Autonomic Wireless Network Management

Kai Zimmermann, Sebastian Felis, Stefan Schmid,
Lars Eggert and Marcus Brunner*

NEC Europe Ltd., Network Laboratories
Kurfürstenanlage 36, 69115 Heidelberg, Germany
{zimmermann|felis|schmid|eggert|brunner}@netlab.nec.de
http://www.netlab.nec.de/

Abstract. This paper presents a decentralized approach for the autonomic management of a group of collaborating base stations to provide efficient and effective wireless network access in highly dynamic environments. It provides a management platform that supports many different management functions based on common mechanisms for information exchange, transactional semantics and security. A central feature of the system is the inclusion of monitored feedback information into the autonomic management process, which can enhance the operation of the management system and the quality of its decisions. An integrated monitoring component provides this feedback information by monitoring the coverage area and analyzing the measurements in real time. A preliminary evaluation of the prototype implementation shows that the autonomic management system scales well. Performance is mostly proportional to the diameter of the network topology and does not heavily depend on the number of base stations present. Further experiments with the wireless monitoring sub-system demonstrate that it is feasible to automatically detected network problems caused by radio interference or active attacks.

1 Introduction

Installations and configurations of large wireless networks that consist of multiple, distributed base stations are challenging, time-consuming and error-prone tasks, even for experts. Once deployed, such wireless networks require continuous management to provide a uniform service environment, recover from faults or maximize overall performance. This is particularly difficult, because wireless environments are typically very dynamic. First, the number, location and traffic patterns of mobile systems in a wireless network change constantly. Second, wireless networks often use unlicensed, shared frequency spectrum, such as IEEE 802.11b/g base stations that operate in the unlicensed 2.4 GHz band. Multiple radio applications share this unlicensed spectrum in an uncoordinated fashion, which causes additional interference on top of outside interference caused by other electronic equipment.

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

To enable effective and efficient networking under these demanding characteristics, continuous network management that proactively and reactively adapts to environmental dynamics is a necessity. Manual network management techniques across a set of diverse, distributed base stations are consequently not an option, requiring fully automated management functionality.

Few wireless network technologies include adequate management mechanisms. Even when such functions exist, they are typically limited to managing physical or link-specific characteristics only and do not cover management of higher-layer internetworking functions. For example, although existing IEEE 802.11a/b/g WLAN base stations can automatically select an available radio channel, transmission power and link speed, they cannot autonomously configure higher-layer settings such as routed IP connectivity. They cannot even intelligently configure link-specific characteristics that require coordination between neighboring base stations beyond what they can immediately observe themselves.

This paper describes an autonomic approach to the management of wireless base stations. The advantage of an autonomic solution is that new base stations that join an existing wireless network integrate themselves seamlessly. The rest of the system adapts to their presence dynamically. This enables a wireless network to automatically configure itself in accordance to high-level policies that specify what is desired, not how it is accomplished. These policies represent the purpose of the network, its overall goals or business-level objectives.

A key principle of autonomic self-configuration is decentralization. Each component is able to operate in a stand-alone fashion. When several components detect each others presence, they then start to coordinate their management actions to increase the efficiency and effectiveness of their shared access network.

Existing approaches to management of wireless networks consisting of multiple base stations are typically centralized. A central master system periodically uses available information to compute a global configuration for the whole network. It pushes this configuration out to the individual base stations in a piecemeal fashion or they pull their respective configurations from the master. However, such a centralized approach has several disadvantages. First, it creates a central point of failure. Failure of the master can make the whole system unusable. Second, a central master limits scalability due to processing and communication overheads, especially in environments that require frequent configuration changes. Third, it complicates the system, because this approach introduces additional infrastructure, *i.e.*, the central master.

This paper presents a decentralized approach for autonomic management of a group of collaborating base stations. The individual base stations aggregate and share network information. They implement a distributed algorithm that uses the shared information to compute a local configuration at each base station such that the overall network-wide configuration is consistent. An important feature of the proposed system is the wireless monitoring component, which provides the necessary feedback for the autonomic logic to take appropriate management decisions.

Section 2 of this paper presents related work. Section 3 defines the underlying autonomic principles that guide the design of the wireless management system. Section 4 describes the basic functionality and operation of the proposed autonomic management system. Section 5 presents the evaluation results of the prototype systems and Section 6 summarizes and concludes this paper.

2 Related Work

Management of wireless networks is possible through centralized, distributed or hybrid solutions. Whereas centralized systems use a single master device to configure the base stations, decentralized, distributed solutions avoid such a single point of failure and collaboratively implement a fully distributed management solution. With any of the three approaches, the challenge is that all wireless base stations must arrive at a consistent, system-wide configuration. This section describes existing approaches for all three paradigms and briefly discusses more recent developments that also follow an autonomic approach.

Several companies provide centralized management solutions for groups of base stations [1][2]. The majority of these systems implement link-layer "wireless switches" that connect base stations that act as wireless bridges to a switched wired network. The link-layer switch implements the management component. This centralized, link-layer approach offers traffic and channel management, policy, bandwidth and access control. However, such centralized link-layer solutions also have drawbacks. Link-layer broadcast domains cannot arbitrarily grow due to the scalability issues associated with broadcast traffic. Additionally, the topology of the wired network may not allow direct connection of the management system to the base stations. Centralized network-layer solutions address this shortcoming.

Decentralized management solutions are popular to configure mobile *ad hoc* networks (MANET) [3]. These management systems typically focus on the challenging task of enabling peer-to-peer communication in highly dynamic, mobile environments [4]. Because of their nature – *i.e.*, every base station decides based on its local scope [5] and no central management station exists – they are closely related to the autonomic approach presented in this paper. Ongoing research efforts [6][7] attempt to design self-configuring solutions for MANETs. However, in contrast to those approaches, the autonomic solution presented in this paper focuses on configuring a stationary wireless access network for mobile clients, with the primary goal of improving efficiency and performance.

With respect to decentralized management of infrastructure-based wireless networks, further work [8][9] focuses on the auto-configuration of base stations, with the goal to achieve the best coverage in a given geographical area. Early results suggest using transition rules that are similar to cellular automata to change the local configuration of a base station when receiving the current states of its neighbors. Although these proposed algorithms can support some of the specific applications that the autonomic approach also implements, such as regulating transmission power, they are not a platform for arbitrary management functions. In contrast, the focus of the autonomic management approach is to develop a management platform that can support many types of management functions.

Hybrid approaches to wireless network management, such as the Integrated Access Point of Trapeze Networks [10], push some functionality from a central system into the base stations, which are therefore slightly more complex than the simple wireless bridges of centralized approaches. Although hybrid systems improve scalability, they do not completely address the drawbacks of centralized systems; *e.g.*, they still have central points of failure.

3 Underlying Autonomic Principles

The high-level principles that guide the design and implementation of the proposed autonomic wireless network management systems are *automatic*, *aware* and *adaptive* operation [11].

Automatic operation: an autonomic system must be able to bootstrap itself when it starts and configure its basic functions according to the status and context of its environment, without involving a user or system administrator. This process consequently requires an autonomic system to anticipate the resources needed to perform its tasks and to acquire and use these resources without involvement of a human. For example, a new base station must integrate and configure itself into an existing wireless network without the involvement of a human administrator. Therefore, the base station must automatically configure its frequency, signal strength, network addresses and routing.

Aware operation: To allow an autonomic system to configure and reconfigure itself under dynamic conditions, it is important for the system to be *self-aware*. The system needs detailed knowledge of its components, resources and capabilities, its current context and status, as well as its relation to other systems that are part of its environment, in order to make the correct management decisions. As a result, a key requirement of an autonomic system is a monitoring mechanism that provides the necessary feedback to its control logic. Continuous monitoring is necessary to identify if the system meets its objectives. The feedback information will be logged and forms the basis for adaptation, self-optimization and re-configuration. In addition, monitoring is also important to identify anomalies or erroneous operation in the system, as it provides the basis for safety and security. Finally, for economic reasons, autonomic systems also need to monitor their suppliers and their consumers to ensure that they are providing/obtaining the agreed level of service.

Adaptive operation: The awareness of an autonomic system allows it to adapt according to the continuously changing context of its environment and to the current requirements of its users. Because of this, autonomic system management never finishes; the autonomic system continuously adapts by monitoring its components and fine-tuning its operation.

4 Autonomic Management System

This section describes an autonomic management system for wireless networks that builds on the autonomic principles defined in the previous section. It defines the basic system elements, specifies the target management functions, describes the wireless monitoring system and finally introduces the developed self-configuration and self-management approach. A more detailed description of the management system is available in [12].

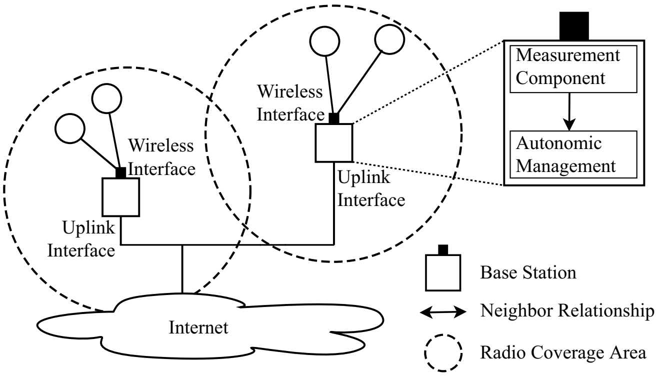

Figure 1: System Overview

4.1 Basic Components and Assumptions

The autonomic management system is completely decentralized across all the base stations of the wireless network. A base station in the decentralized management system has to fulfill several requirements. Each base station is a full-fledged IP 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 clients and a second interface (wired or wireless) for uplink connectivity. Additional interfaces, when present, can act as probe/measurement interfaces, provide multi-homed uplink connectivity or offer additional client connectivity on different channels or link protocols. Figure 1 illustrates the basic architecture of the system.

Base stations automatically distribute the available address space among themselves, configure subnets for client connectivity on their wireless interfaces and configure the addressing of their wired uplinks. IP auto-configuration occurs through an integrated mechanism that was developed as part of an earlier research effort [13].

4.2 Management Functions

The primary task of the wireless management system is to coordinate radio properties, such as frequency use and transmission power, among a group of neighboring base stations and to implement system-wide functions, such as load balancing. By exchanging utilization information, neighboring base stations can distribute client load by increasing or decreasing transmission power or link speeds. A fully loaded base station, for example, can push clients at the edge of its coverage area off to other base stations by lowering its transmission power. An integrated wireless measurement sub-system (see Section 3.3) uses monitored feedback to enable the management system to adapt to changes in its environment.

A second task of the management system is self-protection of the wireless network. Self-protection also relies on the integrated wireless measurement component. It performs the necessary traffic analyses to detect potential security threats and informs the management system, which in turn can take the appropriate actions. The current system is able to detect and counter act against attacks resulting from rogue base stations and MAC address spoofing. The management system blacklists those malicious nodes and disseminates their presence throughout the system, warning the overall wireless network.

A third system function provides a means to obtain a global view of the system, *i.e.*, retrieve local information from all participating base stations of the system, for logging, administrative and monitoring purposes. The decentralized management system can support this functionality without the need of an explicit logging function. Instead, a *virtual neighbor* can disseminate its ID throughout the system and insert it into each base station's neighbor list. The virtual neighbor will then receive the local information disseminated by each base station as if it was simultaneously in radio range of every individual base station. The virtual neighbor can aggregate and export this system-wide information for a variety of uses.

It is important to note that the current system is a *platform* for autonomic management that can support many other management functions. The platform offers common functionality, such as information exchange, transactional semantics or security functions that can provide many different management capabilities.

4.3 Wireless Monitoring for Self-Awareness

A basic capability of a wireless measurement system is capturing and analyzing network traffic, *e.g.*, to identify interference or security attacks, and providing the results to the management system. This feedback forms the basis for the autonomic behavior – self-configuration and self-management – of the system.

Monitoring of a deployed wireless network can pinpoint several causes of problems. For example, inter-channel and cross-channel radio interference can significantly decrease the effective data rate of the network. Traffic measurements can also help to secure and protect wireless networks. For example, analysis of the measurements can detect intrusion attempts and verify that friendly networks are sufficiently protected, *i.e.*, access is authenticated and/or data is encrypted.

One particular 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 visible to the other. Such base stations should become neighbors and coordinate their configurations, but fail to detect each other's presence. Consequently, their configurations will not be coordinated, leading to an inconsistent overall network configuration.

The gathering and analysis of feedback information can address the overlap problem. For example, if clients periodically notify their base station of other clients and base stations within their radio range, the management system can update the neighbor relation when a client enters an overlap area, eliminating or at least significantly reducing the overlap problem. Figure 2 illustrates this feedback process. Moreover, the direct feedback from the monitoring system enables detection of interference or spotty coverage, can identify rogue base stations or aid location tracking.

The autonomic management system presented in this paper uses monitors that provide the results of their continuous measurement efforts as feedback to the autonomic control process (as illustrated in Figure 1). Because dedicated measurements nodes are typically limited to a one or a few wireless interfaces, monitoring the complete spectrum (*i.e.*, on all channels) is difficult. To maximize monitoring effectiveness, the proposed system periodically switches a single interface to scan several frequency bands. When it identifies potential problems, the system focuses its monitoring efforts on the detected occurrence to track the problem at hand.

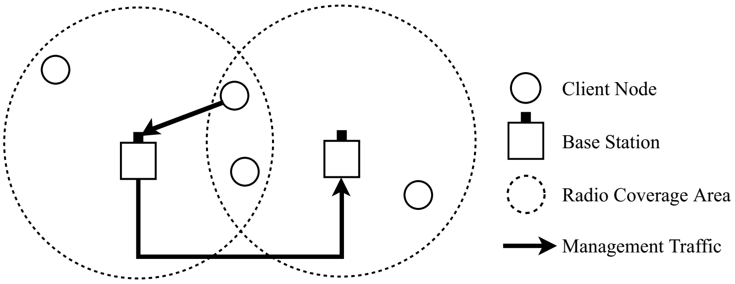

Figure 2: Integration of monitors into the management system.

Apart from the interception of wireless traffic, the measurement system collects additional information from every node that is detected, including the node’s wireless mode (infrastructure or *ad hoc*), frame and byte counts, associated base station information such as the Service Set Identifier (SSID), physical-layer information such as signal strength and statistical information about higher-layer protocol use. In addition to many other measurement systems, this system also collects sequence number information for each captured frame. Analysis of patterns in the sequence numbers of captured frames is an effective technique to determine the presence of various anomalies and attacks [14][15].

For intrusion detection, the measurement system maintains also a database of known MAC addresses that it correlates with the IEEE’s “organizationally unique identifier” list [16]. This can help to identify spoofed MAC addresses. If the rate of occurrence of new MAC addresses is past a configurable threshold, the autonomic management system is informed to take appropriate action.

4.4 Self-Configuration and Self-Management

Although each base station is able to operate in a stand-alone fashion, autonomic management of a group of base stations that provide connectivity to a geographic region requires collaboration. This collaboration occurs through periodic information exchange across the uplink interfaces, which allows each individual base station to adapt its local configuration consistently with its peers.

When a base station starts up, it first performs a probing phase – after a brief randomized de-synchronization delay – before configuring itself to provide service to wireless clients. During the first part of this probing phase, it auto-configures its network components for communication, routing and addressing, *i.e.*, it obtains a subnet delegation for its wireless network and configures its uplink interface, routing table and DHCP server for the wireless network appropriately [13].

After the base station has successfully bootstrapped its communication infrastructure, it performs a channel scan to detect other base stations in its immediate neighborhood and determines their identifiers. In other words, the base station identifies its current context as well as its relation to other systems of the embedded environment. Finally, it contacts these neighbor stations over its uplink interface and, after successful authentication and authorization [12], integrates itself into the network-wide information exchange.

Once configured, the base station starts to participate in global and local information exchanges with its peers, which provides the basis for the collaborating base stations to manage the overall wireless networks by themselves.

The system uses different kinds of exchange mechanisms for different kinds of information. Information that is globally important, such as encryption parameters or attack status, is disseminated throughout the network using an epidemic communication mechanism [17]. Information that is of local significance only, such as radio frequencies, transmit power or link utilization, is only disseminated locally among the affected neighboring base stations. This differentiation by information type is crucial for large autonomic systems in order to improve the scalability properties of the system.

The information that each station maintains falls into three different categories. *Private* information, such as logs, is never disseminated. A base station disseminates *local* information, such as its current channel, transmit power or utilization, to its neighbors, *i.e.*, other base stations within wireless range. This allows a group of neighbors to adapt their configurations in response to local events. A base station periodically disseminates updates about its local state to its neighbors every few seconds and likewise receives their updates.

A third kind of information requires *global* dissemination to all cooperating base stations. System-wide parameters, such as wireless protocol, security parameters or attack status are examples of such global information. The system disseminates global information using epidemic communication. Instead of broadcasting such updates to global state, they are piggy-backed onto the periodic information exchanges between neighbors. This technique prevents broadcast storms when global state updates are frequent.

Disseminating a global configuration change throughout the network in a consistent manner requires transactional semantics. This is a well-known challenge in distributed networks and a wide variety of approaches exist [18]. The current system implements a very simple method of guaranteeing global consistency – election of a central locking service. Future revisions will replace this method with a more scalable variant.

5 Evaluation

This section presents a preliminary evaluation of a prototype implementation of the autonomic management system. Due to space limitations, the evaluation focuses on the most important aspects of the autonomic systems, namely the scalability properties of the epidemic management state exchange and the feasibility of wireless network monitoring.

Scalability is a crucial aspect of autonomic management approaches for wireless networks. Because wireless access networks are expected to grow to very large numbers of base stations in the near future, autonomic management becomes particularly challenging and, at the same time, vital to the operation of the system. With respect to network monitoring, the issue of automatic problem detection – without human support – is a major challenge. The remainder of this section focuses on the evaluation of those aspects.

5.1 Autonomic Management Scalability

This section presents preliminary evaluation results of the scalability characteristics of an autonomic management system. The current prototype is a *Perl* daemon that operates on Linux systems with one or more IEEE 802.11a/b/g WLAN interfaces. The management daemon automatically configures and manages a collection of such machines.

For this scalability evaluation, the use of physical devices is impractical. 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 use this simulation mode to investigate groups of up to 100 base stations.

Also, note that in this simulation mode, the base stations themselves probe and monitor of the wireless network instead of dedicated wireless measurement nodes or interfaces. During the probing, every base station periodically scans, detects and contacts its neighbors to initiate an epidemic information exchange. This operation takes approximately 2 seconds and is repeated every 1800 seconds.

5.1.1 Initial Configuration Convergence

This section evaluates the convergence time of the autonomic measurement system for groups of base stations that 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. The experiments measure 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. 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 behavior for small groups.

Figure 3 shows the performance. For smaller groups of 1-20 base stations, the mean initial self-organization time quickly increases from 17 to approximately 20 seconds. For larger groups of 20-100 base stations, the mean initial self-organization time remains between 20 and 25 seconds. As a result, the network convergence time does not grow significantly in relation to the number of base stations present. Although the simulations only demonstrate this effect for small groups of up to 100 base stations, this trend is expected to continue for larger groups. Future simulations will verify this hypothesis.

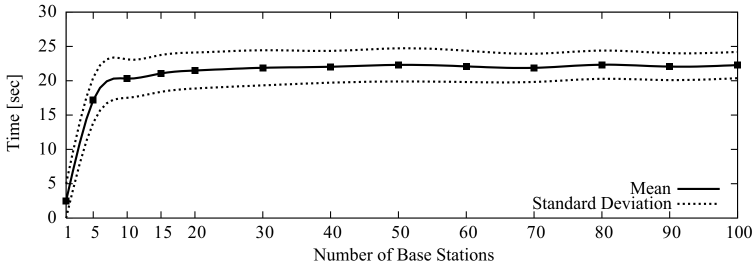

Figure 3: Initial convergence times of groups of base stations.

The results shown here highlight the strength of the decentralized approach in term of scalability with a growing number of attending base stations. However, for larger wireless access networks the distribution time for new *global* configuration settings will grow. The following section will analyze this scenario.

5.1.2 Epidemic Message Spread Time

This section investigates the dissemination times of changes to *global* state for a set of base stations that have already converged. A new *global* configuration setting is inserted at a single, random base station and disseminates throughout the entire network through the epidemic information exchange. 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 behavior for small groups.

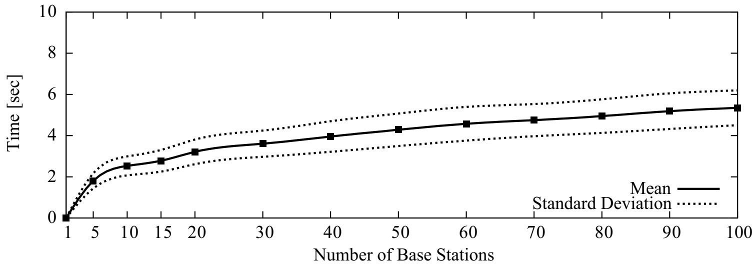

Figure 4: Dissemination times of changes to global state.

Figure 4 shows a growing dissemination time up to 5 seconds. The number appears large, but is a result of the information forward delay of each base station. Each base station informs its neighbors about changes in periodic intervals. The current prototype uses a default of 1 second. That means that a base station forwards a change to its *global* configuration set after at most 1 second.

Additional experiments (omitted here for space reasons) show that the dissemination times of changes to *global* state do not grow significantly with the number of base stations, but instead grow proportional to the topology diameter. This indicates that topology structure has more impact on performance than the number of base stations present.

5.1.3 Management Traffic

The epidemic management approach requires that every node forwards local state changes to its immediate neighbors in order to disseminate the information globally. Figure 5 shows the number of management information exchanges during the initial configuration for different topology sizes. The results indicate that the amount of management traffic grows linearly with the topology size.

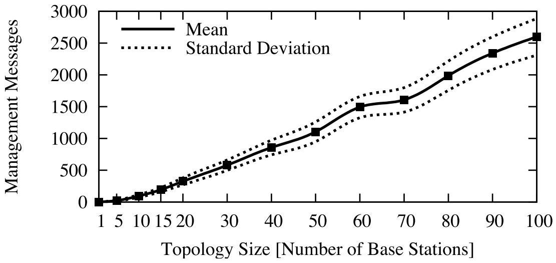

Figure 5: Management traffic to perform initial self-organization.

5.2 Wireless Measurement Nodes

This section evaluates the basic operation of the wireless measurement sub-system described in Section 3. Based on two real-world traffic traces collected inside the NEC Network Laboratories, this evaluation validates the feasibility of using wireless measurements for the autonomic management of wireless networks. Once the measurement nodes detect a problem, *e.g.*, interference or address spoofing, it informs the autonomic management system to take the appropriate actions according to the high-level policies of the network.

5.2.1 Intrusion Detection Using Frame Sequence Numbers

A common technique to attack a wireless network is through MAC address spoofing. If MAC addresses are used to control access to a network, a malicious client could simply probe the MAC address of a trusted client, and then uses this in order to send/receive traffic. The technique evaluated here allows detection of clients that attempt to spoof MAC addresses through analysis of the traffic measurements.

In the 802.11 protocols, a unique sequence number identifies each individual frame sent by a single node to allow detection of duplicates. Sequence numbers are 12-bit counters that monotonically increase from 0 to 4095 and wrap around at overflow. When a network interface starts or is reset, the sequence number counter starts at zero. The minimum time for sequence numbers to wrap around is under one second, but it can be indefinitely longer depending on packet size, send rate and link speed. According to the 802.11 standard, the sequence number counter should be readable but not writable by software. Because of their predictable and hard to spoof order, frame sequence numbers can act as fingerprints that uniquely identify frames sent by a single node over a period of time. Even when a station spoofs its MAC address, the sequence numbers of frames sent with a spoofed MAC address will still continue that stations sequence number pattern. This makes frame sequence numbers much stronger identifiers for specific stations than MAC addresses and thus allows detection MAC address spoofing.

Figure 6 shows a sequence number plot with traffic from two nodes with MAC addresses *A* and *B*. The sequence number curve for MAC address *A*'s at the top of the graph, the plot for MAC address *B* is mainly at the bottom. This trace illustrates how an otherwise well-behaving node with MAC address *A* periodically spoofs traffic to make it appear as if it came from node *B*.

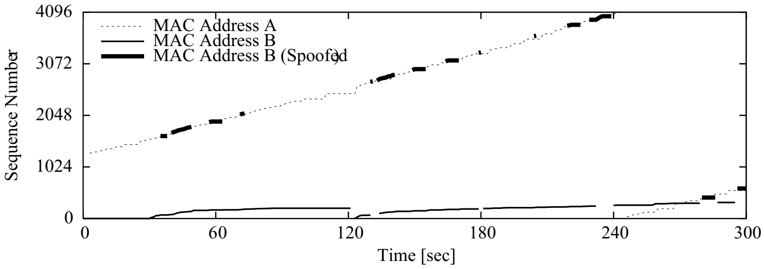

Figure 6: Plot of sequence numbers over time for two nodes with MAC addresses *A* and *B*.

Note that although the two sequence number progressions are clearly distinct, a number of packets are visible that appear to originate at MAC address *B* but have sequence numbers that fit with node *A*'s sequence number pattern. (Figure 6 illustrates these as thicker line segments overlaying node *A*'s curve). Without an analysis of frame sequence numbers, these spoofed packets are difficult to detect; even more difficult is to determine which station originates the spoofed packets.

5.2.2 Detection of Connectivity Problems

Sequence number analysis can also detect connectivity problems in wireless networks. As mentioned above, the measurement system deduces link-layer retransmissions by observing repeated transmissions of *retry* frames with identical sequence numbers. Frequent retransmissions may indicate connectivity issues.

Figure 7 shows the data frame and retransmission rate of the UDP sender (dashed line). It starts transmitting ten seconds into the measurement. The average data rate of the stream is around 75 frames/second until second 24, when the data rate suddenly drops to about half for the next eight seconds before resuming at the original rate. This drop in the data rate goes along with a corresponding increase in the retransmission rate from second 24-32 (solid line).

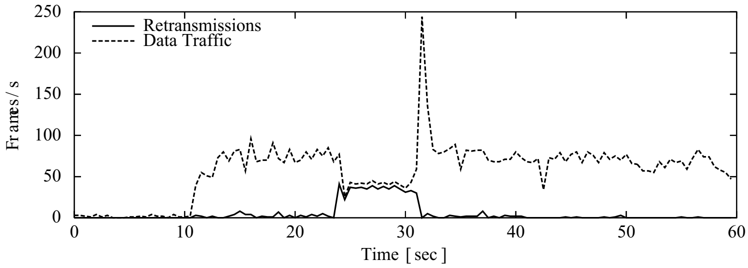

Figure 7: Data frame and retransmission rates of a constant-bitrate UDP sender.

6 Conclusion

This paper presents a decentralized, autonomic configuration and management system for base stations in wireless networks. The proposed system is a generic *platform* for autonomic management that offers generic mechanisms that support many different management functions. This common functionality includes mechanisms for information exchange, transactional semantics or security functions, which are required to realize many different management capabilities.

A novel feature of the autonomic management system is an integrated wireless monitoring component. This component determines common causes of problems through real-time analysis of live network measurements. The monitored feedback provides the system with the necessary awareness of its status and defines context for autonomic control. The feedback also provides a basis for individual base stations to automatically bootstrap and manage themselves.

A preliminary evaluation of the autonomic management systems focuses on the scalability analysis of the epidemic management state exchange and the feasibility of wireless network monitoring for automatic problem detection. The results of the epidemic state exchange show that the time to disseminate global state does not grow significantly with the number of base stations. Instead, it grows proportional to the topology diameter. As a result, the scalability property of the autonomic management system depends primarily on the topology structure and only to a lesser degree on the number of base stations present. For example, the results show that the prototype management system is able disseminate a global state change in a network of 100 base stations in less than 6 seconds, assuming typical connected topologies. The analysis of the measurement component illustrates the effectiveness of the proposed metrics and the measurement system through a series of real-world experiments. The results show that automatic detection of configuration or communication problems is feasible and can aid the autonomic control and management of wireless networks.

A more complete system implementation is currently ongoing. It will investigate the performance of additional system functions such as improved channel allocation, load balancing, rogue detection or location tracking and quantify the quality improvement obtainable by the inclusion of external information. It will also extend the scalability analysis to larger groups of base stations.

Although the current autonomic management system specifically targets WLAN networks, the general idea of decentralized, autonomic management certainly applies to other wireless and wired networks. The proposed system provides a decentralized management middleware built on generic methods for information dissemination that adapt to other network technologies and support many different management functions.

References

1. Airespace Corporation: Putting the Air Space to Work. White Paper (2003)
2. Aruba Wireless Networks: Getting a Grip on Wireless LANs. White Paper (2003)
3. Toh, C-K.: Ad Hoc Mobile Wireless Networks, Protocols and Systems. Prentice Hall Inc., New Jersey, USA (2002)
4. Ji, L., Agre, J., Iwao, T., Fujino, N.: On Providing Secure and Portable Wireless Data Networking Services: Architecture and Data Forwarding Mechanisms. Proc. International Conference on Mobile Computing and Ubiquitous Networking (ICMU'04), Japan (2004)
5. Advanced Cybernetics Group and Meshdynamics: Challenges for 802.15 WPAN Mesh. White Paper (2004)
6. Zhang, H., Arora, A: GS3: scalable self-configuration and self-healing in wireless networks. Proc. 21st Annual Symposium on Principles of Distributed computing, Monterey, California, USA (2002) 58–67
7. Krishnamachari, B., Wicker, S.B., Bejar, R., Fernandez, C.: On the Complexity of Distributed Self-Configuration in Wireless Networks. Telecommunication Systems, Vol. 22 (1-4) (2003) 33-59
8. Mullany, F.J., Ho, L.T.W, Samuel, L.G., Claussen, H.: Self-Deployment, Self-Configuration: Critical Future Paradigms for Wireless Access Networks. Proc. of 1st International Workshop on Autonomic Communications (WAC 2005), Berlin, Germany (2004)
9. Ho, L.T.W, Samuel, L.G., Pitts, J.M.: Applying Emergent Self-Organizing Behaviour for the Coordination of 4G Networks Using Complexity Metrics. Bell Labs Technical Journal, Vol. 8, No. 1 (2003) 5-26
10. Trapeze Networks: Defining An Integrated Access Point. White Paper (2004)
11. Kephart, J., Chess, D.: The Vision of Autonomic Computing. IEEE Computer Magazine (2003)
12. Zimmerman, K.: An Autonomic Approach for Self-Organising Access Points. Diploma Thesis, University of Ulm, Germany (2004)
13. Silva Tobella, J.J., Stiemerling, M., Brunner, M.: Towards Self-Configuration of IPv6 Networks. Proc. Poster Session of IEEE/IFIP Network Operations and Management Symposium (NOMS'04), Seoul, Korea (2004)
14. Wright, J.: Detecting Wireless LAN MAC Address Spoofing. White Paper (2003)
15. Wright, J.: Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection. White Paper (2002)
16. IEEE: IEEE Organizationally Unique Identifier (OUI) List. December (2004)
17. Demers, A., et al.: Epidemic algorithms for replicated database maintenance. Proc. 6th ACM Sympos. on Principles of Distributed Computing, Vancouver, Canada (1987) 1-12
18. Tanenbaum, A., van Steen, M.: Distributed Systems, Principles and Paradigms. Prentice Hall Inc., NJ, USA (2002)