MIT Sloan School of Management

Working Paper 4460-04
January 2004

SELF-CONFIGURATION AND SELF-ADMINISTRATION OF WIRELESS GRIDS

Ashish Agarwal, Amar Gupta, Douglas O. Norman

Editorial Manager(tm) for Journal of Grid Computing
Manuscript Draft

Manuscript Number:

Title: SELF-CONFIGURATION AND SELF-ADMINISTRATION OF WIRELESS GRIDS

Article Type: Special Issue Manuscript

Section/Category:

Keywords: Wireless Networks; Grid Computing; Mobile Computing; MANET; Sensor Networks

Corresponding Author: Ashish Agarwal i2 Technologies

First Author: Ashish Agarwal

Order of Authors: Ashish Agarwal; Amar Gupta; Douglas O. Norman

Abstract:

*** abstract**

ABSTRACT

A Wireless Grid is an augmentation of a wired grid that facilitates the exchange of information and the interaction between heterogeneous wireless devices. The ability of various grid layouts to handle interactions among the grid constituencies is contingent upon the efficient resolution of multiple technical challenges of the grid. These challenges arise due the added complexities of the wireless grid such as the limited power of the mobile devices, the limited bandwidth (including partial connectivity), and the increased dynamic nature of the interactions involved. This paper focuses on the configuration and administration issues of the wireless grid. The proposed grid topology and naming protocol can allow self-configuration and self-administration of various possible wireless grid layouts.

SELF-CONFIGURATION AND SELF-ADMINISTRATION OF WIRELESS GRIDS

Ashish Agarwal (i2 Technologies)

Amar Gupta (MIT)

Douglas O. Norman (The MITRE Corporation)

ABSTRACT

A Wireless Grid is an augmentation of a wired grid that facilitates the exchange of information and the interaction between heterogeneous wireless devices. The ability of various grid layouts to handle interactions among the grid constituencies is contingent upon the efficient resolution of multiple technical challenges of the grid. These challenges arise due the added complexities of the wireless grid such as the limited power of the mobile devices, the limited bandwidth (including partial connectivity), and the increased dynamic nature of the interactions involved. This paper focuses on the configuration and administration issues of the wireless grid. The proposed grid topology and naming protocol can allow self-configuration and self-administration of various possible wireless grid layouts.

Keywords – Wireless Networks, Grid Computing, Mobile Computing, MANET, Sensor Networks.

1 INTRODUCTION

Rapid advances, diminishing prices, wide availability, and attractive form factors have caused wireless technologies to permeate the lives of people from all walks of life. With the ubiquity and indispensability of wireless technologies established, these technologies are now making inroads into Grids.

Grid Computing is envisaged to provide a solution to the challenge of '*flexible, secure, and coordinated resource sharing among dynamic collections of individuals, institutions and resources*' [1]. The ultimate vision of the grid is that of an adaptive network offering secure, inexpensive, and coordinated real-time access to dynamic, heterogeneous resources, potentially traversing geographic, political and cultural boundaries but still able to maintain the desirable characteristics of a simple distributed system, such as stability, transparency, scalability and flexibility.

Traditional applications that can operate in the Wired Grid environment need to expand their scope by extending the interactions to mobile devices. The mobile access interface needs to address the issue of connectivity of mobile devices. At the same time, wireless applications need to share the resources and provide access to additional

computational resources to mitigate the constraints imposed by limited storage, computational capability, and power of mobile device. There is also a need for new applications to respond to the dynamic and unforeseen events introduced by the wireless environment. In addition, the applications must be built to interact with the infrastructure to address the rapid provisioning of major amounts of computational and communications bandwidth required to offer the user experience demanded. The above factors are combining to shape the development of Wireless Grids.

2 TECHNICAL CHALLENGES

The growth and ubiquitous acceptance of wireless grids is heavily dependent on the ability to surmount the following technical issues:

Dynamic Configurability: Wireless grids must offer high degree of temporal flexibility. This is because the mobile nature of the grid components results in topologies that change frequently over time. Accordingly, wireless grids need to provide automated self-configuring and self-administering capability to accommodate these dynamic changes for all relevant grid layouts.

Routing Plasticity: Wireless grids must offer outstanding built-in network optimization capabilities. Efficient routing protocols are required to address the power limitation of the end devices along with the consideration for stable wireless connectivity, route optimization and efficient use of the limited bandwidth.

Discovery Semantics and Protocols: Wireless grids must offer adequate support for overcoming heterogeneities across individual services and sub-systems. Service description protocols are needed to describe the services provided by various components of the wireless grid. Once these services are published, a discovery protocol is needed to map the mobile resources to the services.

Security: Wireless grids must incorporate effective mechanisms to provide adequate security and privacy to end-users. This is a major challenge because of several factors: the inherent nature of the wireless connection, the diversity of the link quality, the potential unreliability of the end-devices, and the power constraints on the mobile devices. The incorporation of effective security techniques will also place a need on the availability of significant computational power that would be required to execute the security algorithms within acceptable periods of time. Further, sufficient radio power would be needed to achieve acceptable signal-to-noise ratio for the encrypted signaling streams. The choice of the access points and the hand-over protocols must be carefully designed in order to address the needs within the constraint of the very limited power available from the individual wireless devices.

Policy Management: Wireless grids must incorporate appropriate policies to support both pre-conceived and agile interactions among the relevant sets of users. The designers of evolving grid architectures need to formulate and nurture policies that govern the usage, the privileges, the access to resources, the sharing level arrangements, the quality of service, and the composability and the automated resolution of contradictory policies among organizations; as well as other technical issues described above.

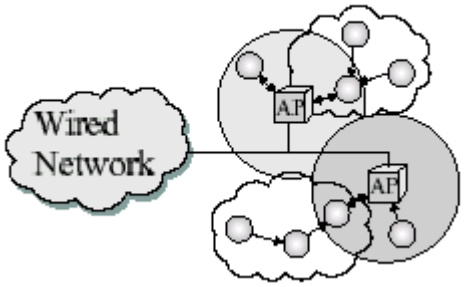
3 SELF-CONFIGURING AND SELF-ADMINISTERING DYNAMIC ADDRESS SERVICES ACROSS VIRTUAL ORGANIZATIONS

Building upon the paradigm of the wired grids [2,3,4], one can identify several alternative architectures for wireless grids. These are characterized by the degree of heterogeneity of the actual devices and the level of control exercised by those who own and administer the associated devices. In order to develop further and to flourish, wireless grids must exist for the benefit of the members and users, and simultaneously impose as few additional constraints on them as possible. One aspect that is of special importance is the ability of the wireless grid to manage itself and to adapt itself as devices enter or leave the wireless grid configuration. In other words, the infrastructures that support wireless grids must address the issue of dynamic updates to the grid in order to respond to the failure of a network node, as well as the entry or exit of nodes for various grid layouts. Previous work on Self-Configuring and Self-Administering Domain Name Service (DNS) has led to a reliable, intelligent and distributed lightweight protocol for automatically adapting to the changes in wired networks [5]; this protocol can be modified and extended for use in the wireless grid environment and the enhanced version is described in the following subsections.

3.1 Grid Topology

A number of researchers have evaluated the topology and configuration of Mobile networks [6,7,8]. However, all the proposed ad-hoc systems are standalone in nature. We believe that the commercial grids will possess some access to the wired Internet infrastructure and thereby follow a hybrid model (fig 1). This hybrid model will consist of Mobile Ad-hoc Networks[1] (MANET) type systems with multiple-hop paths between mobile nodes and access points (AP) to the wired network. Data will flow across the grid using a combination of Mobile IP [9] and Ad-Hoc routing protocols such as DSDV [10], DSR [11], AODV [12] and TORA [13].

[1] http://www.ietf.org/html.charters/manet-charter.html



AP: Access Point

Figure 1. A Hybrid Wireless Network

At a high level, one needs to support the critical role of the management and composition of subnets and arbitrary collections of wireless members. There must be a Root Station (RS) present in some form as well as a Base Station (BS). The RS maintains cognizance over a set of wireless devices and provides the final mapping of logical to physical devices. The BS manages and enforces policy within and among groups. A grid layout can include a root station for a community or an actual organization (AO) of wireless nodes (fig. 2). A RS will maintain up-to-date information about its own network and the associated nodes, as well as serve as the gateway to the wired network. Multiple organizations may come together to form a virtual organization (VO). An AO can belong to multiple VOs. A base station (BS) can be envisaged for a VO. A BS will maintain information about networks for various organizations and the associated root stations. For a homogeneous grid, the same server can perform both the RS and BS functions. In case of an inter-grid, which can span multiple virtual organizations, several BSs are needed to coordinate and maintain the inter-grid information. Adequate redundancy can be established by having secondary servers perform the RS and BS functions. Both RS and BS should not be resource-constrained devices. Instead, each of the RS and the BS could be a simple PC, a workstation, or a server equipped with an appropriate interface that provides the ability to communicate with the edge nodes such as sensor nodes or other mobile nodes.

3.2 Self-Configuration and Administration of Wireless Grid

As previously stated, wireless grids possess a unique dynamic quality that is not found readily in the wired grids. Therefore, technologies that support self-configuration and self-administration are critical to the continued growth of the wireless grid paradigm. A Wireless Grid should allow:

- Configuration of addresses for the grid components: nodes, RS and BS

- Name- to- address resolution for the grid components
- Maintenance of the state information for the grid

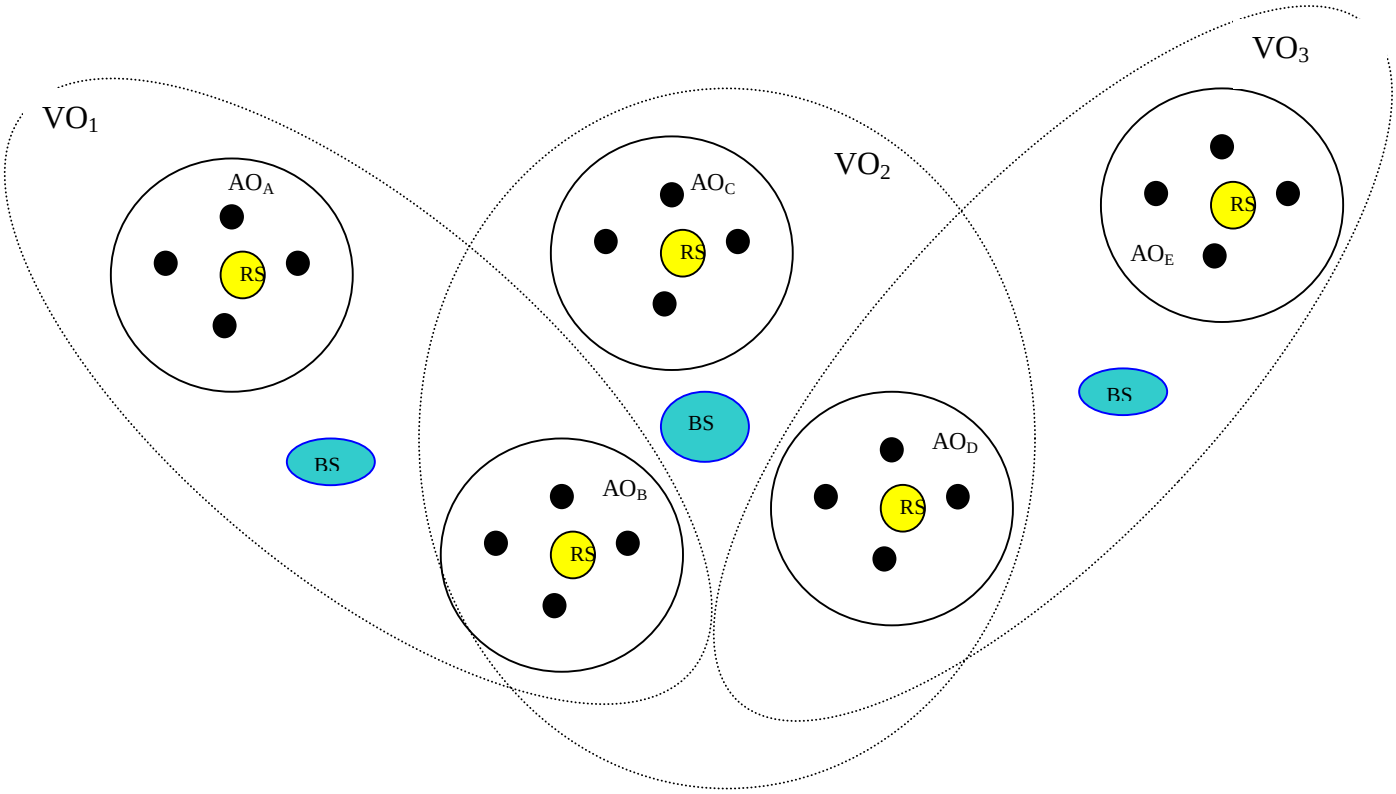


Figure 2. Wireless Grid spanning multiple Virtual Organizations

The address for the nodes can be obtained in several different ways [6]. It is possible that the address may not be an IP address in case the device is a sensor with no IP stack. We envision that an IP incapable node could use, as its own address, either the MAC address of the system chip or a unique serial number provided to it at the time of manufacture of the particular device. A name, unique to the AO domain, can be assigned to the device through an automatic handshake process between the device and the RS. The RS and the BS are connected to the wired infrastructure and can obtain IP addresses using the DHCP protocol [14].

The RS and the BS provide the naming service for resource discovery across the AOs and VOs. The notion of grid service [1] can be extended to the wireless grids. In such a scenario, the RS can provide a naming service for resource discovery based on service description [15] at the node level. Resource discovery can be extended to a virtual organization where a BS can provide a naming service for resource discovery within various actual organizations. Multiple BSs can coordinate to provide service discovery across multiple VOs.

Each node maintains information about itself and the AO it belongs to. The RS maintains information about its AO such as the name and address pairs for its nodes, number of nodes, name of its AO, names of the VOs to which its organization belongs and the associated base stations. The BS maintains information about its VO, the names of associated AOs, names and addresses of associated RSs, and also the names and addresses of other BSs.

3.2.1 Messages

Messages are used for communication between the grid components and serve as the mechanism for resource discovery. Figure 3 shows the structure of a message. It consists of a three-field header followed by a payload section. The header fields are explained in Table 2. The payload holds the data from the message specific to each Opcode. Table 3 lists the possible opcode values.

Table 2. Message Header fields

Header Field	**Description**
Message Id	The unique message id for the message
Opcode	The operation code for the message.
S/R flag	Send/Response Flag. A flag indicating whether the message is a send request or response to a send request

Figure 3. Message Format

Table 3. Opcode Values

Opcode Values	**Brief Description**
Enter_node	Informs members of the entry of the node
Leave_node	Informs member of the exit of the node
Enter_RS	Informs members of the entry of the RS

Leave_RS	Informs member of the exit of the RS
Enter_BS	Informs members of the entry of the BS
Leave_BS	Informs member of the exit of the BS
Discover_node	Used to discover node
Hello	Used to verify if the members exist

3.2.2 Message Behavior

Enter and leave messages are used by the grid components to announce their entry or exit from the overall system. Discover messages are used to discover the grid resources. Hello messages are used to validate the existence of the grid components.

3.3 Grid Operation

3.3.1 Node Management

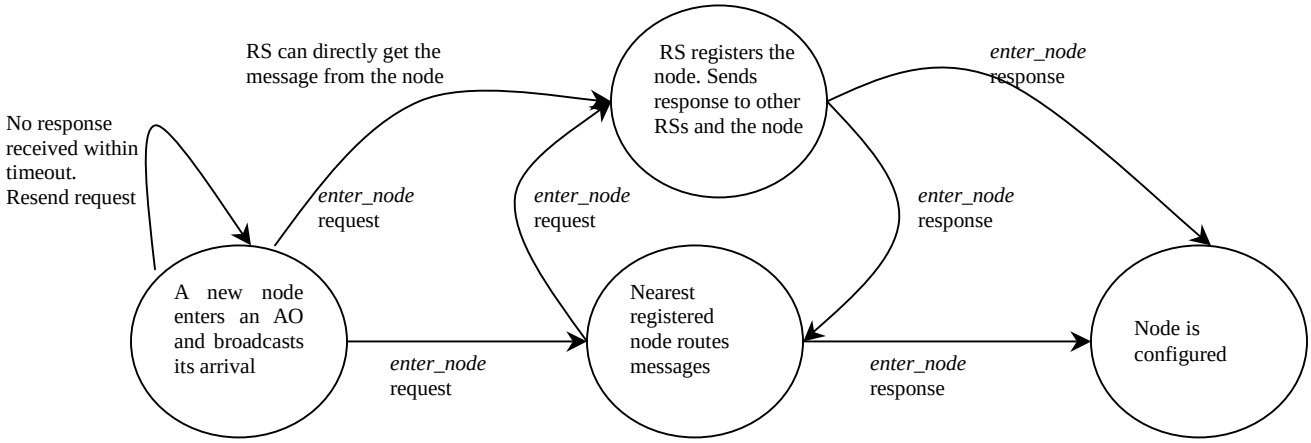
Node Entry or Exit

Mobile nodes register <address, name> tuple with the Root Station (RS) as they enter the network under the RS coverage. The node broadcasts an *enter_node* message (fig 4a). The nearest registered node picks up the message and passes on the registration information to the nearest RS. If the node cannot directly establish connection with the RS, it uses multiple hops to communicate with the RS. It is possible, that the RS directly receives the message from the new node. When the RS receives the request, it sends *enter_node* response to the node and adds the information related to the node. The response includes the information about RS and AO.

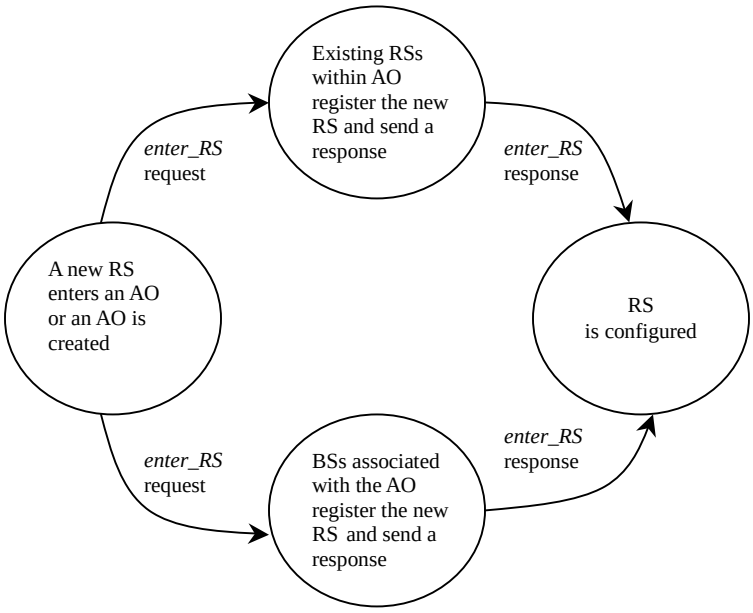
Node Discovery

A *chain-of-responsibility* pattern [16] is used for node discovery. A node N_o sends a *discover_node* request to RS_o seeking connection to a different node N_a. The request contains the name of the requested node. RS_o looks up its AO_o information to locate the node and sends a *discover_node* response to node N_o with the address information of N_a. If node N_a does not exist in the AO_o then RS_o sends the *discover_node* request to the BS_o. This request includes the RS_o information. BS_o in turn broadcasts the request to all the RSs associated with its VO_o. If RS_a locates the node in its AO_a then it notifies the BS_o about the availability of the node. BS_o in turn sends the *discover_node* response to the requesting RS_o with the address of N_a, which is then forwarded to N_o.

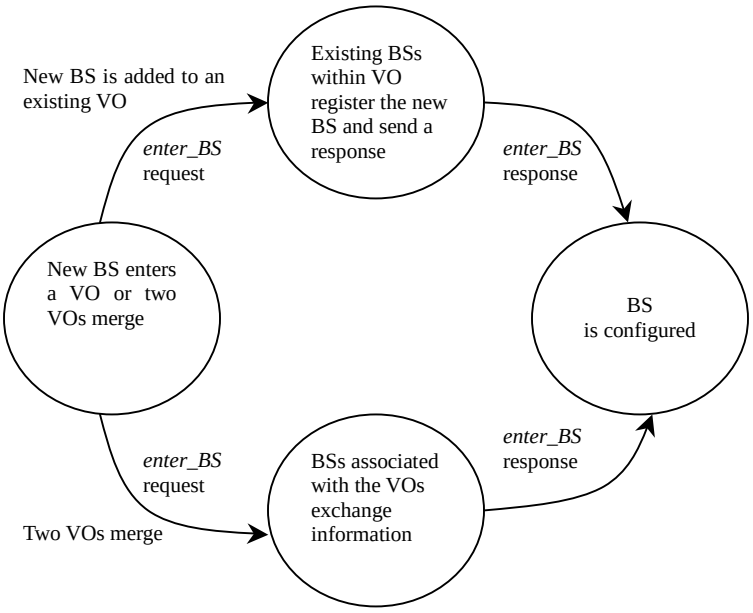
The same mechanism can work if the nodes belong to different virtual organizations. In this case, the request will be routed to all other base stations by the BS_o when it fails to hear back from the RSs in its VO. The broadcast request to the BS will include information about the requested node N_a, requesting node N_o and the associated RS and the BS. Each BS will route this request to its own set of RSs. Node discovery mechanism is shown in figure 5.



a) Node Configuration



b) RS Configuration



c) BS Configuration

Figure 4. Configuration Mechanism for Grid Members

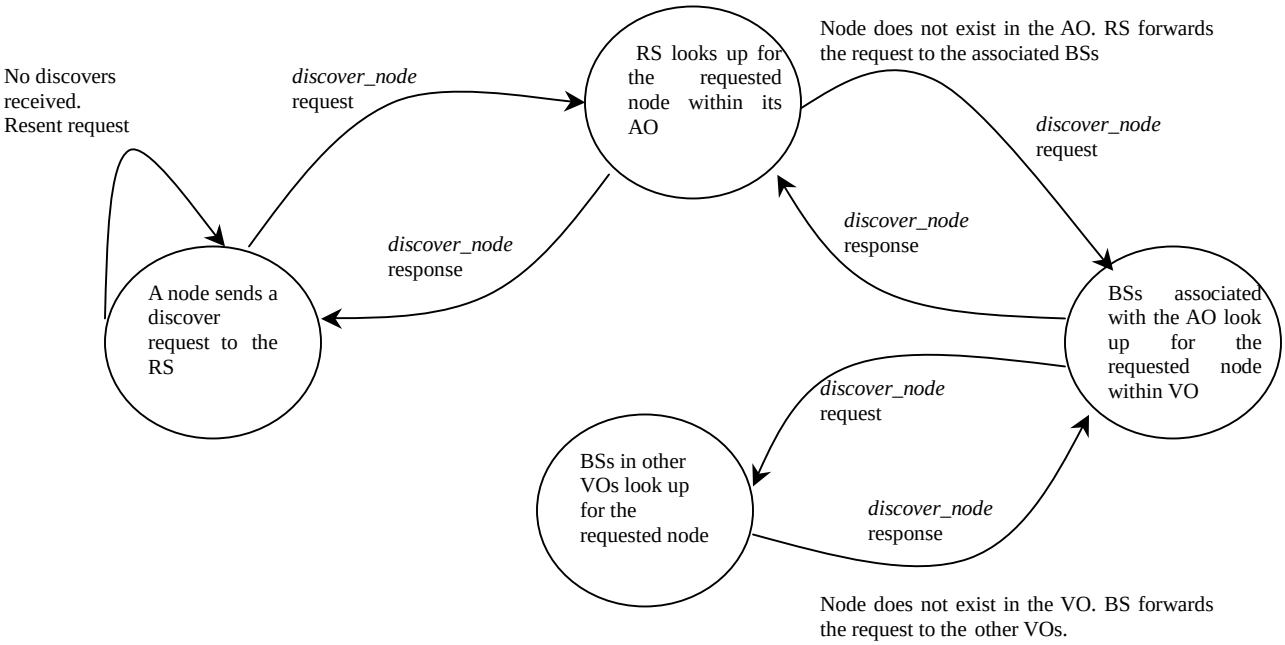


Figure 5. Discovery Mechanism for the node

3.3.2 RS Management

Business partners can engage in a dynamic relationship to form a virtual organization [17]. This can lead to adhoc creation of a VO, dynamic changes to the VO, and the need for resource discovery across several AOs within a VO.

VO Creation

Several AOs will come together to form a VO. An assumption is that a BS will be available to create a VO with a unique name and address. Each RS will send an *enter_RS* message to the BS with the information about AO such as AO name, RS name and RS address (fig 4b). In its response, BS will send the VO information such as the VO name, BS name and BS address. BS will maintain a list of all AOs and the associated RS names and addresses.

RS Entry or Exit

A new AO may join a VO, or an existing AO may leave a VO. Any AO can be associated with multiple VOs at the same time. In such a scenario, we need to provide a capability to dynamically configure the RS. Entry mechanism and registration will be the same as the VO creation. In case an AO is leaving the VO, the RS will broadcast *exit_RS* message to the associated base stations and delete information about the VO. On receiving the message, the BS will delete the RS and AO information from its record.

3.3.3 BS Management

In dynamic markets, two or more virtual organizations can come together to conduct business. This will lead to

dynamic associations between the VOs and the need for resource discovery across several VOs.

BS Entry or Exit

It is possible that two or more BS discover one another. In that case, they will send broadcast messages describing their VO. Each BS will receive an acknowledgement in response and the information about other BS (fig 4c). Through such interactions each BS will be able to generate a list of existing VOs and the names and addresses of the associated BSs. A BS will broadcast its entry or exit using *enter_BS* and *leave_BS* messages. Remaining BSs will accordingly update their lists accordingly.

3.3.4 Multiple RS and BS

In the description so far, we have assumed that there is only one RS for each AO and only one BS for each VO. However, depending on the size of the network and the distances between the components, there could be several RSs per AO and several BSs per VO to facilitate address assignment and resource discovery.

Nodes

Within an AO, the nodes will register with the nearest RS. Each RS will maintain information about all other RS within an AO. It is possible that registration request for a node is sent to more than one RS. In this case, the first RS to receive the information will send an *enter_node* response to all other RSs within the AO in order to avoid duplicate registration. For the node discovery, the RS will first check with the local RSs before forwarding the discover request across the VO.

RS

When a new RS is added to the grid, it will send *enter_RS* message to all the existing RSs within an AO, as well as to the associated VOs and BSs. In response, the RSs will send their information to the new RS. BS will update its list of RSs and send the VO information back to the RS.

BS

In case of multiple BSs within a VO, the entry of a new BS will be broadcasted to all the existing BSs. In response, the BSs will send their information to the new BS. This will include information about their AOs. For the node discovery, a BS will first check with the BSs within the VO before forwarding the request across multiple VOs.

3.4 Addressing Transient Nature of Wireless Grid

Wireless networks are characterized by weak transmission signals and message losses. Power constrained nodes may suddenly crash. These types of events can create inconsistencies in the information maintained by the grid components. The proposed architecture addresses these situations in the manner described in the following subsections.

3.4.1 Node Failure

An RS can detect node failure by periodically sending *hello* requests to its registered nodes. In case it obtains no response from a node, the RS will continue to send the *hello* requests to the specific node. After a predefined number of requests, the RS assumes that the node has failed and deletes the node information.

3.4.2 Message Losses

Message losses can manifest themselves in the same fashion as the node failure. The message initiator, i.e., node, RS or BS, will make multiple attempts to elicit a response from others. One of the retries will succeed in obtaining the response. There may be cases where the messages are lost only for a set of recipients. A RS or a BS can lookup its organization information and send messages to only the set of the recipients that did not respond to the previous attempts. A leaving node or a RS may not wait for a confirmation from all the recipients. Existing members in the network can periodically send *hello* messages to confirm their individual presence. When a RS or BS does not receive a response to the *hello* messages from certain members, it makes the assumption that the concerned members are no longer part of the network.

3.5 Other Considerations

3.5.1 Performance

Network performance is evaluated in terms of the availability of the network components, latency and transmission bandwidth. In case of wireless connections, additional factors impacting the performance are the power consumption of the nodes, the level of interference, and the quality of radio transmission. The Grid topology, the power efficiency of the protocols, and the amount of mobility can influence these factors. A number of studies have been conducted to evaluate the performance of the routing protocols for ad-hoc networks using metrics such as delay, throughput, route

optimality, [18, 19] and energy conservation [20]. It has been shown that the capacity of a random ad-hoc network does not scale well beyond a certain number of nodes [21]. At the same time, the mobility of the node can in fact improve the throughput capacity of the ad-hoc networks [22]. A hybrid network model can improve the connectivity as well as the throughput capacity. However an optimal ratio of wired and wireless nodes must be maintained in order to achieve this benefit [23].

3.5.2 Security Issue

Throughout our discussion, we have assumed that nodes or the stations do not operate in a malicious manner. For a real wireless grid, this is a poor assumption. Among the many security issues written about, denial-of-service is an especially pernicious problem for a wireless grid. A rogue node or a station could manipulate the configuration of the network. By such action, the rogue node could corner a number of addresses, making them unavailable for other nodes that may wish to join the AO. Subsequently, the rogue node could respond on behalf of the phantom nodes making it difficult to clean up their addresses. If IP addresses are in short supply, such an action could prevent some bona-fide nodes from joining the AO. Also, the rogue node could significantly overload the system by generating several requests within a short time. Finally, the malicious node could generate *exit* messages for nodes that are still part of the network.

In order to mitigate the above type of situation, one strategy is to assume the existence of a *Security Association (SA)* between the end hosts. This implies a secure communication scheme and, consequently, the need to authenticate each other on a peer-to-peer basis [24]. This *SA* could be established via a secure key exchange [25], or through initial distribution of credentials.

The attacks mentioned above can be thwarted by the use of digital certificates that the nodes may have obtained a priori from a trusted *Authentication Server (ASs)*. Using such certificates and knowledge of the *AS* public key, the grid nodes and stations can authenticate each other and sign their messages even when the *AS* is not reachable.

3.5.3 Policy Management

Since the end-devices or nodes are usually power constrained, one cannot assume that the devices are capable of running complex protocols such as Lightweight Directory Access Protocol (LDAP) or Common Open Policy Service (COPS). The technical aspects of policy management, such as privileges and access to resources, can be

potentially handled through the root stations and the base stations. The RS should be capable of handling the resource intensive protocols, as well as maintaining the latest information on the nodes in the network and their respective capabilities. The RS could maintain the policy database that could be populated manually or through a messaging mechanism between the nodes and the RS. When a node leaves the local grid, the policies relevant to the node are discarded. Similarly, when a new node enters the local grid, it can configure its policies on the RS through lightweight messaging. Alternatively, the policies could be pre-configured on the RS based on a classification of the resources into one of several classes, i.e., low power resource class, highly secure class, etc. This means that the devices must also communicate their capabilities at the time of registration.

Similar to the RS, a base station (BS) for centralized control can be envisaged for the enterprise or the virtual organization within the intra-grid architecture. For an inter-grid, two or more BSs need to interact with each other in order to conform to end-to-end Quality of Service guarantees while traversing across multiple enterprises.

4 CONCLUSION

The advent of wireless grids can take ubiquitous computing to the next level by providing seamless wireless extensions to the wired grid. Mobile devices can share resources and overcome their power limitation using the grid architecture. Various grid layouts can be deployed to provide data, computing, and utility services for a wide set of application areas. The ability of these models to address needs at the enterprise, partner, and service levels is contingent upon the resolution of technical challenges related to configuration, routing, discovery, security and policy management. The proposed grid topology and naming service can address the self-configuration and self-administration requirement for various grid layouts. This proposed topology provides the foundation to address the discovery and policy management requirements as well.

ACKNOWLEDGMENTS

We thank Hongfei Tiang, Szei Hwei Ong and Madhav Srimadh for their valuable assistance.

REFERENCES

[1] I. Foster, C. Kesselman, S. Tuecke, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations,” International J. Supercomputer Applications, 15(3), 2001.

[2] W. Gentzsch, “Grid Computing: A New Technology for the Advanced Web,” White Paper, Sun Microsystems, Inc., Palo Alto, CA, 2001.

[3] S. H. Ong, “Grid Computing: Business Policy and Implications,” Master’s Thesis, MIT, Cambridge, MA, 2003.

[4] H. Tiang, “Grid Computing as an Integrating Force in Virtual Enterprises,” Master’s Thesis, MIT, Cambridge, MA, 2003.

[5] P. Huck, M. Butler, A. Gupta, M. Feng, “A Self-Configuring and Self-Administering Name System with Dynamic Address Assignment,” ACM Transactions on Internet Technology, Vol.2, No.1, pp. 14-46, February 2002.

[6] S. Nesargi, R. Prakash, “MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network,” in Proc. of INFOCOM’02, August 2002, pp. 1059-1068.

[7] N. H. Vaidya, “Weak Duplicate Address Detection in Mobile Ad Hoc Networks,” in Proc. of Mobihoc’02, June 2002, pp. 206-216.

[8] M. Mohsin, R. Prakash, “IP Address Assignment in a Mobile Ad Hoc Network,” IEEE Military Communications Conference (MILCOM 2002), Vol. 2, October 2002, pp. 856-861.

[9] C. Perkins, “IP Mobility Support,” Request for Comments (Proposed Standard) 2002, Internet Engineering Task Force, October 1996.

[10] C. E. Perkins, P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” in Proc. ACM SIGCOMM Conference (SIGCOMM ’94), August 1993, pp. 234–244.

[11] D. B. Johnson, D. A. Maltz, “Dynamic Source Routing in Ad-Hoc Wireless Networks,” T. Imielinski and H. Korth, editors, Mobile Computing, Kluwer Academic Publishers: Dordrecht, The Netherlands, pp. 153-181, 1996.

[12] C. Perkins, E. Royer, “Ad Hoc On-Demand Distance Vector Routing,” in 2nd IEEE Workshop on Selected Areas in Communication, February 1999, pp. 90–100.

[13] V. D. Park, M. S. Corson, “A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks,” in Proc. IEEE Infocom, Kobe, Japan, April 1997, Vol. 3, pp. 1405–1413.

[14] R. Droms, “Dynamic Host Configuration Protocol,” IETF RFC 2131, March 1997.

[15] W. Adjie-Winoto, E.Schwartz, H. Balakrishnan, J. Lilley, “The Design and Implementation of an Intentional Naming System,” in Proc. 17th ACM SOSP, Kiawah Island, SC, December 1999, pp. 186-201.

[16] E.Gamma, R. Helm, R. Johnson, J. Vlissides, Design Patterns, Addison-Wesley, Reading, MA, 1995.

[17] J. Walton, L.Whicker, “Virtual Enterprise: Myth and Reality,” Journal of Control, pp. 22-25, 1996.

[18] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” in Proc. MobiCom’98, Dallas, TX, October 1998, pp. 85-97.

[19] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, M. Degermark, “Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-Hoc Networks,” in Proc. MobiCom’99, Seattle, Washington, August 1999, pp. 195-206.

[20] B. Chen and C. H. Chang, “Mobility Impact on Energy Conservation of Ad Hoc Routing Protocols,” SSGRR 2003, Italy, July 2 –August 2, 2003.

[21] P. Gupta, P. R. Kumar, “The Capacity of Wireless Networks,” IEEE Transactions on Information Theory, Vol. 46, No. 2, pp. 388-404**,** March 2000.

[22] M. Grossglauser, D. N. C. Tse, “Mobility Increases the Capacity of Ad-Hoc Wireless Networks,” IEEE/ACM Transactions on Networking, Vol. 10, No. 4, pp. 477-486, August 2002

[23] B. Liu, Z. Liu, D. Towsley, “On the Capacity of Hybrid Wireless Networks,” in Proc. of IEEE Infocom’03, San Francisco, CA, 2003.

[24] P. Papadimitratos, Z. J. Haas, “Secure Routing for Mobile Ad Hoc Networks,” in Proc. of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, January 2002, pp. 27-31.

[25] N. Asokan, P. Ginzboorg, “Key Agreement in Ad Hoc Networks,” Computer Communications, Vol. 23, No.17, pp. 1627–1637, November 2000.