WIRELESS WORLD

RESEARCH FORUM

Personal Distributed Environment in the Context of Reconfigurability

Robert C Atkinson., James Irvine, 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@eee.strath.ac.uk**	Terence E. Dodgson Samsung Electronics Research Institute (UK) Communications House, South Street, Staines, Middlesex, TW18 4QE, UK †**Email: terry.dodgson@samsung.com**
Sunil Vadgama, Fujitsu Laboratories of Europe Ltd Hayes Park, Hayes End Road, Hayes, Middlesex, UB4 8BE, UK †**Email: s.vadgama@fle.fujitsu.com**	

Abstract: This contribution to WWRF WG6 addresses Personal Distributed Environments in the context of reconfigurability. An introduction to this relatively new concept is given including a brief history, and a description of a possible PDE architecture along with consideration of its constituent components mentioning specifically the use of a Device Management Entity and configuration/reconfiguration algorithms. The paper moves on to consider Location Privacy before moving on to the conclusion in terms of Recent Developments of work within the Mobile VCE.

***Index Terms* — Personal Area Networks, Personal Distributed Environment, Reconfigurability**

INTRODUCTION

The work detailed in this document is related to combined input from the University of Strathclyde, Fujitsu Laboratories of Europe Ltd. and Samsung Electronics (UK) Ltd, working through the Mobile Virtual Centre of Excellence (which is a unique company, established in late 1996 by the UK's mobile phone industry and academia, supported by UK Government, to undertake technology research to underpin and accelerate such a vision. Reflecting the nature of its industrial members, its vision is global and its research internationally recognised). In particular this work addresses aspects of Personal Networks (PN), where design targets include flexibility and adaptability. The adaptable nature of the work leads naturally to aspects of reconfigurability on a service, terminal, local network and wider network scale.

In order to design reconfigurable modules of any kind, it is necessary to make assumptions about the environment within which such modules will find themselves. Definitions of what a Personal Area Network or a Body Area Network are, are necessary.

For purposes of this document a Personal Area Network (PAN) implies proximity and possibly usage (i.e. Personal) and can be taken to be a collection of devices that find themselves within a certain, limited, area around a user and which can be used by that user. As such a PAN might include the user's own devices and other, foreign, devices which can be accessed by the user. Any device that cannot be accessed by the user is not part of the PAN. A Body Area Network might be said to be devices that are currently

in contact with the user (either wearables or hand-held devices), and could be deemed to form a sub-classification of a PAN.

If the above, general, definitions are used it is not clear as to whether local devices around a particular user share a common air interface (i.e. can communicate with each other directly using RF means). Since it is one of the goals of the work to ensure fast, automatic, and adaptive, reconfigurability it makes much sense to ensure all devices do indeed have a common air interface. Although this is not a prerequisite for a device to be in a PAN, it would allow for immediate detection and registration procedures, in addition to fast and constant updates related to movements of devices, thus sustaining the PAN dynamically and seamlessly for a user.

Network evolution beyond 3G continues to dominate discussion within the cellular community. A variety of issues are being actively debated: requirement for a new air-interface, greater interworking with WLAN and other networks, service driven approach, and potential for increasing market penetration of network-enabled devices. The Mobile VCE vision for beyond 3G encompasses a world that has embraced a disparate range of networked processing and communications devices.

Predicting anything with a good degree of accuracy is a difficult task to undertake when few facts are known and when the prediction spans a relatively large time scale. Estimates might be made by examining passed and current trends. This remains true when considering the mobile communications industry.

It is anticipated that in future there will be a greater proliferation of wireless processing devices. These devices will include wireless enabled-laptops, PDAs and smartphones, together with new and innovative devices such as environmental and biomedical sensors. Each will have its own distinct capabilities and characteristics such as screen size and resolution, ability to support audio/video/other applications and sessions. Thus, users will own and control a plethora of diverse devices, giving rise to the Personal Distributed Environment (PDE) concept [1]. The PDE is a personal networking solution aimed at providing access to a diverse range of services over these multifaceted terminals. User devices are organised into location-based (i.e. both local and remote) subnetworks; PDE is the means by which services can be delivered to the user over heterogeneous networks to these terminals. Unlike many initiatives, the PDE takes a user-centric approach; it is the user who manages the various subnetworks and controls session delivery. The vision of mass distribution of wireless devices, and sensors forming what might be a Ubiquitous User Centric environment, as depicted in **Figure 1** is not unique to PDE.

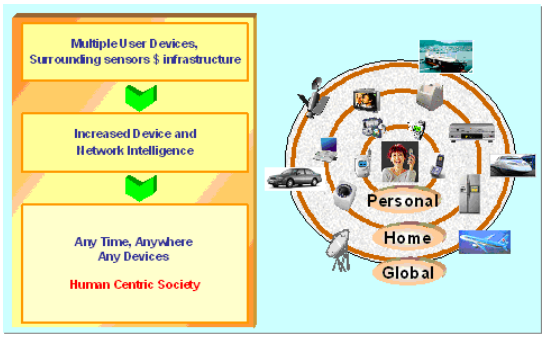

Figure 1: User Centric Reconfigurable Ubiquitous Environment Concept

Much research is being conducted on Ambient Networking [2]; a concept that has many interpretations, though context aware wireless connectivity is central to many of them. A closely related concept is that of Sensor Networks [3], [4]: clusters of wireless interconnected sensors capable of measuring a range of qualities such as temperature and air pressure. Other research is focussing on the Mobile Grid [5]: a collection of wireless processing devices that cooperate to share resources such as processor time and memory. More recently, an EC IST FP6, My personal Adaptive Global NETwork (MAGNET), has begun to examine the concept of personal networking architecture reconfigurability [6], and including aspects such as PAN Device Admission Control [7]. The central theme that underpins these initiatives is that of ad hoc networking and

reconfigurability on multiple levels. In tandem with the research into increased wireless connectivity, interworking of access networks has received much attention recently. Current advances in 802.11 Wireless LAN (WLAN) technologies have motivated standardisation of WLAN-UMTS interworking through 3GPP Release 6. Increased deployment of high bit rate, digital broadcast systems such as Digital Video Broadcasting (DVB) and Digital Audio Broadcasting (DAB) has led industrial players to examine the possibility of DxB-cellular interworking through initiatives such as the DVB group: Convergence of Broadcast and Mobile Services (CBMS).

To summarize the trends outlined above, we can see that there are at least four trends in the industry which are leading to an increased number of devices a single user may have. Summarizing, the trends are;

1. The desire for increased, good quality services on a par with fixed line services: and this implies the use of technology capable of delivering increased data rate applications
2. Convergence: of services, networks and terminals themselves (having multiple devices on one platform).
3. Provisioning access to a diverse range of multifaceted terminals: giving rise to the concept of a Personal Distributed Environment (PDE) and a Personal Area Network (PAN)
4. Reconfigurability: of Services, Networks, and Terminals.

The trends are depicted in Figure 2;

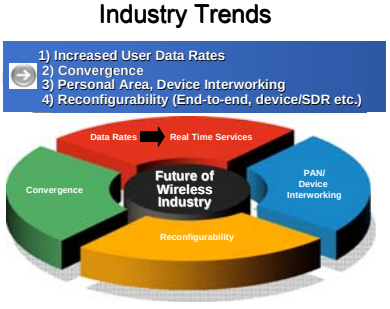

Figure 2: Perceived Current Industry Trends

All four of these industry trends are interlinked, and it is the unification of these current trends in industry that gives rise to the PDE concept pioneered by the Mobile Virtual Centre of Excellence (MVCE) [8] and which is outlined in this contribution to the WWRF WG6.

Personal Distributed Environment – towards total Reconfigurability

Based on the trends highlighted in the previous sections, it is clear that the user will have access to a range of devices that are both local and remote and that some of these devices in the future may be reconfigurable. Consideration of reconfigurable devices leads to subject areas such as Software Defined Radio (SDR) and, although the advent of such devices will have an impact on the PDE/PAN concept, they are not the main thrust of this contribution. This contribution focuses more on architecture and network reconfiguration.

Local devices are defined as those located about the user's person, and remote devices are those owned/controlled by the user but resident elsewhere. Within this context, it is assumed that the user will not have a single communications device but a diverse range of devices forming a Personal Area Network (PAN), and that this network will accompany the user as he moves around his environment. In addition, the user will have a range of interconnected devices located variously within the household or workplace. An example arrangement is shown in Figure **3**.

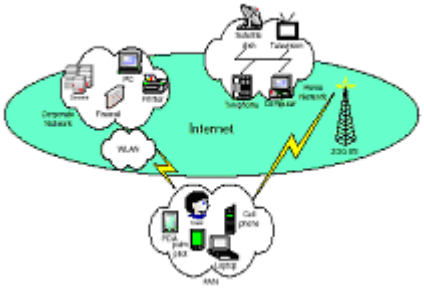

Figure 3: PDE Sub-networks

The user may have a range of devices at other locations, for example a wireless automobile personal area network could easily be included in the figure, along with home personal area networks etc. The PAN can be considered as moving with the user, although devices that form part of this network may change depending on their proximity and attachment to the user. The PAN (and hence the PDE itself) might thus be viewed as being in a continuous state of reconfiguration.

A key objective of the PDE is to provide virtual personal network connectivity in this dynamic (constantly changing/reconfigurable) and heterogeneous environment, irrespective of device location. This enables, not only ubiquitous access to a user's own (personal) devices and network space, but also access to global communication and information services. The design of the architecture is constrained by the need to ensure ubiquitous connectivity; this translates into a requirement for a nominated contact point for each user with a unique address, permitting a DNS-like lookup procedure to readily return that address. Within the context of the PDE, this entity is known as the Device Management Entity (DME). A person-based URI is mapped to the IP address of the DME. All session set-up requests irrespective of their type (voice call, email, etc.) are sent to this URI. Intelligent management functionality resident within the DME preforms intelligent end point determination for each service. The user-centric nature of the PDE gives rise to the notion of a DME containing much of the functionality of a user-based proxy. The proxy operates on behalf of a single individual and is based on the IETF Session Initiation Protocol (SIP) [9]. The idea is that the DME contains the functionality of a SIP proxy and other additional functionality required to manage the PDE. Given the assumption that the user will exercise control over a variety of communication devices, SIP is an ideal technology for a rendez-vous protocol that facilitates location tracking, permitting the user to be contacted irrespective of location. One of the unique aspects of the PDE is that it encompasses both local (e.g. within the user's PAN) and remote (e.g. within the user's household) devices. Thus, SIP can be used to direct session set-up requests to the appropriate device, based on user location and also device capabilities. The session set-up requests from other parties can describe the required characteristics of end terminals using the Session Description Protocol (SDP) [10]. Within the architecture, a Call Processing Language [11] acts as an interface between session requests received via SIP and the information stored in internal DME registers.

Device Management Entity

Central to PDE provision is a controlling logical functional entity known as the Device Management Entity, shown in **Figure 4**.

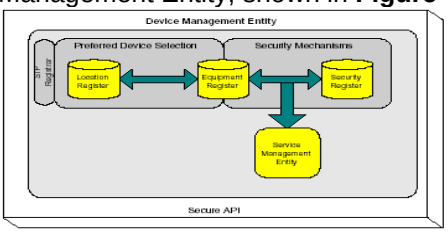

Figure 4 DME Functional Composition

This entity contains a number of functional subcomponents that assist in managing reconfiguration in terms of coordinated device operation and service delivery within the PDE [12].

The equipment register is used to store device capabilities and characteristics. A number of security issues are prevalent in distributed networks such as the PDE; the security register stores encryption keys for devices and security policies for the PDE as a whole.

The PDE may be viewed as a composite of several physically separate subnetworks; in particular some of those networks may exhibit high mobility profiles: e.g. the automobile network. Thus, mobility management within the PDE requires a tracking entity. This task is performed by a DME subcomponent known as the location register: a component that provides a service analogous to the SIP location service. Implementation of the location service is not specified by the SIP specification and can

therefore be implemented using other appropriate technologies. The Berkeley database has been used to implement the location register; it is also being used to implement the other registers. Interaction with the database is conducted through the Lightweight Directory Access Protocol (LDAP) [13]. Conveniently, both the database and the access protocol are implemented in the open source software component, openLDAP [14]. In order to minimise the amount of signalling across the various networks that the PDE transcends, a portion of the DME is devolved to each subnetwork to permit local management, as shown in **Figure 5**.

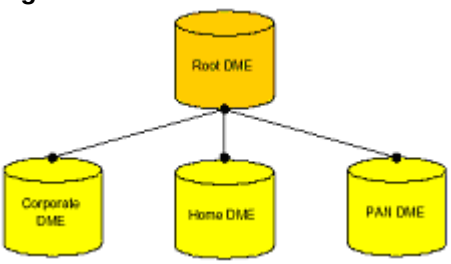

Figure 5: DME Devolution

Thus, each subnetwork is permitted to operate in a semi-autonomous fashion. However, data stored in each of the local DMEs is cached within the root DME. This two-level approach is beneficial since:

1) When a device wishes to determine the capabilities of a device in its own subnetwork, it contacts its local DME, reducing the need to communicate with the root DME directly. This is advantageous because the root DME will generally be further away; the increased hop count will result in increased latency. Moreover, communication with a local device may allow utilisation of non-tariff based links.

2) When a device wishes to determine the capabilities of a device in another subnetwork, it is redirected by its local DME to the root DME, which has visibility of the characteristics of all devices. Thus, signalling is constrained to be local, where possible.

The PAN component of the PDE is likely to encounter a range of foreign devices by virtue of its mobility. These could be either other users' wireless-enabled devices or public wireless devices with onboard services that users may wish to utilise opportunistically. When the PAN encounters a foreign device, it may be added to its local DME's internal registers such that devices within the PAN may access that foreign device/service. Many of these public devices will be designed to provide local services, e.g. a wireless-enabled machine at a railway station may provide travel tickets. The salient point is that local services will only be of value to the user when in the vicinity of those devices/services. Based on the assumption that local user devices are more likely to interact with local services, foreign devices and services need only be mapped locally, i.e. in the local DME. This approach has the potential to minimise signalling of topological reconfiguration to other sections of the PDE, hence reducing the requirement for signalling over the wireless links that may incur a high tariff. The tree-like nature of LDAP permits the characteristics of devices located in different subnetworks to be stored in different branches. This permits delegation of authority to manage this information to the respective subnetworks.

The hierarchical PDE architecture [15] has evolved based on two levels of management. The top-level management entity, the *root* DME, and *local* DMEs that are resident in each of the PDE subnetworks.

Physical Location of the Device Management Entity

Within each PDE subnetwork, local DME functionality will reside on one of the devices. In wireless subnetworks (with dynamic topology) it would be advantageous if the host could change to reflect variations in residual battery power or topology. Topological changes that may require a change of host include addition of a new node or subnetworks becoming co-located. The former implies that a new node may be more able to support the DME management functionality. The latter implies that two or more wireless subnetworks belonging to the same user occupy the same radio environment; in this circumstance one copy of the management functionality may become redundant. An automated algorithm is used

to identify the most appropriate device to host the local DME functionality.

The algorithm considers such factors as availability of power1, processing power, memory constraints, and optionally connectivity. The abundance of powerful personal computing devices, both within the household and workplace, is such that processing, memory and energy constraints are unlikely to be an issue for these devices. Therefore, the selection of a device to host the local DME in the fixed subnetworks is unlikely to be problematic. The same cannot be said, however, for the mobile subnetworks: energy capacity is a significant limiting factor due to the limited battery life of mobile devices. Successive generations of mobile handsets and PDAs have been accompanied by increased processing ability and storage capability. Based on this trend, it is unlikely that these constraints will be the limiting factor. Although available processing power and storage capacity in a mobile device may be subject to temporal variation, it is residual battery power that will be the most dynamic. Based on this premise, the choice of the most suitable device to host the DME in a wireless network may vary with time; this poses the significant problem of how to determine the most suitable host.

The selection may also depend upon the average number of hops between the candidate and other nodes in the wireless (ad hoc) subnetwork, since minimising the hop count would reduce the overall power consumption due to local signalling. The average number of hops will be influenced by two related factors: number of air-interfaces on a device, and its degree of connectivity to other members of the PAN. Significant absorbtion of radio wave takes place for body area networks operating within the 2.4 GHz band and may well be worse for 5.2GHz band. As a result there may be significant levels of shadowing between PAN devices worn on the body. Where a device can communicate directly to a large proportion of other PAN devices, its signalling information need not be relayed (at the expense of battery power) by intermediate nodes. Two broad approaches to local DME host selection are being examined. The first approach is concerned with identifying the most appropriate host, based on its predicted survivability,and is illustrated in **Figure 6**.

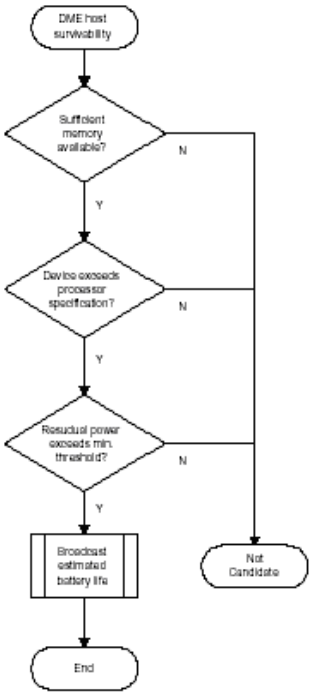

Figure 6: Host Survivability Algorithm

Devices determine if they have sufficient storage capacity and processing power to support the local DME entity. Those which also exceed a predefined minimum power threshold can be regarded as candidates to host the DME. The best candidate is that node which has the highest level of residual power. Each node that has sufficient processing power and storage capabilities (based on predetermined threshold values) broadcasts its estimated battery life on all local interfaces. The broadcast will take the form of a packet that would contain the candidate's address (or range of addresses for a multimodal device), a global PDE identifier, the estimate of battery life, a random number (generated by nodes and inserted into the packet a packet to enable loop detection), and a time-to-live count. The packet may be encrypted so as to prevent other wireless devices from intercepting transmissions. On reception of the broadcast

packet, the other devices in the subnetwork decrement the time-to-live counter. If the counter value is non-zero then the packet is re-broadcast on all available local interfaces. Where a device has multiple interfaces it may receive multiple copies of the packet. In this case the device can use the random number to determine whether it is the same packet or another packet: loop detection; clearly, a node will not broadcast a packet that it has broadcast previously. In this way each device in the subnetwork is made aware of the DME's location, i.e. the MAC address of the DME's host device within the subnetwork. The maximum number of times that the broadcast packet need be transmitted can be determined. For a network containing N devices (D1 - DN), where each device has In local interfaces, then the number of broadcast packets is given by:

$$Pkts = \sum_{n=1}^{N} I_n \qquad (1)$$

All candidates in the subnetwork are able to receive these broadcasts; the candidate with the longest battery life is regarded as the most suitable device. The successful candidate will assume the role of DME host and continue to periodically transmit battery life information packets; given that this quality will decrease with time. The purpose of the broadcast packets is two-fold. Other devices use these to determine the address of their local DME. Their secondary purpose is to allow other candidate hosts to continue monitoring their residual power and compare it with that broadcast. If the incumbent host falls below an acceptability threshold and another candidate has a significantly better projected battery life then it replies by transmitting its estimate to the incumbent host. For another device to be considered as better, two conditions must exist: the incumbent breaches its minimum power threshold, and the candidate has a battery life greater than that of the incumbent plus a hysteresis margin. This approach is adopted in order to avoid unnecessary handover of the DME hosting role, which is undesirable since handover involves transferring computer code and data to the successor, incurring a cost in terms of power & bandwidth consumption. Estimation of battery life may be subject to measurement error; therefore, the hysteresis margin is required to prevent ping-pong handovers. If the incumbent host is able to support the DME despite the presence of another more suitable candidate, a handover is not required. Opting not to handover in this circumstance avoids the cost associated with handover. It is for this reason that a minimum power threshold must be breached before handover is triggered. Whereas the first approach is concerned with identifying a host such that it will minimise the likelihood of DME handovers due to its objective of survivability, the second approach is based upon selecting a host that will minimise power consumption of nodes, due to management functionality, across the entire ad hoc network: network survivability. With this approach, a candidate's degree of connectivity is taken into account in determining the most appropriate location, and is illustrated in **Figure 7**.

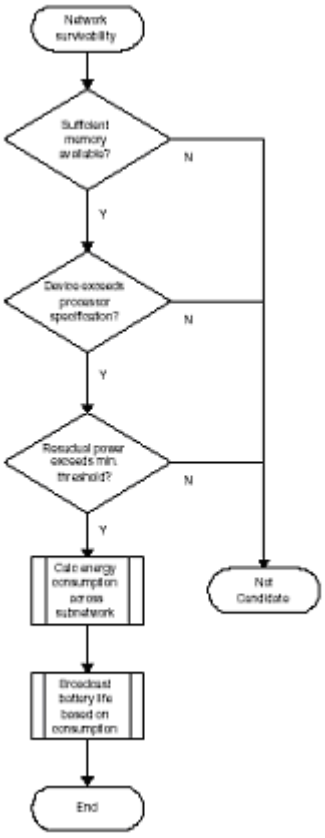

Figure 7: Network Survivability Algorithm

A related issue concerns the procedure to be adopted whenever two PDE subnetworks become co-located. There may be several instances through out a typical day whereby a user enters/leaves his home/car/workplace. If the user is also accompanied with a PAN, then the PAN may merge with the subnetworks already at these locations, assuming they have a wireless interface. It is necessary to define network merging within this context. Each local DME can be regarded as a directory server (in addition to many other roles) for the devices in its neighbourhood (PDE subnetwork). When two or more subnetworks become co-located and can therefore communicate directly via short range wireless technologies, it may be more efficient to manage the combined network by a single controlling entity (local DME). When the local DME of one subnetwork assumes control over the devices of another, then the subnetworks are said to have merged. The benefit of a single DME is derived from battery power conservation, and increased knowledge base. The former implies that it is more power efficient for a single device to be assigned that task of managing a network than to have several devices performing this task in parallel. The latter implies that better decision making is possible by a single DME with access to full information with the subnetwork than by two or more DMEs with access to a subsection of information. As mentioned DME hosts periodically broadcast packets detailing their appropriateness to host the DME. Therefore, when PDE subnetworks become co-located, both hosts will be able to receive each others packets. On mutual reception of packets, that with the longer battery life (plus hysteresis margin) is identified as the most appropriate host. However, it is not necessary to merge both DMEs immediately. It is proposed that merging of DMEs is postponed until a predefined time period has elapsed. The purpose of this time period is to avoid merging and disjoining of local DMEs when PDE subnetworks become co-located for short time periods such as a short car journey. During this period the subnetworks will continue to be managed independently. After this period, however, it is proposed that a single DME entity manages the conjoined subnetworks. Merging of DME logical entities is achieved as follows. The DME host that does not have precedence, i.e. has the lower battery life, indicates that it is willing to handover copies of its registry information to the DME host with precedence. On receipt of an acknowledgement, copies of the records held in the registries are transmitted. It should be noted that the former DME host does not depopulate its database; rather it simply stores it but no longer operates as a DME. The rationale for retaining this information is that it may be needed in the near future if the PDE subnetworks become disjoined again. Within PDE a range of security issues are being examined: Digital Rights Management (DRM), trust of foreign entities, Single Sign-On mechanisms (SSO), and location privacy. DRM mechanisms are required to permit the user to transfer content across their devices but not to others' devices without payment. Trust management is required for opportunistic communication; should a PDE device trust another device or service provider if it has no previous experience of that device? SSO permits the PDE to authenticate to many access networks by authenticating with only one of them; this also facilitates aggregated billing mechanisms. The transfer of signalling traffic between local and root DME entities may reveal the users location to other parties. Indeed, monitoring a media session could also reveal a user's end point. Thus, location privacy is an important consideration in Personal Networking. The issue of location privacy is discussed in the next Section.

Location Privacy

Since each of the PDE subnetworks is physically separate, they will exchange signalling information over intermediate networks: UMTS networks, WLAN networks, and ISP/telcos. Clearly, within the intermediate networks there exists the possibility that a user's location privacy requirements could be violated using traffic analysis. In fact, it is not possible in any such system to completely obscure location

information. However, within the PDE there exists an additional danger to the PDE's location register [16]. Accurate knowledge of the PDE's topology relies on the location register being supplied with true information. From a security perspective, this highlights the need to ensure that the database is not supplied with misinformation regarding topological reconfiguration. The misinformation may arise from two sources: malicious devices/users, and malfunctioning devices/networks. With the former case, a malicious source may attempt to deliberately mislead the location register as to the true topology of the PDE. For example, it may attempt to inform the location register that the devices residing in a user-based PAN are erroneously contactable through a WLAN network (with supplied gateway address). Based on this information the root DME is misled with regards to the true contact information of the PAN. Of course, the malicious entity need not be a source, rather it could be an entity resident in an intermediate network that tampers with originally correct information. This is undesirable since it would result in a section of the PDE (in this case the PAN) becoming detached from the rest (out of contact with the PDE). With the latter case, a malfunctioning node may be attempting to update its own topological database but unwittingly sends the information to the wrong destination (i.e. wrong DME address). Alternatively, a malfunctioning network may route accurately addressed information to the wrong destination: stray messages. In this case, it is possible that a section of a user's PDE becomes conjoined with that of another user. Both cases indicate that interception (substitution) of location information traversing the PDE can lead to sections of the PDE becoming detached from the rest (denial of service), or perhaps sections of another PDE becoming erroneously attached. Thus, interception of location information may have the effect of destabilising the entire PDE. Clearly, there is a need for robust security mechanisms to operate between the root DME and its local components resident in each PDE subnetwork. In order to preserve the topological integrity of the PDE especially during reconfiguration updates, a strong encryption mechanism is required to provide mutual device authentication. A two phase procedure is envisaged, as depicted in Figure 8, whereby the local and root DMEs mutually authenticate, followed by each of the PDE devices mutually authenticating with a nominated local DME.

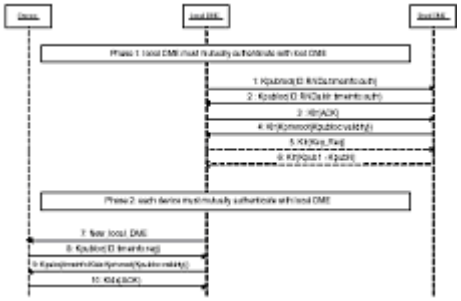

Figure 8: Location Privacy

The first phase operates as follows. The local DME sends an authentication request (auth) to the root DME, this implicitly requests the creation of a session key between the two. The request is accompanied with a random number (RNDa), the local DME's ID, together with time information that consists of a timestamp and a suggested duration of validity of the session key; the time information is required to prevent replay attacks. It is assumed that both the root DME and local DME devices have sufficient computational power to permit Public Key Cryptography to be implemented, and that the root DME has a public ($K_{pubroot}$) and private ($K_{privroot}$) key pair. The authentication request is encrypted using the public key, as shown in message 1.

The root DME is able to decrypt this request using its private key and responds (message 2) with the same time info, random number, authentication request identifier, and session key (Klr). All of this is encrypted by the local DME's public key, K_{public}. By including the random number in this transaction, the root DME indicates that it has the private key and in doing so authenticates itself to the local DME. The local DME then authenticates to the root DME by transmitting an acknowledgement (message 3) encrypted

using the session key contained in message 2. Finally, the root returns (message 4) an authentication token, $K_{privroot}\{K_{lpuboc}$: validity$\}$. The authentication token is the local DME's public key and validity information signed by the private key of the root DME. In this context validity information contains the ID of the local DME, and timing information to reveal the period for which the token can be used in order to prevent replay attacks. The local DME can use this token later to prove to other devices that it has previously been authenticated by the root DME. If the local DME has no prior knowledge of the other *N* devices in its subnetwork, it can request (message 5) a copy of their public keys encrypted using the session key. The root DME subsequently responds (message 6) with a list of keys (public or secret), K_{pub1} to K_{pubN}. It is recognised that not all PDE device will have sufficient computational power to support PKC; therefore, these devices may have a secret key instead.

Phase two involves mutual authentication between local DME and the device in its subnetwork; it is assumed there are *N* such devices. The local DME transmits a broadcast message (message 7) to all *N* devices indicating that it is the local DME. Each device responds with a request to register (reg) with the local DME. Message 8 shows just such a response from a particular device, device 'X'. A similar procedure is adopted to that in phase one whereby the request is accompanied with ID data and timing information to prevent replay attacks. This information is encrypted using the local DME's public key, K_{public}. The local DME is able to decrypt this request using its private key. The local DME then authenticates itself to the device by responding (message 9) with the authentication token, timing information, and a session key to be used between the device and the local DME (K_{ldx}). The device is able to decrypt this message using its private key. Analysis of the authentication token verifies that the local DME has authenticated to the root DME and is therefore part of the PDE. The device is then able to authenticate to the local DME (message 10) by returning an acknowledgement encrypted using the session key, K_{ldx}.

Conclusion/Recent Developments

In a future populated by many more wireless devices, giving the user a seamless environment will place a high demand on the management system. User based mobility management is an important area of research to enable ubiquitous connectivity across a range of terminals. Feature discovery will play an increasing role in service provision owing to anticipated variety in multimedia services. The vision of PDE is centred around the notion of ubiquitous, seamless, and always-on personal networking across both wired and wireless device/networks. It must be easy to use and configure by everyone regardless of their technical expertise – thus indicating a high degree of automatic reconfigurability. The PDE requires robust mobility management to operate in concert with feature discovery mechanisms to handle the challenges of wireless ad hoc environments and enable the provision of optimum service support. Whilst heterogeneous access increases the complexity of choices and configurations to the management system, in the PDE it is recognised that there is a clear need to hide this complexity from the user. This may be achieved through the use of a third party provider that may host, configure, reconfigure and manage the PDE on the user's behalf. As with all distributed networks, security is an area of prime importance. Research in the Mobile VCE PDE and is actively examining the approaches being undertaken in other fora, and translating them to fit PDE requirements.

Currently, the Mobile VCE PDE research programme is investigating mobility management issues such as location tracking and device registration. An algorithm is under investigation to identify the most suitable host for the local DME within a PDE subnetwork, this is of particular importance in those subnetworks which are mobile, and hence the constituent device may rely on battery power.

ACKNOWLEDGEMENTS

In preparing this paper the work of a number of researchers has been drawn on: Alistair

Cameron, David Pearce, Alan Tomlinson, and Scarlet Schwiderski-Grosche. The work reported in this paper has formed part of the Mobile VCE 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] N Niebert et al., "Ambient Networks: An Architecture For Communication Networks Beyong 3G," *IEEE Wireless Communications*, vol. 1, no. 2, pp. 14 – 22, April 2004.

[3] IF Akyildiz, W Su, Y Sankarasubramaniam, and E Cayirci, "A Survey on Sensor Networks," *IEEE Comms Mag.*, vol. 40, no. 8, pp. 101 – 114, August 2002.

[4] S Olariu, A Wada, L Wilson, and M Eltoweissy, "Wireless Sensor Networks: Leveraging the Vitrual Infrastructure," *IEEE Network*, vol. 8, no. 4, pp. 51 – 56, July 2004.

[5] LW McKnight, J Howison, and S Bradner, "Wireless Grids Distributed Resource Sharing by Mobile, Nomadic, and Fixed Devices," *IEEE Internet Computing*, vol. 8, no. 4, pp. 24 – 31, July 2004.

[6] Dodgson T.E. "Reconfigurable Personal Area Networks for 4G Systems", *WWRF#11, Oslo Norway*, June 2004

[7] Dodgson T.E., Al-Rawashidy H., Sivarajah K., Sulaiman T, "Device Admission Control for Personal Area Networks", *WWRF#12 Toronto Canada,* November 2004

[8] http://www.mobilevce.com/,.

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

[10] M Handley and V Jacobson, "SDP: Session Description Protocol," *Internet Engineering Task Force RFC 2327*, April 1998.

[11] J Lennox and H Schulzrinne, "Call Processing Language Framework and Requirements," *Internet Engineering Task Force RFC 2824*, May 2000.

[12] RC Atkinson, J Dunlop, J Irvine, and S Vadgama, "The Personal Distributed Environment," in *Proc. Symp. Wireless Personal Multimedia Communications, Abano Terme, Italy*, September 2004.

[13] M Wahl, T Howes, and S Killie, "Lightweight Directory Access Protocol (v3)," *Internet Engineering Task Force RFC 2251*, December 1997.

[14] http://www.openldap.org/,.

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

[16] 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.