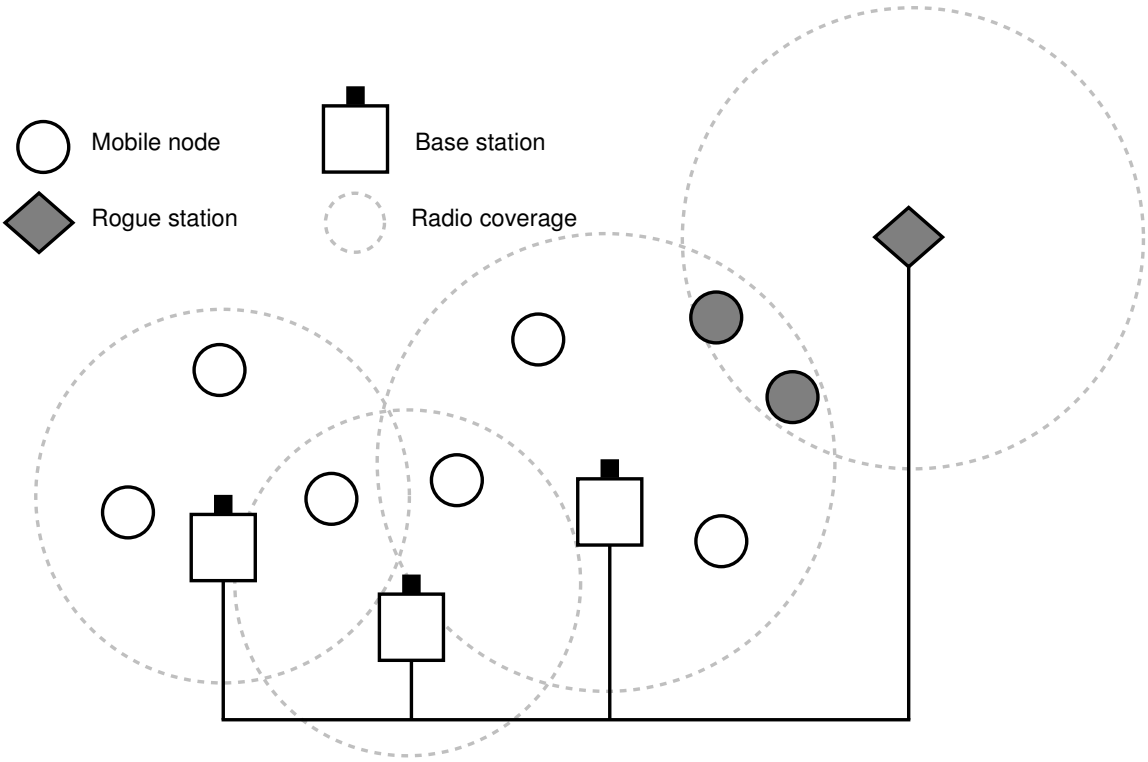

Figure 3.20: Rogue catches mobile nodes.

Figure 3.20 shows a rogue catching two mobile nodes. The rogue forwards the traffic of the mobile nodes to the wired network, thus the mobile nodes do not see the difference to a regular base station. The rogue is now able to eavesdrop and change the traffic of the mobile nodes (*spoofing*).

However, rogue stations are not automatically hackers sitting at a location physically nearby. In most cases regular users are creating there own network inside the coverage area of managed wireless access network without the administrators knowing it [79]. This

is the most common threat and misuse of wireless LANs. Users decide to bring their own base station into the office to be able to connect their Laptop, PDA or mobile phone together. Those base stations typically do not include the same level of security as the enterprise grade base station, *e.g.*, encryption and authentication. The user may give away confidential information into the airspace in an insecure fashion or connect the companies wired network to the airspace without any protection.

As a result, rogues bring several risk factors into the managed wireless access network, *i.e.*, create insecure holes in the network, potentially cause a loss of intellectual property, create a legal liability for the enterprise, deny service to legitimate users, launch man-in-the-middle attacks or degrade wireless performance [79].

The most important issue concerning rogues is that the administrator must know about their existence and about their position. Location tracking (see above) with the help of *external information* solves this task. The *external information* also helps to detect rogues in the first place.

The proposed concept already includes a native rogue detection mechanism. Every base station that was detected during probe phase but was not integrated into the self-managed network may be a rogue. A list of allowed "outsiders" in the *global* information section avoids that every base station that is not part of the self-managed wireless access network gets classified as rogue.

The self-protecting mechanism against such attendees is supported through a *unwanted attendee* list in the *global* information section. These stations are not allowed to connect to any base station in the network. Although this mechanism does not prevent the rogue from providing its "service" to mobile nodes it will make the rogues work harder by not allowing him to forward the mobile nodes traffic to the wireless access network in order to establish a spoofing mechanism. In addition, devices that are used by users as rogue base stations are kept out of the network in order to reduce the risk of having such a user logged into the wireless access network.

Another hint for a rogue is if the hardware address of a managed base station appears

a second time in the coverage area of the managed wireless access network, *i.e.*, a rogue user tries to convince mobile nodes to connect to him instead of a regular station.

As mentioned, the rogues are registered on a *unwanted attendee* list. Next to this, other stations and mobile nodes can get on this list based on there appearance in the network. If a base station for example registers that one of its mobile nodes is effected by a virus or is reacting abnormally, *e.g.*, connecting and de-connecting in short intervals.

However, any member can remove a station from this list, *e.g.*, an administrator who just fixed the mobile nodes. Through this mechanism the self-managed wireless access network is able to deliver a *blacklist* functionality.

Authentication Management

An *access control list* (ACL) is a list of mobile nodes that are allowed to join the wireless access network [21]. Such an ACL is kept in the *global* information section in combination with password/key entries or a link to an authentication server. The values are inserted manually by an administrator or automatically by an authentication system.

Firewall Configuration

In the proposed concept, a firewall helps in several areas. For example, it helps to detect if a mobile node is affected with a *Internet* worm, *i.e.*, the worm tries to reproduce itself and collapses at the firewall, which is monitored by it. Furthermore, it also allows establishing an access control list or it protects the base stations against malicious users. In several cases, the firewall alerts the base station, which then uses the location tracking service in order to find the attacker [15].

However, the firewall may also be configured by the base stations. For example, firewall policies are configured based on a *global* list of unwanted network addresses and services.

There are several choices of how the firewall policies come into the list. There is a static configuration of course, created by a third person from outside the network. Firewall

policies can also be generated by individual base stations in an automated fashion, *e.g.*, based on the previously described *unwanted attendee* list.

Additionally, firewall rules may be part of the *public* information section and base stations configure their firewall based on information from their neighbours. Groups of base stations create different policies to react on circumstances in close range.

Intrusion Detection

Typical intrusion detection systems [69][64] act on individual host basis and warn if a host is compromised. Such an intrusion detection system is plugged into the middleware, running on each base station. If a base station records an intrusion attempt it sets the originating host on a global *untrusted list*. Therefore, the others will ignore him from this point on.

However, intrusion detection in wireless access network has to go further and find out if the wireless access network itself is under attack. Known attacks and attacking utilities, *e.g.*, management frame flood signature, broadcast de-authenticate frame signature, null probe response signature or invalid SSID signature [20], have to be detected and reported. In this case, the location tracking helps to find the attacker. The integration of measurements taken by the mobile nodes can help the base stations to get aware of a possible intrusion [87].

3.9 Summary

This chapter showed the basic functionality of the proposed concept and gave several hints of how it can be improved and extended. It defined assumptions for base stations that want to be part of the network, introduced a information deviation and showed how the different information categories are handled in the concept. In addition, it made several security considerations and showed how the security threats to the proposed concept are solved. Furthermore, it introduced the concept of the integration of external information into the management process. Finally, it introduced a set of examples for management

applications in order to solve the practical needs of the daily management work in modern wireless access networks.

Chapter 4

Evaluation

The previous chapter introduced the proposed self-management concept. This chapter will evaluate the proposed self-management concept in two different directions. First, a qualitative discussion from different perspectives in order to find out how the concept fulfils the targets defined in the introduction. Second, a detailed investigation of the prototype implementation in order to find out how self-managed base stations work in a real live environment.

4.1 Qualitative Evaluation

The qualitative evaluation of the architectural concepts is based on five areas. First, the scalability of the concept, which was one of the main arguments for the decentralised approach, *i.e.*, how does the self-managed wireless access network behaves with a growing number of base stations or mobile nodes. Second, *resilience*, *i.e.*, the network's fault tolerance and robustness. Third, *stability*, *i.e.*, the network does not oscillate between different configurations but should converge to one. Fourth, *performance*, how fast can configuration changes spread though out the network. Fifth, *flexibility*, *i.e.*, the network's capability to handle a wide range of different setups and situations.

4.1.1 Scalability

The scalability of the self-managed wireless access network is discussed in the following areas. First, what happens with a growing number of base stations? Second, what

happens with a growing number of mobile nodes? Third, what happens with growing traffic from the mobile nodes?

As mentioned, the proposed concept has fewer bottlenecks in communication or computing. Compared to centralised approach, where the network link to the central master and computing limits of it create a bottleneck, the decentralised approach distributes the work over all base stations. A growing number of mobile nodes and a growing number of traffic from the mobile nodes can be shared between the base stations.

However, if the mobiles nodes are distributed above the base stations in an unbalanced fashion the base stations with a high load will become the bottleneck. The load-balancing mechanism described above reduces this problem but may not be able to solve it entirely, *i.e.*, it distributes the mobile nodes in a geographic area only better above the stations in that particular area.

Another argument for the proposed concept from the perspective of scalability with a growing number of base stations is the acceptable messages grow. The reason for this behaviour is that the direct neighbours exchange information about their local state, *i.e.*, local information that is primarily important for the neighbouring stations is kept inside the neighbourhood. Only the changes to the *global* information section have to be distributed over the entire wireless access network and this distribution will be piggy-backed on the information exchange between neighbours.

Compared to a central approach the exchange of local information between two neighbours is nearly halved, *i.e.*, neighbours interact directly and do not have to make the indirection above the central device. However, in the centralised wireless access network the master may decide that the information from one station does not have to go to all its neighbours in order to reduce this disadvantage compared to the proposed self-management approach. Additionally, the disadvantage is reduced if a base station has more than one neighbour. If N is the number of neighbours the proposed self-management concept has to sent N messages, the central $N+1$.

A flooding approach, where each base station pushes information to all other stations

in order to bring a *global* information change throughout the network, is an alternative. However, this approach brings high load in networking and computing to the sending station. The proposed concept avoids this, because each station informs only its direct neighbours.

In addition, there are also problems with this approach that have to be taken into account. First, to keep *global* information consistent is harder with a growing number of attending base stations. The spreading of new global information will take a longer period of time, which will result in a growing number of inconsistencies. Base stations start to commit changes before changes committed by other stations are not already spread throughout the whole network.

Figure 4.1 shows first the base station on the left sending a message to its neighbour. In the next step, this neighbour forwards this message while at the same time another base station, which do not know about the sending, sends another message. If both stations erased the *version counter* because of new *global* information they wanted to insert, the two messages have the same version counters, but contain different information sets. The second base station from right retrieves the two messages and detects the inconsistency. As already mentioned, in the prototype implementation it will try to merge the two sets together.

A solution to this problem is a locking mechanism in order to protect the write access to the *global* information as described in Section 3.4.2. Note, this problem arises only with *global* information changes, keeping the information exchange as local as possible will avoid such problems.

Another issue regarding scalability is that the *global neighbour* concept may not work in larger networks. As with the centralised solutions it creates a bottleneck, *i.e.*, the *global neighbours* capabilities. In large-scale wireless access networks it may be a solution to set up several *virtual neighbours* and let them filter the information before sending it to a central information sink.

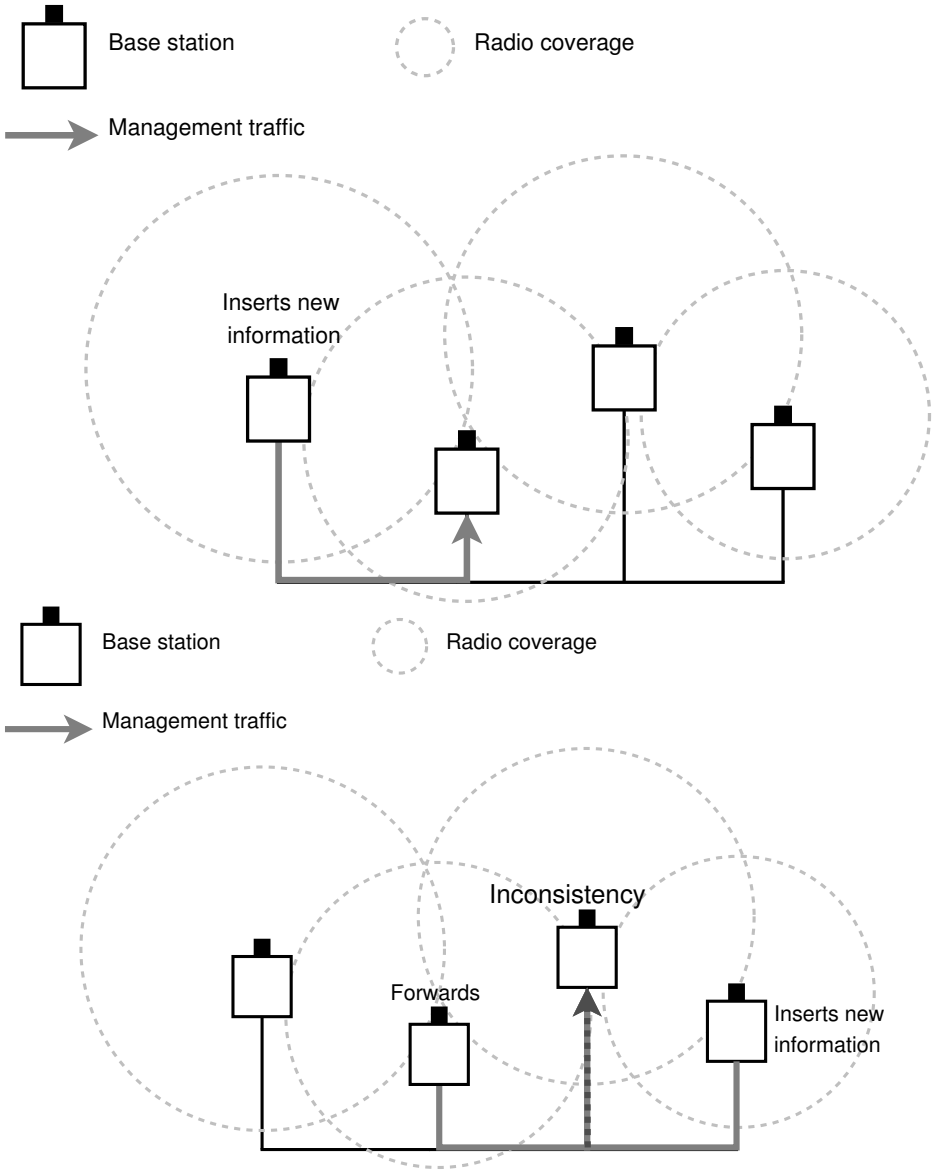

Figure 4.1: Inconsistency in management information.

4.1.2 Resilience

The reliability of the self-managed wireless access network is discussed in the following areas. First, what happens if a base station stops to provide its service? Second, does the concept has a central point of failure?

The proposed concept implements a *self-cleaning* mechanism in order to establish a resilient service. Every base station that stops the self-management process is deleted from the configuration of all its neighbours in a automated fashion. Further management applications may allow the self-managed wireless access network to deliver a fare more resilient service, *e.g.*, coverage hole detection, fault tolerance or load balancing (Section 3.8.1).

Another key point of the proposed concept is avoidance of a central device, thus the avoidance of a *central point of failure*. However, there may problems arise if the network of base stations is at several points only connected through a small number of base stations. If those stations fail, the network will be partitioned.

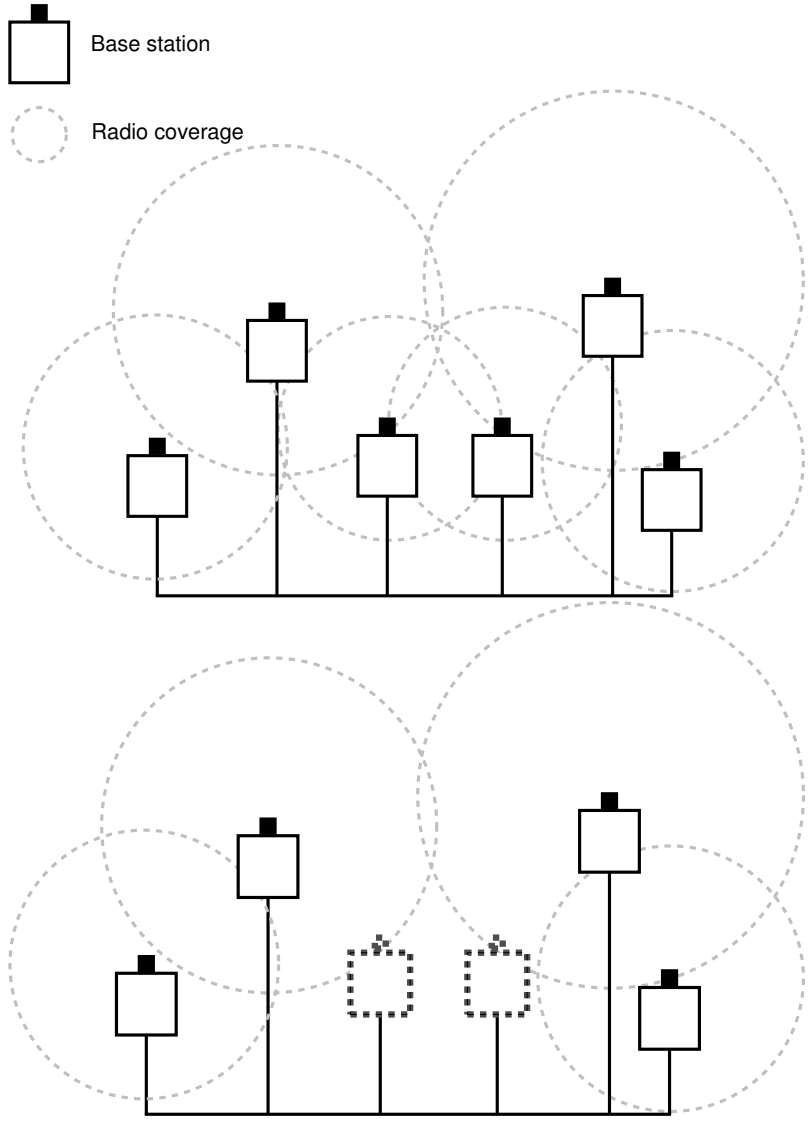

Figure 4.2: The wireless access network partitions after the failure of two base stations.

In Figure 4.2 two stations stop their service. Because each station was informed by its neighbours only about their direct neighbours, it does not know about the stations behind. As result of this situation, the former connected network will disconnect. From this point on two independent networks, exist.

In the current concept, this is the same problem as if the stations on the left and on the right side of the figure have never been connected to each other. However, the question may arise if those two groups do even have to form a whole network. If they have no overlapping coverage areas, there may be no need to exchange information at all. Based on the perspective of local (*public*) information, *e.g.*, channel allocation, signal strength, etc., they do not. From the perspective of *global* information, *e.g.* network wide wireless encryption key or wireless protocol, they may.

There are solutions to this problem. First, an administrator may set up several virtual neighbour relationships around such a problematic point. Second, the wireless access network may perform an internal analysing of the topology, *i.e.*, create an undirected graph, and create virtual neighbour relationships on its own in an automated fashion. This is done before the fallout in order to avoid such problems in the first place or is used after the fallout in order to get the topology graph connected again. Figure 4.3 shows a virtual relationship between the two base stations that will reduce the risk of partitioning. However, such an algorithm is out of the scope of this thesis but may be part of future work in this area. Note, if the base stations come up again, they will reconnect the network.

As a result, the proposed self-management mechanism has an improved resilience compared to the central solution with the drawback of the partitioning risk.

4.1.3 Stability

The stability of the self-managed wireless access network will be discussed in one area. Are the stations able to find a distributed state for their *global* management configuration?

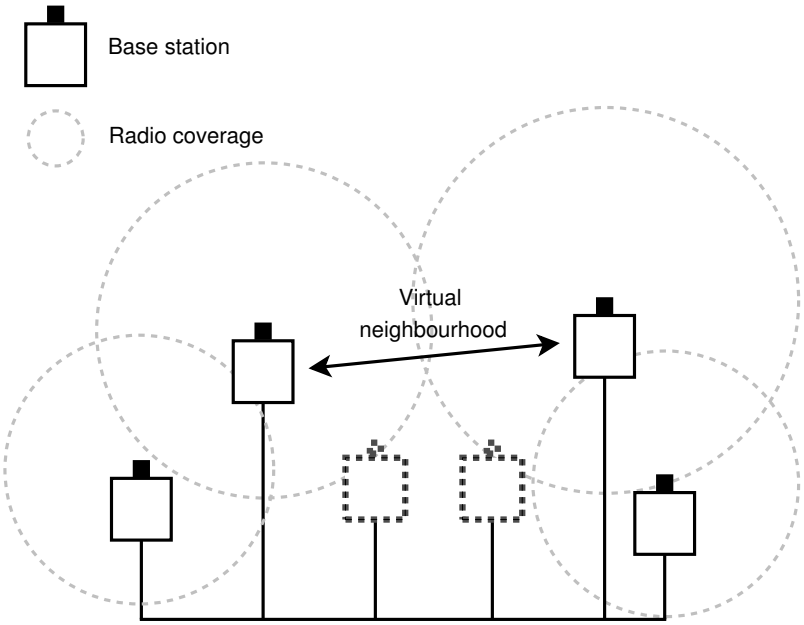

Figure 4.3: A virtual relationship avoids network partition.

The self-managed wireless access network has to avoid that the configuration is continuously changed and the stations cannot find an agreement in configuration setup. Because the network has no central device that is capable to force a single configuration setup other mechanisms have to be used in order to deliver a stable wireless access service.

The proposed concept avoids stability problems in the configuration decision process in two different ways. First, most of the configuration changes are done locally between direct neighbours. That means that only a small number of stations are part of the information exchange and the decision which information to use. If even in those small groups problems concerning stability arise, de-synchronisation delays may help as shown. Second, in a global scope the mechanisms described in Section 3.4.2 help to avoid the wireless access network to stay inconsistent, *i.e.*, *mutual exclusion* for important and information *merging* for less important changes.

As a result, in a decentralised and self-managed wireless access network with autonomic base stations the stability is always at risk, because no central management station can force a stable setup. However, mechanisms to solve that problem are known.

4.1.4 Performance

The performance of the self-managed wireless access network will be discussed in one area. How fast can the base stations make their management decisions, which relates to the question how fast can the management information be exchanged between the base stations.

As mentioned, the neighbourhood approach allows the wireless access network to keep information exchanges in a local scope. That means that the network usage is reduced and the information exchange is performed in small ranges, *i.e.*, between direct neighbours. In the centralised concept every station has to get connected to the central master in order to inform him about information changes and this central master has to get connected to all regarding stations for this information changes. Therefore, every information exchange that regards only a small subset of the managed stations has to go the same way as every information change that is important for all stations.

In the proposed approach, only information that really matters to all stations is distributed to all.

However, there is one performance related problem with in the proposed concept. If information changes have to be global they need more time to get distributed because the change has to go through the neighbourhood from station to station.

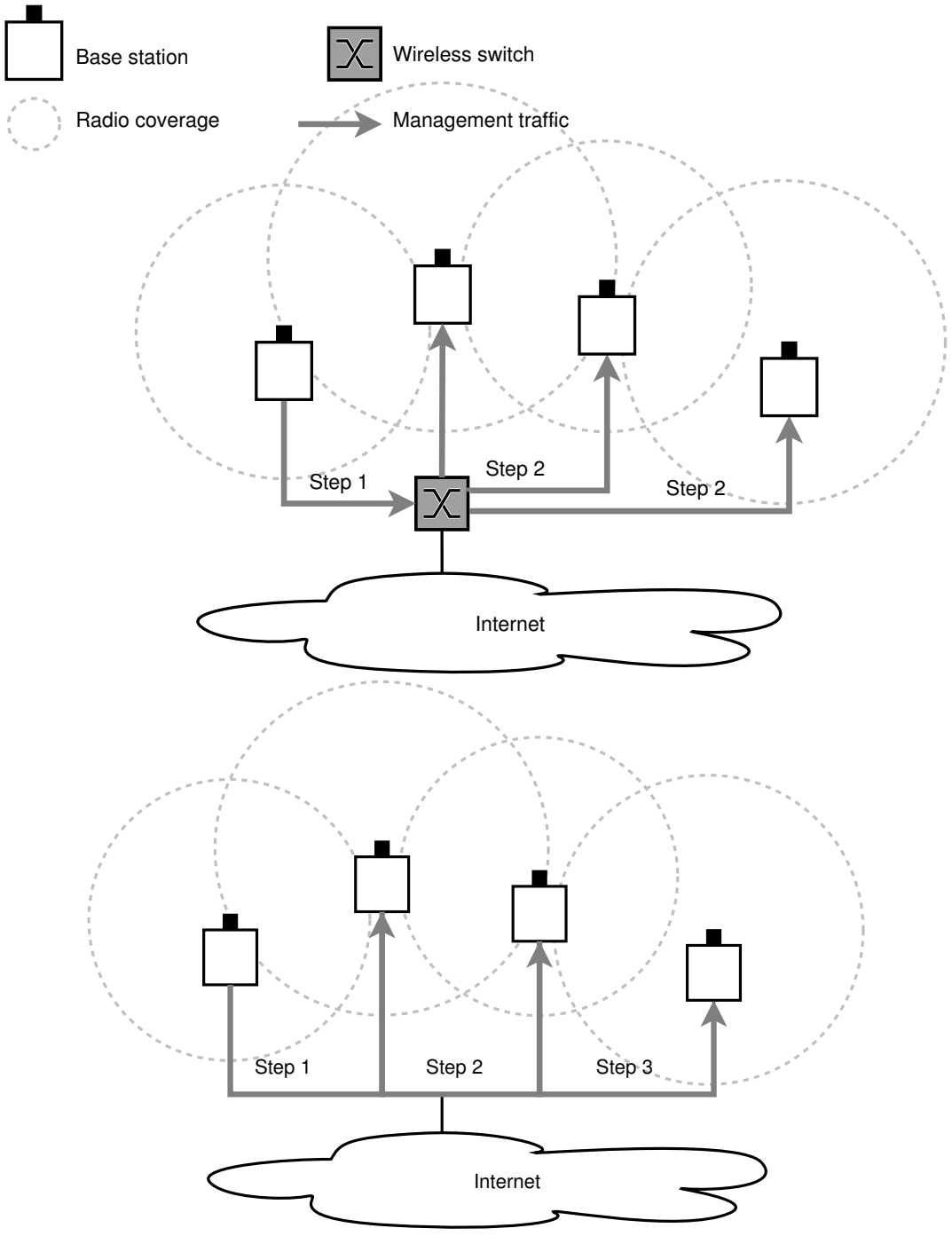

Figure 4.4: The disadvantage of decentralised global information exchange.

Figure 4.4 shows in the top graphic a central solution. The base station with new information sends it to the wireless switch, the switch sends it to all regarding base stations, two steps. The bottom graphic shows the proposed decentral solution. The base station sends the new information to its neighbours, the neighbours forward it to their neighbours, with four base stations that makes three steps. That means that even if the base stations would forward new information immediately, they would still need more time to spread new information throughout the wireless access network.

As a result, a centralised approach may be faster if the amount of global changes to the information base is higher, therefore the proposed concept is faster if the local information changes overweight. Based on the assumption that a typical wireless access networks exchanges more information in a local scope, the proposed concept has better performance capabilities. The performance measurements of the prototype implementation are in Section 4.2.

4.1.5 Flexibility

The true strength of the proposed concept is its flexibility in different environments, different wireless access network sizes and different network and infrastructure technologies.

First, the concept works in wireless access networks with any number of base stations. Because most of the information exchange is kept between direct neighbours, it does not matter how big the wireless access network around that neighbourhood is. However, with a growing network it might be needed to keep the global information changes low in order to avoid performance problems as described above.

Second, the concept needs no special infrastructure, *e.g.*, the central management station itself and the base stations do not need layer two connectivity as a switch does. That includes that the base stations may communicate above any technologies that is IP capable. Furthermore, the management interface can be wired or wireless. That means the base stations may not need a network infrastructure at all.

Third, the concept can work with base stations from different vendors even with different wireless access architectures, if they implement the self-management mechanisms. The *global* information section may contain information relevant to specific architectures, *e.g.*, protocol information and information relevant to all, *e.g.*, an access control list, information for software updates or detected coverage holes.

As a result, the concept is flexible in all three areas.

4.2 Quantitative Evaluation

This section evaluates a prototype implementation of the proposed self-management concept. The results investigate the basic functionality and are preliminary. The current prototype is a *Perl* daemon that is capable of operating on physical hardware, *i.e.*, a Linux PC equipped with IEEE-802.11b WLAN interfaces and a group of such machines within radio range will *self-configure* in interaction with one another. Next to the basic functionality, the prototype implements the channel-selection application.

However, an analysis of the scalability properties using physical devices is impractical, *e.g.*, budgetary problems. Therefore, the prototype offers a simulation mode, where multiple copies of the same code execute on a single PC inside a simulated topology. During the simulation, each base station runs as a single process. The measurements in this section analyse this simulation mode.

During simulation, each (simulated) base station prints the current network ID (ESSID) of its wireless access service in a log file. This file is used to find out if all base stations are convergent, *i.e.*, have the same *global* information. During the simulations, the ESSID is the only value in the *global* information section that has to change.

Furthermore, one log file exists for each used ESSID. The base stations write into this file when (in absolute time) they switched to this ESSID and when they switch away to another. With this information it can be reconstructed how the changes took place.

Additionally, each base station writes into a log whenever it receives management messages. This will allow measurements regarding the amount of management traffic.

Although the prototype normally uses *Internet* sockets, in simulation modes it prefers *UNIX* domain sockets. However, to use *loop back* devices may be an alternative.

The number of base stations that are simulated on a single machine was limited to 100. Larger groups of base stations brought the risk that the amount of computing power, which was needed for simulation, may adulterate the measurement results, *i.e.*, the simulating host became non-idle for longer periods. However, further implementations may be written with usage of programming techniques and languages with better performance capabilities than *Perl*, *e.g.*, in *C*. An even better approach is to implement the concept in a network simulator in order to get measurement results for large-scale networks.

4.2.1 Initial Network Convergence Time

The preliminary scalability analysis investigates the convergence time of the group of base stations if all start up within a few seconds of one another, *i.e.*, the time of the initial *self-configuration*, such as after a power failure. Mobile nodes are not present. The experiments measure the convergence times of 500 repetitions and calculate mean performance and standard deviations. Each experiment uses a randomly generated, connected base station topology, *i.e.*, the aggregate coverage area of the base station group is not geographically partitioned. This is arguably a common deployment case; the usefulness of integrated management of a group of base stations that cover geographically separate regions is unclear. The number of base stations is a parameter of the experiment and grows up to 100 in increments of 10, with two additional group sizes of 5 and 15 to investigate behaviour for small groups.

Figure 4.5 shows the performance. For smaller groups of 1-20 base stations, the mean initial self-organisation time quickly increases from 17 to approximately 20 seconds. For larger groups of 20-100 base stations, the mean initial self-organisation time remains between 20 and 25 seconds.

A single base station self-configures in approximately 17 seconds. This is due to the startup behaviour (Section 3.2.) After the initial randomised 0-10 second de-synchronisation delay, a base station initiates a probing phase to detect and contact its neighbours. This

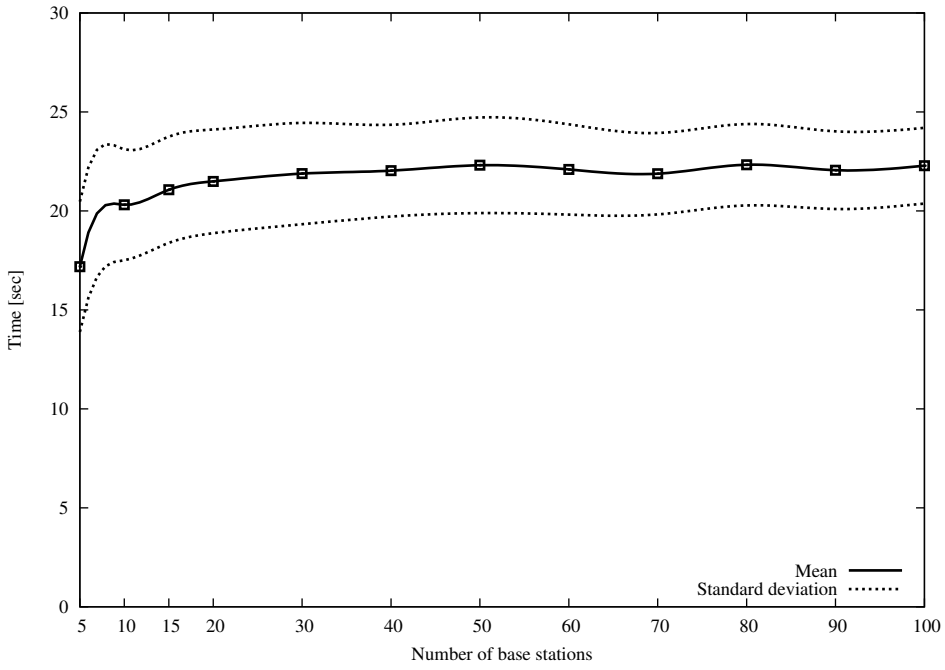

Figure 4.5: Initial convergence times of groups of base stations.

operation takes approximately 2 seconds. When no mobile nodes are associated with a base station, it repeats the probing phase. The second probing phase starts already after 10 seconds in order to allow a base station to detect additional neighbours that were still channel scanning during its initial probing phase. It will then initiate communication with these neighbours and start the information exchange.

The probing mechanism implemented by the current prototype can only detect neighbours that are already offering client connectivity, *i.e.*, have switched to infrastructure mode. A future revision may extend this behaviour to detect neighbours that are themselves still channel scanning. This means that with the current prototype, some base stations do not detect all their neighbours during their initial channel scan.

After the probing phase finishes, self-configuration is complete. If neighbours are present, further processing is required. Further probing phases should be done in larger intervals in order to provide the services for potential mobile nodes that want to connect. The prototype re-probes every 1800 seconds.

As a result, from the measurements, the network convergence time does not grow with the number of base stations. However, based on the existing results this is true at least for small groups of base stations. Note that although this decentralised self-organisation is costly for small groups, it adapts well to larger groups, as indicated by almost constant convergence times for increasing group sizes. Future experiments will verify if this scalability trend holds for groups of several thousand base stations.

Figure 4.5 showed the convergence time based on the number of base stations. However, the number of base stations may not be the best measurement parameter to describe the situation the prototype has to manage. There are differences between topologies that may reflect the requirements for the prototype in a more precise way.

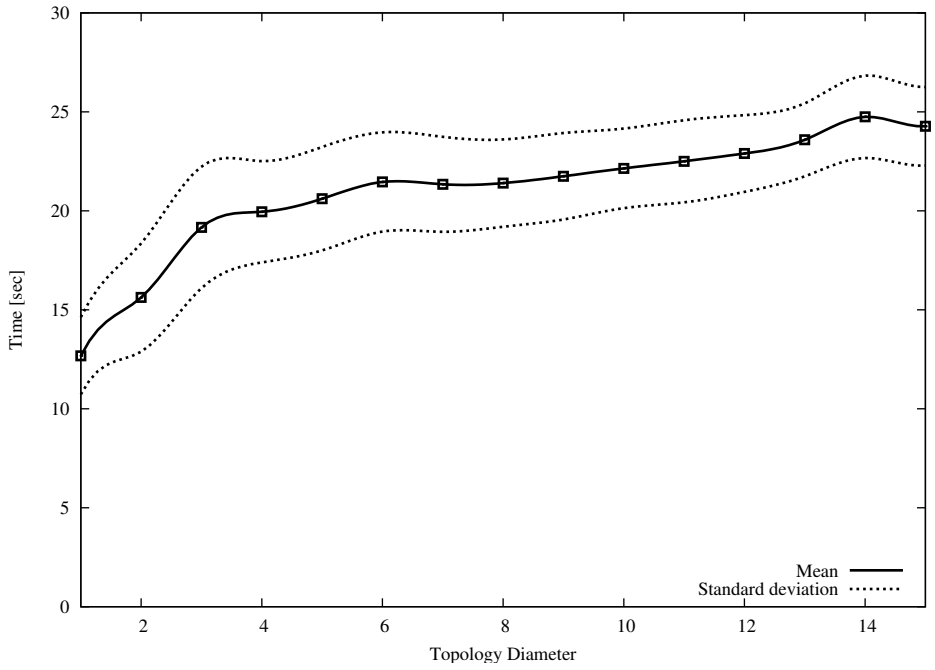

Figure 4.6: Initial convergence times based on the topology diameter.

Figure 4.6 show the network convergence time based on the results of the same experiment but uses the topology diameter, *i.e.*, the longest shortest route between two base stations, on the x-axis. Very few topologies have a diameter larger than 15 (Figure 4.7), thus are meaningless and not shown in the figure.

The network needs more than 20 seconds with a diameter above 8-9 for convergence. However, this amount does not grow significantly with a larger diameter. That is because all the base stations in all different parts of the topology came up at the same time, only with a small de-synchronisation delay. Because of the simple merging mechanism (Section 3.4.2) the first base stations that came up already agreed about one *global* information setup, *i.e.*, with a higher *version counter*. The base stations that come in later on can adopt this agreement.

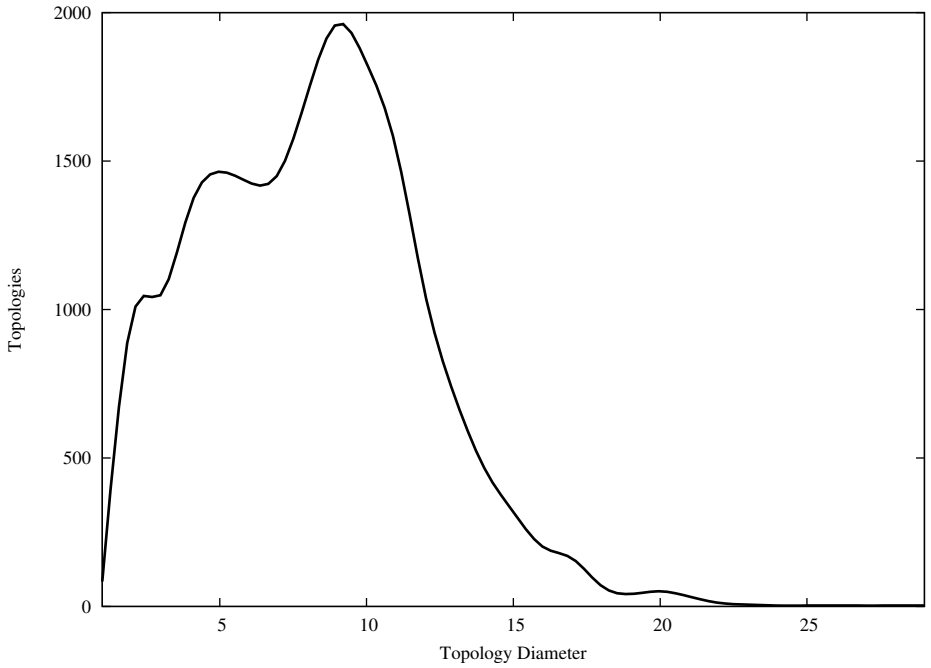

Figure 4.7: Diameters in random generated topologies.

The reason why the mean convergence time in Figure 4.5 is around 20 seconds and the mean convergence time in Figure 4.6 is above for most diameters lies in the amount of topologies with a diameter less than 10. Figure 4.7 shows most of the topologies have a diameter below 10.

The measurement of the network convergence time showed the strength of the decentralised approach in term of scalability with a growing number of attending base stations. However, with a larger wireless access network the distribution time for new *global*

configuration settings will grow. This will be analysed in the following section.

4.2.2 Epidemic Message Spread Time

This scalability analysis investigates the dissemination times of changes to *global* state based on the set of base stations that became connected in the experiment above. That means the base stations already build a wireless access network as a whole. A new *global* configuration setting gets inserted at one random base station. The experiments measure the convergence times of 500 repetitions and calculate mean performance and standard deviations. As in the experiments above, 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 behaviour for small groups.

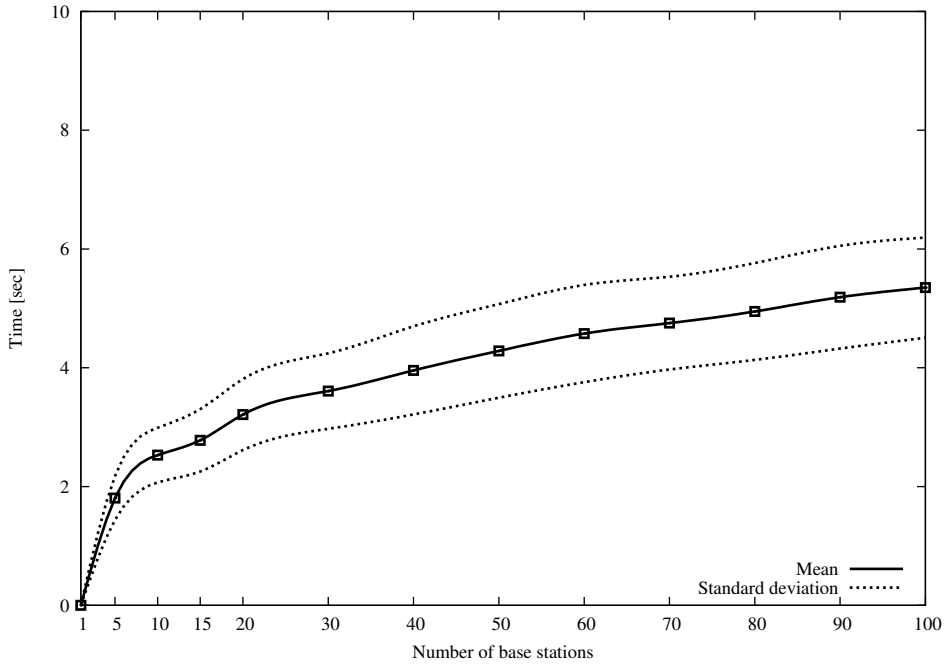

Figure 4.8: Dissemination times of changes to global state.

Figure 4.8 shows a growing dissemination time up to 5 seconds. The number seems to be large but is a result of the information forward delay of each base station. Each base station informs its neighbours about changes in periodic intervals. In the current proto-

type the default is set to 1 second. That means that a change at the *global* configuration set at one base station is forwarded after a second at maximum.

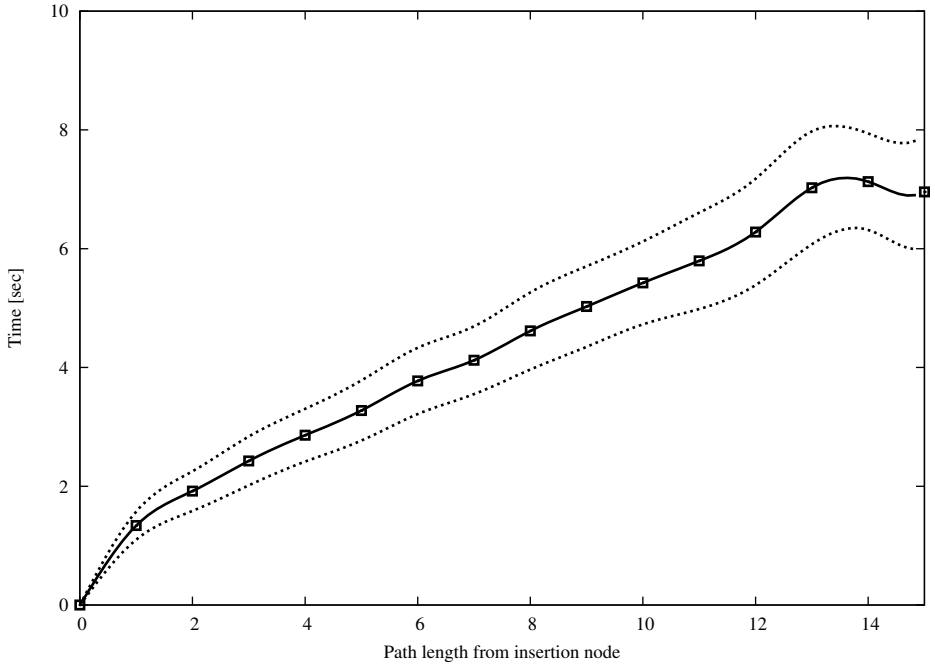

Figure 4.9: Dissemination times of changes to global state based on the path length from insertion node.

Because this happens at every base station, it seems to be interesting how the dissemination time grows with the number of base stations between the point of insertion and the station with the longest shortest path between (*hops*). Very few topologies have more than 15 hops (Figure 4.10), thus are meaningless and not shown in the figure. Based on the results from the experiment above, Figure 4.9 shows a linear growing with the number of stations.

The standard deviation of nearly a second in both directions results to the forward delay of 1 second *at maximum*. If a new *global* information set comes in right after the last forward or right before the next one is random. The growing standard deviation results from very few topologies that had such a high number of hops. Figure 4.10 shows that only a very small number of topologies have more than 16 hops.

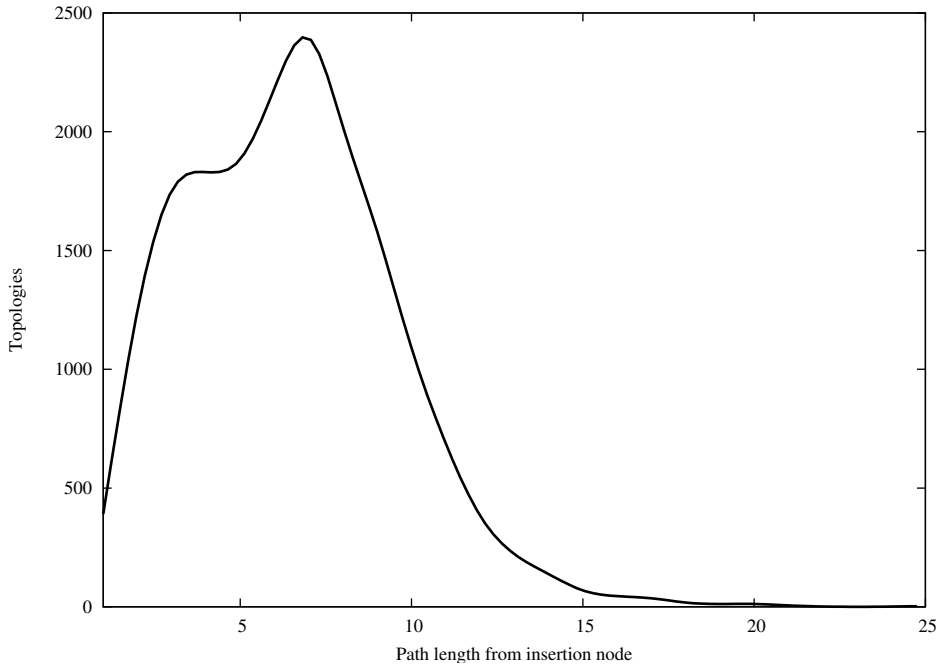

Figure 4.10: Path length from insertion node in random generated topologies.

Figure 4.11 illustrates how the epidemic approach spreads the new information throughout the network in the described experiment. It shows six *snapshots*, the first at time of insertion, each of the following after 1 second. However, the information spread seems to be faster at the beginning but this is related to the *snapshots*. They have been used instead of continuously track of changes for performance reasons during the simulation. Several changes may happen directly before the snapshot or after.

The result from this measurement is that the dissemination time of changes to *global* state does not grow significantly with the number of base stations but it does grow with the path length from point of insertion and the station with the longest shortest path from it. That means that for scalability evaluation it seems to be more interesting how the topology is build up and not how many stations contribute to the wireless access network.

What was not measured during this test were different link capabilities between the base stations. As mentioned, the simulated nodes were connected over *UNIX* domain sockets.

However, Figure 4.9 shows that most of the stations are provided with information over different (logical) links. If the base stations are connected over different links, the fastest one defines the speed for epidemic message spread.

This section showed also that the dissemination times of changes to *global* state depend on the forward delay mechanism at each station. The following section will analyse this dependency.

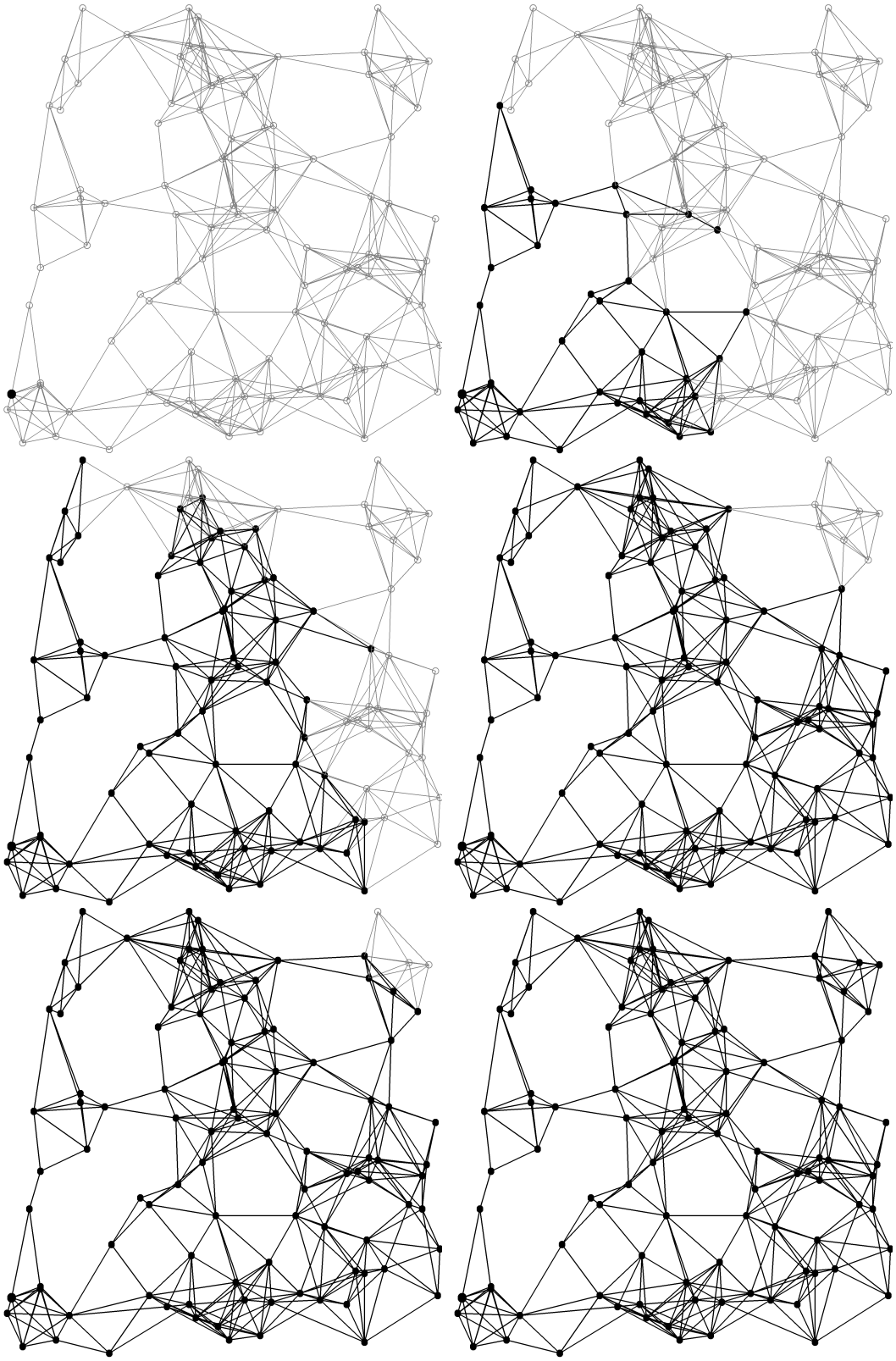

Figure 4.11: Epidemic replication in a set of 100 base stations.

4.2.3 Different Forwarding Delays

To avoid message storms in the network, new information is sent in defined periods by the individual base stations. This is true for new local information that has to go to the neighbours the same way as for *global* information changes that have to be forwarded. This proceeding has several advantages, *e.g.*, avoiding message storms or reducing the load, both on networking and computing, at the individual nodes. The disadvantage is that the dissemination of changes to *global* state takes more time to accomplish.

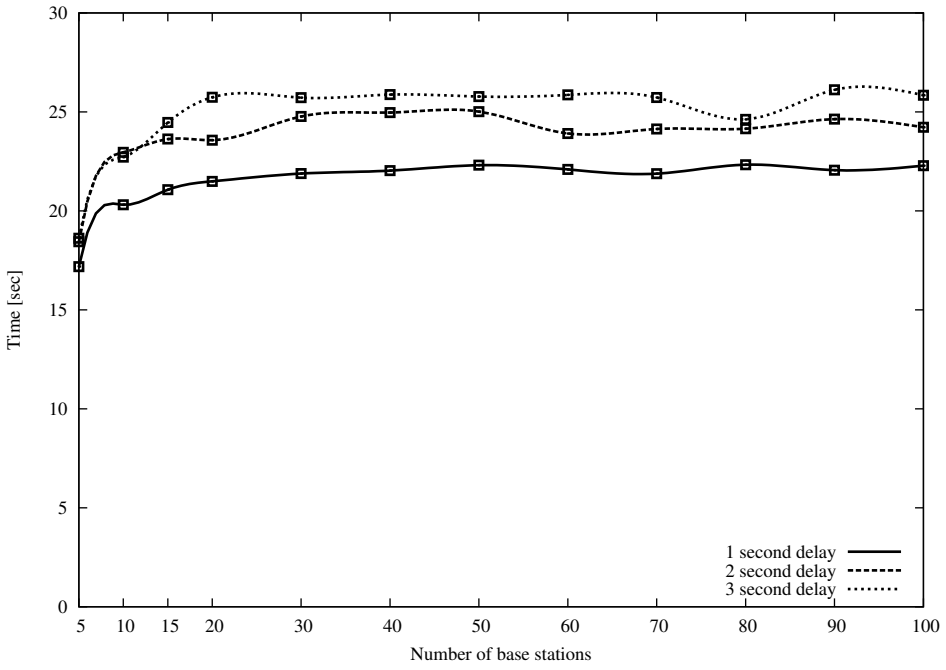

Figure 4.12: Different forward delays in network convergence time.

Figure 4.12 shows the results from the existing network-convergence-time measurements based on the number of base stations. Those measurements have been done with the default forward delay of 1 second. Furthermore, they have been done with an increased delay of 2 and 3 seconds implemented in the same experiment.

As result form increasing forward delay, the mean time of getting the network convergent increases for 3 and 5 seconds for the same number of base stations.

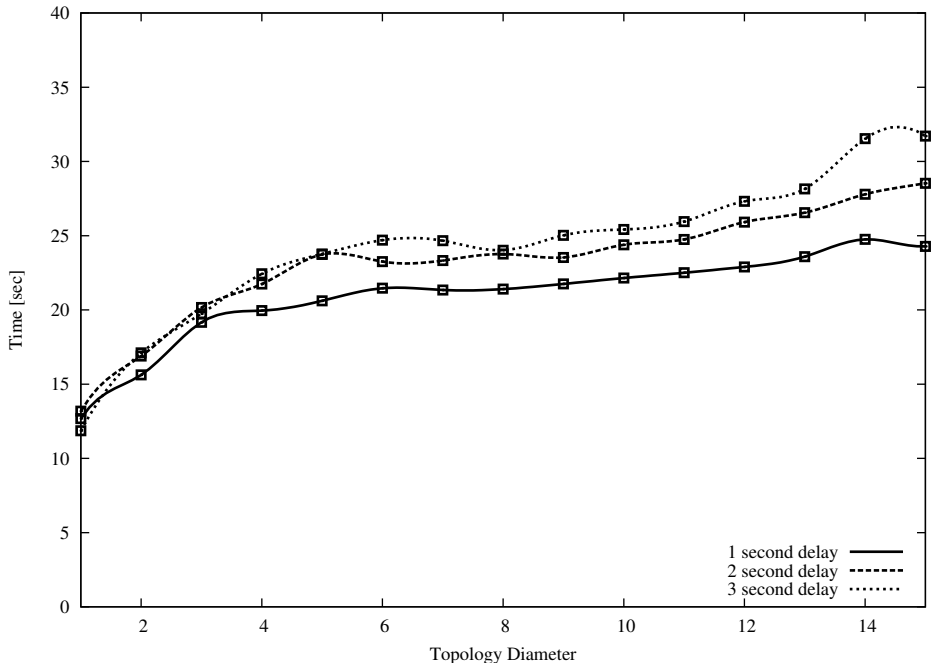

Figure 4.13: Different forward delays in network convergence time based on topology diameter.

Figure 4.13 shows the results from the existing network-convergence-time measurements based on the topology diameter. The topology diameter has a higher relevance than the number of base stations if it comes to a slower message spread throughout the wireless access network.

The reason that the mean time does not change dramatically is that a large part of the convergence time is a result of timers, *e.g.*, the 10-second de-synchronisation delay. That means it seems to be more interesting to analyse the impact of a growing forward delay based on the epidemic message spread time, as it contains no other timers.

Figure 4.14 shows the results from the evaluation of dissemination times of changes to *global* state. Those measurements have been collected with the default forward delay of 1 second. Furthermore, they have been done with an increased delay of 2 and 3 seconds implemented in the same experiment.

As already assumed, compared to the experiment above, the dissemination times increase

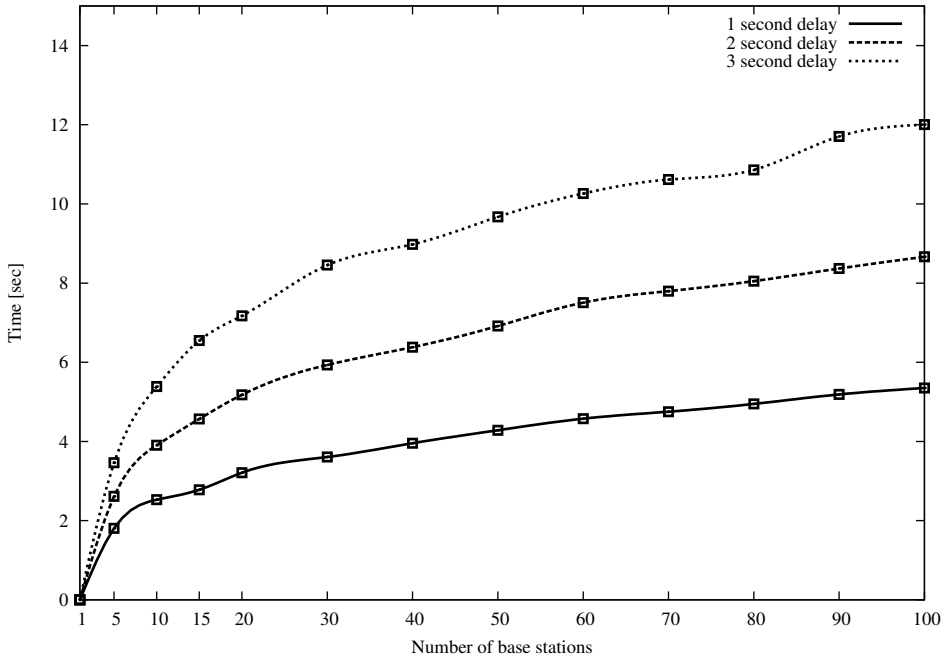

Figure 4.14: Different forward delays in changes to global state.

far more clearly with a growing forward delay. Contrary to the default forward delay of 1 second where the prototype needed around 5 seconds, it now grows to 9 with 2 seconds, with 3 seconds even to 12.

This becomes even clearer in Figure 4.15. The topologies with the shortest largest route from the point of insertion needs with the default delay around 7 seconds, it then goes in the next plot nearly to 14 and then above 19 seconds.

As a result from the analysing of the forward delay it is known, that with a growing delay the prototype needs more time to get *global* information changes throughout the network. However, how this value is set is always a decision between keeping the load, for the stations and the network, low on one side and the overall performance on the other side. However, in the current prototype the delay it set statically but it seems interesting to have an algorithm running on each station that set the delays in an automated fashion. Each station decides between getting information distributed as fast as possible and keeping the amount of computing and network power that has to be invested as low as

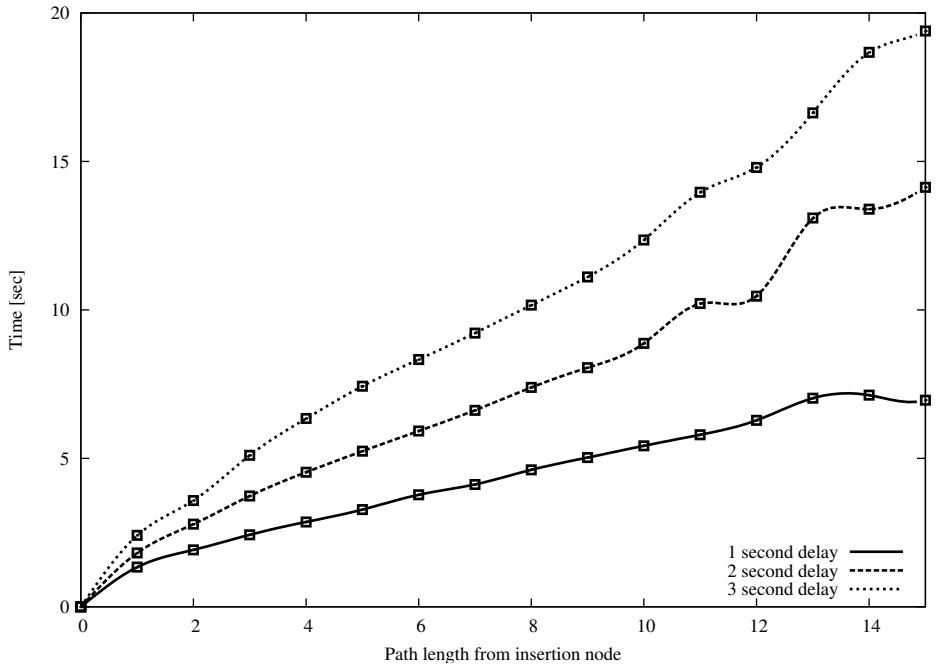

Figure 4.15: Different forward delays in changes to global state based on the path length from insertion node.

necessary.

4.2.4 Management Traffic Overhead

Another question that arises with a decentralised self-management concept is how much information has to be exchanged throughout the wireless access network. This is a key question regarding the scalability of the concept. Contrary to the centralised concept each station only has to inform the central master about changes in the information, in a decentral managed network each base station has to inform all regarding stations, *i.e.*, neighbours for *public* information and all for *global* information, about the change. Additionally, the sending station may not even know which information may interesting for the neighbours, thus informs them about everything. Remember, one basic rule in the proposed concept is that stations get informed but they make their decisions based on their individual collected information autonomously.

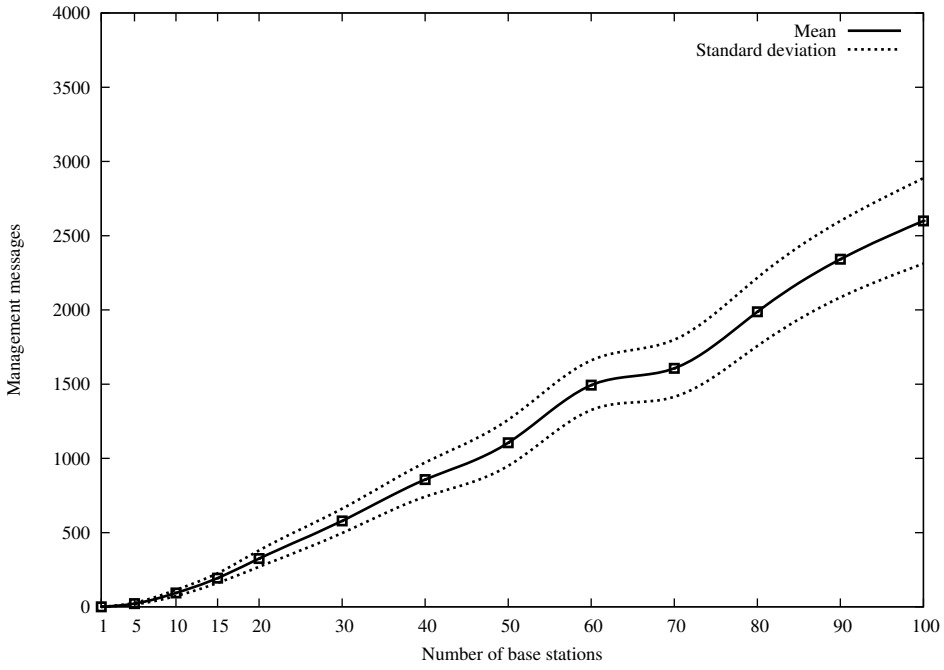

Figure 4.16: Information exchange traffic during network convergence time.

Figure 4.16 shows the amount of information exchanges during network convergence. The results are based on the taken measurements for network convergence time. For 100 base stations, the mean value goes up to 2500 information exchanges. That means that each station was informed 25 times by other stations about their current information. If, for example, each station has five neighbours that means that each station got informed 5 times by each neighbour. An acceptable value that showed that even during convergence time the prototype does not seem to disable itself. Furthermore, the linear growing of the plot seem to implicate this behaviour for larger groups of base stations.

4.2.5 Benefits of External Information

A key part of the proposed concept is the integration of external information. However, the quantitative evaluation of this mechanism is far more complicated then the evaluation of the base functionality as described above. This section picks one possible scenario for the usage of external information and tries to find out how it helps the self-managed base

stations is this area.

The same algorithm that created the topologies for the experiments above was used to create topologies for larger geographic areas in order to become networks of base stations that are not able to get connected based on their own wireless scans. That means without the help of external information or manual configuration of an administrator it is not possible to establish a working self-managed wireless access network.

The number of base stations and mobile nodes in the network was fixed; 100 base stations and 500 mobile nodes. The percentage of mobile nodes that are willing to help and are trusted by the base stations is the parameter of the experiment and varies from 1 to 100. The experiments measured the percentage of topologies that are closed of 1000 repetitions and calculate the mean and standard deviations. For each repetition, a new random topology was used.

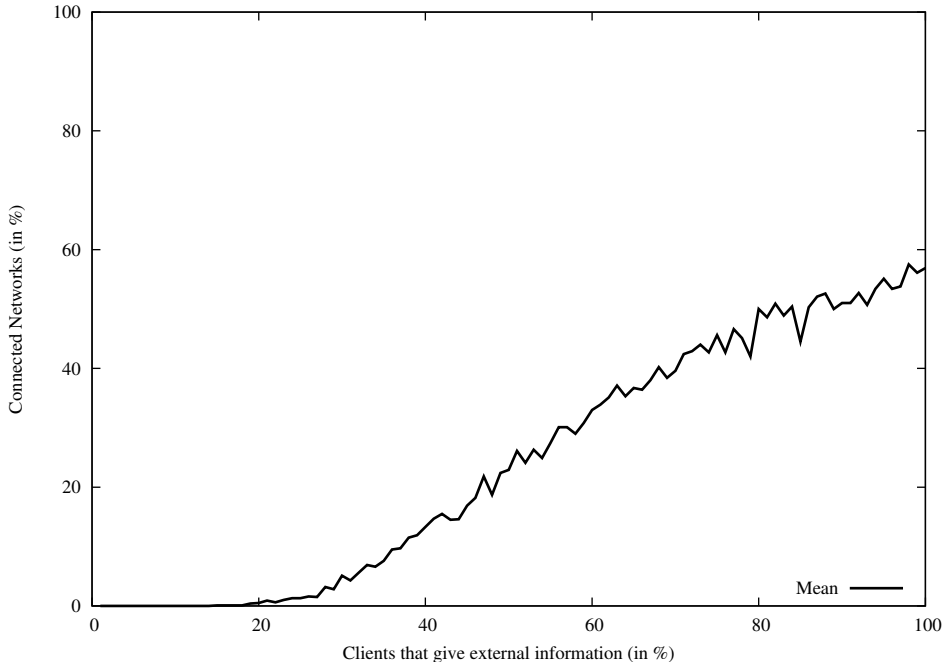

Figure 4.17: Benefits from integration of external information.

Figure 4.17 shows that with the use of 20 percent of the mobile nodes as *sniffers*, the first networks can be connected. With the use of all mobile nodes, around 50 percent of

the networks are closed. This result seems to be low but the reason for this behaviour is that during the experiment the mobile nodes did not move. They gave away only information from their static point of view. Further investigations should include mobile nodes movement. However, to implement these measurements in a simulator that is able to include persons movement in a building was far to much work for the measurements done for this thesis.

As a result, in this specific area the integration of external information can help to solve a problem in a self-managed wireless access network. However, further evaluation is needed in order to evaluate the usage of external information for other management applications.

4.3 Summary

This chapter made an evaluation of the concept of Chapter 3. It showed in a qualitative investigation that the concept scales, performs, is flexible, stable and resilient. Additionally, it made several comparisons to the central approaches. It argues that a decentral approach can work and is superior compared to central concepts in several areas.

The quantitative evaluation of the concept showed that the prototype worked with up to 100 base stations and gave several outlooks of the next steps that have to be done in order to have even better simulation results, especially with larger networks. It showed the message volume in the implemented prototype and finally made a first analysis of the integration of external information.

Chapter 5

Conclusion and Future Work

This thesis presented a decentralised concept for a set of autonomic base stations. A self-managed wireless access network that has no need for any kind of central management device. Chapter 1 made the introduction to wireless access technologies. It gave a brief overview of the history of wireless access networks and described the problem of managing them. It made clear that the existing situation of how wireless access networks, especially WLANs, are managed is unacceptable and how a solution could look like. Chapter 2 described existing related work, especially other management solutions and pointed out the difference to them. Chapter 3 introduced the basic management concept and showed several management applications that may run on the proposed basic management system.

Finally, Chapter 4 described the quantitative and qualitative evaluation. The evaluation showed that the proposed system is able to handle larger number of base stations in wireless access networks with different topologies. The implementation fulfilled the promises that have been made in the Chapter 1. The base stations organised themselves (self-organisation), react to changes in their environment (self-adaptive), protect themselves against malicious users (self-protection) and react on failures of their neighbours (self-healing).

The key features of the proposed concept are the decentralisation of management and the integration of external information into the management process. The evaluation showed

the scalability problems that may arise in a decentralised concept are acceptable and that the integration of external information can help to improve the management results.

However, the question that may arise is what is future? First, the prototype implementation needs more management applications. Next to the applications introduced in this thesis, other applications are thinkable. Second, the concept needs to be merged with the IP configuration work that has already been done the NEC netlabs [76]. Third, the quantitative evaluation of the prototype implementation has to be done with larger environments, *i.e.*, with greater numbers of base stations. Fourth, the concept of self-deploying could be integrated into the work done for this thesis [56]. Fifth, it is thinkable to merge the measurement work done at the NEC netlabs into the proposed management concept [37].

Kai Zimmermann, Heidelberg, 03/31/2005

Bibliography

[1] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.

[2] Announcing the Avanced Encryption Standard (AES), November 2001. Federal Information Processing Standards Publication 197.

[3] Alfarez Abdul-Rahman and Stephen Hailes. A distributed Trust Model. In *Proceedings of the ACM Workshop on New Security Paradigms*, pages 48–60, Langdale, United Kingdom, September 1997.

[4] Karl Aberer and Zoran Despotovic. Managing Trust in a Peer-2-Peer Information System. In *Proceedings of the Tenth International Conference on Information and Knowledge Management (CIKM'01)*, pages 310–317, New York, USA, November 2001.

[5] Henrik Abramowicz, Norbert Niebert, Werner Mohr, Ludwig Hiebinger, Joern von Haefen, Andy Aftelak, Didier Bourse, Karim El-Khazen, Mika Klemettinen, Jukka T. Salo, Rancois Carrez, Fabien Bataille, Pertti Hoelttae, Christian Pehofer, Nigel Jefferies, Jose Enriquez Gabeiras, and Brigitte Cardinael. The Wireless World Initiative: A Framework for Research on Systems beyond 3G. In *13th IST Mobile and Wireless Communications Summit*, Lyon, France, June 2004.

[6] N. Abramson. Development of the ALOHANET. *IEEE Transactions on Information Theory*, 31:119–123, March 1985.

[7] C. Adams and S. Farrell. Internet X.509 public key infrastructure certificate management protocols. Request for Comments 2510, Internet Engineering Task Force, March 1999.

[8] Advanced Cybernetics Group and Meshdynamics. Challenges for 802.15 WPAN Mesh. White Paper, 2004.

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

[10] Agilent Technologies. Wireless LAN Analyzer - Technical Overview. White Paper, November 2003.

[11] Divyakant Agrawal and A. E. Abbadi. An efficient and fault-tolerant solution for distributed mutual exclusion. *ACM Transactions on Computer Systems*, 9(1):1–20, 1991.

[12] AirDefense. Wireless LAN Security - What Hackers Know That You Don't. White Paper, 2003.

[13] Airespace. Airespace Framework for Wireless Security. White Paper, October 2003.

[14] Airespace. AireWave Director Software. White Paper, 2003.

[15] Airespace. Integrating Firewalls into Enterprise Wireless LANs. White Paper, October 2003.

[16] Airespace. Location is Everything - The Benefits of Location Tracking in WLAN Environments. White Paper, November 2003.

[17] Airespace. Minimizing the Costs of Owning and Operating a Wireless LAN. White Paper, 2003.

[18] Airespace. Putting the Air Space to Work. White Paper, October 2003.

[19] Airespace. WLAN Security: Top 10 Cecklist. White Paper, December 2003.

[20] Airespace. Wireless Intrusion Detection and Prevention. White Paper, 2004.

[21] Airespace. Wireless Prevention and Protection. White Paper, January 2004.

[22] Airwave Wireless. The Dangerous Myth: Homogenous Wireless LANs. White Paper, August 2004.

[23] Aruba Wireless Networks. Getting a Grip on Wireless LANs. White Paper, 2003.

[24] Aruba Wireless Networks. The Wireless Grid. White Paper, 2004.

[25] Aruba Wireless Networks. The World of Wireless LAN Switching. White Paper, 2004.

[26] Matt Blaze, Joan Feigenbaum, and Jack Lacy. Decentralized Trust Management. In *Proceedings of the IEEE Symposium on Security and Privacy*, number 96-17, Berkeley, California, USA, May 1996.

[27] P. Calhoun, B. O'Hara, S. Kelly, R. Suri, M. Williams, and S. Hares. Light weight access point protocol (lwapp). Internet-draft, Internet Engineering Task Force, February 2005. work in progress.

[28] V. G. Cerf. Packet satellite technology reference sources. Request for Comments 829, Internet Engineering Task Force, November 1982.

[29] Indraneel Chakraborty. QOS Assurance with Colocated Wireless Access Points. Master's thesis, Massachusets Institute of Technology, May 2003.

[30] S. Corson and J. Macker. Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations. Request for Comments 2501, Internet Engineering Task Force, January 1999.

[31] E. Damiani, S. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante. A reputation based approach for choosing reliable resources in Peer-to-Peer networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security*, pages 207–216, Washington, DC, USA, November 2002.

[32] Alan Demers, Dan Greene, Carl Hauser, Wes Irish, John Larson, Scott Shenkcr, Howard Sturgis, Dan Swinehart, and Doug Terry. Epidemic algorithms for replicated database maintenance. In *Proceedings of the 6th annual ACM Symposium on Principles of distributed computing*, pages 1–12, Vancouver, British Columbia, Canada, August 1987.

[33] T. Dierks and C. Allen. The TLS protocol version 1.0. Request for Comments 2246, Internet Engineering Task Force, January 1999.

[34] R. Droms. Dynamic host configuration protocol. Request for Comments 1531, Internet Engineering Task Force, October 1993.

[35] P. Th. Eugster, R. Guerraoui, A.-M. Kermarrec, , and L. Massoulie. From Epidemics to Distributed Computing. *IEEE Computer*, pages 60–67, May 2004.

[36] Farpoint Group. Rethinking the Access Point: Dense Deployments for Wireless LANs. White Paper, 2004.

[37] Sebastian Felis, JÃ$\frac{1}{4}$rgen Quittek, and Lars Eggert. Measurement-Based Wireless LAN Troubleshooting. In *1st workshop on Wireless Network Measurements (co-located with WiOpt'05)*, April 2005.

[38] Matthew S. Gast. *802.11 Wireless Networks*. O'Reilly & Associates Inc., California, USA, 2002.

[39] Robert Grimm. Coordinating Distributed State in the Internet. Technical report, October 1999.

[40] Seongil Hahm, Yongjae Jung, Seunghee Yi, Yukyoung Song, Ilyoung Chong, and Kyungshik Lim. A Self-organized Authentication Architecture in Mobile Ad-Hoc Networks. In *Proceedings of the Information Networking, Convergence in Broadband and Mobile Networking, International Conference (ICOIN'05)*, pages 689–696, Jeju Island, Korea, January 2005.

[41] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan. Adaptive Protocols for Information Dissemination in Wireless Sensor Networks. In *Proceedings of*

the 5th annual ACM/IEEE international conference on Mobile computing and networking (MOBICOM'99), pages 174–185, Seattle, Washington, USA, August 1999.

[42] Infonetics Research. The Evolution of the Enterprise-Class Wireless LAN Access Point. White Paper, January 2004.

[43] Márk Jelasity and Alberto Montresor. Epidemic-Style Proactive Aggregation in Large Overlay Networks. In *Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS'04)*, pages 102–109, Tokyo, Japan, March 2004. IEEE Computer Society.

[44] Mark Jelasity, Alberto Montresor, and Ozalp Babaoglu. Towards Secure Epidemics: Detection and Removal of Malicious Peers in Epidemic-Style Protocols. Technical report, Department of Computer Science, University of Bologna, Italy, November 2003.

[45] L. Ji, J. Agre, T. Iwao, and N. Fujino. On Providing Secure and Portable Wireless Data Networking Services: Architecture and Data Forwarding Mechanisms. In *Proceedings of the International Conference on Mobile Computing and Ubiquitous Networking (ICMU'04)*, Yokosuka, Japan, January 2004.

[46] J. Jubin and J.D. Tornow. The darpa packet radio network protocols. *Proceedings of the IEEE*, 75:21–32, 1987.

[47] Heikki Kaaranen, Siamaek Naghian, Lauri Laitinen, Ari Ahtiainen, and Valtteri Niemi. *UMTS Networks: Architecture, Mobility and Services.* John Wiley and Sons Ltd., Chichester, England, 2001.

[48] Lalana Kagal, Scott Cost, Timothy Finin, and Yun Peng. A Framework for Distributed Trust Management. In *Proceedings of the Second Workshop on Norms and Institutions in MAS, Autonomous Agents*, Montreal, Canada, May 2001.

[49] Roger Kalden, Ingo Meirick, and Michael Meyer. Wireless Internet Access Based on GPRS. *IEEE Personal Communications Magazine*, pages 8–18, April 2000.

[50] Richard M. Karp, Christian Schindelhauer, Scott Shenker, and Berthold VÃ¶cking. Randomized Rumor Spreading. In *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pages 565–574, Redondo Beach, California, USA, November 2000.

[51] Jeffrey O. Kephart and David M. Chess. The Vision of Autonomic Computing. *IEEE Computer*, 36(1):41–50, 2003.

[52] David Kotz and Kobby Essien. Analysis of a campus-wide wireless network. In *Proceedings of the 8th annual international conference on Mobile computing and networking (MOBICOM'02)*, pages 107–118, Atlanta, Georgia, USA, September 2002.

[53] Bhaskar Krishnamachari, Stephen B. Wicker, Ramón Béjar, and Cèsar Fernàndez. On the Complexity of Distributed Self-Configuration in Wireless Networks. *Telecommunication Systems*, 22(1-4):33–59, 2003.

[54] P. V. Mockapetris. Domain names - implementation and specification. Request for Comments 1035, Internet Engineering Task Force, November 1987.

[55] Michel Mouly and Marie-Bernadette Pautet. *The GSM System for Mobile Communications*. Telecom Publishing, Palaiseau, France, 1992.

[56] Francis J. Mullany, Lester T.W. Ho, Louis G. Samuel, and Holger Claussen. Self-Deployment, Self-Configuration: Critical Future Paradigms for Wireless Access Networks. In *Proceedings of the 1st IFIP WG6.6 International Workshop on Autonomic Communication*, Berlin, Germany, October 2004.

[57] Roger M. Needham and Michael D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. *Communications of the ACM (CACM)*, 21(12):993–999, 1978.

[58] Norbert Niebert, Hannu Flinck, Robert Hanock, Holger Karl, and Christian Prehofer. Ambient Networks, Research for Communication Networks Beyond 3G. In *IEEE 61st Semiannual Vehicular Technology Conference (VTC'05 Spring)*, Stockholm, Sweden, May 2005. to appear.

[59] Norbert Niebert, Mikael Prytz, Andreas Schieder, Lars Eggert, Frank Pittmann, Nick Papadoglou, and Christian Prehofer. Ambient Networks: a Framework for Future Wireless Internetworking. In *IEEE 61st Semiannual Vehicular Technology Conference (VTC'05)*, Stockholm, Sweden, May 2005. to appear.

[60] Linda Dailey Paulson. Will Ultrawideband Technology Connect in the Marketplace?. *IEEE Computer*, 36(12):15–17, 2003.

[61] J. Postel. User datagram protocol. Request for Comments 768, Internet Engineering Task Force, August 1980.

[62] J. Postel. Internet protocol. Request for Comments 791, Internet Engineering Task Force, September 1981.

[63] J. Postel. Transmission control protocol. Request for Comments 793, Internet Engineering Task Force, September 1981.

[64] Niels Provos. A Virtual Honeypot Framework. In *Proceedings of the 13th USENIX Security Symosium*, pages 1–14, San Diego, California, USA, August 2004.

[65] Michael Rabinovich, Narain H. Gehani, and Alex Kononov. Scalable Update Propagation in Epidemic Replicated Databases. In *Proceedings of the 5th International Conference on Extending Database Technology: Advances in Database Technology*, pages 207–222, March 1996.

[66] B. Ramsdell and Ed. S/MIME version 3 message specification. Request for Comments 2633, Internet Engineering Task Force, June 1999.

[67] Kerry Raymond. A tree-based algorithm for distributed mutual exclusion. *ACM Transactions on Computer Systems*, 7(1):61–77, 1989.

[68] R. Rivest. The MD5 message-digest algorithm. Request for Comments 1321, Internet Engineering Task Force, April 1992.

[69] Martin Roesch. Snort - Lightweight Intrusion Detection for Networks. In *Proceedings of the 13th Systems Administration Conference (LISA'99)*, pages 229–238, Seattle, Washington, USA, November 1999.

[70] Palash Sarkar. A brief history of cellular automata. *ACM Computing Surveys (CSUR)*, 32(1):80–107, March 2000.

[71] Eunsoo Shim, Hung yu Wei, Yusun Chang, and Richard D. Gitlin. Low Latencey Handoff for Wireless IP QOS with NeighborCasting. In *Proceedings of the IEEE International Conference on Communications (ICC'02)*, pages 3245–3249, New York, USA, April 2002.

[72] Spire Security. Selecting a WLAN Monitoring Solution. White Paper, December 2003.

[73] Summit Strategies, Inc. Rapid Payback: Managing Wireless LANs for Maximum ROI. White Paper, October 2003.

[74] Diane Tang and Mary Baker. Analysis of a Metropolitan-Area Wireless Network. *Wireless Networks*, 8(2-3):107–120, March 2002.

[75] Andrew S. Tannenbaum and Maarten van Steen. *Distrubuted Systems, Principles and Paradigms*. Prentice Hall Inc., New Jersey, USA, 2002.

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

[77] Chai-Keong Toh. *Ad Hoc Mobile Wireless Networks, Protocols and Systems*. Prentice Hall Inc., New Jersey, USA, 2002.

[78] Joe Touch. Dynamic Internet Overlay Deployment and Management Using the X-Bone. *Computer Networks*, pages 117–135, July 2001.

[79] Trapeze Networks. Detecting Rogue Users and APs in a Wireless LAN. White Paper, 2003.

[80] Trapeze Networks. AP Architecture Impact on the WLAN, Part 1: Security and Manageability. White Paper, 2004.

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

[82] Steven J. Vaughan-Nichols. Achieving Wireless Broadband with WiMax. *IEEE Computer*, 37(6):10–13, 2004.

[83] Wavelink. Rogue Acess Point Detection. White Paper, 2005.

[84] R. Yahalom, B. Klein, and T. Beth. Trust Relationships in Secure Systems - A Distributed Authentication Perspective. In *IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, California, USA, May 1993.

[85] W. R. Young. Advanced Mobile Phone Service: Introduction, Background, and Objectives. *Bell Systems Technical Journal*, pages 1–14, January 1979.

[86] Hongwei Zhang and Anish Arora. GS^3: scalable self-configuration and self-healing in wireless networks. In *Proceedings of the 21st annual symposium on Principles of distributed computing*, pages 58–67, Monterey, California, USA, July 2002.

[87] Yongguang Zhang and Wenke Lee. Intrusion detection in wireless ad-hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking (MOBICOM'00)*, pages 275–283, Boston, Massachusetts, USA, August 2000.