Atkinson, R.C. and Irvine, J. and Dunlop, J. (2004) *A personal networking solution.* In: IST MAGNET Workshop, 2004-11-11 - 2004-11-12, Shanghai.

A Personal Networking Solution

Robert C Atkinson, James Irvine and John Dunlop
Mobile Communications Group,
Institute for Communications and Signal Processing,
Dept. Electronic & Electrical Eng.,
University of Strathclyde,
Glasgow, G1 1XW, UK,
Email: {r.atkinson, j.irvine, j.dunlop}@eee.strath.ac.uk

Abstract— **This paper presents an overview of research being conducted on Personal Networking Solutions within the Mobile VCE Personal Distributed Environment Work Area. In particular it attempts to highlight areas of commonality with the MAGNET initiative. These areas include trust of foreign devices and service providers, dynamic real-time service negotiation to permit context-aware service delivery, an automated controller algorithm for wireless ad hoc networks, and routing protocols for ad hoc networking environments. Where possible references are provided to Mobile VCE publications to enable further reading.**

I. Introduction

Personal Networking [1] is an evolving area based on the interconnection of a range of user devices to form a user-based network. The devices themselves can be interconnected over existing network infrastructure such as cellular technologies, DSL, WLAN, or short range ad hoc networks such as Bluetooth. Thus, Personal Networks (PNs) exist at a level of abstraction above existing networks. The solution proposed within the Mobile VCE Personal Distributed Environment (PDE) work area is based on application layer networking [2]. That is, applications of the constituent devices communicate with each other and are lower level protocol agnostic.

Like other Personal Networking initiatives, it is assumed that the user has a range of wireless devices forming a Personal Area Network (PAN). The PDE will exist against a backdrop of a wirelessly interconnected service environment. A range of wireless devices will inhabit the environment and can provide the PAN with a multitude of services. These service will be many and varied and include additional user interfaces; the PAN could make use of public available screen or keyboard devices. A range of bearer services may become available as the PAN enters hot-spot areas. A wide range of teleservice could also be supported: issue of electronic travel tickets and other context-aware services.

Although it is recognised that the PAN is an essential element of PNs, the requirement for local, context-aware service provision to that PAN should not be allowed to obscure the need for more traditional telecoms services to be supported by the PN. Thus, communication with remote locations/providers must be factored into the solution. Where this approach is adopted the concept of one user subnetwork (wired or wireless) having precedence over another is no longer relevant: the user will have access to a range of subnetworks but there will be no *core* subnetwork. Instead the core is a user proxy resident on service provider infrastructure.

The remainder of this paper is organised as follows. Section II presents an overview of the PDE Personal Networking architecture and the need for a core entity. Section III presents an overview of the Digital Marketplace (DMP) concept: a mechanism to permit real-time negotiation for bearer and teleservice provision to PNs across heterogeneous radio access providers. Provision of context-aware service to PNs depends in large part on the user's location, as the user moves around his/her environment he/she may encounter a range of new devices, access network providers, and localised teleservice providers; determining the degree of trust to assign to these entities is considered in Section IV. Section V provides a brief overview of other security challenges being investigated for PNs. Section VI examines routing issues within ad hoc networking environments. Finally, conclusions and directions for future work are presented in Section VII.

II. The PDE Core & SIP

The central entity in the PDE is a controlling entity that manages session set-up to the various user devices; this entity is known as the Device Management Entity (DME)[1]. The DME is the first point of contact for all remote session set-up requests to the user. The DME is based on a user-based SIP server [3]; all remote incoming session requests are sent to the DME via a single user-based URI. The DME them determines the most suitable user device to handle the request based upon its proximity to the user *and* the characteristics and capabilities of the device.

Within each of the subnetworks resides a local controller to manage the devices therein and to facilitate session set-up to constituent devices. The local control functionality may potentially reside on any one of the devices in a subnetwork, assuming that the device has the capability to act as a host. In order to be a suitable host, a device must have sufficient available memory and processing ability to support that functionality. Another important attribute of a host, in a wireless/mobile subnetwork, is residual battery power; it is necessary that the host can support the controller functionality for a sustained period of time. Since battery power will

[1] The Device Management Entity in this architecture is not related to that defined as part of 802.15.3.

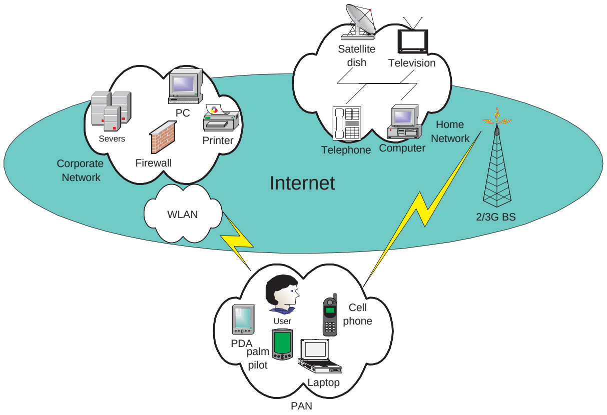

Fig. 1. PDE Subnetworks

decline with time, it may be necessary to periodically change the host such that the wireless subnetwork always has an active controller. Thus, a change of host becomes a distinct possibility. It is well accepted that battery power is a significant constraining factor in the operation of PANs. Battery power will deteriorate with time, and the rate of consumption will depend on many factors including processor usage. When a device is chosen as a host for the local controller there will be an associated overhead in terms of processor usage and hence power consumption. Any algorithm concerned with host determination must take into account the residual battery power of that device. Furthermore, the algorithm must take into account measurement error associated with battery power estimation. Estimates of remaining battery life are prone to fluctuations that vary with time since their projections are based on short term historical measurement of power consumption. Thus, a short but intense period of power consumption may produce a significant though transitory reduction in projected battery life.

Within the Mobile VCE research programme, an algorithm for intelligent and dynamic host identification is being undertaken.

III. The Digital Marketplace

In order to allow the concept of the PN to grow beyond the PAN, we require a system whereby a user's devices can access whatever access network can most effectively provide connectivity in that location. Traditional solutions involving a single operator which 'owns' the user, supported by roaming agreements to foreign networks, are not satisfactory. They are inherently unscaleable, and are not well suitable to highly homogeneous network technologies where connectivity may be provided by one of many different wireless or wired technologies.

One system which does provide a scalable, user-focussed solution to the problem of establishing possibly short term connections over different network types is the Digital Marketplace [4]. The digital marketplace (DMP) provides an environment facilitating real-time bearer negotiation across heterogeneous access networks. Within the marketplace are three main types of entities, each implemented as software agents. *Network Operator Agents* (NOA) represent each network which can provide connectivity to users within the area served by the DMP. *Service Provider Agents* (SPA) are created within the market to represent users who require service within the DMP area. This assumes that users would have a relationship with a service provider to manage their service package and provide billing, etc. In fact, this need not be the case and with suitable payment schemes and depending on the DMP policies, users could create their own agents to negotiate on their behalf. Such agents would act in a similar manner to SPAs. Finally, the DMP has a number of agents – *Market Provider Agents* (MPAs) which provide support and security functions for negotiations and market operation.

The basic system of DMP operation is as follows. When a user wishes to make a call or connect to a service, they contact their Service Provider through the *Logical Market Channel* (LMC). The LMC operates as a random access channel and will be implemented in all the access technologies provided by Network Operators in that particular DMP. Physically provided by one or more of the network operators, the LMC is contracted by the DMP, so a user may use an LMC provided by one operator to access the DMP, whereupon they will eventually negotiate to use another operator to provide the service. The first operator would still be paid by the DMP for the use of the LMC.

Once contacted by the user, the service provider will activate a SPA in the DMP, which will then invite bids from the NOAs to provide the service. The negotiating strategy could be as simple a choosing the lowest price, or may offer the option of choosing different quality options. For example, an MP3 may be available at a range of price levels, but also at a range of sampling frequencies. Thus, a quality-cost trade-off analysis is required.

If the user wants to be able to receive calls some form of paging arrangement has to be set up. In the DMP this is done by the SPA negotiating for a registration and paging contract, whereby the user will be managed by the contracted network, with location updates and paging done through that network. If the user only makes outgoing calls (as would be likely in the case of a data user), the registration and paging contract, and its associated cost, is not required.

To take into account the statistical nature of a wireless interface, the contract includes the concept of commitment, which is the degree of confidence that the network will be able to fulfill the contract on its original terms through to its conclusion. In addition, both NOA and SPA have a reputation, which represents the confidence that they will fulfill agreements (such as, for example, the specified commitment). Reputations are built up over a number of transactions and are controlled by the MPAs. Full details of DMP operation can be found in [4].

The DMP has a number of advantages. By including all networks in a given area, it allows micro-providers such as local WiFi operators access to customers. By allowing competition, it keeps costs low. The splitting of signaling costs makes these costs transparent, while still retaining the flexibility for service providers to provide a wide range of service plans, and by linking cost to commitment, it provides a framework for charging for QoS. However, for the PDE, its main benefit is it provides a distributed, scalable method of arranging connectivity over heterogeneous networks.

As well as providing a mechanism whereby the PDE can negotiate for connectivity opportunistically on available access technologies, the PDE allows a number of enhancements to DMP operation. In the PDE, the DME monitors PAN connectivity and the external networks devices to which the PAN can connect. When initial contact is made with the DMP through the LMC, a list of available networks can optionally be sent to SPA with the connection request. While not so important with ubiquitous coverage networks such as UMTS, this is a useful feature to assist with local, discontinuous networks such as WiFi hotspots. To enhance security, a two stage process is proposed for bidding when the DMP is used with the PDE. In the first stage, the SPA would invite expressions of interest from NOAs who feel they would be in a position to offer service. This first stage could be pre-arranged, so that certain networks could say that they would always be interested in provide service meeting certain characteristics. Only those NOAs which respond positively, and which the SPA is willing to negotiate [5] with (which will depend on whether the SPA is willing to trust them, as discussed in the following section) will be sent the full information about the service request to allow them to respond with a price. Note that NOAs will not know at this stage which other NOAs have been invited to bid, although to avoid collusion, certain information is made available by the MPA in a time delayed fashion so that the different market actors can assure themselves of the correct functioning of the market.

Registration and paging contracts work slightly differently in the PDE context as well. Paging for a PDE sub-network will be under the control of the local DME for that network, in that the signaling information has to go to that entity. The paging contract could be via any access technology which one of the devices in that sub-network can receive, with that network access device forwarding any page to the local DME. Since the local DME is aware of the connection status of each device in the sub-network, should the device which the registration and paging contract is working through become disconnected, either from the sub-network (i.e. the sub-network splits) or from the access network, the local DME will be able to contact the DMP through the LMC to arrange a new registration and paging contract through another access network or device. This allows registration and paging contracts to be let through less robust, but potentially cheaper, networks such as WLAN, whereas the original DMP proposal envisages high coverage networks like UMTS being used for such contracts.

IV. Trust of Foreign Devices and Service Providers

Central to the concept of context-aware service provision is support for opportunistic communication. Within the PAN that is the ability to interact with localised infrastructure over short range wireless links in an ad hoc basis, but the DMP extends this capability to the possibility of interacting with access networks in a similar manner. This implies utilisation of bearers and services supplied by providers that the user does not have a long term subscription contract with, and hence these suppliers can be regarded as foreign entities. It is only after a degree of trust [6] has been established between the PN and the foreign service/device that the service can be delivered to he user.

In order to manage interaction with foreign entities a framework for trust establishment is required such that the user's security requirements are not breached. Such frameworks are by necessity complex. Several actors can be identified – the user themselves, the corresponding party, the provider(s) of the communication link and the provider of the content. The providers of the link and content may be the same as the user or corresponding node, depending on application. Within the PN there will be devices which:

- The user owns and controls fully;
- The user owns but does not control fully;
- The user does not own but controls at least partially;
- Corresponding entities which the user may use or communicate with but over which he has no control (like a foreign printer or display unit).

Since PNs are highly dynamic, with devices entering and leaving, it is also necessary for devices to be able to specify the trust they place in corresponding parties' ability to undertake agreements, both from their underlying capability and the capability of the communications link, and as regards their willingness of the device to perform as agreed. As can be seen, a rich method of specifying trust policies is required.

Mobile VCE is developing a Trust Management Architecture which allows the complex trust arrangements within the PDE to be managed. An overview is given in Fig. 2. Three domains are identified:

- *PDE Domain*: a zone that consists of devices and entities owned and trusted by the PDE user.
- *Service Domain*: a zone whereby only trusted computing environment, users, devices, applications, agents, data sources are permitted to access when sufficient security procedures/ mechanisms are performed.
- *Other domain*: an untrusted zone as perceived by a PDE user. It consists the PDE networks of other users, 3rd party devices, service providers, content providers, access providers and transport providers.

Having separate domains allows different security policies to be defined for different domains. The crucial element in the framework is the *"trust engine"* between the *PDE* and the *Service* domains. Different trust requirements can be identified and classified in this region. The trust engine provides a formal mechanism for expressing trust requirements and identifying security constraints for the trust policy. The trust information provided in the trust engine will vary over time.

Key inputs to the trust engine, shown to the left in Fig. 2, are included in the trust specification: Trust Reputation, Risk Assessment, Pre-assigned Trust Level, Performance Capability, Trusting Period and Types of Access. In detail, these are:

- *Trust Reputation* In our architecture, Trust Reputation (which is distinct from the DMP reputation), is based

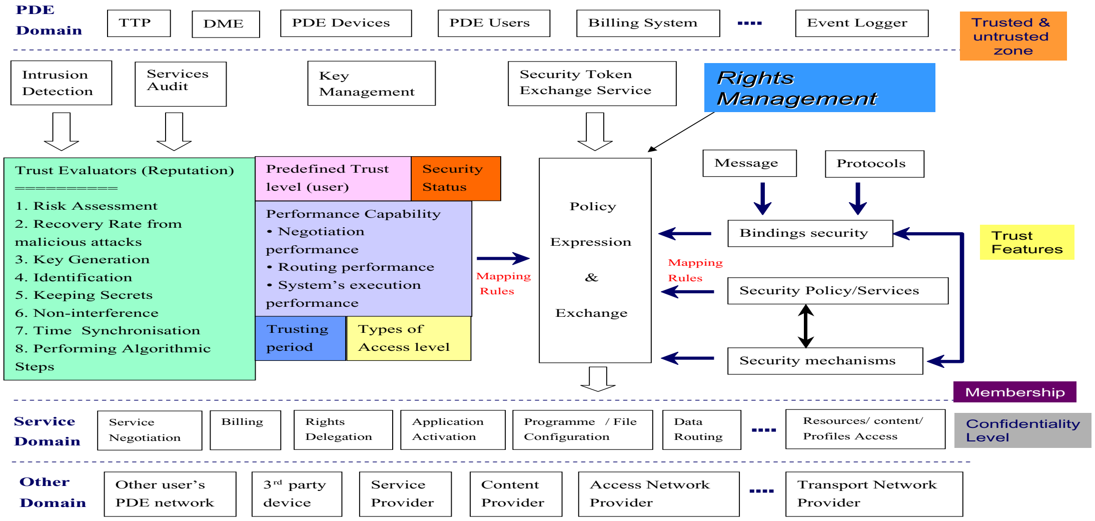

Fig. 2. Trust architecture for PDE

on eight cryptographic evaluators: *Risk Assessment*, the amount of risk to other devices should the device not be trustworthy; *Recovery Rate from Attack*, the ability of a device to detect and repair itself from intrusion; *Cryptographic Processing*, the ability of the device to undertake cryptographic functions, such as Key Generation; *Identification*, the confidence that can be placed on the device's identity; *Confidentiality*, the ability of the device to keep secrets; *Non-interference*, the ability of the device to resist attack; *Time Synchronisation*, the ability of the device to tell the time accurately (to resist replay attacks, for example); and the *Security of any Execution Environment*. If direct information is not available, the reputation (or trust value) can still be based on indirect observations or evidence from the auditing service and the intrusion detection system. These trust evaluators are necessary to guard against any indirect risk which could be inherited should an honest and authenticated entity become compromised.

- *Pre-assigned Trust Level*, defined by the user, where flexibility is required in both the trust allocation and mapping.
- *Performance Capability*, the ability to deliver the promised services or tasks in the agreed manner.
- *Trusting Period*. Three different trusting periods are defined: *Pre-Trust, Mid-Trust and Post-Trust* periods. Pre-trust is defines the period before any interaction with the device. Mid-trust is the period during which negotiation is undertaken with the device, and Post-Trust is the trust level after that negotiation, which would presumably involve authentication and key exchange. Each level requires that the entity satisfy the security rules set by the previous trust periods before it can be granted any additional rights from the new period.
- *Security Status* is the security level that an entity has obtained.
- *Types of Access* is the types of required membership.

To set up a dynamic trust policy, we also require:

- Agreed *Protocols and Message* for exchanging information on which trust decisions may be based.
- A mechanism of including any existing *Security Policy/Services* such as privacy policy and authorisation function so that they can be re-used and integrated as part of the new trust policy.
- *Security Mechanisms* such as digital signature and encryption assure security functions (e.g. integrity & confidentiality) to enforce various service qualities between the end-users.
- *Bindings Security* to tie security characteristics from the *Security Mechanisms* to the agreed *Protocols and Message*.
- *Security Token and Exchange Service* to provide a set of rules to the trust engine to create and exchange an entity's characteristics such as name, group and capability.
- *Policy expression & exchange* where an ideal policy language is identified and is used to express the capabilities or constraints of PDE security. It also facilitates service requests and providers to exchange dynamically security (and other) policy information in order to establish a negotiated security context between them.

Unlike the OSGI's Web Services (WS)-Trust Specifications [7], the PDE's trust architecture anticipates that a trusting relationship should not be established by just using trusted proxies. Evaluation of trust and interrelationships between the outcome of the security execution and the access rights are also vital to building a trusting relationship. If not, issues may arise when a relationship is built with no clear understanding on the referring or requiring trust component.

We have used a structured and widely adopted language, eXtensible Markup Language (XML)[8], as our policy representation and implementation. XML is increasingly used to integrate applications and communicate between systems in many environments, and provides a good foundation for our policy specification. Further details of the trust management architecture and examples of policy specification can be found in [9].

V. Security Challenges

The foregoing discussion on Trust Management does not represent the totality of research into the security issues within PN solutions, a wide variety of research is being conducted into addressing the various threats that have been identified thus far [10], attempting where possible to learn lessons from the Grid Community [11].

When a device is first purchased by a user and is to be inducted into his/her PN and initialisation procedure in needed. An initialisation procedure is currently under investigation that permits secure induction. Mutual authentication of the devices that form the PN is another area of active research [12]. Communication between constituent devices is only permitted after mutual device authentication.

The work area also examines the challenging issue of Digital Rights Management (DRM). In particular how to permits multiple devices belonging to a single user to share and access copyrighted material yet prevent that material being forwarded to third parties. Given that the PDE will exist at several locations simultaneously due to its distributed nature, there is a requirement to ensure that local blackout regions for DxB-T technologies can still be maintained [13].

The need to provide the user with a degree of location privacy is also addressed [14].

VI. Ad Hoc Routing Strategies

The research programme considers 2 key ad hoc routing problems: secure routing and QoS provision versus battery power. With the former, a 2 Hop Acknowledged Routing Protocol (2HARP) has been proposed to detect and avoid non-cooperative nodes. These node include malicious nodes or selfish node — nodes that do not forward packets in order to conserve battery power. The latter is concerned with MAC optimisation to minimise battery consumption by synchronising node sleep cycles [15], [16]. The need for QoS in ad hoc networks is also addressed [17].

VII. Summary

There is a great deal of overlap between areas of research with the Mobile VCE Personal Distributed Environment Work Area and the MAGNET initiative. Areas of commonality include

- An Automated algorithm to determine the most appropriate node to act as the controller in an ad hoc networking environment;
- The requirement for a Trust Architecture to mitigate against attacks by foreign devices, whilst enabling communication;
- Identification of the need for dynamic service negotiation via a user agent;
- The need for secure ad hoc routing protocols to take account of non-cooperative nodes.

VIII. Acknowledgements

The work reported in this paper has formed part of the PDE work area of the Core 3 research programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, http://www.mobilevce.com whose funding support, including that of EPSRC, is gratefully acknowledged. Full detailed technical reports on this research are available to industrial members of Mobile VCE.

References

[1] IG Niemegeers and SM Heemstra De Groot, “Research Issues in Ad-hoc Distributed Personal Networking,” *Wireless Personal Communications*, vol. 26, no. 2-3, pp. 149 – 167, May 2003.

[2] J Dunlop, RC Atkinson, J Irvine, and D Pearce, “A Personal Distributed Environment for Future Mobile Systems,” in *Proc. IST Summit*, June 2003.

[3] J Rosenberg et al., “SIP: Session Initiation Protocol,” *Internet Engineering Task Force RFC 3261*, June 2002.

[4] J Irvine, “Adam Smith Goes Mobile: Managing Services Beyond 3G with the Digital Marketplace,” in *Proc. European Wireless 2002, Florence, Italy*, February 2002.

[5] S Paurobally and NR Jennings, “Verifying the Contract Net Protocol: A Case Study in Interaction Protocol and Agent Communication Language Semantics,” in *Proc. AAMASC*, 2004.

[6] SK Goo, J Irvine, and J Dunlop, “Trust with the Mobile VCE Personal Distributed Environment,” in *Proc. ubiNet, Cambridge, UK*, May 2004.

[7] Della-Libera et al., “Specification: Web Services Trust Language (WS-Trust),” http://www.ibm.com/developerworks/library/ws-trust/index.html, December 2002.

[8] T Bray et al., “Extensible Markup Language (XML) 1.1,” http://www.w3.org/TR/2004/REC-xml11-20040204.html, February 2004.

[9] SK Goo, JM Irvine, RC Atkinson, and J Dunlop, “Trust Architecture for a Personal Distributed Environment,” in *Proc. VTC-2004 Fall, Los Angeles, USA*, September 2004.

[10] S Schwiderski-Grosche, A Tomlinson, SK Goo, and JM Irvine, “Security Challenges in the Personal Distributed Environment,” in *Proc. VTC-2004 Fall, Los Angeles, USA*, September 2004.

[11] A Tomlinson and S Schwiderski-Grosche, “Application of Grid Technology to Personal Distributed Environments,” in *Proc. GADA-2004*, 2004.

[12] K Billington and A Tomlinson, “Mutual Authentication of B3G Devices within Personal Distributed Environments,” in *Proc. IEE 3G 2004*, October 2004.

[13] A Tomlinson and E Gallery, “Conditional Access in Mobile Systems: Securing the Application,” in *Proc. PIMRC-2004*, 2004.

[14] RC Atkinson, SK Goo, J Irvine, and J Dunlop, “Location Privacy and the Personal Distributed Environment,” in *Proc. International Symposium on Wireless Communications Systems, Mauritius*, September 2004.

[15] Y Zhou, D Laurenson, and S McLaughlin, “High Survival Probability Routing in Power Aware Mobile Ad Hoc Networks,” *Electronics Letters*, 2004.

[16] Y Zhou, D Laurenson, and S McLaughlin, “An Effective Power-Saving Scheme for IEEE 802.11-Based Multi-Hop Mobile Ad-Hoc Network,” in *Proc. VTC-2004 Fall, Los Angeles, USA*, September 2004.

[17] E Tan, S McLaughlin, and D Laurenson, “Providing QoS Support on Mobile Wireless Ad-Hoc Networks,” in *Proc. VTC-2004 Fall, Los Angeles, USA*, September 2004.