# CONTENTS

i. ABSTRACT 1  
ii. INTRODUCTION 2  
iii. CURRENT EMBEDDED TECHNOLOGY 3  
iv. UBIQUITOUS/PERVASIVE COMPUTING 5  
v. DISTRIBUTED COMPUTING ENVIRONMENT 6  
   a) AMBIENT INTELLIGENCE 6  
   b) MOBILE AD HOC NETWORKING 8  
vi. ARCHITECTURE 11  
vii. IMPLEMENTATION 16  
   a) DEVICE REQUIREMENTS 16  
   b) COMMUNICATION 17  
   c) CONTEXT AWARENESS 18  
   d) ADAPTATION 19  
   e) STEERABLE INTERFACE 20  
   f) SECURITY POLICY 21  
viii. HAVi – AN IMPLEMENTATION PROTOTYPE 24  
ix. CONCLUSION 26  
x. REFERENCE 27
ABSTRACT

Pervasive computing refers to embedding computers and communication in our environment. Pervasive computing provides an attractive vision for the future of computing. The idea behind the pervasive computing is to make the computing power disappear in the environment, but will always be there whenever needed or in other words it means availability and invisibility. These invisible computers won’t have keyboards or screens, but will watch us, listen to us and interact with us. Pervasive computing makes the computer operate in the messy and unstructured world of real people and real objects. Distributed devices in this environment must have the ability to dynamically discover and integrate other devices. The prime goal of this technology is to make human life more simple, safe and efficient by using the ambient intelligence of computers.
INTRODUCTION

Pervasive computing environments involve the interaction, coordination, and cooperation of numerous, casually accessible, and often invisible computing devices. These devices will connect via wired and wireless links to one another as well as to the global networking infrastructure to provide more relevant information and integrated services. Existing approaches to building distributed applications, including client/server computing, are ill suited to meet this challenge. They are targeted at smaller and less dynamic computing environments and lack sufficient facilities to manage changes in the network configurations. Networked computing devices will proliferate in the user’s landscape, being embedded in objects ranging from home appliances to clothing. Applications will have greater awareness of context, and thus will be able to provide more intelligent services that reduce the burden on users to direct and interact with applications. Many applications will resemble agents that carry out tasks on behalf of users by exploiting the rich sets of services available within computing environments.

Mobile computing and communication is one of the major parts of the pervasive computing system. Here data and computing resources are shared among the various devices. The coordination between these devices is maintained through communication, which may be wired or wireless. With the advent of Bluetooth and Ad hoc networking technologies the wireless communication has overtaken the wired counter part.

The reduction in size and cost of processor chips made it possible to implement it in every field of life. Nowadays about 99% of processors made are for embedded devices compared to the PC applications. Voice and Gesture recognition along with steerable interface will make the interactions and use of these devices more user friendly. Efficient security and privacy policies along with power management can enhance the performance of such systems.
CURRENT EMBEDDED TECHNOLOGY

Embedded technology is the process of introducing computing power to various appliances. These devices are intended to perform certain specific jobs and processors giving the computing power are designed in an application oriented way. Computers are hidden in numerous information appliances which we use in our day-to-day life. These devices find there application in every segment of life such as consumer electronics, avionics, biomedical engineering, manufacturing, process control, industrial, communication, defence etc…

Embedded systems, based on there functionality and performance requirement are basically categorized as:

i. Stand alone systems
ii. Real time systems
iii. Networked systems
iv. Mobile devices

Stand alone systems work in stand alone mode, taking inputs and producing desired outputs. They do not have any dependence on other systems. Embedded systems in which some specific work has to be done in a specific time period are called Real time systems. Meeting the dead line is the most important requirement of a real time system. In Hard real time systems, missing a deadline may lead to a catastrophe and in Soft real time systems such problem is not present. Systems which are provided with network interfaces and accessed by networks such as LAN or the Internet are called Networked Systems. Networking may be wired or wireless. Mobile devices are devices which move from one location to another, like mobile phones, PDA’S etc.

Today, many people carry numerous portable devices, such as laptops, mobile phones, PDAs and mp3 players, for use in their professional and private lives. For the
most part, these devices are used separately i.e, their applications do not interact. However, if they could interact directly, participants at a meeting could share documents or presentations, business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone, as commuters exit a train, their laptops could remain online; likewise, incoming email could now be diverted to their PDAs.

In such a distributed environment where several embedded devices has to communicate and co-ordinate with each other. For this a communication link is required which may be wired or wireless. In initial stages of Networked embedded system environments wired connection was preferred as it provided a safer and faster channel for communication. But the cost, immovability and the cables running around the floorboards became less attractive. On top of this, dishing out the cash for network cards, cables and a hub/switch reserved this practice to the more elite computer users, until wireless networking hit the scene.

Infrared communication was initially used for wireless communication because of the low cost offered by it. But it suffered from the limitation that it can be used only within Line Of Sight. IEEE introduced 802.11 as the international standard for wireless LANs. This used a 2.4GHz transmission band while maintaining a steady 1-2 Mbps bandwidth rate. Being that this was extremely slow compared to 100Mbit wired LANs, it took a while for the 802.11 standard to develop into a viable solution, achieved shortly after with the 802.11a, b and g standards, offering bandwidth ranging from 11Mbps to 54Mbps. Although this is still considerably short of the 100Mbit found in cabled networks, 802.1 x wireless technologies is now literally regarded as the future of networking. Bluetooth, Wi-Fi, Wi-Max are the latest solutions, under the 802.1x standard, for wireless communication over short, medium and long range communication respectively.
UBIQUITOUS \ PERVASIVE COMPUTING

Pervasive computing can be explained in two different perspectives:

i. User view

ii. Technology view

User view

For an end user Pervasive approach act as a method of augmenting human abilities in context of tasks. It provides Interaction transparency which means that the human user is not aware that there is a computer embedded in the tool or device that he or she is using.

Technological view

It means access to information and software applications are available everywhere and any where. Technically pervasive computing involves in embedding intelligence and computing power to devices which are part of our daily life. As the word ‘Pervasive’ means, we create an environment with intelligence and which can communicate with each other. This technology is intended for mobile as well as localized devices. It must also posses the ability to locate an object or a user using provisions such as Global Positioning System (GPS). After positioning, a dynamic link must be setup for communication which may use the recent concept of ADHOC networking. User can interact with and control these devices using steerable interfaces, using voice and gesture recognition facilities.
DISTRIBUTED COMPUTING ENVIRONMENT

The essence of that vision was the creation of environment saturated with computing and communication capability, yet gracefully integrated with human users. The field of distributed systems arose by the intersection of personal computer and Local Area Network. With the appearance of wireless LANs embedded systems for mobile clients was introduced. These two laid the foundation for the concept of Pervasive computing.

Ambient Intelligence

Objects in pervasive environment are considered to have Ambient Intelligence. Ambient Intelligence refers to a vision of the future, in which people are empowered by an electronic environment that is aware of their presence, and is sensitive and responsive to their needs. It aims at improving the quality of life by creating the desired atmosphere and functionality via intelligent, personalized interconnected systems and services. The transition to such a world requires a paradigm shift in user-system interaction. Speech and gesture recognition modalities address user benefits such as freedom of movement, and are natural candidates for such interactions.

However, implementing these modalities in e.g. a home environment is radically different from implementing known methods such as buttons, dials and remote controls. Smart objects may play an important role in bridging this gap. People have a life-time experience in manipulating tangible objects, and can perform these manipulation tasks with a minimal amount of attention.

Ambient Intelligence refers to electronic environment that are sensitive and responsive to the presence of people. It builds on advanced networking technologies, which allow robust, ad-hoc networks to be formed by a broad range of mobile devices and other objects. By adding adaptive user-system interaction methods, based on new
insights in the way people like to interact with computing devices, digital environments can be created which improve the quality of life of people by acting on their behalf.

Key characteristics of such environments are: ubiquity, awareness, intelligence, and natural interaction. Ubiquity refers to a situation in which we are surrounded by a multitude of interconnected embedded systems, which are invisible and moved into the background of our environment. Awareness refers to the ability of the system to locate and recognize objects and people. Intelligence refers to the fact that the digital surrounding is able to analyze the context, to adapt itself to the people that live in it, to learn from their behavior, and eventually to recognize as well as show emotion. Natural Interaction finally refers to advanced modalities like speech-, gesture- and object recognition, which will allow a more natural communication with the digital environment than is possible today.

Evolutionary development of Pervasive computing environment and Relation between Pervasive computing with Distributed systems and mobile computing
We envisage that in the near future, mobile and embedded devices will be capable of providing customized information, services and computation platforms. People will need the cooperation of services available in their resource rich vicinity to satisfy their information needs. Service composition systems for the pervasive computing environment need a different design approach than those developed for wired services. Service composition architectures in wired infrastructure assume the existence of a centralized composition entity that carries out the discovery, integration and execution of services distributed over the web or network. This Client/Server based computing, are ill suited to meet this challenge. They are targeted at smaller and less dynamic computing environments and lack sufficient facilities to manage changes in the network configurations.

Mobile Ad hoc Networking

So we introduce a system architecture which provides an integrated and comprehensive framework for building pervasive applications. It includes a set of services that help to structure applications and simplify the task of coping with constant change. So a pervasive computing environment is expected to be based on the recent progresses and advances in computing and communication technologies. Next generation of mobile communications is likely to be based on an infrastructure less Mobile Ad hoc Networks (MANETs).

A MANET is a collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. Ad-hoc mode essentially eliminates the need for an access point. An Ad-Hoc network only requires wireless adapters to communicate hence significantly reducing the cost and maintenance compared to a network structured around an access point. Most or all nodes in the network participate in the network tasks. While traditional networks are static, i.e., nodes do not move and new nodes are not attached to or detached from the network on a frequent basis, the ad-hoc network is extremely dynamic. The nodes are autonomous and may have varying mobility, and they may
enter and leave the network for some reason or another, for example, a mobile node may move out of reach of other nodes, thus being unable to send or receive information, or a node may suffer from power failure or destruction and often act as routers at the same time. Another important difference between traditional and ad hoc networks is that traditional networks tend to be wired, where as an ad hoc network most likely is wireless, which increases their complexity even further.

MANET has the following features:

1) Autonomous terminal: In MANET, each mobile terminal is an autonomous node, which may function as both a host and a router. In other words, besides the basic processing ability as a host, the mobile nodes can also perform switching functions as a router. So usually endpoints and switches are indistinguishable in MANET.
2) Distributed operation: Since there is no background network for the central control of the network operations, the control and management of the network is distributed among the terminals. The nodes involved in a MANET should collaborate amongst themselves and each node acts as a relay as needed, to implement functions e.g. security and routing.

3) Multihop routing: Basic types of ad hoc routing algorithms can be single-hop and multihop, based on different link layer attributes and routing protocols. Single-hop MANET is simpler than multihop in terms of structure and implementation, with the cost of lesser functionality and applicability. When delivering data packets from a source to its destination out of the direct wireless transmission range, the packets should be forwarded via one or more intermediate nodes.

4) Dynamic network topology. Since the nodes are mobile, the network topology may change rapidly and unpredictably and the connectivity among the terminals may vary with time. MANET should adapt to the traffic and propagation conditions as well as the mobility patterns of the mobile network nodes. The mobile nodes in the network dynamically establish routing among themselves as they move about, forming their own network on the fly. Moreover, a user in the MANET may not only operate within the ad hoc network, but may require access to a public fixed network (e.g. Internet).

5) Fluctuating link capacity. The nature of high bit-error rates of wireless connection might be more profound in a MANET. One end-to-end path can be shared by several sessions. The channel over which the terminals communicate is subject to noise, fading, and interference, and has less bandwidth than a wired network. In some scenarios, the path between any pair of users can traverse multiple wireless links and the link themselves can be heterogeneous.

6) Light-weight terminals. In most cases, the MANET nodes are mobile devices with less CPU processing capability, small memory size, and low power storage. Such devices need optimized algorithms and mechanisms that implement the computing and communicating functions.
ARCHITECTURE

Pervasive computing is characterized by a high degree of heterogeneity: devices and distributed components are from different vendors and sources. Support of mobility and distribution in such a context requires open distributed computing architectures and open protocols. Openness means that specifications of architectures and protocols are public documents developed by neutral organizations. System architecture is designed for performing the services such as:

- Automatic discovery or devices added or removed from the network
- Addressing scheme and message-transfer service
- Lookup service for discovering resources
- Posting and receiving local or remote events
- Streaming and controlling data streams
- Reserving devices and performing scheduled actions
- User interaction

Various architectures with particular domain oriented features are present. Here a reactive service composition architecture is being discussed, as it is somewhat general and simple. Service Composition can be defined as the process of creating customized services from existing services by a process of dynamic discovery, integration and execution of those services in a planned order to satisfy a request from client. We have designed a distributed architecture to perform service composition in pervasive computing environment. Central to our system is the concept of a distributed broker that can execute at any node in the environment. An individual broker handles each composite service request, thus making the design of the system immune to central point of failure. A broker may be selected based on various parameters such as resource capability, geometric topology of the nodes and proximity of the node to the services that are required to compose a particular request. Current prototype of our system can be implemented over Bluetooth. We shall refer to a client as a device from where the service composition request originates. A broker is a device that coordinates the different components to calculate the result.
Layered architecture

Network Layer:

The Network Layer forms the lowest layer in the architecture and encapsulates networking protocols that provide wireless/ad-hoc connectivity to peer devices in the vicinity. We assume the existence of a suitable network layer that provides us with connectivity to the neighboring devices.

Service Discovery Layer:

The service discovery layer is required for the proper functioning of the composition platform. There is a direct dependence of the success of the composition techniques on the underlying service discovery mechanisms. This layer encompasses the protocol used to discover the different services that are available in the vicinity of a mobile device. Our design of the service discovery mechanism is primarily based on the principles of Peer-to-peer service discovery, Dynamic caching of neighboring service descriptions, Semantic description based service matching, service request routing and propagation control. We do not employ central lookup-server based service discovery and maintenance. Each device has a Service Manager where the local services register their information. Service Managers advertise their services to neighboring nodes and these advertisements are cached. Services are described using a semantically rich language which is used in service matching also. On cache miss, the service request is forwarded to other neighboring nodes.

Service Composition Layer:

This layer is responsible for carrying out the process of managing the discovery and integration of services to yield a composite service. The process model of the composite service is supplied as input to this layer.
Service Execution Layer:

The Service Execution Layer is responsible for carrying out the execution of the different services. Prior to this, the service composition layer provides a feasible order in which the services can be composed and also provides location and invocation information of the service. This layer has a module called the “Fault Recovery Module”, which is responsible to guard against node failures and service unavailability. The Service Execution Layer and the Service Composition Layer are tightly coupled with each other due to their dependence on each other.

Application Layer:

The application layer embodies any software layer that utilizes our service composition platform. The application layer encompasses different GUI facilities to display the result of a composed service and provides the functionality to initiate a request for a composite service

Dynamic Broker Selection Technique

This approach centers on a procedure of dynamically selecting a device to be a broker for a single request in the environment. In the following section, we describe three distinct features of the Dynamic Broker Selection Technique.

Broker Arbitration and Delegation:

When a request for service composition arrives at the service composition module in a mobile device it finalizes a platform that is going to carry out the composition and monitor the execution. Once the platform has been chosen, the device is informed of its responsibility. The mobile device acting as the broker is responsible for the whole composition process for a certain request. The selection of the broker platform may be dependent on several parameters: power of the platform (battery power left), number of services in the immediate vicinity, stability of the platform, etc. The brokerage arbitration might make the originator of the request to be
the broker for that particular composition. Each request thus may be assigned a separate broker. This makes the architecture immune to central point of failure and the judicious choice of brokerage platform has the potential of distributing the load appropriately within the different devices. This avoids the problem of swamping the central composition entity by numerous requests.

Service Integration and Execution:

The assigned broker’s first job is to discover the services from its vicinity. The broker progressively increases its search “radius”, a number of devices that it can reach by asking other devices in its radio range to forward service request, to discover all of the different services necessary for the composition. The broker returns failure when it fails to discover all of the required services. Service discovery and integration is followed by service execution. The information obtained during the service discovery (service address, port, invocation protocol) is utilized to execute the services.

Fault Recovery:

Faults in ad-hoc environment may occur due to a service failure, due to a sudden unavailability of the selected broker platform, or due to network partition. The standard solution to this problem is to make the requester to initiate a new request for every composite service. This is very inefficient and not applicable in our environment due the relatively high occurrence probability of the above failures. The fault-tolerance module in the architecture employs check pointing to guard against such faults. The broker for a particular request sends back checkpoints and the state of the request to the client of the request after a subtask is complete. The client keeps a cache of this partial result obtained so far. If the broker platform fails, the source node detects the unavailability of updates.
Distributed Brokering Technique

The key idea in this approach is to distribute the brokering of an articular request to different entities in the system by determining their ‘suitability’ to execute a part of the composite request.

Broker Arbitration:

This module performs almost the same set of actions described in the previous section. However, the key difference is that it only tries to determine the broker for the first few services (say S1 to Si) in the whole composition. This layer tries to utilize the resources available in the immediate vicinity instead of looking for the resources required to execute the whole composition. Thus, a single broker only executes a part of the whole composite process (based on the resources that it currently has available to it).

Service Integration and Execution:

The broker is responsible for composing the services S1 to Sn. The broker decides on a service search “radius”. The composition is carried out among services discovered within this radius. Suppose a broker determines that it has services S1 to Si available in its vicinity (within radius r). It goes ahead and carries out the partial integration and execution. It then informs the requester (source node) about the ‘current state’ of the execution. Secondly, it uses the ‘Broker Arbitration’ Module to select another broker which has the ability to carry out a subset or whole of the remaining composition. In this manner, the composition hops from one node to another till the final result is obtained. Then the current broker returns the final answer of the composition to the client.
IMPLEMENTATION

There are many middleware technologies that provide a set of application programming interfaces (APIs) as well as network protocols that can meet the network requirements. It establishes a software platform enabling all devices that form the network to talk to each other, irrespective of their operating systems or interface constraints. In these environments, each device provides a service to other devices in the network. Each device publishes its own interfaces, which other devices can use to communicate with it and thereby access its particular service. This approach ensures compatibility and standardized access among all devices. There are many implementation technologies and protocols developed by various companies like: Sun’s Jini, Microsoft’s UPnP, IBM’s Tspace. The possibilities of Bluetooth is utilized by technologies like Jini for pervasive environment. Bluetooth environment can be used to implement standard TCP/IP protocol.

DEVICE REQUIREMENTS

Two device-related challenges must be addressed by the pervasive computing infrastructure; these are the wide differences between heterogeneous device types and the problems caused by device mobility.

Device heterogeneity:

Heterogeneity in computing systems will not disappear in the future, but instead will increase as the range of computing devices widens. Devices in a pervasive computing environment will include sensors and actuators that mediate between physical and virtual environments; embedded devices in objects such as watches and shoes; home and office appliances such as videos, toasters and telephones; mobile devices, such as handheld organizers and notebooks; and traditional desktop machines. Heterogeneous devices will be required to interact seamlessly, despite wide differences in hardware and software.
capabilities. This will require an infrastructure that maintains knowledge of device characteristics and manages the integration of devices into a coherent system that enables arbitrary device interactions (for example, between a mobile phone and a desktop workstation).

Device mobility:

Mobility introduces problems such as the maintenance of connections as devices move between areas of differing network connectivity, and the handling of network disconnections. While protocols for wireless networking handle some of the problems of mobility, such as routing and handovers, some problems cannot be solved at the network level, as they require knowledge of application semantics. It should be the role of the computing infrastructure to cooperate with applications in order to perform tasks related to device mobility, such as management of replicated data in cases of disconnection.

COMMUNICATION

BLUETOOTH:

Blue tooth is an economical communication technology that allows communicating with one another wirelessly within a 30 feet or 10 meter radius. Blue tooth is specially designed for short range communication. An important outcome of this design is the low power consumption which in turn makes these devices portable. Bluetooth wireless technology makes use of radio frequency technology to communicate through the air. RF incorporates high power transmitters and receivers tuned to a particular frequency range for long ranges as in TV. Short range requires less power and thereby batteries can suffice the power requirements. RF can penetrate the obstacles and there is no requirement of line sight communication. Bluetooth technology operates in 2.4 GHz spectrum. It has a data transmission rate of 700 Kbps. Bluetooth link between two devices consists of of a master and a slave. A piconet consists of a single master and all slaves in close proximity. Only one master is allowed in a single piconet. The ability to form piconets is a significant advantage for
pervasive computing environment design. We can use TCP/IP protocol on top of Bluetooth technology. Bluetooth has protocols for “inquiry” and “connection” between devices. First Bluetooth piconets are formed and then using TCP/IP protocol is used for establishing communication between the devices in an environment.

Various other wireless standards which can be used in mobile, distributed systems are,

- Wireless LAN IEEE 802.11b (Wi-Fi), having a range of about 200 m. It uses a radio frequency of 2.4 GHz band with data transmission rate of 11 Mbps.
- GSM phone with transmission rate of 9.6 Kbps.
- UMTS – 3G mobile 114 kbps (vehicle), 384 Kbps (pedestrian) 2 Mbps (stationary)
- HIPERLAN & IEEE 802.11a using RF of 5 GHz band with data rate currently 20 Mbps eventually 54 Mbps
- Home RF derived from DECT 10Mbps
- Infrared transmission gives a rate of 4Mbps, but can be used only for line of sight communication (so not preferred).

CONTEXT AWARENESS

Context awareness translates to adaptation of the behavior of an application as a function of its current environment. This environment can be characterized as a physical location, an orientation or a user profile. A context-aware application can sense the environment and interpret the events that occur within it. In a mobile and wireless computing environment, changes of location and orientation are frequent. Invisibility of applications will be accomplished in part by reducing input from users and replacing it with knowledge of context.
Context aware software components will exploit information such as the activities in which the user is engaged, proximity to other devices and services, location, time of day and weather conditions. Knowledge of context will also be required to enable adaptation to changing environmental conditions, such as changing bandwidth and input and output devices, which can be brought about by mobility. The infrastructure for pervasive computing should support context awareness by facilitating the gathering of information from sources such as sensors and resource monitors; performing interpretation of data, carrying out dissemination of contextual information to interested parties in a scalable and timely fashion. Location identification of user is needed for a better understanding of context. For this Global Positioning Systems (GPS) are employed.

A very challenging aspect is interpretation, which involves steps such as integration of data from different sources, inference, prediction based on context history, resolution of inconsistencies between context data from different sources, and provision of estimates of the accuracy of contextual information. Capture and storage of past experiences can be used to solve new problems in the future. Experiences are made of events and computers have the ability to record them automatically. Human users only have to recall that information from the computer when it is needed.

ADAPTATION

Adaptation is required in order to overcome the intrinsically dynamic nature of pervasive computing. Mobility of users, devices and software components can occur, leading to changes in the physical and virtual environments of these entities. Moreover, applications can be highly dynamic, with users requiring support for novel tasks and demanding the ability to change requirements on the fly. It should be the role of the infrastructure for pervasive computing to facilitate adaptation, which may involve adapting individual software components and/or reconfiguring bindings of components by adding, removing or substituting components. Adaptation may be done in an application-aware or application-transparent manner. Dynamic adaptation
can involve complex issues such as managing the adaptation of software components that are used simultaneously by applications with different requirements, and maintaining a consistent external view of a component that has behavior that evolves over time.

STEERABLE INTERFACES

They are a new class of interactive interfaces that can be moved around to appear on ordinary objects and surfaces anywhere in a space. By dynamically adapting the form, function, and location of an interface to suit the context of the user, such steerable interfaces have the potential to offer radically new and powerful styles of interaction in intelligent pervasive computing spaces. We propose defining characteristics of steerable interfaces and present the first steerable interface system that combines projection, gesture recognition, user tracking, environment modeling and geometric reasoning components within a system architecture. An essential element to realize this notion of “computing woven into space” is a ubiquitous interface to computing access to pervasive computing resources should be available everywhere. For instance, access to computing services has been through computer monitors, touch screen panels, keyboards, mice, PDAs, cellular phones etc, all special surfaces and devices available in the environment or carried by people.

In this paper, we pursue an alternate vision for the pervasive computing interface, especially in the context of intelligent environments. We propose that as computing disappears into the physical environment, what matters most to the user is the interface to computing. The interface should appear whenever the user needs it, wherever the user needs it, and in a form most suitable for natural interaction. In particular, both input and output interfaces should be available to the user anywhere in space, without the need for special devices.

To realize this, we introduce the concept of a steerable interface to computing that can be moved around a physical environment on to ordinary objects or surfaces.
Steerable interfaces are important as they provide interaction wherever it is needed in a space. In many cases, the interface just appears when needed and where needed, as a natural extension to the physical environment, without the user having to perform any deliberate actions. And as the user neither carries nor approaches any special devices, the interaction is casual. The user can also request for the interface anywhere through natural actions such as simply asking or making a specific gesture. Steerable interfaces have the potential to change how we access information in a number of different domains and applications.

For example, during shopping, information about a product can be made available right at the product location when a shopper is in the vicinity of the product. At home, a television or a computer can appear on demand on any wall or table or countertop. Steerable interfaces can also result in new forms of entertainment such as games in the real world with virtual characters and hybrid theater combining the real and the virtual.

SECURITY POLICY

A security policy is a set of rules for authorization, access control, and trust in a certain domain, it can also contain information about some users’ roles and the abilities associated with those roles. Theft of service is the actual number one security problem in cellular networks. A similar problem exists with computer network services. Solutions devised for cellular telephony can be applied. Control of access to services relies on a form of identification. Either a user or a device may be identified. However Device identification may be considered equivalent to user identification in
cases where the device is a personal belonging of the user. Indeed, in contrast to a
desktop which can be shared by several members of a family, a PDA is a personal
assistant. Identification of the palmtop means as well identification of its user. Each
Bluetooth device has a 48-bit identifier that can be used for that purpose. Secret key
authentication can also be used to identify users or devices. Authentication is
supported by most of the service discovery protocols. RF fingerprinting can be used
as well to identify a device (more exactly its air interface).

These strategies are inadequate for the increased flexibility that distributed
networks such as pervasive computing environments require because such systems
lack central control and their users are not all predetermined. Mobile users expect to
access locally hosted resources and services anytime and anywhere, leading to serious
security risks and access control problems. We propose a solution based on trust
management that involves developing a security policy, assigning credentials to
entities, verifying that the credentials fulfill the policy, delegating trust to third parties,
and reasoning about users’ access rights. Distributed trust management approach
involves,

• articulating policies for user authentication, access control, and delegation.

• assigning security credentials to individuals.

• allowing entities to modify access rights of other entities by delegating or
deferring their access rights to third parties and revoking rights as well.

• providing access control by checking if the initiators’ credentials fulfill the policies.

Access rights are not static but change based on delegations and revocations.
Users are assigned generic rights, based on their credentials, the security policy, and
other users’ delegations—that can be used to request access to other services.
Appropriate users with these access rights can in turn delegate the requested right.
Users can access a service only if they have the right to do so or if an authorized user
has delegated that right to them; they can delegate all rights that they have the
permission to delegate. Rights can likewise be revoked.
Each domain has security agents that enforce the policy. The domain’s services and users can additionally impose a local policy. Services register with a security agent in their space and rely on it to provide security. Only users with the right to delegate a certain action can actually delegate that action, and the ability to delegate itself can be delegated. Users can constrain delegations by specifying whether delegated users can re-delegate the right and to whom they can delegate. Once users are given certain rights, they are responsible for the actions of the users to whom they subsequently delegate those rights and privileges. This forms a delegation chain in which users only delegate to other users that they trust. If any user along this delegation chain fails to meet the requirements associated with a delegated right, the chain is broken. When users make requests to the security agent controlling the service, they attach their credentials—an ID certificate or a delegation certificate—to the request. The security agent is responsible for honoring the delegation, based on the delegator’s and delegate’s credentials and the policies. Security agents may generate authorization certificates that users can employ as tickets to access a certain resource. The system allows a foreign user, to access certain services without creating a new identity for him or insecurely opening up the system in any way.
HAVi- An Implementation in Consumer Appliance Environment

HAVi is a standard for home appliances consisting of a set of APIs, services, and a standard for communication. HAVi’s primary goal is providing a dynamic service environment in which software components can discover and interact with other. It provides mechanisms for devices to discover, query and control other appliances on the home network, and provides system services such as message and event.

Eight major consumer electronics manufacturers have come up with an open standard enabling home entertainment devices to communicate intelligently with each other. The HAVi (Home Audio Video Interoperability) standard promises to bring true platform independent interoperability to consumer devices using high bandwidth IEEE 1394 (FireWire) as the connecting medium. Major consumer electronics, software, semiconductor and computer manufacturers, namely Grundig, Hitachi, Panasonic, Philips, Sharp, Sony, Thomson and Toshiba along with now over 30 other participants, have formed a non-profit organization called HAVi (Home Audio Video Interoperability) for promoting the development of interoperable consumer products. The goal of HAVi organization is to provide a standard open architecture for intelligent audio and video devices to interoperate with each other regardless of manufacturer, operating system, CPU or programming language used for implementation.

The simplest example can be time synchronization between different devices. TV set might get the correct time from the broadcast stream and the other devices can query the TV and set their own clocks according to it. Setting the VCR to record a program is a familiar situation users usually have problems with. With HAVi enabled devices this task can be made very easy. User can select the program he wishes to record with the Electronic Program Guide (EPG) residing on a digital TV set (or set-top-box). The TV then locates an available recorder (e.g., a VCR or a recording DVD device) and commands it to record the program supplying it with the time, length and channel parameters taken from the EPG. Thus, the user doesn’t need to program or touch the recording device in any way.
CONCLUSION

The trends in pervasive computing are increasing the diversity and heterogeneity of networks and their constituent devices. Pervasive computing is expected to bring an explosion in the number of devices in our local environments. This paper presents a vision of a future computing landscape characterized by the ubiquity of computing devices, the autonomy, dynamicity and the heterogeneity of system components. This paper also provides a discussion of the challenges associated with such a vision, framed around our conceptual model of pervasive computing which encompasses devices, users, architecture, networking and communication, user interfaces and security policy. With more progress in the fields like MANET, Artificial Intelligence, Natural language processing capabilities and energy management, the infrastructure limitation present currently is supposed to be broken, which will result in revolutionary changes through the implementation of Pervasive computing technology.
REFERENCE

The Ultimate Reference by Dr. K.V.K.K Prasad

Electronics Maker May 2004 Vol.5

www.wileydreamtech.com
www.havi.org
www.bluetooth.com
www.pervasive.ifi.lmu.de/