# Location Privacy and the Personal Distributed Environment

Robert C Atkinson, Swee Keow Goo, James Irvine and John Dunlop
Mobile Communications Group, University of Strathclyde
Royal College Building, 204 George Square
Glasgow G1 1XW UK
{r.atkinson,sweegoo,j.irvine,j.dunlop}@eee.strath.ac.uk

***Abstract*— The Personal Distributed Environment is a new concept being developed within the Mobile VCE Core 3 research programme whereby users have access to their services and data through a distributed set of terminals, wherever their location: ubiquitous access. Devices are co-ordinated by Device Management Entities (DMEs), which are either Local DMEs, controlling devices within a single PDE subnetwork at a user's home or office. For example, or an overall Root DME providing universal co-ordination and a single point of contact. While such a structure allows very flexible service delivery, it has serious security concerns, as the presence of signalling between Root and Local DMEs will allow the location of the user to be determined at all times. In this paper, we analyse the security threats to the DME structure proposed for the PDE, and introduce a system of tunnelling and mix networks to provide security and privacy.**

## I. INTRODUCTION

It is well known that in order to transmit information securely in a distributed network, authentication and encryption are required. Authentication is required to prevent malicious entities from spoofing, i.e., masquerading as either a message source or intended recipient. Encryption is required to prevent intermediate entities from discerning the content of the message, i.e. provision of confidentiality. Used together, both techniques can be utilised to prevent intermediate entities from tampering with the message to alter its content. Privacy extends to cover user location and the nature of the messages, since although the content of a message may not be discernible, it may be possible through traffic analysis to determine which type of service the user is utilising, e.g. web browsing or standard telephony. Analysis of IP datagrams may provide information as to the user's location even though the contents are encrypted. Compromising a user's location privacy may be undesirable in a traditional distributed network; however, the operation of the network remains intact. The same cannot be said for the PDE, as will now be explained.

The Personal Distributed Environment [1] is a novel concept being developed within the Mobile VCE research programme whereby users have access to their services and data through a distributed set of terminals, wherever they happen to be. Devices are co-ordinated by Device Management Entities (DMEs) [1]. The PDE operates over a distributed network that can be decomposed into physically separate subnetworks, as shown in Figure 1. Some of the subnetworks that comprise the PDE may be stationary: corporate LAN, household network, while others may be mobile: Personal Area Network (PAN), automobile-based network. Whilst the stationary networks are likely to be connected over fixed links, their mobile counterparts are likely to be connected to the others via a range of heterogeneous wireless technologies. Furthermore, the members of the PAN and automobile-based network may change with time due to mobility and also due to status: on or off. Thus, it is apparent that the topology of the PDE is dynamic in nature.

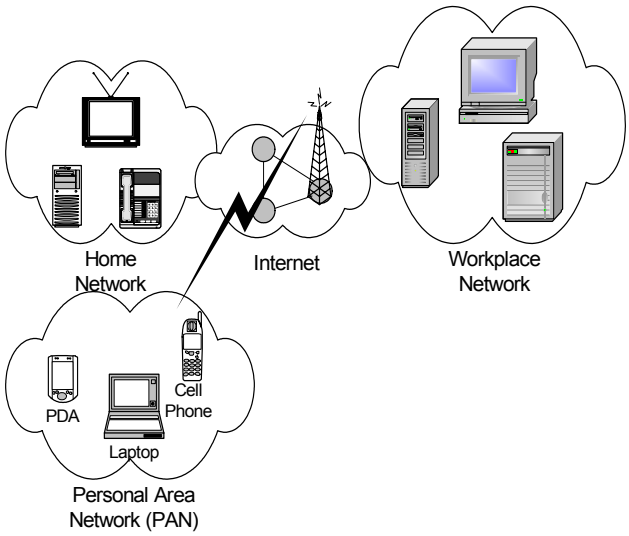


**Figure 1: PDE Subnetworks**

In order to facilitate interconnection of the PDE subnetworks a functional entity known as the Device Management Entity has been defined. Among its many functions is the maintenance of a topology database of the PDE, held in its location register. The location register is notified of changes to the PDE topology via location update messages issued by the devices themselves. The location register is a necessary component, required to direct incoming session requests to the appropriate PDE device. The determination of which device is most appropriate will depend on a number of factors: suitability of the device to support the session, tariff due for communication with end device, proximity of device to user. At present, there are a plethora of different wireless devices: PDAs, smartphones, digital radio, etc. Each of these devices have their own characteristics: screen size & resolution, support for cellular/Bluetooth/802.11

transmission technologies, and suitability for certain services such as email and file transfer.

The subnetworks may contain a number of devices, if each of the devices within, say the PAN, were to inform a centralised DME functional entity of their new location as they moved then large volumes of signalling would occur. Thus in order to permit scalability, a portion of the DME may be devolved to each subnetwork, giving rise to a distributed DME functional entity, as shown in Figure 2.

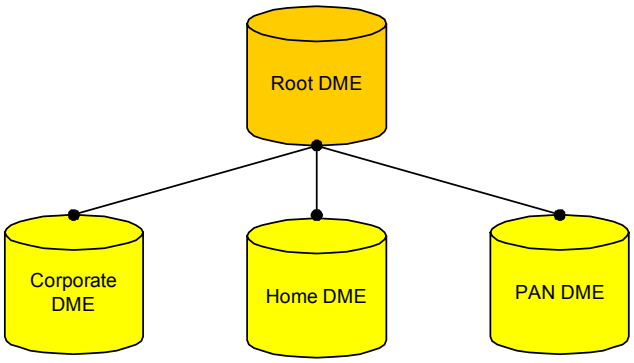


**Figure 2: DME Decomposition**

Adopting this approach means local changes in topology need only be transmitted to the local DME component. This has the effect of reducing signalling in two key ways: local devices can determine how to contact each other by contacting a *local* entity and thereby negating the need for signalling across the whole distributed network (this has the additional benefit of reduced delays), and signalling is reduced between the subnetworks and the root DME since the local DME component can store local updates then transmit them together in a more efficient fashion: group location updates. Indeed, the latter point exploits the fact that the PAN or automobile-based network is likely to move as a consistent unit, therefore, only a single (group) location update for the entire group of devices (subnetwork) may be necessary.

The remainder of this paper is organised as follows. Section II provides an overview of why location privacy is not only desirable for users but essential for PDE topological integrity. Section III discusses the security requirements for voluntary disclosure of location information to 3rd parties. Section IV discuses potential threats to location privacy from traffic analysis. Section V offers a proxy-based solution for location concealment from end users and explains why this approach is particularly suited to the PDE. Section VI provides a possible mechanism by which the PDE could circumvent attempts at traffic analysis. Section VII details how mutual authentication is used to counter threats to the PDE's topological integrity. Finally, Section VIII presents overall conclusions.

## II. Topological Threat

Since each of the PDE subnetworks is physically separate, it is practical to assume that in general 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 due to 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.

Accurate knowledge of the PDE's topology relies on the location register being supplied with accurate information. From a security perspective, this highlights the need to ensure that the database is not supplied with misinformation regarding topological changes. 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.

Set against the need for location privacy is the realisation that disclosure of just this type of information, to authorised parties, may form a valuable revenue raising service. For example, parents may wish to track their childrens' whereabouts, rescue services may locate those in danger etc. Thus there is a need to provide access to location information to trusted 3rd parties at a well designed and secure interface. A number of requirements must be satisfied to fulfil this, as described in Section III.

## III. Security Requirements

The concept of disclosing a degree of location information as a service requires management functionality behind the interface, and good interface design. In order to provide access

to location information, a number of requirements must be met. They should be able to cope with a range of design constraints; the constraints are based upon those developed for disclosure of status information in Instant Messenger applications [2]:

- The possibility of making location information available as a service gives rise to a necessity of making such information verifiable: the entity requesting this information must be able to determine that it has not been tampered with en route.
- Polite blocking must be an inherent part of the design. When an entity requests access to PDE location information. This request can be accepted and the information provided, or accepted but the information *not* provided (so called polite blocking), or refused and a reason for refusal offered.
- Where location information is supplied to an outside agency, it must be forwarded in a fashion that only that entity is capable of reading it.
- Where multiple entities/user request access to PDE location information, they should not be aware of each other's requests.
- Provision of location information must be able to accommodate concealing the IP addresses of the PDE device or the entity that requested the information.
- In order to preserve privacy of a user's location, it must be possible for a device or group of devices (e.g. an entire PDE subnetwork) to cease transmission of location information, i.e. the device may temporarily halt updating the location register. Similarly the device should have the ability to continue updating the location register but instruct the DME not to divulge this information to 3rd parties.

Another entity (other than an administrative function within the DME) must not be able to force a device or subnetwork to stop transmitting location updates.

- A PDE device or subnetwork must be able to opt out of *receiving* location updates from others; this may be desirable in situations where the local DME is connected to the rest of the PDE through a low bandwidth (or extremely expensive) link.
- A 3rd party must not be able to force a subnetwork to stop receiving location updates.
- Each device within the PDE must be able to determine whether its location is being disclosed to 3rd parties.

It is clear then that location information must be transmitted across the PDE through intermediate networks such that unauthorised entities are not able to mount a substitution attack leading to fragmentation of the PDE topology, or indeed unauthorised conjoining with other PDEs. Furthermore, location information must be accessible at a predefined interface to authorised 3rd parties and government agencies[1].

[1] To enable lawful interception.

In order to prevent substitution attacks from disrupting the operation of the PDE, a strong authentication mechanism is required between the root DME and its devolved components in each of the subnetworks. As mentioned, sections of the PDE may consist of low-power wireless devices with limited processing ability, hence potentially limiting the use of robust authentication mechanisms across wireless subnetworks due to the heavy processing loads they produce. However, it must be assumed that the device within wireless subnetworks that operates as the seat of the DME (and hence the location register) has sufficient processing capability. This device, therefore, is not subject to the constraints of the others in the wireless subnetworks and is consequently able to make use of more computationally expensive and robust authentication mechanisms such as Public Key Cryptography (PKC) approaches or private key schemes such as Kerberos [3].

## IV. POTENTIAL THREATS

It is anticipated that the root DME will reside in an Internet Service Provider (ISP) domain, and that a charge will be levied for providing this service. This location provides a number of benefits. When the root DME functionality is hosted on service provider hardware, rather than a user device, it is more likely to be supported by robust backup hardware in case the primary host malfunctions. Furthermore, given that the root DME is the first point of contact for incoming sessions, it is essential that it can always be contacted; this translates into a requirement to be situated within a reliable network. Wireless/mobile subnetworks may not be able to guarantee ubiquitous connectivity.

A popular approach for protection of data across the network is to have a secure tunnel that employs security mechanisms such as IPSec & AAA protocols (Figure 3) [4, 5]. However, in the PDE case, this approach will indirectly reveal location details of the management entities whenever an update of information is conducted, since although the information content is protected, the existence of the source can be determined.

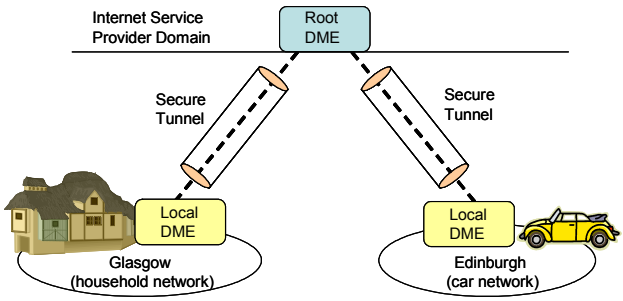


**Figure 3: Employing Secure Tunnel in PDE**

In order to aid comprehension of potential solutions, 3 key threats are highlighted:

1. Monitoring the links between the root and local DMEs, and between the local DME and the other devices in the various PDE subnetworks may reveal the hierarchical structure of the PDE. The may reveal that the root DME is

the top of the hierarchy and would be an optimal point for further eavesdropping.

2. Monitoring the connections between the root DME and each of the local DMEs may permit the location of the user to be inferred from the frequency of update messages.
3. A malicious party may monitor the size of signalling messages transmitted between the entities or nodes. For example, short messages may indicate pre-registered devices changing their points of attachment, suggesting that the user is located at the source subnetwork.

The above makes it clear that a DME's privacy can only be preserved when the three criteria - the DME's hierarchy structure (or relationship), the identity, and the signalling message types are protected.

## V. Concealment from End Users

There are a number of possible solutions to the privacy issue within the PDE.

Concealment of location from end parties can be achieved by the use of a proxy employing address translation. This approach fits well with the PDE architecture since the functionality of the root DME is based upon a SIP proxy [6]. SIP proxies act as intermediaries between communicating parties during the set-up phase of a call. The technology also permits the media session to be routed through that proxy as an option. Thus, where the user desires that location information should be concealed, a configuration option permits this. With this approach location information of a user's devices is still stored at a single location, enabling lawful interception and disclosure to authorised parties. Whilst this satisfies the need to preserve location information from end parties, it does not prevent interception within networks by malicious parties intent on discovering a user's location. Countermeasures against this will now be discussed.

## VI. Prevention of Traffic Analysis

To counter the threat of traffic analysis, a simple solution would be to attempt to obscure information flows by ensuring an active communication pattern between PDE nodes and with other non-PDE nodes: cover traffic. This may include each local DME to send regular update messages even if the devices under their control do not require it. Additionally, "dummy" nodes can be created to send redundant messages to other DME hosts. Padding may be required in order to form consistent message sizes so that the types of message (i.e. is it a signalling information or a normal message?) cannot be determined. Although simple, such a solution is highly inefficient. Signalling between the PDE subnetworks and the root DME will go over intermediate access networks, and this may incur a charge. Moreover, the wireless nature of many of these access networks (and associated PDE devices) is such that increased radio transmission will result. This is a significant disadvantage since RF transmissions drain the battery power of portable devices – often the most precious resource of many mobile devices.

Another countermeasure against traffic analysis is the use of Mix Networks, as shown in Figure 4.

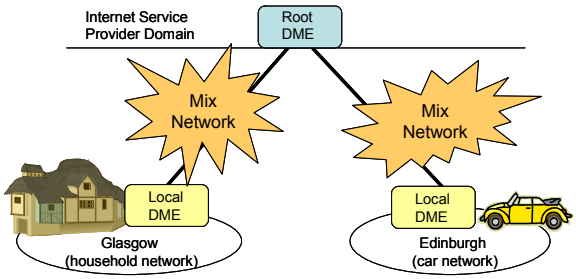


**Figure 4: Using Mix Network in PDE Network**

Mix networks have been proposed [7] with the intention of offering anonymous communication facilities. The traditional relaying nodes are supplemented with special mix nodes that prohibit message tracing from source to destination by another party. This solution certainly addresses the threats discussed previously. However, the delay introduced by the mix network approach of packet reordering and scheduling may prove prohibitive with regards to call set-up times. Furthermore, given that all traffic emanating from a particular PDE subnetwork is associated with a single user, scrambling of flows of a particular user cannot provide location privacy. Finally, the effectiveness of mix networks is such as to bring concerns as to the feasibility of lawful interception and monitoring.

The solution proposed in this paper leverages the knowledge that mobile subnetworks (e.g. PANs) will be connected to the Internet (and hence the root DME) via a range of heterogeneous access networks (WLANs, cellular etc.). If the choice of access network over which to send location update messages were chosen at random then it would be nontrivial to determine the source of the messages. Moreover, this approach would require an eavesdropper to monitor a range of separate proprietary networks simultaneously.

## VII. Topological Integrity

In order to preserve the topological integrity of the PDE, a strong encryption mechanism is required to provide mutual device authentication. A two phase procedure is envisaged, as depicted in Figure 5, whereby the local and root DMEs mutually authenticate, followed by each of the PDE devices mutually authenticating with a nominated local DME.

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.

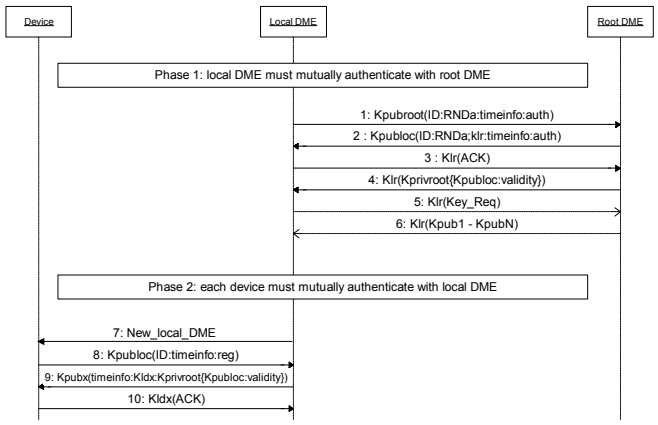


**Figure 5: Authentication**

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 ($K_{lr}$). All of this is encrypted by the local DME's public key, $K_{publoc}$. 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) a digital certificate, $K_{privroot}\{K_{lpuboc}$:validity$\}$. The digital certificate 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 certificate can be used in order to prevent replay attacks. The local DME can use this certificate 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[2] encrypted using the session key. The root DME subsequently responds (message 6) with a list of keys (public or secret), $K_{pub1}$ to $K_{pubN}$.

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, $K_{publoc}$. 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 digital certificate, 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 digital certificate 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, $K_{ldx}$.

[2] Note: 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.

## VIII. CONCLUSIONS

The PDE concept introduces great potential for users to have access to all their applications, services and data wherever they happen to be. However, this potential comes at a cost: that in order to provide services in any location, information about that location will leak easily from the network. This paper has described the requirements and constraints which have to be imposed on the PDE to ensure that this does not happen. Protocol design within the PDE has taken these issues into account to give the correct balance between service and security.

A three headed approach is proposed consisting of proxy-based anonymity, random access network utilisation, and strong mutual authentication.

## ACKNOWLEDGEMENT

The work reported in this paper has formed part of the PDE area of the Core 3 Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, 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] J. Dunlop, R.C. Atkinson, J. Irvine, D. Pearce, "A personal distributed environment for future mobile systems", *IST Mobile & Wireless Communications Summit*, June 2003.

[2] M. Day et al., Instant messaging / presence protocol requirements, IETF RFC 2779, February 2000.

[3] J. Kohl & C. Neuman, The kerberos network authentication service (v5), IETF RFC 1510, September 1993.

[4] S Kent & R Atkinson, Security architecture for internet protcol, IETF RFC 2401, November 1998.

[5] J. Vollbrecht et al., AAA authorization application examples, IETF RFC 2905, August 2000.

[6] J. Rosenberg et al., Sip: Session initiation protocol, IETF RFC3261, June 2002.

[7] A. R. Beresford, F. Stajano, "Location privacy in pervasive pomputing", *IEEE Pervasive Computing*, 2(1):46-55, 2003.