ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SELF DIRECTING AND DECOMPOSITION ADMINISTRATION OF WIRELASS SESORS NETWORKS

Dr.V.V.S.S.S.Balaram*
Professor & Head, Information Technology,SNIST,India

ABSTRACT

In this Paper, we proposed an selfdirecting and decomposition administration rules to wireless sensor networks. Most interesting is the application of autonomic properties and behaviors including adaptive, aware, and automatic operation in a decentralized setting. In particular, we present a generic and autonomic management architecture for decentralized management of wireless access networks, such as GERAN/UTRAN, E-UTRAN, WiMAX or WLAN. For evaluation purposes, we apply this architecture to the management of a Wireless LAN network, and we evaluate the architecture and some of the autonomic management functions through simulations, a prototype implementation and the setup of a real-world testbed for experimentation with the proposed management approach.

KEYWORDS: Wireless Networks, Radio Access Networks,selfdirecting,administration.

INTRODUCTION

Installation and configuration of large wireless networks in heterogeneous environments are challenging, time-consuming and error-prone tasks, even for trained people. Once deployed, such wireless networks require continuous intervention to provide the operational environment required for services to run smoothly, recover from faults, or maximize overall performance of the network. This is particularly difficult, because wireless environments are typically very dynamic. First, the number of mobile devices as well as their mobility and traffic patterns changes constantly in a wireless network. Second, wireless networks often use shared, unlicensed spectrum, like IEEE 802.11a/b/g base stations. As a consequence, different wireless access networks share this unlicensed spectrum in an uncoordinated fashion, which can generate additional disturbance on top of outside interference caused by other electronic equipment. To provision effective and efficient network services under these demanding conditions, continuous network management that adapts to environmental changes both reactively and/or proactively is important.

Manual network management, whereby a human operator takes care of the continuous observation, operation, aintenanceand optimization, is therefore very costly. Since such high operational costs are not affordable by wireless access providers, the need for automated management functionality strongly arises. Few wireless network technologies already include some adequate management mechanisms. However, even though such functions exist, they are typically limited to managing physical or link-specific characteristics and do not cover management of higher-layer internetworking operation. For example, existing IEEE 802.11a/b/g WLAN base stations can automatically select the radio channel, transmission power and link speed; however, they cannot intelligently configure link-specific characteristics that require coordination between neighboring base stations beyond what they can immediately observe themselves. Even more so, they are not able to autonomously configure higher-layer settings such as routed IP connectivity.

This article describes an autonomic approach to the management of wireless access networks. The advantage of an autonomic solution is that new network elements (e.g., base stations) joining an existing wireless network integrate themselves seamlessly. The rest of the system adapts to their emergence dynamically. This enables wireless networks to automatically configure themselves in accordance to some high-level rules or policies that specify what is desired, not how it is accomplished. These rules or policies define the purpose of the network, its overall goals or business-level objectives. A novel idea of this article is the application of autonomic management paradigms in a decentralized manner. Each component must be able to operate fully autonomously, in a stand-alone fashion. When several components detect or sense each others' presence, they then start to coordinate their management actions to increase the efficiency and effectiveness of the overall system. This article presents a decentralized approach for autonomic

management of collaborating network elements. The individual network elements aggregate and share network information. They implement a distributed algorithm that uses the shared information to compute a local configuration at each network elements, which is consistent with the overall network purpose and goal. More specifically, we apply this scheme to the management of wireless access networks, whereby the network elements are base stations. An important feature of the specific system is the wireless monitoring component, which provides the necessary feedback for the autonomic logic to take appropriate management decisions.

Existing approaches to management of wireless networks, even if they expose some autonomic properties, are typically centralized. Traditionally, a central network controller periodically analyzes available information and computes a global configuration for the whole network. It pushes this configuration out to the individual base stations in a piecemeal fashion;alternatively these devices pull their respective configurations from the controller. However, such a centralized approach has several disadvantages. First, it creates a central point of failure, which renders the whole system unusable when the controller fails. Second, a central controller limits scalability, because it represents a bottleneck for processing and communication functions, especially in environments that require frequent configuration changes. Third, it complicates the system, because it introduces additional infrastructure, i.e. the central controller.

LITERATURE SURVEY

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 autonomicapproach. 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, as well as 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. Solutions that operate at the network-layer overcome this shortcoming.

Decentralized management solutions are popular to configure mobile ad hoc networks (MANETs). These management systems typically focus on the challenging task of enabling peer-to-peer communication in highly dynamic, mobile environments . Because of their nature — i.e., every base station decides based on its local scope and not because of a central manager — they are closely related to the autonomic approach presented in this article. Ongoing research efforts attempt to design self-configuring solutions for MANETs. However, in contrast to those approaches, the autonomic solution presented in this article focuses on the configuration of stationary wireless access networks for mobile clients with the primary goal of improving efficiency and performance.With respect to decentralized management of infrastructure- based wireless networks, related work focuses on the auto-configuration of base stations with the goal to achieve the best coverage in a given geographical area. Earlyresults 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 work presented herein is to develop an autonomic and decentralized management platform that can support many types of management functions — not limited to the configuration of radio parameters. Hybrid approaches to wireless network management, such as the Integrated Access Point of Trapeze Networks 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.

SYSTEM MODEL

The high-level properties that every autonomic system and thus also the proposed autonomic network management system should exhibit in order to self-govern its operation and to fulfill its purpose or goal are automatic, aware and adaptive operations.

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. Moreover, this also implies for the system to be able to self-control its internal resources and functions. 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 in a dynamic environment, 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 toother systems that are part of its environment, in order to make informed management decisions. As a result, a key requirement of an autonomic system is a monitoring mechanism that provides the necessary feedback to its control and management logic. Continuous monitoring is necessary to identify if the system meets its purpose. The feedback information 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 and hence provides important input for safety and security mechanisms. Finally, for economic reasons, autonomic systems must also be able to monitor the obtained services of their suppliers and the offered services for their consumers to control or adhere to the agreed level of service.

Adaptive operation: The awareness of an autonomic system allows the system to adapt to changes in the operational context and the environment (guided by its current policies and purpose). Because of this, management in an autonomic system never finishes; the autonomic system continuously adapts by monitoring its components and fine-tuning its operation. For a system to be able to adapt, it must be able to control its internal operations, i.e., its configuration, state and functions. Adaptation will allow the system to cope with temporal and spatial changes in its operational context either in short term (e.g., in case of exceptional conditions such as malicious attacks, faults, etc.) or in long term (e.g., for the purpose of optimization).

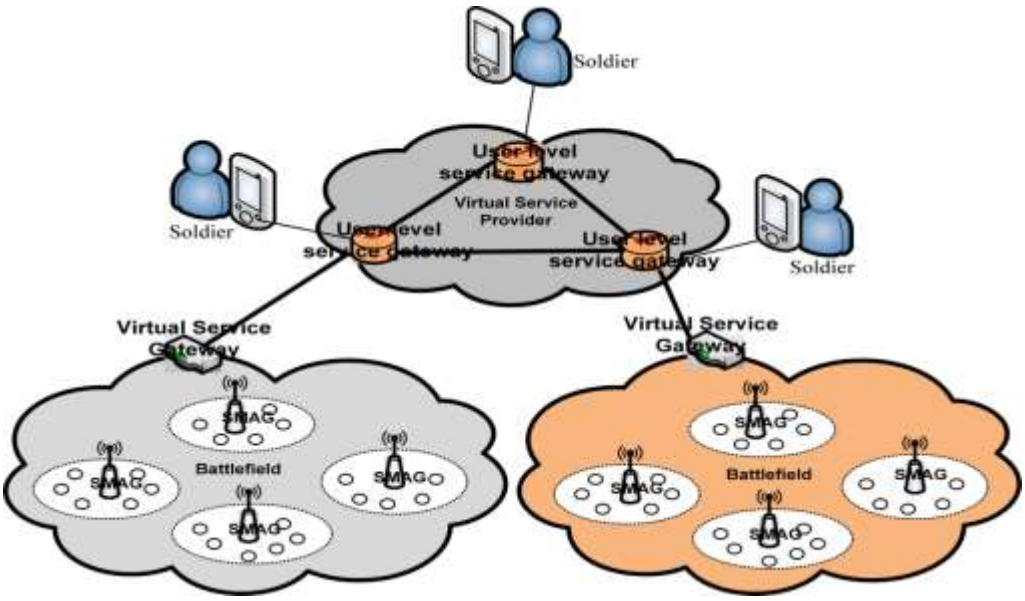

Fig 1 : Automatic and Decentralized Architecture for Wireless Sensor Networks

As illustrated in Fig. 1, the autonomic and decentralized management architecture consists of a set of serving network elements running the decentralized and autonomic management framework. The autonomic management system is distributed across all serving network elements; in the application sce-nario discussed here, the serving elements are the wireless network base stations. Base stations exchange information to have an updated view of the current status of their neighbors. In this way, autonomic functions can make local decisions based on the knowledge of their network context. This process is referred to as "synchronization with neighbors" in Fig. 1. The autonomic management node architecture illustrated in Fig. 1 is integrated into the network elements. It contains a local data store of management data that is synchronized with the local control software and hardware (or can be read on demand) over an application programming interface (API).This API is basically an abstraction layer towards the physical resources of the wireless base stations (which is already present in many advanced platforms today). Moreover, the decentralized management framework includes a dedicated component for synchronizing management information with neighboring network elements. It is assumed that a network element can have different neighbor relationships depending on the application. For example, in Fig. 1 one relationship is based on potential radio coverage overlap, while another one is built among stations that implement a certain feature. A base station has typically one or several radio interfaces and at least one fixed line uplink interface. In many cases the uplink is also wireless, but emulating fixed line interfaces such as ATM over wireless. Due to the higher reliability of the uplink interface, it is assumed that this interface is typically used for the communication at the management plane.

The primary task of the autonomic and decentralized management system is to coordinate and control the element functionsand operation. When applied to a wireless network application, this includes the coordination and control of radio properties, such as frequency assignment and transmission power, among a group of neighboring base stations and to implement system-wide functions, such as load balancing. By exchanging utilization information with neighboring network elements, base stations can distribute load by increasing or decreasing transmission power. 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 sensing or monitoring sub-system provides the necessary feedback information to the autonomic applications to enable adaptation to changes in the operational environment and context. A second task of the autonomic management system is self-protection of the network elements and thus of the overall network. Self-protection also relies on the integrated sensing or monitoring component. For example, traffic monitoring and analysis can be used to detect potential security threats and informs the management system, which in turn can take the appropriate actions to protect the network element. Protection from rogue network elements and MAC address spoofing are examples of attacks that can be detected and counteracted against in this way in a WLAN environment. The management system blacklists those malicious nodes and disseminates their presence throughout the system, warning the overall wireless network. It is important to note that the proposed management system is a *platform* for autonomic and decentralized 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.

The autonomic management system requires a set of supporting functions as part of the framework. First of all, neighborhoodmanagement is a process that discovers and maintains a list of neighboring network elements. An autonomic element can define different neighbor relationships with other nodes: each application running on the autonomic element is responsible to build such relationships. For example, to define the neighbor relationship in terms of wireless coverage, the system needs to find neighboring base stations, which have overlapping cell areas. Such a list of neighbors is also supported in the management framework of WiMAX , where it can be used for handover, but the list needs to be populated through the management interface . The delegation of this process to an autonomic module would clearly cut the costs associated with a manual configuration of the neighbor list. Second, the policy system is in charge of guiding the autonomic applications by imposing rules on them, and to configure thresholds or other constraints for the autonomic behavior. Note that the policy system here does not directly interacting with the networking part of the device as usually proposed in the literature . Finally, security is of major concern. And again depending on the deployment scenario or the application different mechanisms are required. For certain scenarios co-operative trust systems, which slowly build-up trust between individual entities in an autonomic fashion based on the perceived behavior of other entities, can be used. In such cases, trust is established over a long time in which a neighbor

proofs to function correctly and does not try to cheat. In commercially sensitive deployments, trust will be established through configuration of the appropriate keying material and security mechanisms when installing the equipment.

An autonomic network element is able to change some of its parameters autonomously according to changes of the environment. A network of such autonomic elements promises increased scalability, low installation costs and better performances. However, such solutions introduce new possible causes of failures due to the inherent complexity of a fully distributed configuration algorithms: common problems are loop configurations, oscillations of information changes and network traffic overload. The lack of a sophisticated monitoring system for autonomic processes and remote control functions is expected to cause serious doubts for operators to adopt autonomic solutions in existing networks. Especially in the beginning, when autonomic systems are deployed, it is crucial for operators to be able observe the behavior of the autonomic system and interfere with the autonomic process until they have developed trust in the new technology. For this purpose we propose that an autonomic node should maintain a north-bound interface towards a central monitoring application. This interface should be regarded only as an optional element. In general, monitoring of the autonomic process be accomplished through observing and filtering local and neighbor synchronization processes. The monitoring process should allow tracing of the actual changes in the configuration or just the frequency of parameter changes and/or samples of the configuration state.

The filtering mechanism should allow the operator to block the synchronization of some values/parameters in order to overrule the autonomic process and to overwrite the synchronization of particular settings through manual configuration of the value/parameter. In the remainder of this section we apply the proposed autonomic management system to a wireless network based on IEEE 802.11a/b/g Wireless LAN base stations. Note however that the same algorithms can be adopted for the management of other radio networks, such as 3GPP UTRAN or evolved UTRAN .

CONCLUSION

This article presents a decentralized, autonomic management architecture and its application to the management of wireless networks. The proposed system is a platform for autonomic management that offers generic mechanisms supporting various 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 the integrated wireless monitoring component as part of the base stations. 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. Furthermore, we have not studied the interworking of the autonomic base stations with an autonomic centralized management system. So far, the centralized management system is only used for configuring the policies, monitoring the autonomic process, but not for any autonomic control based on overall network knowledge. For this we anticipate the problem resulting from interacting control loops with potentially contradicting results and decisions. Finally, as detected in the real implementation, the scanning is not error free. The study of that effects of erroneous measurement results used in an autonomic decision engine is a very interesting future work item to be studied, potentially even in a general way.

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] C.-K. Toh, Ad Hoc Mobile Wireless Networks, Protocols and Systems,Prentice Hall Inc., New Jersey, USA, 2002.
[4] L. Ji et al., “On Providing Secure and Portable Wireless Data Networking Services: Architecture and Data Forwarding Mechanisms,” Proc. Int’l.Conf. 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] H. Zhang and A. Arora, “GS3: Scalable Self-Configuration and Self-Healing in Wireless Networks,” Proc. 21st Annual Symp. Principles of DistributedComputing, Monterey, California, USA, 2002, pp. 58–67.
[7] B. Krishnamachari et al., “On the Complexity of Distributed Self-Configuration in Wireless Networks,” elecommunication Systems, vol. 22, no. 1–4, 2003, pp. 33–59.

[8] F. J. Mullany et al., "Self-Deployment, Self-Configuration: Critical Future Paradigms for Wireless Access Networks," Proc. 1st Int'l. Wksp. Autonomic Commun. (WAC 2005), Berlin, Germany, 2004.
[9] L. T. W. Ho, L. G. Samuel, and J. M. Pitts, "Applying Emergent Self-Organizing Behaviour for the Coordination of 4G Networks Using Complexity Metrics," Bell Labs Tech. J., vol. 8, no. 1, 2003, pp. 5–26.
[10] Trapeze Networks: Defining An Integrated Access Point, White Paper (2004)
[11] J. Kephart and D. Chess, "The Vision of Autonomic Computing," IEEE Computer Mag., 2003.
[12] K. Zimmerman, "An Autonomic Approach for Self-Organising Access Points," Diploma Thesis, University of Ulm, Germany, 2004.
[13] S. Tobella, J. J. Stiemerling, M., Brunner, "Towards Self-Configuration of IPv6 Networks," Proc. Poster Session of IEEE/IFIP Network Operations and Management Symp. (NOMS'04), Seoul, Korea, 2004.
[14] J. Wright, "Detecting Wireless LAN MAC Address Spoofing," White Paper, 2003.
[15] J. Wright, "Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection," White Paper (2002).
[16] IEEE, IEEE Organizationally Unique Identifier (OUI) List, Dec. 2004.
[17] A. Demers et al., "Epidemic algorithms for replicated database maintenance," Proc. 6th ACM Sympos. on Principles of Distributed Computing, Vancouver, Canada, 1987, pp. 1–12.
[18] A. Tannenbaum and M. van Steen, Distributed Systems, Principles and Paradigms, Prentice Hall Inc., NJ, USA, 2002.