Service Discovery Protocols for Ad Hoc Networking

Michel Barbeau
School of Computer Science
Carleton University
1125 Colonel By Drive
Ottawa, ON K1S 5B6 Canada
www.scs.carleton.ca/~barbeau

1. Introduction

There are two types of mobile and wireless network configurations: infrastructure-based configurations and ad hoc configurations. Infrastructure-based networks are more scalable but also less flexible. Ad hoc networks are by definition infrastructure less. They offer flexibility at the price of scalability [Vars 00].

Service discovery protocols are a key technology of mobile and wireless networks. They give to devices the capability to advertise and discover each other's services on a network. For instance, a service discovery protocol equipped palmtop, once attached to a network, can automatically discover a laptop advertising data synchronization services.

There are presently leading service discovery technologies: JINI [Sun 99], Salutation [Salu 99], Service Discovery Protocol (SDP) of Bluetooth [Blue 99], Service Location Protocol (SLP) [Gutt 99], and UpnP [Micr 99].

Service discovery is an issue common to both infrastructure-based networks and ad hoc networks. In this paper, we explore some of the problems of service discovery in ad hoc mobile and wireless networks, namely: architecture, service selection facilitation, and security.

Architecture, service selection facilitation, and security are respectively discussed in Sections 2, 3, and 4. we conclude with Section 5.

2. Architecture

The following terminology is adopted. A user agent (UA) represents a consumer of services, a service agent (SA) represents a provider of services, and a directory agent (DA) represents a store of service advertisements.

For ad hoc networks, it is clear that technologies that can fly without DAs are more desirable. By definition, an ad hoc network doesn't rely on infrastructure. In the sequel of this section, we discuss DA less operation with SLP and JINI.

Figure 1 pictures operation of SLP in a DA less architecture. A UA sends, using UDP above IP multicast or broadcast, a Service Request (SrvRqst) to SAs. The characteristics of the required service are specified in the SrvRqst as a service type name and a predicate over service descriptive attributes. When a listening SA finds a match between a requested service and a service it offers it replies to the UA by

sending a Service Reply (SrvRply) using unicast. The SrvRply contains a Service Access point (SAP) which provides information required by the UA to contact the SA (e.g. name of the protocol).

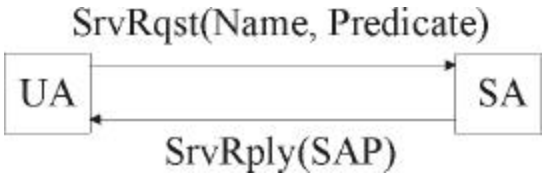

Figure 1. UA and SA interaction.

In JINI, the DA, SA, and UA are respectively called the Lookup Service, Service Provider, and Client. A lookup Service in JINI is not mandatory. For discovery of a service, when there are no Lookup Services, a Client can apply a technique called *peer lookup*.

The client sends a message called identification to request registration messages from Service Providers (the identification message is normally sent by a Lookup Service). The client then receives registration messages from service providers among which one can be selected.

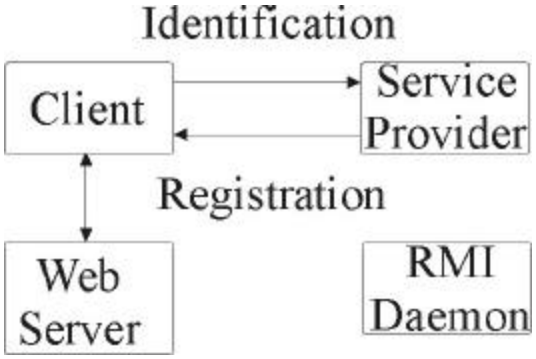

Figure 2. Client and Service Provider interaction.

In addition to the clients and service providers, JINI requires two servers. When a service is discovered a proxy object is downloaded from the service provider. Only the data members are downloaded. The implementation class must be downloaded separately. A Web server is required for downloading the code.

JINI is based on Remote Method Invocation (RMI). A RMI activation daemon is required to start Java server objects on demand. The Web server and the RMI daemon can run on the service provider device.

3. Service Selection Facilitation

When a UA requests instances of a type of resource, the selection of any instance of that resource type will often not suit the needs. For example, given the need to fax a document, several fax machines can be discovered. There is, however, most probably one of them that is more appropriate than all the others because of physical proximity. For instance, two faxes may be discovered but, for a user located on the first floor, the one situated on the first floor is more attractive then the one situated on the twentieth floor. An issue is, how can the selection of the most appropriate service to fulfil a certain need can be facilitated? Service selection can be facilitated with the help of tools. Some approaches are discussed hereafter.

Selection of a service can be facilitated with a service browser. Such a browser is presented in Ref. [Hugh 00]. It provides the user with a view of the available services on a network. Figure 3 illustrates a view in which service access points (SAPs) are listed (upper area) and descriptive attributes of a service are posted (lower area). Using the browser, a user queries the network for a service

and selects one of the found services by visual inspection of the listed SAPs and attributes. The user selects manually the service to use.

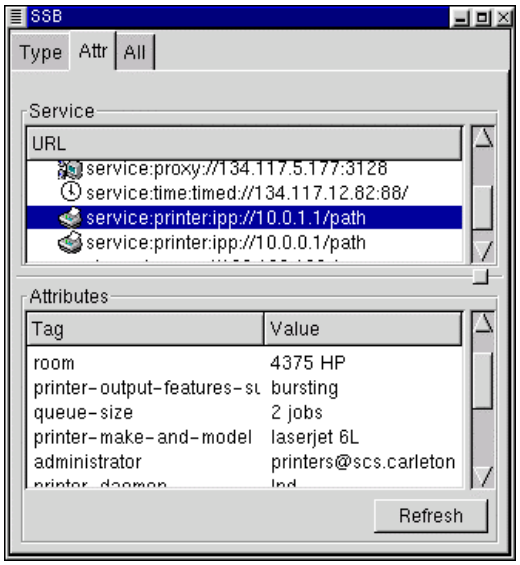

Figure 3. SAP and attribute view of the SLP Service Browser.

Service selection transparency can be achieved. McCormack has developed a mechanism that ranks services with respect to one another [McCo 00]. The rank is determined by a function over the attributes of services. The function is formulated by the user and is a model of the desirability of a service. The service with the highest rank is selected.

Contextual information of the user and services can be used to take a service selection decision Physical location, because of its relevance, is a type of contextual information that can be used to facilitate service selection. Physical location often amounts to physical proximity of the user and service, such as in the same office, same floor or same building. Location tracking solutions based on networks of sensors or triangulation may not be suitable in an ad hoc network environment because of the infrastructure required.

Close proximity can detected as follows. User and service devices may be equipped with infrared ports and use successful establishment of a communication through the infrared ports as a confirmation of proximity.

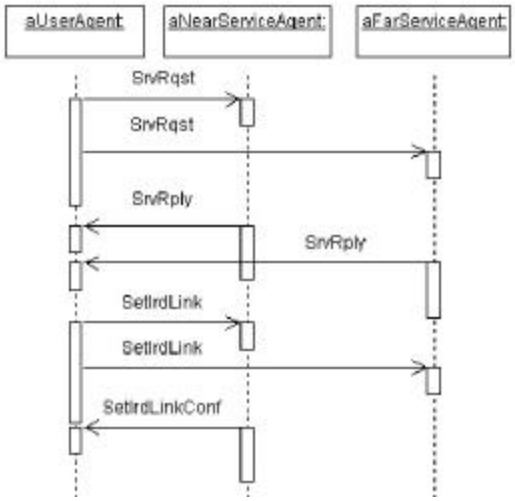

Figure 4. Service discovery and close proximity based selection.

Figure 4 pictures integration of a service discovery protocol with a close proximity based selection protocol. There are a UA, a near SA, and a far SA. They are all within RF reach of each other. The UA sends using broadcast a SrvRqst. It is received by both SAs and they both send using unicast a SrvRply. This completes the service discovery phase. To achieve close proximity based selection, the UA sends using multicast a message called SetIrdLink through the infrared port. This message is, however, received only by the near SA which replies with a message called SetIrdLinkConf. This completes the service selection phase.

4. Security

Theft of service is the actual number one security problem in cellular networks [Riez 00]. A similar problem exists with computer network services. Solution devised for cellular telephony can be applied.

Control of access to services relies on a form of identification. Either a user or a device may be identified. The most desirable form, in the context of service access control, is user identification because it is independent of the device utilized by the user to access the network.

Identification of a user may be done with an identification number entered by the user before a service is accessed. Further automation can be achieved by using instead a fingerprint captured by a biometrics sensor integrated to the device. Although, the number or fingerprint must not be transmitted in clear over the air because they can be copied by malicious listeners. Encryption can be used for that purpose and it is supported by most of the service discovery protocols.

Device identification may be considered equivalent to user identification in cases were the device is a personal belonging of the user. Indeed, in contrast to a desktop which can be shared by several members of a family, a palmtop is a personal assistant. Identification of the palmtop means as well identification of its user.

Secret key authentication can also be used to identify users or devices. Authentication is supported by most of the service discovery protocols.

RF fingerprinting can be used as well to identify a device (more exactly its air interface). It has been observed that radio transmitters that are built according to the same specifications all exhibit unique signal characteristics. The characteristics are obtained by measuring parameters of the signal, e.g. the time-frequency relation of the signal at the start of a transmission.

5. Conclusion

In this paper, we discussed architectures of discovery protocols suitable for ad hoc network configurations, service selection, and security.

Both SLP and JINI can be configured for ad hoc network configurations. On the service selection side, non transparent selection can be facilitated by a browser. Transparent selection can be achieved using a ranking function approach or proximity detection protocols. A security issue is theft of services. Control of access can be performed either through user identification or device identification, when the device is personal and identified to the user.

Acknowledgements

The author would like to thank the following persons who helped to clarify some of the ideas presented in this paper: V. Azondekon, F. Bordeleau, J. Govea, E. Hugues, R. Liscono, and D. McCormack.

References

[Blue 99] Bluetooth, Specification of the Bluetooth System, www.bluetooth.com, December 1999.

[Gutt 99] Guttman, E., Perkins, C., Veizades, J., and Day, M., Service Location Protocol, Version 2, IETF Request for Comments: 2608, June 1999.

[Hugh 00] Hughes, E., McCormack, D., Barbeau, M., and Bordeleau, F., An Application for Discovery, Configuration, and Installation of SLP Services, The 5th Mitel Workshop on Innovation in Technology and Application (MICON 2000), Ottawa, August 2000. Available at : www.scs.carleton.ca/~barbeau.

[McCo 00] McCormack, D., Service Recommendation in SLP, Report for hounours project, School of Computer Science, Carleton University, August 18, 2000. (available from: www.scs.carleton.ca/~barbeau)

[Micr 99] Microsoft Corporation, Universal Plug and PLay: Background, www.upnp.org/resources/UPnPbkgnd.htm, 1999.

[Riez 00] Riezenma, M. J., Cellular security: Better, but foes still lurk, IEEE Spectrum, June 2000, pp. 39-42.

[Salu 99] Salutation Consortium, Salutation Architecture Specification, 1999, www.salutation.org/specordr.htm.

[Sun 99] Sun Microsystems, JINI Architecture Specification, November 1999.

[Vars 00] Varshney, U. and Vetter, R., Emerging Mobile and Wireless Networks, Communications of the ACM, Vol. 43, No. 6, June 2000, pp. 73-81.