Grid High Performance Networking Research Group

GRID WORKING DRAFT

Document: draft-ggf-lwmcknight-wgissues-0
Category: Informational Track

Dr. Lee. McKnight

Syracuse University.

Dr. Mark Gaynor
Boston University.

Dr. Junseok Hwang
Syracuse University.

Dr. Joon Park
Syracuse University

Dr. Hwa Chang
Tufts University

Dr. Amar Gupta
MIT

Dr. Bernhard Plattner
Swiss Federal Institute of

Technology - Zurich

James Howison
Syracuse University

Praveen Aravamudham
Syracuse University

Ozlem Uzuner
MIT

Bor-rong Chen
Tufts University

Wireless Grid Issues

Status of This Memo:

This memo provides information to the Grid community. It does not define any standards or technical recommendations.

Distribution is unlimited.

Copyright Notice

Comments:

Comments should be sent to the GHPN mailing list (ghpnwg@gridforum.org).

Table of Contents

1. Introduction and Background

A computer grid is a collection of distributed resources that are shared among a group of users. The "grid" schedules and coordinates resources to offer a diverse collection of services over a network of connected wireless devices. These devices may be both plentiful and very diverse. The continuing growth of wireless services brings many new devices, new applications, as well as many new technical, economic and policy challenges, to wireless Internet access to virtual markets on the grid [Lehr 2003, McKnight, 2002a, Anius 2003]. These challenges include resource discovery and sharing in dynamic ad-hoc network environments, power and bandwidth management including for power constrained devices, user interface design for mobile devices, business models, and policy infrastructure [Gaynor 2003, Hwang 2003, McKnight 2002b]. The Virtual Markets for Wireless Grids (VMWG) research team focuses on the challenges outlined above and in addition is exploring a middleware architecture for peer-to-peer computing within wireless grids, security challenges for WLAN's and some innovative ideas for wireless grid applications. The purpose of this document is to provide information on our early work which may be of interest and relevant to the broad Global Grid Forum community, and more specifically to the high performance networking research group.

Our interdisciplinary Wireless Grid team is conducting research, under the aegis of an NSF award (contract #0227879). The team comprises of faculty and graduate students from a number of leading universities (Syracuse, Boston, Northeastern, and Tufts Universities as well as MIT and the Swiss Federal Institute of Technology – Zurich), companies (British Telecom, Cisco, and Novell among others), and Telecom City (established by the cities of Medford, Malden and Everett under the aegis of the Commonwealth of Massachusetts). The ultimate vision of this interdisciplinary team is the development of an adaptive wireless 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 for wireless devices.

2. Need for Wireless Grids

Advances in network architecture and proliferation of bandwidth are driving the rethinking and redesign of the way applications and services are delivered. Until now applications have been shrink-wrapped bundles loaded on PCs or individual servers. Going forward, instead of speaking of applications, we expect that the wireless industry will consider "service grids" - collections of separate wireless services that are brought together from across the network.

Also under rapid growth are sensor networks of tiny inexpensive nodes capable of relaying information about their environment, to support business and healthcare as well as national and homeland security applications. The opportunity exists to apply the principles of grid computing to these new power-constrained devices, greatly enhancing

their capabilities through ad-hoc aggregation of available resources, where network links between nodes are based on physical proximity and dynamic network configurations at any given point in time. Furthermore there are opportunities to make wider grid services available to mobile devices and the advanced data gathering abilities of sensor networks available to the wider grid.

This vision raises significant challenges not the least of which is ensuring that the networks are trustworthy despite the limited capabilities, in both processing and battery power of the mobile devices. When grid computing and wireless networking are combined, trustworthiness and feasibility challenges increase exponentially. However, the integration of these wireless devices into the Global Grid will result in benefits with increased resources extensibility such as increased network bandwidth and demand for new and better ways for computation.

3. Applications and Use Cases

At this early stage in our research we are beginning to develop an understanding of classes of applications, which the wireless grid may make possible. The applications fall into three sometimes-overlapping classes:

- Applications aggregating information from the range of input/output interfaces found in nomadic devices.
- Applications leveraging the locational and contextual characteristics in which the devices will be found
- Applications leveraging the mesh network capabilities of groups of devices.

Wireless devices such as mobile phones or pagers can be used as sensors or captors in new and interesting ways [Hwang 2003]. The wireless grid team is exploring medical applications of these sensors. Also regarding the quality of wireless connection of individual mobile phones, very small interferences like the movement of body parts and heartbeats can be detected with 90 percent certainty within 50 cm distance of human body to produce valuable information of pulse and breathing rate for healthcare applications. The enormous overload of data captured say; every millisecond can be structured along a Grid network to provide this capability. This research work is being developed by Helsinki Institute of Physics [Tuisku].

Another typical application scenario could be downloading audio/video content to mobile devices. A user has an open session from a PDA terminal connecting to Internet sites via a Wireless LAN. Applications are multimedia intensive and include some download and streaming of audio and/or video. As the user travels outside into a congested bandwidth area, higher data rates, potentially resulting in higher quality, are not available. In order to control congestion and maintain service, one mechanism would be to utilize devices available within the Grid network to maximize bandwidth and also delivering acceptable QoS with control.

Resource sharing amongst mobile devices would enable innovative applications. One

exciting class of application could be built around the Input-output resources, which will be available on these devices [McKnight 2003a]. Consider this scenario: *A group of friends meet for a night out clubbing and head out with their devices. During the evening two friends capture footage of their friends dancing from two different angles. They then instruct their devices to render the footage into a montage according to predesigned templates. The devices discover one another, exchange meta-data on the footage available and discover the devices of the friends and others in the club for assistance in the processor (and thus battery) intensive rendering of the footage. Once this has been completed the device access the video screen provided by the nightclub and request that their footage be shown – to the great enjoyment of their friends. [McKnight 2003a]*

4. Characteristics of Wireless Grids

Wireless grid application requirements may have significant effects on advanced network architectures. Research on wireless power-constrained device and grid application requirements may also help clarify some of the remaining critical research challenges to be overcome [Park 2003]. One key area of research is the design of a resource discovery protocol that fits in with the fast changing environment of a wireless grid.

Ian Foster [Foster 2001] discusses the virtual nature of organizations built around distributed computing because the boundaries of the physical organization are ephemeral when working in a distributed computing environment. Business partners can be incorporated into a virtual organization at will; users of like interests can form into their own virtual organizations. The mobility of small, wireless devices create tremendous opportunities to grow the diversity of devices and users that utilize the grid, and enhance the services available on the grid. These mobile devices have very different constraints than typical grid servers and clients. Their communication and computation abilities are limited because of power constraints, small screen real estate, and the transitive nature of their connection to network infrastructures. Once integrated into the grid, we expect that this new generation of small, mobile devices will enhance the benefits of belonging to a virtual organization.

Wireless grid networks inherit the three main characteristics of the general grid in a wireless networking environment: 1) decentralized resource coordination 2) standard and open service and protocols 3) nontrivial QoS support [Foster 2002a]. However the ad-hoc dynamic nature of small mobile devices differs from traditional grid servers and clients.
In this paper, we propose that decentralized resource coordination could happen through markets and their enabling mechanisms. These markets will consist of heterogeneous and dynamic resources that need to be coordinated (not centrally) in wireless grid networks. Devices and users of devices will come and go, altering the services desired, and the variety of those grid services and applications offered on the local wireless portion of the network. This ever-changing virtual marketplace needs dynamic methods of service discovery because of the ad-hoc nature of wireless network devices. Methods for identification and ultimately protection of intellectual property are also needed for robust

wireless grid markets to emerge [Uzuner 2003].

5. Sharing Protocol

This section describes in detail the "Sharing Protocol" for ad-hoc resource-sharing agreements.

5.1 Resource Description

Before any group of devices can discuss their needs and available resources they must agree on the manner in which they are to describe these resources. There are a variety of schemes available for the description of resources, none of which cover all resources but which together define the resources that are to be shared. For example, if a group of devices wishes to be able to share processor cycles they must first be able to describe the processing requirements. Resource description protocols are included in standards such as the IETF's ZeroConf, Universal Plug and Play, the Grid Resource Description Language (RDL), standardized service specific definitions using the Web Services Description Language (WSDL) and bandwidth descriptions from various QoS standards (RFC). Different resource sharing systems undertake the task of resource description in different ways, for example P2P music sharing networks utilize the file name to describe the resource using, to various levels of standardization, the artists and song name.

5.2 Resource Discovery

Once language for description has been agreed, devices are able to formulate their needs and publish their resources – this is the abstract process of Resource Discovery. Different resource sharing systems accomplish this step in different manners, for example the Globus system utilizes the Meta Directory Service (MDS) which is based on the Lightweight Database Access Protocol (LDAP) while the Web Services community has defined the UDDI [UDDI] and its associated protocols to provide a database of services available. ZeroConf uses multicasts through the LAN.

5.2.1 Distributed UDDI Approach

Once a Web Service is deployed, other applications and Web Services can discover and invoke that service. Also, technologies like the Java 2 Micro Edition (J2ME) [J2ME] contain specifications (Midlets) developed for wireless devices like pagers, mobile phones and PDA's for smaller virtual machines and leaner API's. If Information Resources of a wireless device or even device parameters can be made as "Web Service" stored in a Distributed UDDI registry with descriptions about usage and the services they offer in XML, then potentially device "yellow pages" are created that are made available to other roaming ad-hoc devices. [Hwang 2003] The distributed UDDI approach also enhances non-grid wireless devices to discover grid-enabled wireless devices. Properties like location based device discovery or resource based device discovery are probable

enhancements with information resources dynamically updated in distributed UDDI nodes. [McKnight 2003a] Figure 1 provides an example of a resource based MIDP Midlet application that is published as a "Web Service" in a distributed UDDI for Midlet groups. The example outlines a simple "speech-to-text" conversion Midlet loaded in mobile devices, which can be located through the distributed UDDI. It also provides protocol binding information (SOAP binding), application specific details and finally URL's for downloading. We are currently working on creating a resource generic protocol with API's for a distributed UDDI for non-grid and grid enabled.

```
<wirelessEntity wirelessKey="some-key"
          operator="www.syr.edu/~jshwang/wirelessGrid/uddi"
          authorizedName="paravamu">
<discoveryURLs>
  <discoveryURL useType="wirelessEntity">http://www.syr.edu/~jshwang/wirelessGrid/uddi/
get?wirelessKey=some-key</discoveryURL>
  <discoveryGroups>Midlet Groups</discoveryGroups>
 </discoveryURLs>
 <deviceName>Sharp-3G-PDA-Type-CellPhone </deviceName>
 <description xml:lang="en">PDA-style 3G cellular phone with Bluetooth capability
 </description>
 <contacts>
  <contact useType="Owner">
   <personName>Praveen Aravamudham</personName>
   <phone useType="Founder" />
   <email useType="Founder">paravamu@syr.edu</email>
  </contact>
 </contacts>
<wirelessServices>
  <wirelessService serviceKey="some-key"
            wirelessKey="some-key">
   <name>Speech-to-Text conversion Midlet</name>
   <description xml:lang="en">Provides a dynamic speech to text conversion</description>
   <bindingTemplates>
    <bindingTemplate bindingKey="some-binding-key"
              serviceKey="some-key">
     <description xml:lang="en">SOAP binding for speech to text conversion</description>
     <accessPoint URLType="http">http://www.syr.edu/~jshwang/wirelessGrid/uddi/
      speechtotextmidlet</accessPoint>
     <tModelInstanceDetails>
      <tModelInstanceInfo tModelKey="some-model-key" />
     </tModelInstanceDetails>
    </bindingTemplate>
   </bindingTemplates>
  </wirelessService>
 </wirelessEntity>
</wirelessDetail>
```

Figure 1. A distributed Location-Resource based UDDI entry.
Source: Aravamudham and Hwang 2003

5.3 Clearing Mechanisms

A resource sharing transaction has as its third step a clearing mechanism. By this we refer to the conditions under which a partner device (or group of devices) will extend access to the requesting device or group. We use the term "clearing" in its economic sense where it refers to the action (usually payment) required to "clear" or settle a market transaction. [McKnight 2003a] Currently most resource sharing systems do not implement complex conditions for access to resources. Typically access to resources is granted based on the ability of a device, service or user to prove membership of an appropriate class – this is

commonly known as the process of authorization. Common protocols for this step are Kerberos and x509. This is the clearing mechanism identified with B2B partnerships and virtual enterprise formations. We identify this as a free exchange based on community membership.

P2P sharing networks typically employ some form of quid-pro-quo exchange on their users. This sometimes means requiring users to run the full client which means that they are, in exchange for access to the network and by default, making the files which they download available for sharing. Other systems, such as Kazaa, provide superior service to network nodes that are sharing files. We identify this clearing mechanism as an indirect Barter arrangement. A anticipate resource sharing situations in which a barter of available resources, for the period of their use, will make economic sense. This might occur in a situation where the power is effectively being traded. This is an aspect of the virtual market that we intend to build economic models and simulations to study.

B2C Web Services are typically conceived as market based in that access will be based on clearing the transaction via a financial payment – whether this is transaction or subscription based. We anticipate that the development of true virtual markets with their associated financial negotiation protocols, payment schemes will be of use to wireless grids and provide market based clearing mechanisms.

Each of these economic transaction types will be modeled and studied.

5.4 Coordination Systems

They are systems that actually allow one device to utilize the resource of another device, or permit the pooling and scheduling of resources. Each resource potentially has a range of suitable mechanisms. For example, if the resource being shared is disk space then the coordination mechanism might be NFS, Samba or WebDav, if the resource being shared is processor cycles then the coordination mechanism might be the algorithms embodied in the distributed.net or the Globus Grid Resource Allocation Manager (GRAM).

5.5 Trust Establishment

The establishment of "Trust" is essential for any resource sharing transaction. However it is our contention that this cannot usefully be abstracted as a unique step of a transaction. This is because each element in a transaction may require a different type of trust establishment. [McKnight 2003a] For example in order to provide a description of your available resources you may wish to be certain of the identity of the device or user that you are talking with, perhaps via an institutionalized identity system such as PKI or Kerberos. However this trust establishment may be very different from that required in order to have assurance in the results of code executed on a cycle aggregation system, which might involve, as is done by SETI@HOME, the checking of duplicate data units by other clients of the distributed system. We therefore do not model trust establishment as a step in an abstract resource sharing transaction – rather it is a process incrementally

distributed throughout the process. However we do recognize that a requirement of any negotiation process is to be assured that the identity of the partner with whom one is communicating does not change during the process or from step-to-step. There is no sense undertaking a complex clearing negotiation if the device, which utilizes the agreed coordination system, is different from that which was cleared. In other words, resource-sharing transactions must be resistant to highjacking. Therefore we add as an element the use of a system that can assure the partners of at least a persistent anonymous identity. This is similar to the problem identified with MobileIP systems, which must be sure only that the device requesting a change in the redirection of packets is the same device that was previously known to it [Bradner et al].

6. Middleware Architecture for Wireless Grids

An architecture to support large numbers of mobile devices in a computational grid must address issues such as device heterogeneity, low-bandwidth, high-latency connectivity; possibly extended periods of disconnectivity; device power consumption; and software interoperability [Tuisku]. In order to present these challenges in a tangible manner and to suggest appropriate research directions, we are currently conducting research on a clustered architecture that utilizes new and convergent "Web Service" technologies, J2ME frameworks for minimal device computations and maximum use of Grid technologies through Globus. A middleware architecture for wireless grids could mainly deal with the network and QoS adaptation between the wireless devices and network infrastructure. The prototype under development runs the Globus middleware and interacts directly with the Monitoring and Discovery Service [Czajkowski] of the Global Grid through dynamic SOAP request/response mechanisms to communicate the availability of resources in the nodes, which it represents. Information Resources available within a wireless device can be published as a "Web Service" to other peer devices. In the case of resource-constrained devices, a proxy could have the intelligence to take into account the order in which the job was submitted, what nodes are available and will take the responsibility to maintain the required QoS with any change in environment. [Hwang 2003] It could also do monitoring of the mobile nodes, providing measurement and reporting on actual QoS being delivered. The proxy serving the resource-constrained devices could also be responsible for making the necessary reservations on the resources and enforcing it, when it receives a request form a node on the Grid. The proxy could also take the responsibility of making and enforcing reservations for the requested resource and lastly for terminating or canceling reservations for this resource once the requested tasks have been completed, or if the node cannot offer its resources for sharing.

6.1 Power Efficient Routing for Wireless Grids

Providing a power efficient routing mechanism is an essential issue for wireless grid networks when most devices are power constrained. This may be an area where insights from the advanced networking research community can be especially relevant to further

development of grid computing applications and services. Many wireless ad hoc routing protocols have been proposed for wireless network connectivity and a variety of bandwidth related performance studies have been done. However, the power efficiency issue still needs much more exploration for integrating power efficient capability into wireless grids. In the early stage of the wireless grid project, we are studying the critical power consumption characteristics of current routing protocols. It has been shown that the power efficiency of ad hoc routing protocols is highly dependent on the mobility and traffic pattern in the wireless grid it is running on [Chang 2001, Chen 2003].

The research team is characterizing mobility and traffic models for wireless grids, and intends to propose a power-efficient resource-sharing infrastructure.

7. Security and Trust

This section focuses on the security architecture of 802.11 by examining the WEP (Wired Equivalent Protocol) used for security services in 802.11b, bringing together various analyses to study the shortcomings of WEP thus suggesting recommendations that could improve the security architecture. The intent is to offer an example of how trust in wireless grid networks can be threatened, and improved [Park 2003].

7.1 Limitations of WEP

WEP is a security protocol that was designed, complying with the criteria defined by 802.11. Over time the shortcomings of this protocol were exposed. WEP is based on RC4 [Riv92] cryptographic algorithm developed by RSA Data security Inc. WEP is a symmetric algorithm in which, both the client and the access point have the same WEP key Usually, the WEP key length is either 64 bits or 128 bits.

WEP provides limited security to WLAN this is because of the drawbacks in the RC4 algorithm it uses. One of the most critical drawbacks in the algorithm is associated with the IV (Initialization Vector). Firstly, many access points (especially from the same vendor) share the same IV in plaintext. Therefore, an attacker can easily collect an IV and use it to retrieve the WEP keys for different access points. Some systems generate the IV sequentially, which are incremented with the transmission of each packet. This was later addressed by few systems that incorporated random generation of the IV. However, this is still vulnerable as long as they continue to share the first IV value (which is default for systems produced by the same vendor).

Secondly, the length of the IV is not long enough. Currently, the length is limited to 24 bits. Thus there are only 224 possible combinations, which guarantees that a single IV value will be used for multiple packets in networks with heavy wireless traffic. Depending on the amount of activity over a company's WLAN, a single IV value could be used many times in a given day.

Thirdly, WEP only encrypts the data units and not the IV or the header fields. The IV is

sent in plain text; hence it is visible to anyone. This means that attackers can see the first 24 bits of every key. Although the industry has concentrated in increasing the number of encryption bits from 64-bit to 128-bit, 152-bit, or 256-bit encryption. However, this does not address the shortcomings of the unsafe IV at any key size [Walker]. Furthermore, WEP's implementation of CRC-32 adds to the shortcomings of the protocol. To maintain data integrity called Integrity Check Value (ICV) this field is not encrypted and could result in "Side Channel" attacks

Another issue associated with WEP is static WEP keys, which compromises the security of the network. If the laptop is stolen, the key could be recovered and used at will. In a given WLAN infrastructure due to complexities associated with key management the keys remain unchanged for long periods of time this further compounds the problem. Dynamic key management solutions could help in addressing key management and mitigate the threat of WEP keys falling in undesired hands.

Finally, WEP encrypts all layer-3 information but it does not encrypt the packet header containing the MAC address, which is sent in clear text format. This MAC address can easily be used to build "man in the middle attacks" on the network. As seen from the above set of analysis, WEP provides inadequately weak security to WLANs. The solution lies not in repairing or working around RC4 but in replacing the algorithm with a new one that not only fulfills the 802.11 specifications but also offers stable solutions to the above problem. There are a number of systems that adopt this approach, which we examine in the following section.

7.2 Potential Security Solutions in Future WLANs

This sub-section discusses a few protocols/standards developed to counteract the limitations associated with WEP, which may undermine trust in wireless grids.

7.2.1 Temporal Key Integrity Protocol (TKIP)

The known security problems of WEP are addressed by TKIP [Housley, Whiting] in 802.11i, which was initially called WEP2. It attempts to secure the IV by introducing IV hashing (random IV generator). This offsets any attempts made by the hackers to identify the WEP key by snooping on the packets that are being transmitted. TKIP offers enhanced data integrity, without TKIP it would be possible for an unauthorized user to modify the traffic by introducing packets that can enable him to crack the key; TKIP uses message integrity check to prevent this from happening. Per-packet key mixing rules are also defined in TKIP to further strengthen the security. The above modifications do increase security, however, they also take up more CPU cycles and cause some degradation in the overall throughput.

7.2.2 Advanced Encryption Standard (AES)

AES (Advanced Encryption Standard, [Nechvatal]) is a Federal Information Processing Standard (FIPS) Publication, which details the cryptographic algorithm to be used for all government documentation. The encryption algorithm selected is Rijndael [Daemon]. It has been selected based on security, performance and flexibility. The use of AES in WLAN would be a major advancement over the existing WEP protocol. Its design is based on the criteria laid down by 802.11 but it makes an attempt to overcome the pitfalls of WEP at the cost of increased CPU cycles. Since most of the systems today use 802.11b (11mbps), which has an average throughput of about 5.5 mbps an increase in CPU cycles could mean an overall system that will not be able to withstand burst traffic.

7.2.3 IEEE 802.1x and EAP

The 802.1x takes advantage of the EAP (Extensible Authentication Protocol, [Blunk]) and is under development by the task group I of the IEEE 802.11 committee. 802.1x uses a "client port" to enable authentication to take place. During authentication only 802.1x traffic is allowed to pass though the port as defined by 802.1x and the authentication is defined by EAP. Since there are no established standards defining EAP, it is subject to vendor interpretations. Implementations of EAP must define the user authentication mechanism and the underlying encryption protocol to bring about this authentication. Typically this method uses a background authentication server, which could be a domain controller such as a RADIUS server in conjunction with an LDAP server.

In this architecture, the authentication server handles the authentication while the access point shall acts as a forwarding agent. When the client requests an association with the access point, the access point first initializes a port for 802.1x traffic to pass through. It then forwards the request to the authentication server The authentication server requests an EAP identity from the client; on receiving the client's response it then sends an authentication request. If the client's response is a success this information is passed on to the access point, which now opens the port for the client's data traffic to pass though.

7.3 Digital Fingerprinting

Recent technological developments have created new challenges for the protection and enforcement of intellectual property rights, which could be exacerbated by the emergence of wireless grids if innovative solutions to distributed digital rights management are not developed to proactively address this challenge. The amendments to existing legislation in response to these technological developments, and legal and academic reactions to these amendments, indicate that existing laws cannot be easily extended, applied to, and enforced on new networks and media [Uzuner 2003]. So far, efforts to protect digital intellectual property have focused on protecting copies of works by preventing unauthorized uses. We agree with Gerovac and Solomon that protecting copies is not equivalent to protecting revenues. Revenues can be protected even if copies are not. One way of protecting revenues is by tracking the distribution volume of works. We propose a

distribution volume tracking system, which keeps track of distribution volume of works by identifying, and verifying their unique fingerprints based on their content and expression. [Uzuner 2003] For ease of communication, we refer to this system simply as DVT1. The DVT system described in this paper extends existing proposals to implement "non-commercial use levy" to ensure proper compensation to authors for works distributed in networks. The purpose of this DVT system is to ensure that content owners are compensated proportionally to the level of use of their works. We believe that DVT systems combined with payment mechanisms provide a potential solution to the digital copyright problem on many networks including wireless grids. The solution supported by DVTs ensure proper rewards to copyright owners while increasing the value the content users can extract from creative works.

7.3.1 Distribution Volume Tracking Systems (DVT's)

A distribution volume tracking system could offer a solution to the digital copyright problem for wireless grids. Such a solution if properly designed would take both the worries of the content owners and the interests of the content users into consideration. It should allow the users to use original works without infringing copyrights while providing the content providers with the peace of mind they need in order to publish their works. [Uzuner 2003]

We believe that while the worries of the content owners regarding loss of their revenues are not groundless, focusing on protecting revenues is not equivalent to protecting copies. As also argued by Gerovac and Solomon, revenues can be protected even if copies are not. To protect revenues, Gerovac and Solomon propose the use of digital tracking technologies [Gerovac].

We agree that digital tracking is on the right path to contribute to a solution to the digital copyright problem. However, given our goals of protecting privacy and fair use, we propose limiting the scope of tracking mechanisms to simply the distribution volume of the content. [Uzuner 2003]

Most work related to digital tracking has used digital headers that identify a work, making tracking works very easy. However, digital headers can easily be removed or altered, preventing identification of works. As an alternative to headers, we propose using fingerprints.

DVT mechanisms that can fingerprint works based on their content and expression and identify works based on these fingerprints can facilitate revenue protection. These mechanisms complete the compensation systems that are based on the rate of circulation of works in networks, by providing accurate information about distribution volumes.
We envision DVT systems as having two components: Fingerprint generator and Fingerprint verifier.

The fingerprint generator analyzes the content and expression of a work and creates its unique identifier based on these features. [Uzuner 2003] The fingerprint verifier checks the fingerprint and recognizes the document using this information, keeping track of its rate of distribution. The fingerprint generator and verifier are intended to work together to recognize slightly modified versions of the same work and label them as similar.

As a proof of concept, we are currently working on building fingerprint generators and verifiers for text documents. [Uzuner 2003] We are using natural language processing techniques to identify the unique fingerprint of each document, in terms of its content and expression. We are experimenting with different ways of forming this fingerprint, so that slightly modified versions of the works can still be recognized as similar.

So far, we have identified and automated extraction of 24 elements of expression and content of documents. [Uzuner 2003] These elements include stylistic features that indicate the expression of an author, as well as content-based features that indicate the tone, affect, or position presented in the documents. We hypothesize that some elements of expression are unique to authors, and would help us identify the work of a certain author. On the other hand, some elements of expression are unique to a domain, and all documents in the domain have to share the same expressions to a certain extent. The unique fingerprint of the document must be determined by the combination of the expression of the owner and the expression dominant in the domain of the document.

8. Business Models for Wireless Grids

This section identifies and examines key components of business models of virtual markets in the wireless grids [Gaynor 2003].

8.1 Information and Resource Sharing Marketplace

Wireless grids can create a virtual market where voluntary users share their information and resources thanks to the networked environments evolved from distributed ad-hoc wireless devices and systems. [Gaynor 2003] As in various P2P file sharing network initiatives, such as Napster, Gnutella, Morpheus, Limewire, Freenet, etc, a wireless grid can evolve as a voluntary marketplace where voluntarily motivated (with their own responsibilities and risks) users come and share their resources. A technical architecture for this kind of virtual market for sharing resources would follow from open source software-based approaches to application development and employ distributed management in order not to create any concentrated risks and responsibility. Each user node would have control over its self-organization, routing and other control functions for managing these ad hoc networks. Gnutella is one of the popular examples to create the sharing place in this way. In the Gnutella network, each node manages the membership and conduct search to form P2P networks. Public or pseudo- Public memberships (where no individual user has responsibility in the public group) and their value added service would generate revenue (or value) source for this kind of business functions of virtual market. Also, this public place would become a good marketing and meeting place (such

as in newsgroup in the Internet) to advertise private sharing opportunity where robust and closed transactions are possible. Again, business values would not directly come from the information and resources shared but from the network values (network externality) improved thanks to such open sharing in this place. [4] For this virtual marketplace to function effectively, openness, interoperability, scalability and security are key technical issues requiring further research.

8.2 Collaborative and Cooperative Marketplace

Wireless grid networks (resembling P2P networks) can provide a space for people to collaborate on projects that require a number of participants. The traditional approach is to use a single computer that stores all data and participants make modifications directly on this central server. Scalability becomes critical especially for the large population collaboration in such places. [Gaynor 2003] Similarly the processing necessary to handle these requests can make the application unstable. Ad-hoc based wireless grid and P2P networks can eliminate these problems by having the processing and the data spread among all the participants. Groove Networks is an example of P2P networks employing resource sharing and coordination for collaborative editing services. The revenue source can directly come from various applications and software to support this type of P2P networks.

9. Policies for Wireless Grids

This section addresses emerging social, significance, and policy divides potentially emerging from the nascent development of wireless grids.

9.1 Public Policies for the Grid

The pace of development and deployment of the Grid will depend upon many different factors, including how quickly the computer and telecommunications industry agrees upon standards for the Grid, how quickly the basic technology matures, how aggressively companies invest in the infrastructure needed for the Grid, how many cost-effective, compelling Grid applications are developed, and how quickly potential users of the Grid accept and adopt this new way of purchasing computing resources [Nelson]. Government policy can influence each of these factors. Just as the pace of development of the Internet has varied by country and industry, the pace of development of the Grid will vary widely, influenced by the policy environment and the stage of economic development. It is clear that governments can do a great deal to ensure that the Grid is available to different classes of users, including:

- Funding the creation of Grids for university researchers;
- Harnessing Grids for distance education, e-learning, and continuing education;
- Adopting telecommunications policies that foster investment in the high-speed networks for companies and organizations of all sizes to use the Grid;
- Revising procurement policies in order to encourage government agencies to make use of Grid computing rather than investing in more IT hardware; and

"Future-proofing" policies on e-commerce and e-government to remove potential barriers to the widespread use of the Grid (just as laws on signatures, contracts, advertising, and consumer protection had to be updated to accommodate the Internet).

In addition, it is clear that the Grid could raise some new policy challenges in several areas, including intellectual property protection, liability, privacy, and security. Since the technology is evolving so quickly, it is critical that policy makers start today to explore the implications of the Grid.

9.2 Nomadicity Divide

The creation of virtual markets for the trading in a wireless computation and communication grid of services including information access is progressing in fits and starts. Peer to peer computing similarly has seen significant failures of business models and practices (e.g., Napster). At the same time, industries such as music and film have failed to prevent, or profit from, massive sharing of content on a global scale. Few have considered the significance of these trends from the perspective of the benefits of international development of knowledge networks. We postulate that a wireless grid could both help alleviate and exacerbate these challenges, if efforts are not made to bridge the nascent Nomadicity divide [McKnight 2003b].

The Nomadicity divide engendered by unequal access to wireless grids cannot be prevented from occurring, as early adopters who have strong needs, and deep pockets, gain early access to advanced technology. But the growth of grassroots peer-to-peer information flows points to the potential for social innovations to come from the other direction. As the two forces collide in wireless grids, policy makers, business and technology leaders, as well as scholars across multiple disciplines, in developed and developing economies, would do well to ponder technical and social solutions for the challenges posed by emerging wireless grids.

9.3 Policy Problems for Grids

This section addresses problems like quality of the service, reliable delivery of goods and services of wired and wireless grids through a high-performance, scaleable and extensible system, which requires interoperability of the involved devices in order for the grid and the markets to function properly [McKnight 2002a].

9.3.1 Quality of Service Parameters

One of the main concerns is the provision of end-to-end QoS for all available resources at all levels within the wireless grid. There is only a limited understanding of how the quality of end-to-end broadband services might be assured in today's nascent multi-service, multi-provider environment. The absence of generally accepted and standardized mechanisms for assuring service quality is a significant barrier to

competitive broadband access. A key question is how to optimally manage QoS for virtual markets in a wireless communications grid. In implementing a framework, which encompasses all the QoS requirements, we need to define the mechanisms, which will govern the requirements. Our framework will need to effectively map the pre-defined QoS requirements to the actual resources on the network. Ideally some of these QoS requirements will be defined at the local system level to minimize protocols utilized at the middleware layer, however we need to address the problem of combining different kinds of QoS from the multiple resources available in the grid and between multiple grids.

9.3.2 Guaranteed Service/Differentiated Service

Current Internet protocols offer simple point-to-point delivery service, based on the best effort delivery model as the network's guarantee that the data will be delivered using the Internet protocols. However within the grid, where dynamic relationships are continuously being created and destroyed, and where real-time access to data is required, the traditional best effort model is no longer adequate. Differentiated service (though service for priority traffic is not guaranteed) offers a more reasonable solution for the grid network than Guaranteed service, however the challenge lies in defining the policies governing priority levels within a wireless commercial grid.

9.3.3 Performance Related Issues

The peer-to-peer platform offers some amount of fault-tolerance since no single entity can bring down the entire system. However, beyond the issues of availability, latency and bandwidth when measuring network performance, certain characteristics of wireless transmission – such as shadowing, multi-path effect, fading, interference, etc – need to be addressed. For a specific station to transmit successfully, a proper power level is required. In cellular systems, every mobile station has to communicate through a base station; therefore it is feasible to achieve uniform SINR (Signal to Interference and Noise Ratio) for all communication links. Power control in existing cellular systems is easier than that of systems that utilize a shared broadcast channel, as ad hoc networks typically do; the higher the power level, the better the transmission (or throughput) for the link. However, a powerful link may interfere and limit the ability of other stations to receive from other transmitters, thus reducing the total throughput of the network.

9.4 Public and International Policy Issues

The Internet is a geography-independent system. The wireless grid shares this property of the Internet. This section addresses several jurisdiction based laws and regulations such as taxes, for example, which are more complicated to administer in these domains.

9.4.1 Clear Jurisdiction and Geography

The grid environment places service providers on a global competitive basis – users and service providers are no longer restricted to providing service for users based on their geographical location. Would grid entities operate within the regulatory framework of the local location? Currently the legal and regulatory framework governing online transactions (across geographical borders) is still evolving. [McKnight 2002a] How can consumer protection and antitrust laws be adequately enforced (by a country's local federal agencies such as the FTC in the U.S.) within the grid environment? [Nelson]

9.4.2 Major Stakeholders

In deciding on proper policy architecture for the wireless grid, we need to consider the concerns of the following stakeholders.

Consumers and end-users:
In order for consumers to get the most out of the grid experience, the grid has to offer them the levels of security and privacy they are accustomed to. In addition, the service has to be reliable and the delivery of the goods and services to the right person at the right time has to be guaranteed. Of course, the cost of using the grid is also factors into the decision of the consumers to use the grid. Finally, the laws and regulations governing the grid and the transactions that take place over it affect the quality of the grid experience for the consumers. Some related laws are intellectual property laws and tax laws. [McKnight 2002a]

Commercial entities that want to provide goods and services through the grid:
These entities have overlapping concerns with the consumers. They are concerned with security of the transactions and the correct delivery of the goods and services to the right place at the right time. Also, the grid has to provide them with proper profit incentives if the commercial entities are to provide services over the grid, i.e., the cost of delivering over the grid should not be greater than the profits obtained from using the grid. Also, due to the vague definition of jurisdiction in a wireless environment, the laws and regulations that protect the commercial entities from improper interceptions, fraud and theft should be clearly defined.

The owners of the grid infrastructure:
The grid provides an exciting challenge for the infrastructure owners. In order to be worth the cost and the effort, the infrastructure has to meet certain criteria. It has to be secure, both for the end users and for the infrastructure owners. It has to be scalable and extensible. It has to be able to accommodate a heterogeneous set of devices and a heterogeneous set of services, addressing the diverse needs of different users. It has to ensure interoperability and it has to do all of this in a cost efficient way.

The service providers operating on the grid:

Service providers, i.e., the connectivity providers, face interesting challenges with respect to proper pricing of the services they are providing. Do they charge by connectivity time? Or, does it make more sense to charge based on the kind of data that is being transferred? How do people choose which service provider to use and how do the service providers co-operate and collaborate to provide a better service over the grid?

Local, national and international entities, including organizations involved in setting global standards:
The grid offers different challenges for the standards organizations, international entities as well as local governments. For example, how do tax laws apply in the grid? More importantly, whose tax laws apply? On the intellectual property side, if peer-to-peer becomes really prevalent, then who keeps track of what belongs to whom and how? How are the correct amounts of compensation transmitted to the right people in the grid? And finally, assuming we are able to come up with laws that make sense on a global level, who enforces these laws and how?

9.5 Solution Approach for Wireless Grid Policies

We propose to approach the problem of designing and implementing the wireless grid in three main steps:

1. First we need to explore the capabilities of wireless grids to determine protocol options for integrated wireless networks that account for diverse user and device access. At this stage, we will design protocol platforms and models for network performance, service detection and negotiation, security and confidentiality, resource allocation, and device extensibility. The technical feasibility of grid services will be considered based on existing and emerging wireless infrastructure, propagation, software, and embedded architectures.

2. Second, we will explore market issues to determine fair and efficient policy guidelines and profitable business models in the new wireless grid access paradigm. We will develop protocol rules and economic models to predict market performance under multiple wireless grid protocol designs. The presence and role of market failures in wireless grid network economies will be considered as will the potential role of regulation in solving those failures. Fair and efficient policy guidelines will be proposed and profitable business models for network operation and utilization will be considered.

3. Finally, we will establish virtual and community test-beds or simulation environments in order to examine technical performance and market behavior. We will build virtual and/or physical testing environments. Economic modeling scenarios will be overlaid on the end-to-end technical characteristics to create a well-defined picture of the wireless grid environment. Educational and commercial environments may be tested in physical grid-enabled geographies. Regional, national and international markets will be tested in virtual testing environments

Within the three stages outlined above, we will evaluate different network architectures for the optimal power levels for uninterrupted transmission of data and services, the optimal levels of security and privacy, and the ease and effectiveness of using cryptographic primitives and protocols for authentication, digital signatures, anonymous payments, and micropayments. In addition, network architectures need to be evaluated for the usual tradeoffs between efficiency, security, robustness, collection of data that may make the grid more useful or efficient, and protection of the privacy of users.

Management of the grid is another consideration. There are many ways to manage a grid of computing devices, from very centralized, to completely distributed, each style of which has advantages and disadvantages. The grid must promote experimentation with new applications, which implies a need for distributed structure, but the grid must also be efficient, and secure, which argues for centralized management architecture. These tradeoffs must be investigated and an infrastructure designed for wireless grid computing that is both flexible enough to allow innovation, yet still efficient and secure.

10 Conclusion and Future Work

Utilizing the Grid network for dynamic job submission and completion provides an effective path for peer and resource communication in a distributed wireless environment. Also, Virtual Organizations provide a seamless bound layer for peers to begin “trusted interactions” with other peers for information exchange. Compared to the unlimited resource capabilities of multiprocessor computers, wireless devices have far more restrain on computational or storage features. Adapting wireless devices to communicate to Grid networks enables an extensive rich set of capabilities which devices can utilize as a consumer or even as a publisher for other peer device utilization.

In addition to the sharing protocol discussed, providing a power efficient routing mechanism is an essential issue to wireless grid networks when most devices are power constrained. [Chen, Chang] Many wireless ad hoc routing protocols have been proposed for wireless network connectivity and a variety of bandwidth related performance studies have been done. However, the power efficiency issue still needs much more exploration for integrating power efficient capability into wireless grids. In the early stage of the wireless grid project, the team is studying the nature of power consumption characteristics of current routing protocols. It has been shown that the power efficiency of ad hoc routing protocols is highly dependent on the mobility and traffic pattern in the wireless grid it is running on. We are currently characterizing mobility and traffic models for wireless grids, and addressing to propose a power-efficient resource-sharing infrastructure.

The existing WLAN vulnerabilities can, if not properly dealt with, permit unauthorized access into the enterprise network and this increases the security concerns associated with the implementation of the WLAN technology at an enterprise level. Since there is a pressing security need from the industry, we have addressed the existing security challenges and countermeasures by emphasizing planning, design, policies,

administration and configuration. Current WLAN technologies require more robust security services such as those described. In the future when vendors incorporate new standards, such as 802.11i, with advanced security solutions like AES, 802.1x and EAP, WLANs will be more secure. However, the risks a wireless network faces can only be mitigated and not eliminated completely.

A ubiquitous wireless grid will face policy problems on a larger scale than has ever been seen as diverse heterogeneous market and policy requirements must be simultaneously resolved. Governments will seek to strike a balance between public rights to access information and communication networks and commercially viable models of network and service operation. The radio spectrum, over which networks operate, has traditionally been a public good that could be utilized in the public interest, or bought and assigned as a property right for commercial use. The emergence of technologies that efficiently utilize unlicensed spectrum or co-exist with the existing users of assigned spectrum presents a challenge to the established policies. The fair use of a grid network must be determined based on research on how to reconcile the needs for public rights of access and private ownership of network and information resources. Network and information resources and services must efficiently be traded in a virtual market if a wireless grid is to function.

Last but not least, a wide variety of national and international policies will affect the viability of wireless communication and computation grids, in developed as well as developing countries, on and off the battlefield and virtual marketplace. Spectrum management and national telecommunications policies will be crucial for the eventual commercial success of wireless grid services. Other grid requirements significantly affected by public policy choices include easy public access to the grid infrastructure, and legal and economic frameworks for managing property rights for networked resources.

As discussed, the ultimate vision of this interdisciplinary team is the development of an adaptive wireless 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 for wireless devices.

In sum our teamwork thus addresses the following current research areas:

- Integration of grid and web services and its applicability to the realm of wireless grids
- Technical mechanisms for the proposed sharing protocol
- Security and trust for wireless grids
- Commercialisation of the wireless grid – business applications and policy issues

We will inform the GGF as additional research results relevant to Grid High Performance Networking are developed by the interdisciplinary Wireless Grids research team, and welcome feedback and contributions to this emerging research area.

11. Author Addresses

- Dr. Lee.W.McKnight, Syracuse University: lmcknigh@syr.edu
- Dr. Mark Gaynor, Boston University: mgaynor@bu.edu
- Dr. Junseok Hwang, Syracuse University: jshwang@syr.edu
- Dr. Joon Park, Syracuse University: jspark@syr.edu
- Dr. Hwa Chang, Tufts University: hchang@eecs.tufts.edu
- Dr. Amar Gupta, MIT: agupta@mit.edu
- Dr. Bernhard Plattner, Swiss Federal Institute of Technology-Zurich: plattner@tik.ee.ethz.ch
- James Howison, Syracuse University: jhowison@syr.edu
- Praveen Aravamudham, Syracuse University: paravamu@syr.edu
- Ozlem Uzuner, MIT: ozlem@mit.edu
- Bor-rong Chen, Tufts University: brchen@eecs.tufts.edu

12. References

[Anius 2003] Diana Anius, Technology and Policy for Caribbean Wireless Grid Applications, International Conference on Computer, Communication and Control Technologies (CCCT '03)/ 9th International Conference on Information Systems Analysis and Synthesis (ISAS '03), Orlando, Florida, July 31-August 2, 2003, (http://www.iiis.org/CCCT2003)

[Blunk] L. Blunk, J. and Vollbrecht. PPP Extensible Authentication Protocol (EAP). RFC 2284, March 1998.

[Bradner et al] Bradner, S., Mankin, A., Schiller, J (2003) A Framework for Purpose Built Keys An Internet-Draft http://www.ietf.org/ietf/1id-abstracts.txt

[Chang 2001] J. Jabs, C. Hwa Chang, R. Kingley, Performance of a Very Low Power Wireless Protocol, IEEE Globecom 2001, Texas, Nov 25-29, 2001

[Chen 2003] Bor-rong Chen, C. Hwa Chang, Mobility Impact on Energy Conservation of Ad Hoc Routing Protocols, SSGRR 2003, Italy, July 28-Aug 2, 2003

[Czajkowski] K. Czajkowski, S. Fitzgerald, I. Foster, C. Kesselman, Grid Information Services for distributed resource sharing, Proceedings of the Tenth IEEE International Symposium on High-Performance Distributed Computing (HPDC-10), IEEE Press, August 2001.

[Daemon] J. Daemon and V. Rijmen, AES Proposal: Rijndael, November 2001. http://csrc.nist.gov/encryption/aes/.

[Gerovac] Branko Gerovac and Richard J. Solomon. Protect Revenues, Not Bits: Identify Your Intellectual Property. Coalition for Networked Information. (http://www.cni.org/docs/ima.ipworkshop/Gerovac.Solomon.html)

[Foster 2001] Ian Foster, Carl Kesselman, Steven Tuecke, The anatomy of the GRID: Enabling Scalable Virtual Organizations. IJSA 2001

[Foster 2002a] Ian Foster What is the Grid? Three Point Checklist Grid Today, Vol. 1 No. 6, July 22, 2002 (http://www.gridtoday.com/02/0722/100136.html)

[Gaynor 2003] Mark Gaynor, Junseok Hwang, Lee McKnight, Overview of Wireless Grids, International Conference on Computer, Communication and Control Technologies (CCCT '03)/ 9th International Conference on Information Systems Analysis and Synthesis (ISAS '03), Orlando, Florida, July 31-August 2, 2003, (http://www.iiis.org/CCCT2003)

[Housley] R. Housley and D. Whiting Housley. IEEE P802.11 Wireless LANs: Temporal Key Hash.Document Number: IEEE 802.11-01/550r3. IEEE Task Group I. 20 December 2001.http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-550.zip.

[Hwang 2003] Junseok Hwang and Praveen Aravamudham, Bandwidth Management for Wireless Grids, International Conference on Computer, Communication and Control Technologies (CCCT '03)/ 9th International Conference on Information Systems Analysis and Synthesis (ISAS '03), Orlando, Florida, July 31-August 2, 2003, (http://www.iiis.org/CCCT2003)

[J2ME] J2ME: Sun J2ME Framework: http://java.sun.com/j2me/

[Lehr 2003] William Lehr and Lee W. McKnight, Wireless Internet Access: 3G vs. WiFi, Telecommunications Policy, Vol. 27, Issues 5-6, June-July 2003, pp. 351-370.

[McKnight 2002a] Lee W. McKnight, Diana Anius, and Ozlem Uzuner, Virtual Markets in Wireless Grids: Peering Policy Obstacles, 30th Annual TPRC, Alexandria, VA, Sept. 28-30, 2002 (http://www.tprc.org)

[McKnight 2002b] Lee W. McKnight and William Lehr, Show Me the Money. Agents and Contracts in Service Level Agreement Markets, in INFO, February, vol. 4, no. 2, February/March 2002, pp. 24-36 (http://www.emeraldinsight.com)

[McKnight 2003a] Lee W. McKnight and James Howison, Towards a Sharing Level Protocol for Distributed Resource Sharing, International Conference on Computer, Communication and Control Technologies (CCCT '03)/ 9th International Conference on Information Systems Analysis and Synthesis (ISAS '03), Orlando, Florida, July 31-August 2, 2003, (http://www.iiis.org/CCCT2003)

[McKnight 2003b] Lee.W.McKnight “Broadband Divides” March 27-28, 2003 Oxford Internet Institute

[Nechvatal] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback. Report on the Development of the Advanced Encryption Standard (AES). National Institute of Standards and Technology (NIST), October 2000. http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf

[Nelson] Mike Nelson, IBM, "Broadband Divides" March 27-28, 2003 Oxford Internet Institute

[Park 2003] Joon Park, James Howison and Amarpreet Nanda, WLAN Security and Trusted Wireless Grid Research Challenges, International Conference on Computer, Communication and Control Technologies (CCCT '03)/ 9th International Conference on Information Systems Analysis and Synthesis (ISAS '03), Orlando, Florida, July 31-August 2, 2003, (http://www.iiis.org/CCCT2003)

[Tuisku] M. Tuisku, "Wireless Java-enabled MIDP devices as peers in Grid infrastructure", Helsinki Institute of Physics.

[UDDI] UDDI: Universal Description, Discovery and Integration http://www.uddi.org/

[Uzuner 2003] Ozlem Uzuner, Copyright Infringement Detection System for Wireless Grids, International Conference on Computer, Communication and Control Technologies (CCCT '03)/ 9th International Conference on Information Systems Analysis and Synthesis (ISAS '03), Orlando, Florida, July 31-August 2, 2003, (http://www.iiis.org/CCCT2003)

[Walker] Jesse R. Walker. Unsafe at any key size; an analysis of WEP encapsulation. IEEE P802.11. Doc.: IEEE 802.11-00/362, October 27, 2000.

[Whiting] R. Housley and D. Whiting Housley. IEEE P802.11 Wireless LANs: Alternate Temporal Key Hash.Document Number: IEEE 802.11-02/282r2. IEEE Task Group I. 23 April2002. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-282.zip.

Intellectual Property Statement

Full Copyright Notice