Position Statement for the "Interconnecting Smart Objects to the Internet Workshop", March 25th in Prague

Authors:
Neeli R. Prasad, CTIF, Aalborg University, Denmark
Sateesh Addepalli, Advanced Architecture & Research, Cisco Systems Inc., San Jose, U.S.A.

Introduction

There continues to be an explosion of inexpensive yet powerful devices/ smart objects for the home, office, and other mobile/embedded environments that everyone owns and utilizes daily. The market need is finally aligning with recent advances in wired/wireless networking, and advances in pervasive software platforms. Additionally, advances in IP-based sensor networking and more open-standard Geo-spatial techniques, offers newer ways to realize the potential of interconnecting smart objects to the Internet.

The pervasive applications that will enter the market in 2011 and beyond will span all of the devices we use today, and impact every aspect of our lives…how we work, learn, communicate, receive medical care, shop, drive, play, watch sports, and protect ourselves, while opening up an entirely new world of business opportunities for the entrepreneur, and established corporations alike. Collaborative applications will also join the hard to collaborate environments of public-private-partnerships where dozens to hundreds of entities must work in a secure, but borderless approach (e.g. interworking between different technologies and network domains) to address or capitalize on common community causes from vital resource management of water, energy, and forest to the social inclusion, economic development, and sustainability of large urban centers.

These applications will be powered by a next generation software platform that will seamlessly operate in your home, office, auto and mobile and move with you, as you transition from/to the devices used in each setting. It will run on all wireless/mobile networks, allow devices and sensors to discover themselves in an ad-hoc manner, and form dynamic communities that are hosted on virtualized federated servers running on routers/switches in the home, office and enterprise, while seamlessly interoperating amongst themselves along with any enterprise system, public/private clouds or combinations thereof.

Extreme personalization and immersive experiences will characterize the pervasive applications, which turn mobile and embedded devices into wireless learning machines that can detect (and eventually anticipate) information needs/findings that can be either retrieved (locally or from remote device communities) or distributed to the device communities that have expressed interest in such. For example, based on a user's location, time or day, work or play, these devices or device communities will deduce a user's needs and proactively deliver highly individualized content without requiring the user to "Google", or even think about it.

The authors proposes and looks into the following area to achieve the need for a unified, pervasive platform to bring more intelligence to the networks, ubiquitous access to the applications, running on the ever expanding types of devices that is used and will be used in our daily lives.

Pervasive Platform Architectural/Software Requirements

Pervasive Applications need to be built upon a Pervasive Borderless Middleware Platform that provides object level mobility, which hides network usage decisions from user applications. Applications written on such a platform can run anywhere, anytime, and exchange any type of data without loosing connectivity with any other peer objects, device, router, switch, system, and/or cloud.
In this scenario, anywhere means any device and any network.
In other words, applications can maintain their connectivity context while residing on a mobile device and traversing multiple networks, such as Telco, 3G/4G, WiFi and Bluetooth.
Similarly, applications can maintain their connectivity data and execution context while they move from one device to another device using runtime application migration schemes.
This "follow-me" application state follows the user as they cross network boundaries, or change devices

(home-->mobile-->auto-->office), or the underlying middleware platform decides to utilize a different network for connectivity. The virtualized federated server running on the routers/switches that connect devices and span networks are ideally situated to assist in the migration of application context from device to device.

Increased Network Scalability, Survivability & Discovery

A next-generation platform must enable filtering and analyzing of data at the source to minimize network traffic, handle unreliable and/or limited network connections, and adjust to hardware failures or CPU load.

Therefore, these devices must be able to persist data via a micro relational or objects database. Additionally, the software components or agents running on edge devices need to support multiple wireless protocols (e.g., GSM, CDMA, WiFi, UWB, Bluetooth, NFC, RFID, 4G/WiMax/LTE, etc.) and associated networks (e.g., Telco, Wide Area, Local, Personal, etc.). Ideally, they will dynamically reconfigure themselves to use a communication protocol that best matches the capabilities of their current network connection and the current node(s) they are in communication with. Also via the pervasive platform, devices must support dynamic discovery of services, services provisioned across the various OSI layers running on nodes in the same network, nodes and trusted layers in a federated network, and trusted nodes in swarming and wolf pack networks. Community hosting, discovery of device services, application data persistence, and software distribution are all capabilities that will be provided by advanced routers/switches located in proximity and federated across the networks to greatly augment network scalability, survivability and performance.

Configurable, Adaptable Security Framework

In a ubiquitously networked world, it will often be necessary to maintain data on edge devices. The security concerns facing enterprises today will need to incorporate solutions that extend to a collaborative environment. Pervasive platforms must provide a high level of security to ensure object identification, privacy and protection. This will involve security agents and agent managers that provide capabilities above and beyond the current encryption, authentication, and authorization that are currently employed in today's centralized client server applications.

As with every capability within the pervasive platform, the security capability including identity Management needs to be configurable and pluggable, to allow for adaptable and custom security features specific to the data and/or services being hosted on any particular node. For example, encryption, authentication, and authorization around peer-to-peer and peer-to-group application/event exchanges should all have pluggable security capabilities that tap into the various security services from networks, to clouds and to applications.

Conclusion

Every aspect of the platform's flexibility and support for heterogeneous the nodes, protocols, networks, messaging and discovery capabilities should be fully leveraged in such a scenario.

There is the need for a federated, efficient, high-performance, network-friendly, pervasive platform that provides interoperability, data sharing, mobile collaboration, and seamless "follow-me" content and services across most public and private industries. There is also an equal need to accomplish such while utilizing networks more efficiently, reducing hardware and energy.