Issues in Context-Aware and Adaptive Middleware for Wireless, Mobile Networked Systems

Position Paper

Dr. Joseph Loyall
Dr. Partha Pal
Dr. Kurt Rohloff
Matt Gillen

BBN Technologies
10 Moulton St.
Cambridge, MA 02138

jloyall@bbn.com
ppal@bbn.com
krohloff@bbn.com
mgillen@bbn.com

1 Introduction and Problem Statement

Computing devices, including the obvious PDAs, GPSs, iPods, cell phones and laptops, as well as the less obvious ones embedded inside automobiles, appliances, smart buildings, and even greeting cards, permeate our daily lives. Many of these computing devices are already interconnected and more are becoming so, frequently through wireless connections and increasingly in an ad hoc manner. The devices and users are often mobile and it is not always obvious what devices are present, reachable, and connected.

In an environment where mobile computing devices of various footprints interact over wireless and ad hoc networks, quality of service (QoS) management is necessary to effectively utilize the constrained and shared resources for the complex and feature rich applications that are increasingly found in such environments. Similarly, security is necessary to prevent undesired information leakage and protect against the vulnerabilities introduced by the ad hoc interconnections.

The wireless ad hoc domain and explosion of devices and interconnectivity has introduced additional challenges not commonly considered in QoS management and security research. Whereas QoS management typically considers resources such as CPU, bandwidth, and memory, these new environments must consider additional *resources* that can be constrained and easily overloaded, such as *human attention* and *screen real estate*. Likewise, these environments present new challenges for security mechanisms, for instance *eavesdropping* becomes much easier; *ad hoc discovery* and *transient connections* expose new vulnerabilities and introduce new risks; and increased *distraction* of the user and frequent *changes in situations* opens up more opportunities for compromise.

These additional challenges motivate an emphasis on not only *proactive* and *autonomic computing* (as opposed to computing that is *reactive,* and requires *explicit user inputs*), but *context-aware* and *adaptive* computing. *Context-awareness* involves awareness of characteristics of the user and his situation (that is, his *context*)*,* and *adaptation* covers changing behavior, resource usage, and security settings as the context changes.

This paper presents key aspects, issues, and directions in context-aware, adaptive middleware for proactive computing in wireless ad hoc networked systems, specifically with regard to the QoS management and security aspects of these systems.

2 The Need for Context-Aware Adaptive QoS and Security in Wireless, Mobile Networked Systems

Wireless ad hoc networked systems have the following common characteristics:

- Connectivity is ad hoc and intermittent. Links are formed opportunistically and can be dropped due to range, motion, obstacles, failures, weather, and other factors; communication is often spontaneous, i.e., devices beacon and respond to interrogations.
- Resources are tight. Network bandwidth, computing power, screen real-estate, battery power, memory and secondary storage all are limited.
- Devices and platforms are diverse in terms of hardware as well as technology (e.g., broadcast as well as line of sight communication)

In addition, these systems frequently have the following characteristics due to the *context* or situations in which they are used. First, the user can expend only limited and varying attention on the system. Second, due to mobility, location can change, potentially rapidly and frequently. Third, dynamic and unfolding situations imply changing needs and baseline service requirements. The dynamism also makes a priori established shared secrets or associations harder to manage (limiting the feasibility of solutions such as PKI). Finally, small footprints combined with varying network access and bandwidth imply that there may not always be time or space to load new applications.

These characteristics motivate the need for several inter-related capabilities *built-into* the software of the devices and the systems of interconnecting devices. Clearly, *QoS management* is needed to monitor the limited available resources, allocate the available resources to the most important communication and processing requirements, and to configure critical processing and information dissemination to the resources available. Similarly, *security* is needed to protect information, maintain the integrity of the device's functionality (i.e., resist or tolerate cyber attacks),

and mediate the tension between the *need to share* and the *need to protect* in distributed interoperation that might span many administrative domains or federated enclaves.

But above all, these capabilities need to be *adaptive* as resource availability and contention changes; as the user, device, and system needs and situations change; as security policies and situations change; and as the makeup of the interoperating organizations, domains, and/or participants change (e.g., from a tight community of interest to a loose coalition or consortium). These change drivers collectively form the *context* in which computation takes place.

As an example of changing needs, consider a user of a device with a map imaging application, such as Google Earth. Depending on his mission, resource tradeoffs may force him to dynamically switch among the following:

- A high resolution image of a limited area (bandwidth needed for resolution; CPU needed for rendering)
- Map of a large area (zoomed out), potentially of lower resolution (bandwidth used for more imagery; CPU used for mosaicking and rendering).
- Ability to pan and zoom (size of images requested larger than screen real estate; bandwidth used for more imagery; CPU used for mosaicking, rendering, and user interactions).
- The ability to transmit and receive encrypted images (encryption reduces the efficacy of bandwidth reduction techniques such as compression; CPU used to encrypt and decrypt).

One way to support the adaptation to dynamically manage the resource tradeoffs above is to submit the changes as additional inputs into the policy decision points of the QoS and security management system. To lower the cognitive burden on the user and because neither application nor the user may have the time to *react*, our position is that applications and system should be *context-aware,* and adaptation should be autonomic, driven by the context-awareness rather than explicit user input.

To keep from adding to the memory and processing footprint of every application, the necessary resource monitoring, control, adaptive QoS management and security should be developed in an *adaptive middleware layer* that can manage the resource allocation, changes in information exchange (prioritization, shaping, and configuring information provision and processing), policies, and processing on behalf of the applications in response to changes in QoS preferences, user needs, aggregate system utility, threat situation, and user context. To the extent possible, the adaptive middleware should be provided as *services* or *components* to keep the QoS and security management behavior separate from the functional behavior of the system, enabling each to be developed and to evolve separately, created by QoS, security, and business logic experts, respectively.

3 Issues and Directions in Context-Aware Adaptive QoS Management

A context aware system is one that can sense and act upon attributes of and changes in its environment in conjunction with a level of understanding of the user's profile and mission objectives. While context can be defined broadly, we are primarily interested in context information that affects any or all of the following:

- QoS requirements – Context that changes or determines the desired behavior for a system or user.
- Perception of quality – Context that changes the way quality attributes are perceived, e.g., a high rate of information delivery can be either welcome or distracting depending on the user's context.
- The ability to deliver service – Context that relates to the feasibility and effectiveness of service delivery mechanisms, including applicable security requirements.

We have been researching context-aware QoS management in information brokering systems, in which clients with information to share make it available through *publication*. Clients that need information can request it from future feeds (using a *subscription*) or from archives (using a *query*). Interoperation is based on active management to locate, broker, and administer information between providers and consumers. Information brokering systems eliminate the need to know the address of the source of information, the need to know when the information becomes available, and handling the scale of many one-to-one connections. However, they also raise a challenge pertaining to how to request needed information in such a way to avoid any of the following undesirable situations:

- *Too narrow* a request might return no results.
- *Too broad* a request might overwhelm the requestor with information, burying the most useful.
- *A significant increase in effort to find the needed information.*

Context information can be used to improve the quality of information discovery, brokering, and dissemination. We have identified a large number of context elements, and broken them into the following categories of context elements that can be used to improve the QoS of information brokering and dissemination:

- Context about the human users of the infrastructure, such as location, affiliation, or attention.
- Context about overall mission or system requirements, the roles of each client and/or type of information in them, and the relative importance of elements.
- Client preferences, in terms of importance of information elements and the ranges of acceptable behaviors.
- Context about the resources, devices, and connections in the system, such as display size, memory capacity, variations in communications, and power.

With this context information, the information brokering and QoS management services can prioritize and order information delivery based on which information elements are most important to the user, shape information to the resource availability and capacity of the device, select information processing based on user characteristics and resources, and allocate resources to the most appropriate brokering and client-side operations.

4 Issues and Directions in Context-Aware Adaptive Security Management

Historically, security solutions are rigid and inflexible, denying access by default and granting access according to policies that change glacier-like, and utilizing a fixed set of protections based on past vulnerabilities and that may or may not cover unknown future threats. The following are some research topics that need to be investigated in providing context aware, adaptive security in wireless ad hoc networked systems:

- Despite limited footprint and resource availability, a single way to authenticate, encrypt or sign will not work in wireless and mobile environments. An application may ride over Bluetooth in one situation and over 802.11 in another. Support and strength of link layer authentication or encryption will change, and application level security needs to be adapted accordingly – a capability the envisioned context-aware middleware should offer.
- Because the uncontrollable nature of open/running applications when the platform moves combined with the spontaneous nature of communication (e.g., automatically connecting to or responding to interrogation), a device may connect to two networks at the same time (e.g., a laptop with wireless active plugged into a docking station with Ethernet). Therefore, the envisioned middleware needs to strictly control who can communicate with what.
- To support discovery and mobility of nodes, "spontaneous" communication needs to be allowed. However, this may disclose your location, network or device id and introduce vulnerabilities. Approaches to prevent this can include providing visibility only on discrete time slices and keeping the default level of access at a level that cannot be abused by malicious users
- If the underlying network changes from line of sight (IR or highly directional radio) to WiFi, an application that was sending data in clear text may start broadcasting data in the open. The application needs to recognize the change in context and seamlessly switch to encrypting at both ends with minimal disruption. Once again, the envisioned middleware is the right place to host the required supporting services.

5 Conclusions

As wireless and networked devices have become more ubiquitous, QoS and security management in systems of small-footprint computing devices with ad hoc and mobile interconnections has become more challenging. This management must be autonomic and proactive so as not to increase the cognitive burden on the user. But most importantly, the autonomy and proactive aspects must be *aware of* and *adaptive to* the user *context*. This position paper has introduced some of the concepts, issues, and directions in *context-aware adaptive* QoS and security management. The issues go deeper and the directions broader than we can cover in a short position paper. There are significantly hard problems such as capturing and interpreting user's intention with respect to his current (mission) situation; mediating the differences in semantics, format, units, and rate of context information; combining aspects of context, including those that conflict; and policy driven strategies for responding to changes in context. Advances in any and all of these topics would provide a significant step forward in support for effective *situational-aware proactive computing in wireless ad hoc networks.*