Abstract

JXTA is a peer-to-peer technology that enables developers to easily create distributed computing software. This paper describes JXTA (short for "juxtapose") in general and focuses on its applicability for mobile-networked systems. Since mobile devices like PDAs, mobile phones, or laptop computers are much more likely to interoperate with each other in the absence of a coordinating authority such as a server, there is an obvious need for a technology above the hardware abstraction level of IrDA and Bluetooth. JXTA enables mobile devices running on various platforms not only to share data with each other, but also to use functions of their respective peers. In this paper a general overview of the JXTA specification, the corresponding protocols, and mobile peer-to-peer aspects is presented. Furthermore, the current status of an open source JXTA implementation for Java is briefly outlined. This paper analyzes to which extend mobile devices are suitable for a peer-to-peer approach and how this approach can be realized with JXTA. To emphasize the practical impacts of a peer-to-peer approach some applications are described, which are based on the authors’ current projects. This includes a hospital scenario, as well as an example for a distributed electronic patient health record. These examples are helpful, because they include security, data protection, wireless and mobile technology, and reliability.

Keywords: Mobile Devices, Peer-to-Peer, Wireless Communication Technology, Security, Ubiquitous Computing

Classification (CR 1998): C.2.0, C.2.1, C.2.4, D.4.6

1. Introduction

Mobility and mobile personal computers are elements of our daily life. Mobile phones and Personal Digital Assistants (PDAs) are self evident in the same way as the world wide web, shopping via Internet and payment with a debit or credit card. In the year 2000 about 201.87 million people participated in the cellular phone network across Europe. In 2004 about 263.97 million people are expected [19]. This results in a market penetration of 78%. Since 1998 the number of mobile phone holders has nearly trebled.

A similar trend is expected within the Bluetooth and wireless LAN market. The annual turnover in Europe (2001) was about 4.141 billion US-Dollar. In four years (2006) the market researchers suppose an increase of the turnover up to 51.124 billion US-Dollar [19]. This development shows that the trend for mobility, mobile and ubiquitous computing is unbroken. Not only during journeys and business trips, but also in the office or at home, demands exist for mobile information access and mobile computing.

People sharing information have to communicate with each other. In the common world they are using email systems, bulletin boards, fax and phone devices in order to share any kind of data. This way of communication is normally limited by different resources, bandwidth and communication devices. Independent of the way of information sharing, the sender and receiver of the information have to communicate directly with each other (peer-to-peer).

People communicating through the Internet in the traditional way use centralized facilities like web servers, shared file systems, and video conference servers. Under some circumstances this indirect communication is very inefficient. Especially people using mobile devices are often out of office, for instance at the customers’ site. If they want to share data or use functions together without any additional centralized infrastructure they will have to establish communication using a suitable set of protocols and interoperable
Peer-to-peer computing becomes even more relevant taking into account that today’s small mobile devices have an enormous potential of computing power that can and should be utilized for a shared purpose using a peer-to-peer approach. This also means avoiding hot spots, which could easily become a bottleneck. Compared to a stationary computer, a PDA has very limited resources. Both facts together, which are (a) a PDA has enough resources to make them worth sharing, but has (b) less resources than potentially needed for a particular purpose, encourage us to think about using mobile devices working peer-to-peer.

While desktop computers working in peer-to-peer mode are still relatively stable bound to an environment, mobile devices will encounter and lose other devices frequently. This occurs when mobile devices come into range of another WLAN, Bluetooth or IrDA equipped device. Applications have to tolerate the sudden coming and going of individual peers [20]. Working peer-to-peer means a different type of cooperation compared to working in a hierarchical relationship. Devices have to find each other, and have to realize what functions the other peers offer. Important aspects for a peer-to-peer community are availability and performance. This paper describes how device mobility influences these characteristics. It shows whether mobile devices are suitable for a peer-to-peer approach and how this approach can be realized using JXTA. Additionally, selected security aspects are outlined.

2. General Benefits of Peer-to-Peer and Mobile Scenarios

In a peer-to-peer structure the relevant end user nodes communicate and cooperate directly. A hierarchical structure is avoided. There is virtually no need for a centralized infrastructure. This leads to the following benefits:

- Peer-to-peer systems as distributed systems are more reliable, when multiple peers exist for one service. They also avoid single network paths that might become congested or unavailable. In contrast to Jini [16] or Corba [23] they also avoid dedicated servers such as lookup servers and brokers (ORBs).
- Peer-to-peer systems have better network performance and require smaller bandwidths. Bottlenecks can be avoided by appropriate routing algorithms between peers, for instance in a cluster architecture.
- Administrative and configuration efforts for centralized infrastructure can be avoided in a self-configuring system.
- Shared resources can be used more efficiently. If a peer does not need a special resource it could offer it to other peers. In exchange a peer can get needed resources from other peers.
- The peer-to-peer approach supports end-to-end communication security via a secure channel. It avoids single data exchange points, which might become subject to interceptions.
- Peers with the same interface can communicate directly without an additional environment.

Mobile devices have limited resources compared to stationary devices. They usually have less computing power and less memory, are connected via small bandwidths, are being moved around and therefore frequently loose connections, no matter if they use Bluetooth, IrDA, WLAN, GSM, GPRS, DECT, and so on. They have lower standby times caused by limited battery capacities, have reduced possibilities for extensions, and get damaged, lost, or stolen more often. This altogether implies the need for a reliable backup strategy as well as data protection and encryption mechanisms.

A typical obligation of mobile devices is the synchronization of databases and repositories with stationary computers. Although, JXTA can be used in master-slave scenarios, where either the stationary system controls the mobile device or vice versa, these scenarios are beyond the scope of this paper. The paper focuses on other peer-to-peer scenarios including two or more devices that want to share data and functions.

JXTA enables the development of networked interoperable peer-to-peer applications including the following aspects [3]:

- Finding other peers on the network with dynamic discovery across firewalls.
- File sharing and sharing of computing resources with anyone across the network.
- Creation of peer groups wherein peers can find each other, across firewalls, on any device.
- Remote monitoring of peer activities.
- Secure communication with other peers on the network.

There are very successful recent examples showing that peer-to-peer really works, e.g. Gnutella [5], OBEX [21] or JetSend [22]. Since mobile devices have the shortcomings mentioned before, there are much higher potential benefits from sharing limited resources. On the first hand, it makes rarely sense to give others what one is running out of. But on the other hand, if all devices share their resources as much as even possible there will be a benefit for
everyone. Additionally, common mobile devices have a variety of well-known wireless interfaces, which makes them suitable for peer-to-peer communication. In some cases the devices involved in a peer-to-peer communication will use the same interface technology. For instance a PDA might be equipped with Bluetooth while a mobile phone has an IrDA interface only. The paper also addresses this issue and shows how JXTA deals with it (see Section 3.3).

Using wireless interfaces means transmitting data through the air. This makes the communication vulnerable against interception [12]. It also makes the mobile device itself subject to hacking assaults. In most peer-to-peer scenarios there will be a communication between untrusted or even anonymous peers. JXTA provides security features to prevent sensitive information from being eavesdropped and peers from being misused.

3. JXTA Architecture

The architecture consists of three layers, JXTA Core, JXTA Services, and JXTA Applications [25]. Basic functionality resides in the core, while the two layers above are more application specific. In the middle is a service layer that provides functions such as indexing, searching, and file sharing. The services provided by this layer make use of the core features. The application on top uses these services. Figure 1 shows the layered architecture of JXTA software.

3.1. JXTA Terms

A peer is any networked device (sensor, phone, PDA, PC, server, and so on) that implements one or more of the JXTA protocols [9] which are described in section 3.2. It works independently and asynchronously of other peers. A peer group is a collection of peers that have a common set of interests.

The basic communication means used in JXTA are pipes. A pipe is a virtual unidirectional connection between peers. Input and output pipes exist that can be bound at runtime to different peers. A pipe works asynchronously. There are special pipes that can be bound to multiple endpoints.

JXTA does not define a single transport protocol, such as TCP or HTTP. JXTA relies on the features provided by the transport protocols and does not add any own functionalities which are already available from those protocols, such as routing or error detection and correction. Messages are sent as unreliable datagrams to an endpoint and addressed through a URI. [11]

All entities (resources), such as peers, peer groups, pipes, or services, are described by advertisements. These are XML structured documents. Advertisements are programming language neutral metadata structures and may refer to a WSDL document [14] for instance.

JXTA defines a three layer architecture:

- The JXTA Core is responsible for basic level operations such as communication. The core includes protocols and provides general security mechanisms. In this way the JXTA Core is comparable to the kernel of an operating system. It controls features like peer groups (building), peer pipes, and peer monitoring.

- JXTA Services support higher-level functions such as searching, file and resource sharing, indexing, and caching. JXTA Services enable features needed for platform independent collaboration.

- JXTA Applications use peer services as well as core layer functions. Example applications are content management, shared searching, distributed computing, and instant messaging.

3.2. JXTA Protocols

JXTA defines six protocols [9]. Every peer has to implement the self required protocols only, not all of them. The protocols are shown in Figure 2.

- The Peer Endpoint Protocol (PEP) is the routing protocol of JXTA. It is used to find a route to another peer. A route is a sequence of nodes from one endpoint to another. This does not mean the actual routing in terms of TCP/IP or a similar transport protocol. The PEP works independently from the underlying network transport protocol. PEP ignores firewalls and the presence of logical networks built with an IP Network Address Translator (NAT) [17].

- The Peer Resolver Protocol (PRP) is the mechanism by which a peer can send a generic query to other peers. It is a query-response protocol. Each query contains a unique ID, which matches the ID in the response.
The Peer Discovery Protocol (PDP) is used to discover any published resources which are mandatory represented as advertisements. The PDP is based on the use of rendezvous peers (see Section 3.3). Rendezvous peers have all peer properties. Furthermore, they can cache advertisements needed to help peers discover resources and can forward requests for advertisements to other peers. They also interact with different rendezvous peers.

The Pipe Binding Protocol (PBP) is used to establish pipe connections between peers. With the help of the PBP peers bind the two or more endpoints of a pipe.

The Peer Information Protocol (PIP) is used to exchange status information between peers. These information include state, uptime, traffic load, and so on.

The Peer Membership Protocol (PMP) is the mechanism by which peers can organize themselves to form groups. Peers use the PMP to join or leave existing peer groups. A single peer can belong to multiple peer groups. Peer groups are discovered using the PDP.

3.3. Rendezvous Peers

JXTA defines special peers with the ability to either cache advertisements, or to forward requests, or both. These special peers are named rendezvous peers. Rendezvous peers are used for instance to discover advertisements, and to bridge them between different network segments, even running different transport protocols. There is no message routing provided by rendezvous peers. This has to be provided by lower network layers used by JXTA. Rendezvous peers can tunnel information through firewalls or into segments using NAT [17].

Rendezvous peers may have a relationship to other rendezvous peers. They can forward requests between each other. Peers learn about the presence of rendezvous peers using a bootstrap algorithm. Peers can have an initial list of rendezvous peers.

3.4. Current Implementation of JXTA

JXTA is an open source project supported by Sun Microsystems [4] and was founded in 2001 following ideas of Bill Joy and Mike Clary. The project has grown to more than 10,000 individual members. Currently many sub projects are under development, such as protocol enhancements and service implementations. Most of the software contributed to the project is released under The Sun Project JXTA Software License [7], which is similar to other open source licenses.

As of this writing the current implementation (size smaller than 250 Kb) of JXTA is version 1.0 which is based on the JDK 1.1.4 [2]. Releases for Java 2 Micro Edition (J2ME) [1] are discussed in the JXTA community. The protocol specification is in revision 1.2.1. Currently, JXTA supports TCP/IP and HTTP as its transport protocols. Other protocols are under development.

The current software release includes default implementations of almost all concepts where the specification leaves the concrete realization open to the developers. This includes encryption algorithms, as well as protocol implementations or other security features.

3.5. Nontypical Use of JXTA

Parts of JXTA, especially some protocols, can be used in an untypical manner. For instance, JXTA can be utilized in synchronization processes between stationary and mobile devices. Beside non standard solutions developed by many companies, JXTA can be used underneath the new synchronization standard SyncML [8]. SyncML provides protocols to synchronize repositories within devices. A telephone book could be synchronized between an address database and a mobile phone or a PDA or between all three. SyncML itself can, similarly to JXTA, be built upon a variety of wide spread transport protocols. Using JXTA in all of those devices would result in a more flexible synchronization process across the boundaries built by different interfaces and network protocols. JXTA might become a hardware abstraction layer for SyncML. Using this approach would enable peer-to-peer functionality on many devices. JXTA has an open architecture, which makes it usable for almost all...
point-to-point connections. Point-to-point is referred here as the connection between exactly two nodes.

4. Mobile Aspects

Mobile devices have fewer resources and are carried around in a hostile 'wilderness'. This implies different needs and possibilities in respect to peer-to-peer networking. For instance, wireless communication channels used between mobile devices are usually open for interception, unless secured by appropriate cryptographic techniques.

4.1. JXTA on Mobile Devices

JXTA adds further high-level protocols to the protocol stack. Since JXTA uses XML it requires a lot of computing power to interpret the protocols and hence generates a significant overhead. Every peer has to fulfill more complex parsing operations compared to low-level protocols. Considering standard parser implementations such as those in the JAXP [15] package this allocates many resources especially memory and CPU time.

The JXTA protocols do not require periodic messages. There are no polling, link status sensing, or neighbor detection messages. This is very useful for mobile devices, since it saves energy and bandwidth.

Mobile devices will preferably be equipped with wireless interfaces to communicate with their environment. Wireless transmissions have limited ranges, Bluetooth and IrDA, for instance, bridge at most 10 meters (except for some special solutions) [24]. In a stationary LAN the true distance between two peers does not really matter. In a wireless networked system this becomes important. If two peers that want to collaborate are not in range of each other, rendezvous peers are necessary. A rendezvous peer that forwards messages between two peers should be placed in an area that is visible to both peers. Rendezvous peers are in this manner more important to ensure the correct function of a mobile peer-to-peer community.

Bluetooh, WLAN, IrDA, and other similar technologies have a market penetration that cannot be ignored. This makes it necessary for a new standard to provide additional features without destroying legacy possibilities. For political and marketing reasons it is impossible to establish new and perhaps better standards from scratch when introduced standards exist. JXTA disregards those considerations and uses existing standards for its own needs. The JXTA specification [9] leaves intentionally all parts blank that might conflict with existing ideas.

4.2. Security Aspects for Mobile Devices

Security, trust, and protection of privacy occupies a central position in every communication environment. The use of the Internet, WLAN, Bluetooth, and so on as a communication medium between two counterparts is an approach, but actual problems, which every user is dealing with, should and must be solved, too. Email worms and Trojan horses, stolen credit card numbers and user observations including profile generation and security shortcomings in LANs are only some examples, which do not place confidence in the new technological possibilities.

The basic security requirements for every communication, including peer-to-peer as well, are confidentiality, integrity, and availability. A trustworthy peer-to-peer security architecture must guarantee at least the following aspects:

- **Authentication and authorization**: The security layer must guarantee the correct and authenticated data and resource access. All data, which can be associated with a "user" of a peer must be adequately secured.

- **Encryption and secure communication**: The security layer must enable the encrypted transmission of data and must support the usage of digital signatures including public and private keys and digital certificates. Cryptographic algorithms can be DES, DES3, RSA or the advanced encryption standard (AES) Rijndael [10] for example.

- **The security layer must support aspects like context management, key generation, key exchange and hashing / signature.**

- **The security layer must support multilateral security, should support the integration of security interests of all communication partners, audit and non-repudiation techniques.**

Beyond this, a negotiate function has a favorable effect on peers because it enables the adaptation of communications if there are different and / or contrary opinions and interests. Therefore, three different levels of security can be considered [18]:

- **Personally available security (unilateral security).**

- **Security between two parties, without another third party to be integrated (bilateral security).**

- **Security which can be achieved by cooperation of several parties (multilateral security).**

JXTA as a peer-to-peer enabling technology integrates general mechanisms for security in the JXTA Core layer.
Although JXTA is independent of specific security approaches, JXTA version 1.0 implements a comprehensive set of security primitives to support different security solutions of corresponding JXTA services and applications. This includes the following features:

- Hash functions, symmetric and asymmetric encryption algorithms.
- Authentication framework modeled after PAM (Plug-gable Authentication Module).
- Password - based login scheme.
- Access control mechanisms based on peer-groups.
- Transport security mechanisms.

All these implementations are based on standard(ized) and common cryptographic techniques and algorithms, e.g. RSA public key exchange, RC4 byte stream cipher, SHA-1 hash algorithm, and so on [10]. JXTA's implementation is based on an a peer-to-peer "Web of Trust" comparable to the web of trust known from the electronic email exchange in Pretty Good Privacy (PGP) [6].

5. Applications in e-Medicine

Documentation and data exchange are some of the most time consuming activities in the public health sector. Not only the management of patient records in physician’s practices or hospitals, but also the documentation and data processing in case of an emergency is a critical situation. Today, most of the incidental (mobile) data are written down on paper. Later, these data are often transferred and manually typed in electronic, stationary computing systems. The reasons for the documentation are among other things memory, colloquy and legal functions.

The electronic patient health care record and data acquisition with mobile devices like PDAs are often cited expressions in the last few years. Now with the decreasing prices, the nearly unbroken trend for miniaturization and new communication technologies like Bluetooth and WLAN a new level of health support can be achieved.

Within the health system different actors exist which can be the basis for a peer group within an institution. Possible peers can be persons (with a corresponding communication device), e.g. health professionals, patients and supporting organization employees, organizations, e.g. health care and supporting organizations and other entities, e.g. electronic equipment, regulated medical devices or applications.

They altogether can form a special peer group with various access rights in order to exchange different data and other kind of information.

5.1. The Distributed Electronic Patient Health Record

A person going to a physician automatically creates a (new) record in the database / archive of the health professional. This archive is sometimes paper based and nowadays more and more in an electronic form stored on a personal computer. Data from different health professionals are not linked together, so it is not possible to collect all entries of a corresponding patient and to create a complete patient data set. This has data protection advantages but there is also the danger of desiderative data. Results from different tests and all medications other physicians have prescribed are required many times. In addition to that information (data records) from laboratories, hospitals, and pharmacies are desired.

A family physician for example is often not informed about if there are (a) additional family doctors a patient is seeking, and (b) what an ophthalmologist, gynaecologist or dentist has prescribed. Today, the information exchange is done by phone and by dictated and later written down paper based physician letters. Hereby, a lot of transformation errors and other mistakes can occur. In addition to that a long time delay exists until the data are available in a written form.

The idea is to share the patient records online [13] comparable to Gnutella. Health professionals form an own peer group, secured by authorized log-in mechanisms and secure communication channels. A health professional is able to select what kind of data should be online available and what kind of data should not be available for confidentiality reasons.

The secure sharing of medical / clinical data, including patient demographics, laboratory results, medications / allergy lists, test results and radiology reports, is possible. Direct download possibilities from the entities make central servers storing the data superfluous. Rapid and mobile access to all information through wireless beaming technologies secured by e.g. biometric access control and digital certificates is also possible.

5.2. Peer-to-Peer in Hospitals

The section above demonstrated a few of the new possibilities obtained through peer-to-peer technology. Content is available within the local area network and can be obtained via peers (like modified PDAs for health professionals). One to one communication between physicians and data sharing during visitations of sick people enables a new level of patient care. Furthermore, the following advantages can be mentioned:

- Data transfer from the clinical data processing unit (server, electrocardiogram, ultrasound, etc.) to the mo-
bile PDA; The ad-hoc availability of patient data and information for every authorized person (physician and administration) can be guaranteed.

- Electronic patient records: Digital data input and processing, no media breaks.
- Reduction of hand writing activities, hand written data transfers and possible transfer mistakes.
- Searching and data retrieval within large data bases is possible with distributed computing. Searching is done on a server via an air link between the PDA and a server (e.g. drug reference books and different data bases).
- Integration of different classification systems (peer-to-peer link to mobile device), e.g. the International Classification of Diseases (ICD), the International Classification of Procedures in Medicine (ICPM) and the Diagnosis Related Groups (DRG).
- Data exchange and synchronization during house calls of physicians. During emergency calls as well as during regular visits, up to the minute data access and synchronization is possible.

6. Summary

As we have shown in this paper JXTA is suitable to work with mobile devices as a peer-to-peer solution as well as a point-to-point protocol. Its usage has many benefits but some disadvantages. The benefits are easier software development, higher level of platform independence, standardized protocols, and built-in or prepared security features. Currently JXTA is not lightweight. It requires JDK 1.1.4 and therefore needs many hardware resources, but mobile devices usually have restricted resources. The JXTA community has addressed this problem by developing a special release based on Java 2 Micro Edition.

JXTA can be used in a variety of situations such as in medicine or wherever no centralized infrastructure is available or desired. It is independent from transport protocols. Therefore it can rely on many protocols already available for mobile devices and it is open for upcoming developments. JXTA supports the efforts being made in the area of ubiquitous computing.

References