**UNIT -V**

**PART –III**

**Device Connectivity**

Pervasive computing devices do not develop their full potential unless they are connected to applications and services through the Internet. This chapter covers protocols for device-to-device and device-to-server interactions that are relevant in the pervasive computing domain, including wireless protocols, mobile phone technologies, Bluetooth, the Mobile IP, synchronization protocols such as SyncML, and transaction protocols and protocols enabling distributed services, such as Jini. In addition to those protocols, we investigate further algorithms and protocols that address security issues. Because system and device management will become a big challenge to support millions of devices, the last section will discuss device management in the pervasive space.

**4.1 Protocols**

Standardized protocols are basic prerequisites for meaningful use of pervasive computing devices. Most devices are not very powerful or useful when used stand-alone. They need to exchange data with other devices, for example via wireless protocols.

Wireless protocols will support IP in the near future, making Mobile IP (a specially tailored IP for the needs of mobile devices) very important. We introduce this protocol below and explain its relation to the IPv6 protocol.

Another important topic is the consistency of databases and their data (e.g., calendar entries) between a server and various pervasive computing devices. This problem is solved with synchronization (also called replication). The major protocols supporting this concept are discussed below.

As connected pervasive devices form a distributed network, distributed services and architectures such as Jini are gaining interest in the pervasive computing domain and are explained in this chapter.

To ensure the delivery of the data in an environment where the device can be switched off or the connection can break down at any time, message and transaction protocols are used to maintain integrity. These protocols are explained in the section on message- and transaction-based protocols.

Today, the main focus is on connection protocols such as WAP and Bluetooth. The first step of a large-scale deployment is to get the devices connected. Soon, these protocols will be established, then data-related protocols will become more important. They will help to ensure security and guaranteed delivery of messages expected by device users. Only when this infrastructure is in place will e-commerce using mobile devices have a substantial basis.

### 4.1.1 Wireless protocols

Wireless protocols are the natural communication choices for small handheld devices such as PDAs and mobile phones. By definition, no cables are required in order to communicate with other devices.

Several wireless protocols already exist, and most are evolving rapidly. This section offers an overview of WAP and discusses Object Exchange (OBEX), IrDA, Bluetooth, and mobile phone technologies. The 802.11B protocol, a wireless local area network (LAN) protocol with high bandwidth (11 Mbps), will not be covered here. It is more suited for wireless connection of laptops to a LAN, than for pervasive computing devices. However, it may be used in a hybrid solution, where the pervasive device can make use of 802.11 inside an office and UTMS while outside.

WAP/WML WAP is a technology designed to provide mobile terminal (i.e., mobile phones) users with rapid and efficient access to the Internet. WAP was conceived by Ericsson, Nokia, Motorola, and OpenWave Systems, and is now driven by the WAP Forum industry association with over 200 members. WAP integrates telephony services with browser technology, and enables easy-to-use interactive Internet access from mobile handsets. Typical WAP applications include over-the-air e-commerce transactions, online banking, information provisioning, and messaging.

The WAP protocol is similar to HTTP, a high-level Internet communication protocol. WAP has been optimized, not only for use on the narrow-band radio channels of second-generation digital wireless systems, but also for the limited display capabilities of today’s mobile terminals. The wireless equivalent of HTML is WML, which defines a textual format and a compressed binary format (WBXML). Unfortunately, there is currently no end-to-end security available in WAP, but this will change in the future through a working group that has been set up to solve this issue.

WAP is still a very young standard, and at the moment there are discussions under way as to whether WML can be integrated into Extensible Hyper Text Markup Language (XHTML) to unify HTML and WML. Mobile access to the Internet will increase with new phone technologies and more user-friendly devices (e.g., PDA devices with an integrated phone). Therefore, WAP will become enormously important in the near future.

**OBEX**

OBEX was originally defined for IrDA as IrOBEX, but it is independent from the underlying transport protocol. With the creation of the Bluetooth standard, OBEX has become the high-level protocol to use in order to wrap an IrDA communication as completely as possible, thereby dramatically simplifying the development of communication-enabled applications. It has pull and push commands for bidirectional communication (unlike HTTP, which has only pull) and consists of two models:

* **The session model** structures the dialog between two devices. It uses a binary packet-based client/server request/response model.
* **The object model** carries information about the objects being sent, as well as containing the objects themselves. The object consists of a sequence of headers. A header is an entity that describes some aspect of the object, such as the name, length, descriptive text, or the object body itself. The headers can be parsed, similar in concept to the headers in HTTP.

OBEX also specifies an authentication method with a challenge/response scheme, but does not specify an encryption scheme. The two transport layers of choice for OBEX are IrDA and Bluetooth. Both have their advantages and disadvantages and therefore complement each other.

**Bluetooth**

Bluetooth is an RF specification for short-range data exchange. It is named after Herald I. Bluetooth, 910–85, who was the king of Denmark and first unified the country. Bluetooth was founded by Ericsson, IBM, Intel, Nokia, and Toshiba, and now has more than 1300 members. Bluetooth has the following characteristics:

* **Frequency band.** Bluetooth operates in the 2.45 GHz industrial-scientific-medical (ISM) band.
* **Security.** There are several security mechanisms defined by the Bluetooth specification, such as authentication based on private keys and encryption.
* **Transmitting capabilities.** Bluetooth is omnidirectional and has a range up to 10 m. It supports isochronous and asynchronous transmitting services.
* **Bandwidth.** Bluetooth is capable of providing a data transfer rate up to 1 Mbps.

**Device connectivity**

* **Speech.** There is support for three digital speech channels simultaneously.
* **Cost.** Bluetooth is still relatively expensive, with an expected price of $5–$10 per Bluetooth module.

Bluetooth is the protocol of choice to connect two or more devices that are not in direct line of sight to each other. For example, a digital camera can send pictures to a hard disk that is in a nearby briefcase. Figure 1 shows a headset for a mobile phone connected via Bluetooth to the mobile phone in the user’s pocket.



Figure 1

Because the user of a Bluetooth device has very limited capabilities to control who can talk to the device (by turning it on or off), there must be some mechanism in place to protect the device. Bluetooth offers different security modes, including authentication based on private keys and encryption, to solve this problem.

**IrDA**

The IrDA specifies several infrared communication standards, but the important ones for pervasive computing devices are IrDA-Data and Infrared Mobile Communications (IrMC).

**IrDA has the following characteristics:**

* **Frequency band.** Infrared light is used as the physical transport medium.
* **Security.** Unlike Bluetooth, IrDA has no security concept, but relies on higher-level protocol security.
* **Transmitting capabilities.** Because IrDA is based on infrared light, it consists of point-to-point connections with a narrow angle (30-degree cone) between sender and receiver. IrDA is designed for short-distance communication (0–30 cm).
* **Bandwidth.** IrDA supports data rates up to 4 Mbps, with 16 Mbps under development.
* **Speech.** There is support for only one digital speech channel.
* **Cost.** IrDA senders and receivers are mass-produced, therefore they are very cheap ($1–$2).

IrDA is perfectly suited for high-speed data connections (e.g., connecting a device to a wired network). To initiate a data exchange, it requires a device to be in direct line of sight to the other IrDA device (e.g., to exchange virtual business cards).

**4.1.2 Mobile phone technologies**

The low-level communication protocols of mobile phones are radio-based and suited for long-distance communication (up to about 100 km). However, the technologies used today have a very limited bandwidth, meaning that data exchange rates are very slow. This will change with the third-generation protocols, like UMTS. Table 4.1 provides an overview of the different mobile phone communication protocols and their properties.

**Table 4.1 Overview of different generations of mobile phone communications**

* **1G**
  + **Protocol:** AMPS, C-Net
  + **Technology:** Analog, circuit-switched
  + **Speech Quality:** Poor
  + **Bandwidth:** Low
  + **Security:** None
* **2G**
  + **Protocol:** GSM, TDMA, CDMA
  + **Technology:** Digital, circuit-switched
  + **Speech Quality:** High
  + **Bandwidth:** Low
  + **Security:** Depending on protocol, low to high
* **2+G**
  + **Protocol:** GPRS, HSCSD, EDGE
  + **Technology:** Digital, circuit- or packet-switched
  + **Speech Quality:** High
  + **Bandwidth:** Medium
  + **Security:** High
* **3G**
  + **Protocol:** UMTS, W-CDMA
  + **Technology:** Digital, packet-switched
  + **Speech Quality:** High
  + **Bandwidth:** High
  + **Security:** High

The limited reach of transmitters is certainly a disadvantage if mobile services must be delivered to a large area because many transmitters are required. However, the limited reach of senders allows reuse of scarce frequency bands between distant transmitters. Thus, a large number of mobile stations can be serviced.

Figure 2 shows that there might be dark spots where no mobile services are capable, even when senders are placed with care. Location and size of black spots may vary with weather conditions and mobile device characteristics. Frequently, the high investments for a complete coverage cannot be justified in rural areas, thus in many cases, mobile services are restricted to densely populated areas or the main serviced areas are mobile service providers typically publish maps where serviced areas are indicated. However, buildings and other objects may disrupt the signal. Therefore, applications based on mobile systems must be designed to allow for non-availability of service or disruption of services. Typically this is achieved through a combination of online and offline operation.

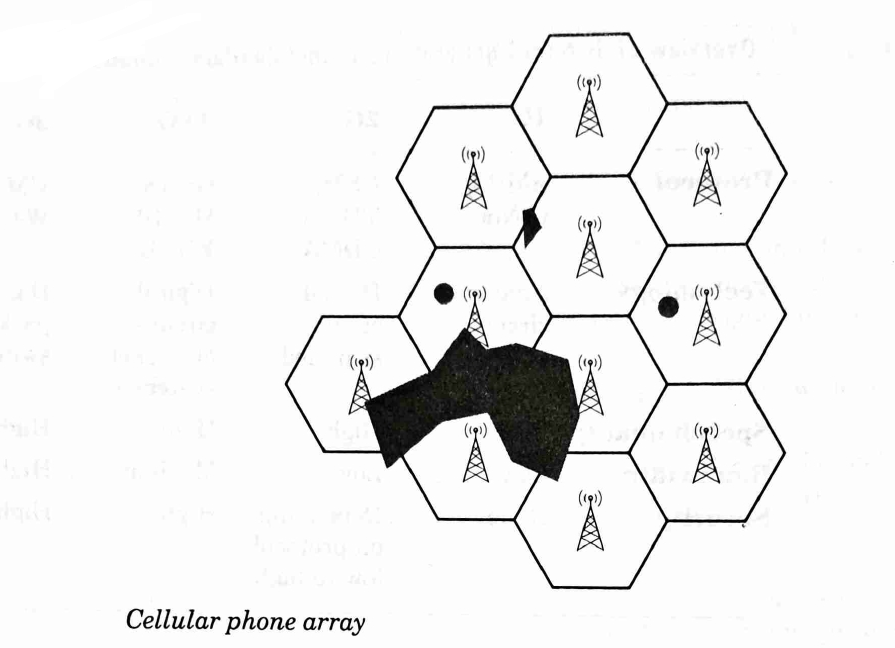


Figure 2

Mobile stations are normally receiving signals from the station that connects to the transmitter with the strongest signal. A moving station, e.g. a mobile phone in a car, may travel from one cell to another. The GSM system has been designed to allow movement of stations at a speed up to 150 km/h. Multiple base stations typically receive the signal of a transmitter. Signal delay is indicative for the distance between the transmitter and the mobile station. The station can be located through triangulation with accuracy of 30–150 m by combining the signal.

**Cellular phone array**

The information from three stations (this can also be achieved with two stations and a combination of angle of arrival (AOA) and time difference of arrival (TDOA) measurements). This allows the location of the mobile station to be detected, e.g., in case of an emergency call or to offer location-based services. Because such information is sensitive and user-related, many countries have laws to prevent unauthorized use of these data (e.g., the Wireless Communications and Public Safety Act of 1999 in the USA).

**First-Generation mobile systems**

Usable wireless systems first came to market in the 1970s. In Germany, the B-Net, which needed heavy transmitters and receivers, was successful as a car phone system, and in northern European countries the Nordic Mobile Telephone (NMT) system was later launched. The successor of the B-Net, the C-Net, was in use in Germany until the end of 2000. In 1983, AMPS started the wireless phone market in North American countries.

All first-generation (1G) systems are analog, circuit-switched systems. Circuit-switched means that there is a dedicated point-to-point connection between the two ends of the call. As the systems were analog-based, they had poor speech quality and a low bandwidth for services like fax or data transmissions. Some analog systems are still in use (e.g., AMPS throughout the Americas), primarily because there is near 100% coverage for them. Analog systems have no built-in security for data transmission or user authentication.

**Second-generation mobile systems (2G)**

The second-generation (2G) mobile phone communication systems are digital, circuit-switched systems. The switch from analog to digital technology improved the speech quality enormously and allowed for some additional services, such as encryption of the signal, authentication of the user, authorization, anonymity, and the ability to send short, alphanumeric messages. However, due to the circuit-switching technology, data transmission rates were still low (9.6–14.4 kbit/s).

Because there were a lot of incompatible analog mobile phone standards in Europe, the European Union in 1982 decided to develop a common standard, Groupe Spécial Mobile (GSM). GSM was finally standardized in 1991 and renamed Global System for Mobile communications. It works at 900 MHz, offers full international roaming, automatic location services, signal encryption, user authentication and authorization, anonymity, SMS, fax, and data service. SMS is becoming the most popular service of GSM, with about 12 billion messages sent per month worldwide (data from October 2000). The GSM-900 standard is adopted worldwide in over 160 countries, and is the most popular mobile phone system, with more than 400 million users worldwide (including GSM-1800 and GSM-1900 by year and 2000). This results in a market share of about 60%, followed at the earlier stages AMPS with a share of about 20%. To get a higher user density per cell in cities, GSM-1800 was developed. This works like GSM-900, but in the 1800-MHz frequency band, and offers better speech quality.

The USA also switched to digital systems, but largely stayed with their 850-MHz frequency range from AMPS. Because there were no standardization movements as in Europe, the result was three incompatible systems: the old analog AMPS, and the new digital TDMA and CDMA systems. In contrast to GSM, TDMA and CDMA do not support encryption, authentication, or SMS. With the user density in big cities becoming a problem, CDMA and TDMA switched to the same 1900-MHz frequency band, therefore called GSM-1900. The reason for all these different frequencies is the lack of standardization. UMTS will be the first telephone standard that also defines worldwide valid frequencies.

**Table 4.2** shows the development of the wireless phone market. The first three rows show the most popular digital systems: the GSM system has by far the most subscribers. The figure also displays the trend towards digital systems, as the number of digital system subscribers has grown by more than 25% in six months, and the number of analog system users has declined by 10% in the same time.

**Two-and-a-half-generation mobile systems**

Between the 2G and 3G mobile phone systems lies an intermediate step, generation 2G. In contrast to a generation 3G system, a generation 2G is...

**Table 4.2 Worldwide wireless phone subscribers (millions)**

|  | **April 2000** | **October 2000** |
| --- | --- | --- |
| **GSM** | 304 | 397 |
| **CDMA** | 62 | 76 |
| **US TDMA** | 44 | 56 |
| **Total digital** | 457 | 579 |
| **Total analog** | 83 | 75 |
| **Total wireless** | 540 | 654 |

The system requires only minor hardware and software changes by the phone companies. In Europe, 2G systems like GPRS and High-speed Circuit-Switched Data (HSCSD) are already in operation. However, users need new mobile phones in order to use these services.

The easiest way to achieve a higher bandwidth than GSM is by aggregating multiple GSM channels, for example in the HSCSD technology. In HSDSC, multiple basic traffic channels are bundled to achieve data rates of up to 57.6 kbps. Different numbers of channels can be assigned to upstream or downstream data transmission. HSCSD can provide a fixed bit rate in transparent mode, or a variable bit rate in non-transparent mode. The advantage of HSCSD is that it is still compatible with GSM technology and therefore requires no major changes or investments by the service providers. Static assignment of channels is not well suited for the typical requirements of Internet applications, where a small burst of data is sent from the client to the server, followed by a large burst of data as response. Therefore, most GSM-based systems will not implement HSCSD, but will move directly on to the next generation of packet-oriented data transmission.

GPRS has been standardized by the European Telecommunications Standards Institute (ETSI) as part of the GSM Phase 2+ development. It gives GPRS providers a smooth transition to the third-generation (3G) networks, as network architecture, services, and business models are similar. It represents the first implementation of packet switching within GSM. Rather than sending a continuous stream of data over a permanent connection, only in circuit-switched systems, packet switching utilizes the network as in where the data to be sent. This results in a more efficient use of the network, as one physical connection can be shared. The transmission rates range from 20 kbps to 171 kbps. The drawback of packet switching is that there is no guaranteed bandwidth.

Bandwidth, which can be important for live video streams, is a key concern. Technologies such as ATM, where guaranteed bandwidth can be reserved even with packet-switched networks, exist. By breaking the transmitted data into packets instead of sending them as a continuous stream, mobile devices remain connected 'virtually' to the server, using airtime only when data are actually being sent. This optimizes airtime use (and possibly associated connection costs) thereby making it cheaper and therefore more attractive.

The packet-based GPRS protocol is ideally suited for burst-data applications, such as email or Internet access, and also enables virtually permanent connections to data sources, allowing information to arrive automatically rather than being sought (push model instead of a pull model). Another benefit of the packet-based approach is that being connected to the Mobile Internet does not interfere with receiving a phone call, because the data session may be suspended while the call is answered. Furthermore, it enables broadcast, multicast, or unicast message services that cannot be achieved using standard circuit-switched networks.

**Third-generation mobile systems**

3G mobile phone systems will bring packet switching and high data rates in the range of several Mbps. This will be a breakthrough for mobile computing, making high data rates and full Internet access using the standard Internet TCP/IP protocol possible for pervasive devices. It will also support bandwidth-hungry multimedia applications, such as full-motion video and video conferencing.

Requiring new hardware for transmission, it will be some time before the 3G networks offer good coverage. 3G networks are expected to be in operation in Japan by 2001, in Europe and Asia/Pacific by 2002, and in the USA by 2003-4.

The UMTS is part of IMT-2000, the 3G wireless services specification of the International Telecommunication Union (ITU). The UMTS Forum was established to focus on spectrum availability, licensing issues and long-term market surveys for third 3G. The UMTS frequencies in the USA are still used by TV stations that have contracts running until 2003-4 with an option to extend it. There are discussions and negotiations about how to make UMTS happen as soon as possible. It is expected that worldwide coverage will be achieved by the year 2005.

UMTS is based on wide-band CDMA (W-CDMA), which was originated by Japan’s NTT DoCoMo and is now adopted for 3G use by ETSI. In addition to speech and data, W-CDMA also supports high-speed multimedia services, such as video films, video conferencing, and Internet access, and offers data throughput up to 2 Mbps. Table 4.3 shows how the data transmission rate influences the availability of offered services. For reference, the wired-line ISDN is inserted.

**Table 4.3 Delivery time of different services for different phone technologies**

| **Service** | **ISDN** | **2G (GSM)** | **2+G (GPRS)** | **3G (UMTS)** |
| --- | --- | --- | --- | --- |
| Email file (10 kB) | 1 s | 8 s | 0.7 s | 0.04 s |
| Web page (9 kB) | 1 s | 9 s | 0.8 s | 0.04 s |
| Text file (40 kB) | 5 s | 33 s | 3 s | 0.2 s |
| Large report (2 MB) | 2 min | 28 min | 2 min | 7 s |
| Video clip (4 MB) | 4 min | 48 min | 4 min | 14 s |
| TV Quality Movie (6 GB) | 104 h | 1100 h | 52 h | ~5 h |

Since the patent issues about CDMA seem to be resolved, W-CDMA will soon get a wide availability because the GSM community, which supplies the dominant technology today, supports it. Among the supporters of W-CDMA are NTT DoCoMo, Ericsson, Nokia, and Qualcomm. UMTS and W-CDMA are important for future mobile devices because they offer the high data rates needed for accessing the Internet via mobile devices.

### 4.1.3 Mobile Internet Protocol

As soon as high-speed mobile connection is available, the next step is to use this connection from a mobile device to access the Internet. This section explains the standard IP and the Mobile Internet Protocol (Mobile IP). Finally, the new Internet Protocol v6 and its effects on the Mobile IP are discussed.

Standard Internet Protocol and mobile devices At the moment, the standard protocol used in the Internet is IP version 4 (IPv4). IPv4 defines nodes that have a unique and fixed address consisting of a quadruplet. The Internet addressing scheme is similar to that of the telephone network, the addressing scheme consists of a number for the country, a number for the city, and then a number for the individual telephone connection. IP addressing also has a prefix that determines the subnet the address is part of. This prefix can be followed by a group and subgroup prefix before the address number for the individual device.

The messages that are sent through the Internet are called packages. They incorporate the sender’s address and port number, and the recipient’s address and port number. A scenario for sending a package over IP can be seen in Figure 3.

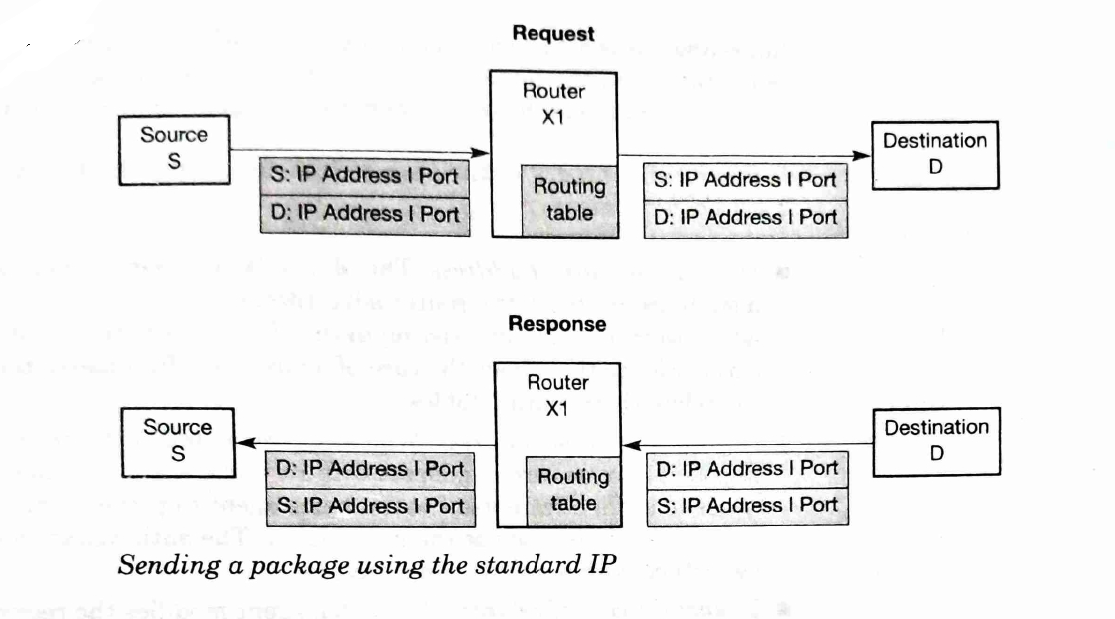


Figure 3

**Sending a package using the standard IP**

The delivery of packages via intermediate hosts is called routing. The routers take the destination address, mask out the low-order bits, and then look up the resulting network address in their routing table. Thus, the IP address typically carries with it information that specifies where it belongs in the IP topology. The routing table contains the next routing host for each network address, and tells the routing host to which host the received package has to be forwarded. There can be many routing hosts between the sender and the receiver of a package.

IPv4 was designed for PCs that do not move around, and it works quite well for this purpose. When using IP with mobile devices, the problem is maintaining an existing transport layer connection with the device. Preferably the device should keep its IP address and port number fixed. As the mobile device moves, it reaches new points of attachment with a different IP address range. The device can now get a new IP address from this point of attachment, but then the connection to its old address will be broken. Mobile IP provides a way to solve this problem and how to enable mobile devices to communicate over IPv4.

**Mobile Internet Protocol**

The Mobile IP was created to overcome the problems of IPv4 for mobile devices. In 1996, the Mobile IP working group submitted an IPv4 Mobile Host Protocol to the Internet Engineering Steering Committee (IESC). To overcome the address problems of IPv4 for mobile nodes as described above, Mobile IP uses two IP addresses: a fixed home address and a care-of address that changes at each new point of attachment. The care-of address allows the mobile device to remain connected and reachable at a new location while still retaining a consistent identity across the network.

**Home address and mobile IP**

The home address is attached to a home agent, so whenever the mobile node is not attached to the home network, it gets all the packages intended for the mobile node and forwards them to the mobile node’s current point of attachment.

For establishing a connection to a mobile node, the following steps must be performed:

* **Discover the care-of address.** The Mobile IP discovery is built on top of a standard protocol, the router advertisement. The router advertisements already existing in the IP standard are extended to carry information about the care-of addresses. This enables the routers to update their routing tables.
* **Register the care-of address.** Whenever the mobile node moves, it registers its new care-of address with its home agent. The mobile node needs to authenticate itself to the home agent to prevent unauthorized nodes from registering at the home agent. The authentication is performed with a digital signature.
* **Tunnel the care-of address.** The home agent modifies the received packages so that the care-of address appears as the destination IP address. This is called redirection or tunneling. When a packet arrives at the care-of address, the reverse transformation is applied. This results in a packet that once again has the mobile node’s home address as the destination IP address. Figure 4 shows this tunneling process for the request. As the sender address is unchanged, the reply from the mobile node goes directly to the sender, not via the home agent. This results in asymmetric routing – a triangle routing – and can cause routing inefficiencies.

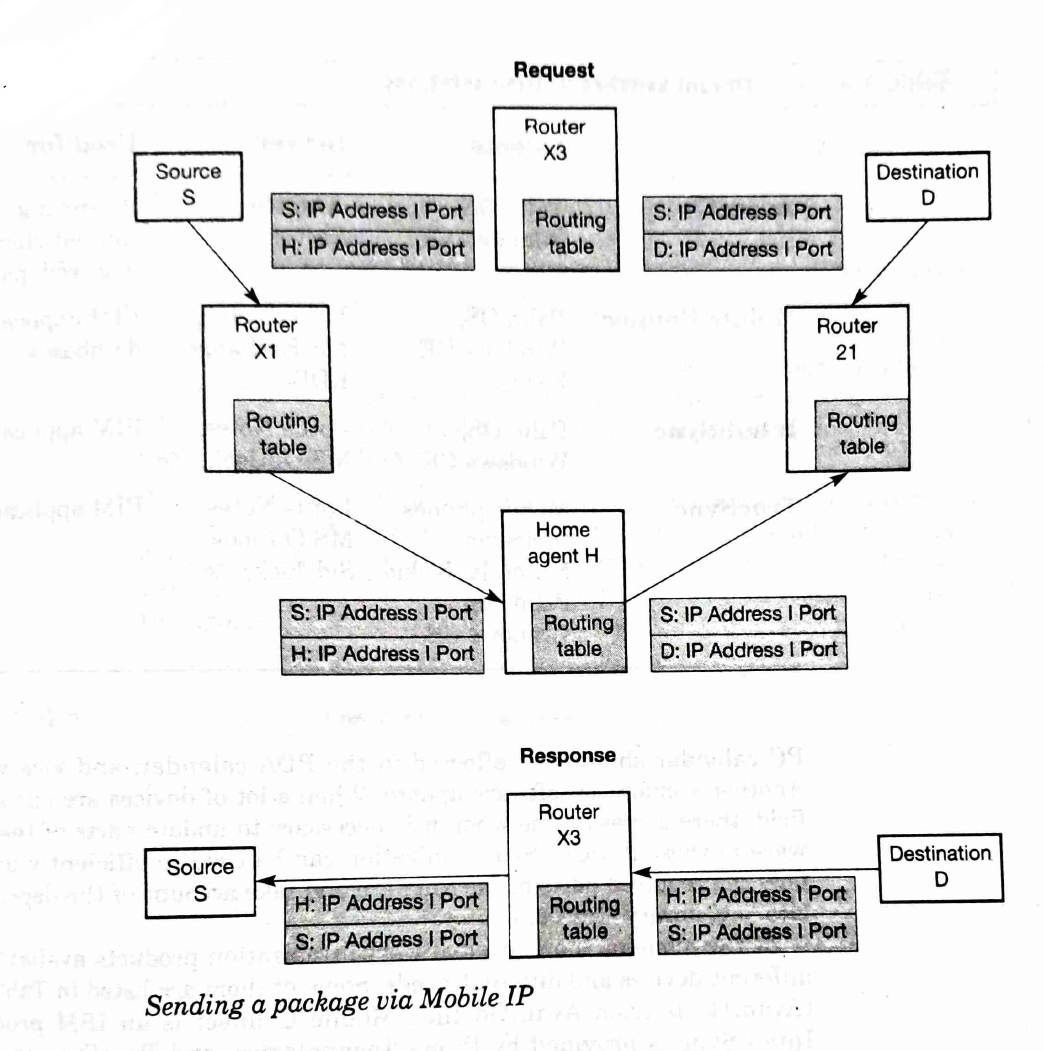


Figure 4

Mobile IP is still an ongoing effort and under discussion. One of the open points is the firewall concept. Firewalls block incoming packages that do not meet specific criteria. One of these criteria is that no incoming packet can have an internal IP address as source. But with the Mobile IP protocol, this is exactly the case if a mobile node outside its home network wants to send a packet to its home network.

**Changes to Internet Protocol Version 6**

IPv6 will include many features for mobility support that are currently missing in IPv4. IPv6 features relevant for Mobile IP are stateless address autoconfiguration and neighbor discovery. With these features, a mobile node can create or obtain a topologically correct care-of address for the current point of attachment, without the need for a foreign agent to provide the mobile node with such address.

A big difference between IPv4 and IPv6 is that IPv6 expects all nodes to implement strong encryption and authentication features. Therefore, efforts are made to enhance Mobile IP to be fully compatible with IPv6, which will improve security and address management.

**Figure 4** **Sending a package via Mobile IP**

Request:

* Source S
  + S: IP Address | Port
  + H: IP Address | Port
* Router X1
  + Routing table
* Router X3
  + S: IP Address | Port
  + D: IP Address | Port
* Home agent H
  + S: IP Address | Port
  + H: IP Address | Port
  + Routing table
* Router 21
  + Routing table
* Destination D
  + S: IP Address | Port
  + D: IP Address | Port

Response:

* Router X3
  + S: IP Address | Port
  + H: IP Address | Port
  + Routing table
* Destination D
  + S: IP Address | Port

**Mobile IP for IPv6** can use the IPv6 security features, and need not provide its own security mechanism. Although IPv6 will support mobility to a greater degree than IPv4, it will still need Mobile IP to make mobility transparent to applications and higher-level protocols such as TCP. Therefore, the Mobile IP working group will submit an IPv6 Mobile IP protocol to the IESG for standardization.

**4.1.4 Synchronization and replication protocols** Synchronization, also called replication in the database area, keeps data consistent between different devices. An example of synchronization is having an electronic calendar on the PC and on the PDA. Changes in the PC calendar should be reflected in the PDA calendar, and vice versa. Another scenario is software update. When a lot of devices are out in the field, there comes a time when it is necessary to update parts of the software in these devices. Synchronization can be used to efficiently update only the required parts of the software and take account of the dependencies (e.g. library versions).

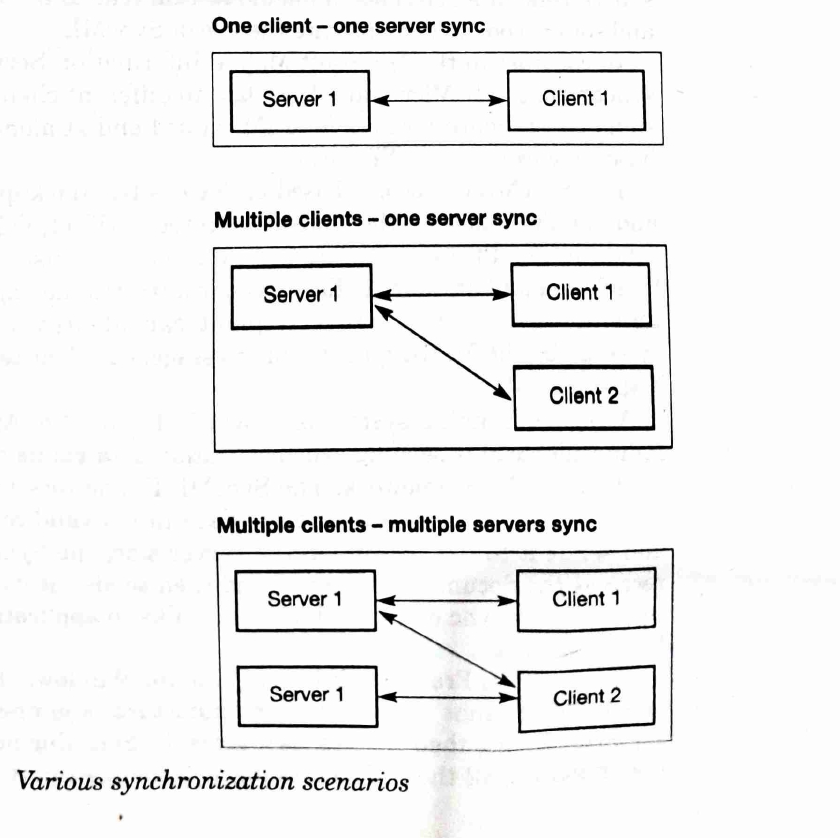
**Table 4.4 Different synchronization solutions**

| **Clients** | **Server** | **Used for** |
| --- | --- | --- |
| AvantGo | AvantGo Server | Retrieving content channels (e.g., Web pages) |
| Mobile Connect | Lotus Notes, MS Exchange, RDBS | PIM applications, databases |
| IntelliSync | Lotus Notes, MS Outlook, etc. | PIM applications |
| TrueSync | Mobile phones (Ericsson, Motorola, Nokia), Sidekick, Palm OS, Windows CE | PIM applications |

**Synchronization principles** To synchronize data, such as calendar entries or address books, between several pervasive computing devices, there are two strategies: device – server synchronization; and device–device synchronization. As can be seen in Figure 5, this can result in complex scenarios, where different device clients can even synchronize with different servers. When performing device-to-device synchronization, one device needs to act as a server. To handle out-of-sync situations, a special protocol is needed. Synchronization protocols typically consist of the following steps:

1. **Presynchronization.** To prepare the actual synchronization, some action must be taken before this can happen. These actions fall into the following groups: authentication, authorization, and determination of device capabilities. Authentication ensures that the server is who it claims to be, and that the client is who it claims to be. Authorization checks whether the client is allowed to perform the requested action (e.g. delete, update, or create new entries). Finally, the server determines the device capabilities (e.g. maximum buffer size) to optimize the data flow to the device.
2. **Synchronization.** This is the part in which the synchronization data are exchanged. Between two synchronization partners, all local IDs of data entries are mapped to global IDs known to both partners. Every partner therefore has a mapping table to map local to global IDs. Only the updated, new, or deleted entries are exchanged. If both partners update the same data entry, there will be a conflict. This update conflict can be resolved in different ways: attempt to merge the updates, duplicate the entries, let one entry win over the other, or do nothing and report the conflict so that the user can solve it.
3. **Post-synchronization.** At this point all the clean-up tasks are performed, such as updating the mapping tables and reporting unresolved conflicts.

**Figure 5**

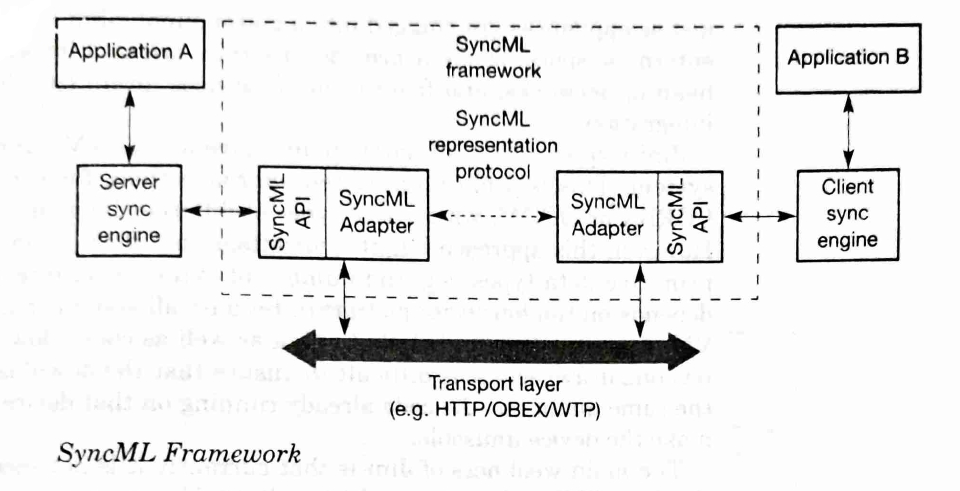


* One client – one server sync
* Multiple clients – one server sync
* Multiple clients – multiple servers sync

SyncML is a technology for distributed software systems. It was founded by major companies including Ericsson, IBM, Lotus, Motorola, Nokia, Palm, Psion, and Starfish. SyncML aims to provide a standardized data synchronization protocol that supports a wide range of applications and devices. It supports standard formats like vCard and vCalendar and allows for synchronization between different types of devices using a uniform protocol. The SyncML Framework is designed to be integrated into various devices and platforms, offering tools for developers to easily incorporate SyncML support into their products.

**Figure 6**

* Diagram showing SyncML synchronization system setup



**4.1.5 Distributed services** Many pervasive computing scenarios consist of networked components that build a distributed system, like mobile phones or PDAs with wireless connectivity. These systems face challenges such as reliability, security, and scalability. As networks become more interconnected and the number of interacting systems grows, the importance of robust distributed services increases. Examples include Sun’s Jini and Microsoft’s Universal Plug and Play, which provide frameworks for seamless interconnectivity and device integration within a distributed system.

**Jini Technology Overview:** Jini is a service-oriented infrastructure, ideal for federating services within an enterprise space. It requires all participants to have a Java VM, aligning closely with CORBA or DCOM for data type handling but is more restricted and depends heavily on the Java platform for distribution of data and code.

* **Discovery:** Service that finds other Jini members in the community.
* **Look-up:** Directory that understands the Java hierarchy and provides service proxies to clients.
* **Leasing:** Ensures the Jini network is self-healing by requiring services to renew their availability.
* **Remote Events:** Allow Jini services to notify participants in the Jini community.
* **Transactions:** Similar to database transactions, enabling consistent state after computations.

**Challenges and Limitations:**

* Jini is currently not as secure, missing critical authentication and authorization services.
* The downloaded code from Jini might not always integrate seamlessly with existing systems, posing risks to device usability.

**SyncML and Jini Comparisons:**

* **SyncML** is focused on broad device interoperability across different platforms using standard formats like vCard and vCalendar.
* **Jini** facilitates dynamic service composition within Java environments, with a strong focus on spontaneous networking but is limited by the need for Java compatibility.

**Universal Plug and Play (UPnP):** Created by Microsoft and supported by major companies like IBM and Intel, UPnP allows for zero-configuration networking, differing from Jini by utilizing HTTP and XML for communication instead of Java, which may offer more open standards compatibility but possibly less security.

**Scenarios in Jini Services:**

* Describes a Jini service consumer using a service provider through Java VMs, where services like printers are dynamically accessed and controlled via a look-up service. This avoids bottlenecks by allowing direct service interactions after initial connection setups.

**UPnP (Universal Plug and Play) Protocols and Services:**

* **IP Addressing:** Devices on a UPnP network get an IP address through DHCP or Auto IP.
* **Discovery:** Utilizes SSDP (Simple Service Discovery Protocol) for service discovery.
* **Description:** Devices provide a description in XML format which includes vendor-specific data and available services.
* **Control:** Control points can send requests to devices based on SOAP protocols which allow remote function calls.
* **Events:** Devices subscribe to events using GENA (General Event Notification Architecture), allowing them to send and receive notifications related to service events.
* **Presentation:** Devices can specify a presentation URL for remote configuration via a browser.

**UPnP Operation Steps:**

1. **DHCP Discovery:** Client requests an IP from DHCP server, beginning interaction.
2. **Service Advertisement and Discovery:** Using SSDP, the device advertises its services, which are then discovered by control points.
3. **Service Description and Connection:** Device sends an XML document describing its services to the control point, facilitating connection and interaction.

**Message and Transaction-based Protocols:** These protocols ensure reliable message delivery and transaction integrity in pervasive computing environments, which are crucial for applications like e-commerce where guaranteed and atomic operations are necessary.

* **Messaging Systems:** Use of queues to ensure delivery and allow for asynchronous communication.
* **Transactional Databases:** Use SOAP for ensuring that transactions are processed in a consistent and reliable manner.

**Message Queuing Scenarios:**

* **One-to-one queues:** A direct sequence where Queue A sends to Queue B, then to Queue C.
* **One-to-many queues:** Queue A distributes messages to multiple queues (B, C, D).
* **Many-to-one queues:** Multiple sources (Queue A and B) sending messages to a single destination (Queue C).

**Transactional Databases and Messaging Systems:**

* Discuss the integration of smaller, more efficient transactional databases suitable for pervasive computing devices, with examples including IBM’s DB2e and Oracle’s Oracle Lite.
* Mention of major messaging products like ExpressQ and MSMQ, highlighting their fit for embedded systems.

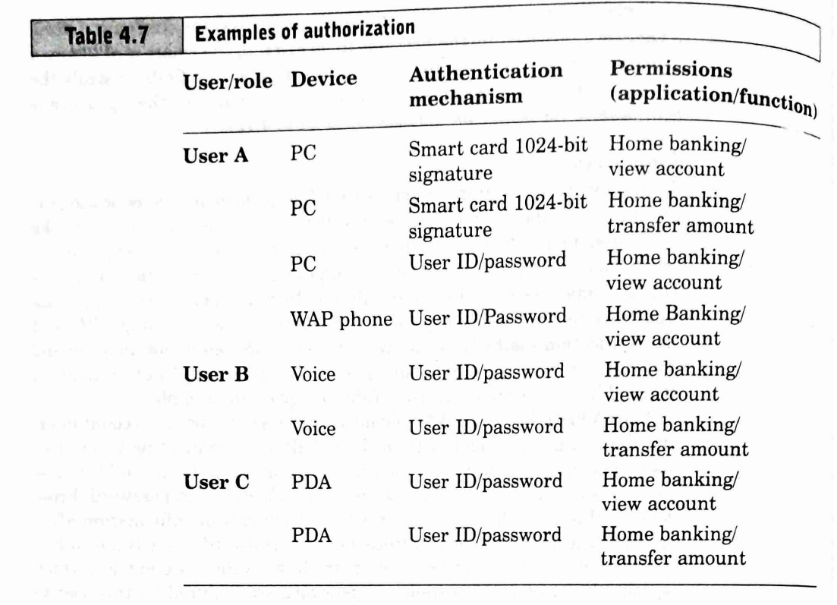
**Security in Pervasive Computing:**

* Introduction to security aspects in pervasive computing, focusing on server-side security concepts such as identification, authentication, authorization, and non-repudiation.
* Details on how cryptographic protocols are utilized for secure transmission of data.
* Explanation of various identification and authentication methods, including user IDs, smart cards, and more sophisticated systems involving public key infrastructure (PKI).

**Authentication Protocol Example:**

* Illustration of an authentication protocol using a smart card, where the user must authenticate with a password and the server challenges the smart card to provide a signature, ensuring secure identification and transaction.

**Examples of Authorization (Table 4.7):**



* **User A:** Utilizes a PC with smart card 1024-bit signature or User ID/password for home banking (view account, transfer amount).
* **User B:** Uses voice identification with User ID/password for home banking on a voice interface.
* **User C:** Operates a PDA with User ID/password for both viewing account details and transferring amounts.

**Transaction Authorization:**

* **Digital Signatures Endorsed by a Password:** Secure transaction method where a token generates a signature only after the user provides a password.
* **Transaction Authorization Numbers (TANs):** Used for sensitive transactions, issued in blocks to the user who must acknowledge their receipt and keep them secret.

**Device Security:**

* Discusses the varying levels of security in pervasive computing devices, highlighting how some devices are very secure and others less so due to their ability to download arbitrary software or lack of memory protection.

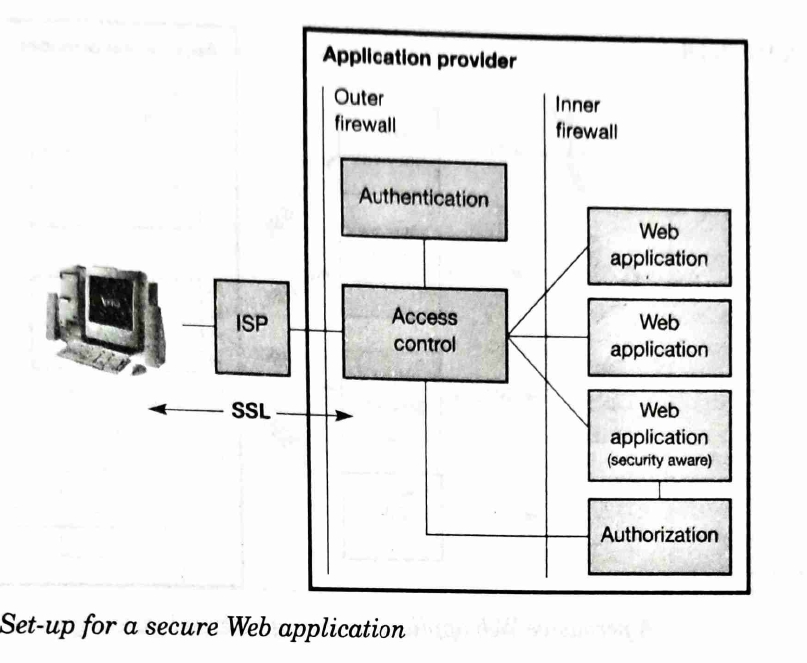
**Server-Side Security:**

* Emphasizes the need for robust server-side security measures, including the setup of demilitarized zones and dual firewalls to protect sensitive data and control access to web applications.

**WAP and PDA Security Concerns:**

* Details the vulnerabilities associated with WAP phones and PDAs, noting potential risks like Trojan horse attacks and the limitations of encryption methods.

**Setup for a Secure Web Application :**



* Describes a setup that utilizes SSL for secure communication between the user’s PC and the application provider’s servers, ensuring that sensitive data remains protected during transmission.

The below figures 7 and 8 illustrate the setup of a pervasive Web application that uses external and proprietary gateways to enhance security:

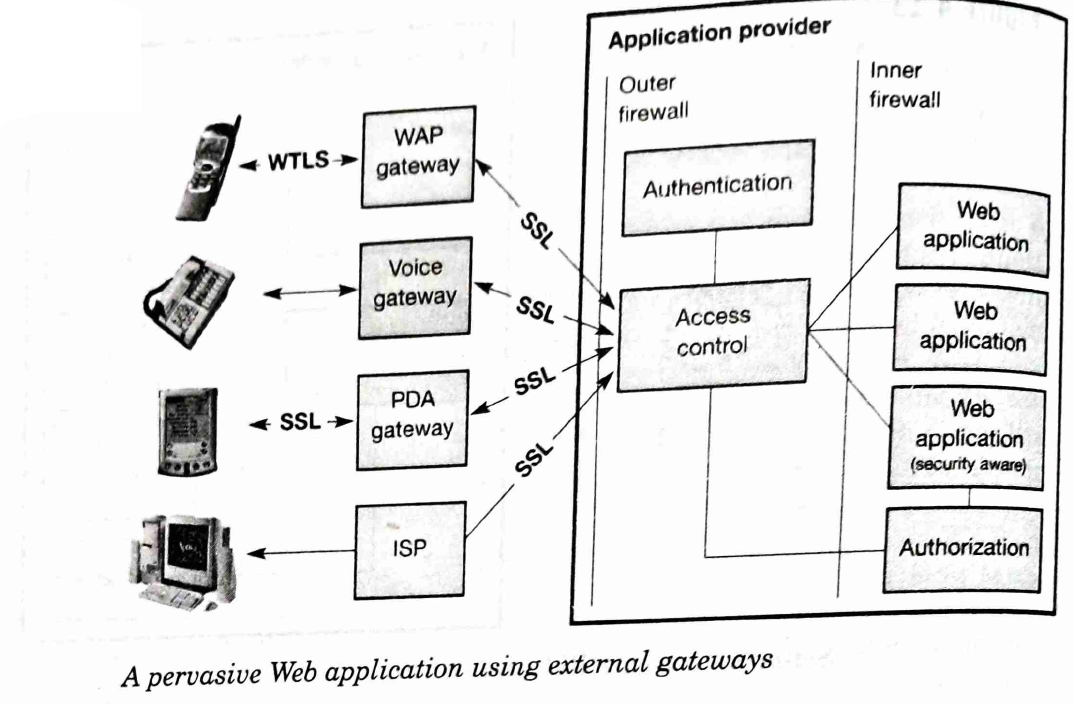


Figure 7

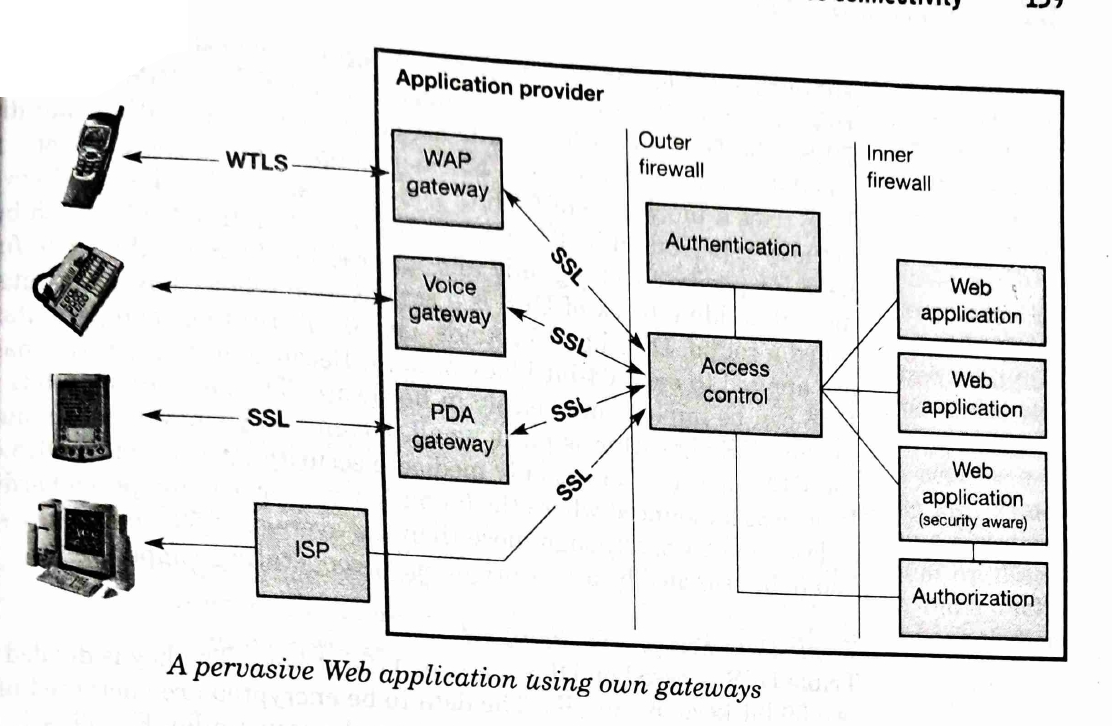


Figure 8

* **Figure 7**: Shows the interaction between different types of devices (like WAP phones, PDAs) and their respective gateways, each using SSL for secure connections. The diagram emphasizes how these devices connect through an application provider’s setup that includes outer and inner firewalls, authentication, access control, and web applications.
* **Figure 8**: Similar to Figure A but depicts the application using its own gateways for WAP, voice, and PDA interfaces, which could potentially offer more controlled security by keeping the infrastructure within the provider's direct control.

**Cryptographic Algorithms Overview:**

* **Symmetric Cryptographic Algorithms**: Fast and suitable for encrypting large amounts of data. The same key is used for both encryption and decryption, which poses a security risk unless the key is transmitted securely.
* **Data Encryption Standard (DES)**: A block cipher with a block size of 64 bits and a key size of 56 bits, which became less secure over time due to its susceptibility to brute force attacks.
* **Triple Data Encryption Standard (Triple DES)**: Enhances DES by using three keys for encryption, significantly increasing security against brute force attacks.
* **Advanced Encryption Standard (AES)**: Successor to DES, using keys of 128, 192, or 256 bits to encrypt data, which makes it robust against all known attack methods and efficient in both software and hardware implementations.

**Public-Key Algorithms**:

* Describes the concept of public-key cryptography, where a pair of keys (one for encryption and one for decryption) are used, making it impossible to derive the decryption key from the encryption key alone. This was a significant development in cryptographic technology.

**Public-Key Cryptography:**

* Public-key algorithms use a pair of keys for encryption and decryption. The private key is kept secret and the public key is distributed openly. It is computationally infeasible to derive the private key from the public key.
* RSA (Rivest-Shamir-Adleman) is the most notable public-key algorithm, which is based on the difficulty of factoring large prime numbers. RSA uses key pairs involving a modulus and a public exponent to secure data.

**Digital Signature Algorithm (DSA):**

* Developed by the NIST in 1991 for the Digital Signature Standard (DSS), it relies on the security of cryptographic hash functions and uses asymmetric keys for creating and verifying digital signatures.

**Elliptic Curve Cryptography (ECC):**

* Uses elliptic curves over finite fields for faster and more secure public-key encryption, particularly suitable for devices with limited processing power due to its smaller key size requirements compared to RSA and DSA.

**Device Management:**

* The integration of pervasive computing devices into business environments introduces challenges such as device tracking, managing software updates, and securing device access. The cost and complexity of managing such devices are significant, with the average cost per device cited as high due to the need for ongoing support and updates.

**Software Distribution and Version Management:**

* Discusses the importance of managing hardware capabilities and software versions in a fast-evolving technological landscape. Effective management must account for the diverse hardware specifications and software compatibility issues that arise with rapid iteration cycles in device and software releases.

**Library Management and Device Connectivity:**

* **Library Management**: Critical for ensuring that devices run compatible software versions without conflict. This includes managing different versions of libraries needed by various applications and ensuring these libraries are updated or removed as needed without causing system instability.

**Device Management Issues:**

* **Connection Issues**: Devices may not always be connected to the network, leading to challenges in managing software updates or synchronization.
* **Security Concerns**: Insecure and unstable connections can jeopardize data integrity, necessitating robust encryption and secure communication protocols.
* **Software Updates**: Managing and updating device operating systems and applications are crucial to maintaining security and functionality. This often involves modular updates to minimize disruption.

**Approaches to Device Management:**

* Discusses the necessity of incorporating advanced management techniques, such as unique device identifiers and database integration, to effectively manage hardware and software configurations across various devices.
* **Figure 9 Illustration**: Shows a schematic of a device-management system that integrates database and gateway technologies to handle updates and synchronization for devices like PDAs and smartphones.

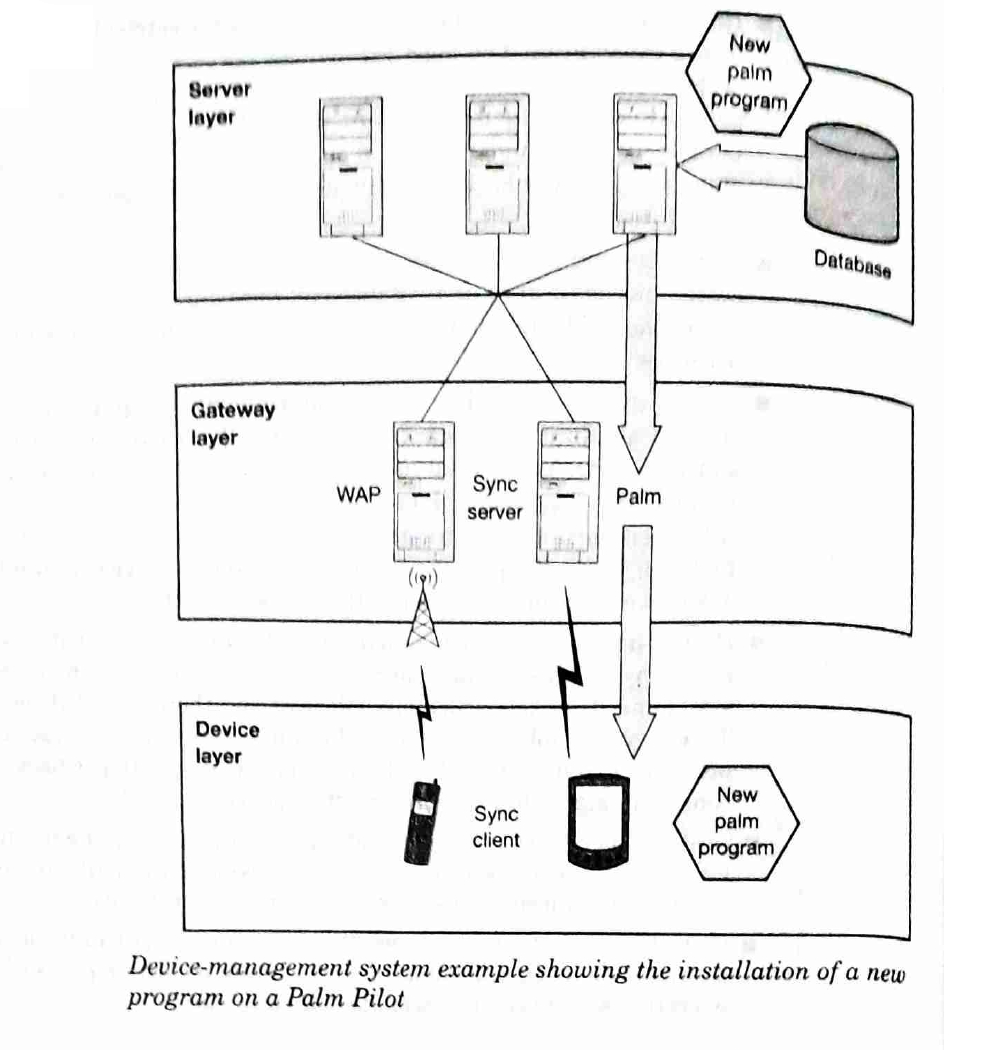


Figure 9

**Summary of Device Management:**

* Stresses the complexity and cost implications of managing pervasive computing devices, particularly as the number of devices exponentially increases. Effective management strategies are essential to control costs and ensure efficient operation.