Architectural and QoS Aspects of Personal Networks

T.J.M. Coenen, P.T.H. Goering, A. Jehangir,
J.L. van den Berg, R.J. Boucherie,
S.M. Heemstra de Groot, G.J. Heijenk
University of Twente, Enschede, The Netherlands
{t.j.m.coenen, a.jehangir, p.t.h.goering}@utwente.nl

S.S. Dhillon, Weidong Lu,
Anthony Lo, P. Van Mieghem, Ignas Niemegeers
Delft University of Technology, Delft, The Netherlands
{w.lu, s.dhillon}@ewi.tudelft.nl

***Abstract*—Personal Networks (PNs) are future communication systems that combine wireless and infrastructure based networks to provide users a variety of services anywhere and anytime. PNs introduce new design challenges due to the heterogeneity of the involved technologies, the need for self-organization, the dynamics of the PN composition, the application-driven nature, the co-operation with infrastructure-based networks, and the security hazards. This paper discusses the challenges of security, service discovery and QoS provisioning in designing self-organized PNs and combines them all into an integrated architectural framework.**

I. INTRODUCTION

The future mobile communication system is envisaged to be the convergence of wireless ad-hoc networks and infrastructure based networks to provide the user a variety of services anywhere and anytime. Personal networks [1] as user-centric enablers for future mobile communications, start from the user and extend the user's personal area network (PAN) to a global coverage of his personal devices and services in his home, car, office etc. as well as other foreign networks and services regardless of their geographical locations.

In order to realize a self-organized PN, the following topics require specific attention. First of all, a secure PN architecture at the network layer, which is independent of underlying network technologies, needs to be defined. On top of that, PN communication, service discovery and provisioning mechanisms could be implemented. Finally, QoS needs to be provided to live up to customer expectations and to support current and future multimedia applications. This paper discusses these challenges in designing self-organized PNs.

The organization of this paper is as follows. Section II presents the secure PN architecture. Sections III proposes a service discovery framework for PNs. Section IV discusses the QoS aspects of PNs. And Section V gives a conclusion.

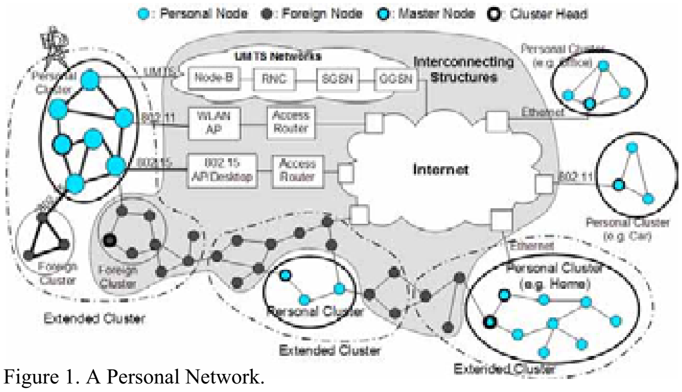

Figure 1. A Personal Network.

II. SECURE PERSONAL NETWORK ARCHITECTURE

An abstract personal network is illustrated in Figure 1. We start to introduce the PN from its basic element, a personal node. Personal nodes are distributed over different locations, for example, staying with the person, at home or office, in a car, etc. Personal nodes in close vicinity of each other may form Personal Clusters by interconnecting with each other in an ad-hoc fashion without intervention of any foreign nodes. Personal clusters are denoted with thick circles in Figure 1.

Moreover, each personal cluster will elect a Master Node, which is responsible for the management of that cluster. The roles of the master node are multifold: First of all, it acts as a security agent to authenticate new nodes that join the cluster, initiate periodic cluster key updates and generate cluster advertisements. The master node is also responsible for trust relationship establishment between different personal clusters and between personal clusters and foreign clusters if they need to communicate with each other. Additionally, the master node is able to evict members on demand and is also responsible for setting the cluster policy which lets devices joining the cluster know about various cluster parameters like the frequency of cluster advertisements and key updates, as well as the duration of timers, etc. Secondly, the master node is responsible for route management within the personal cluster and exchanging route information with master nodes of other clusters. Thirdly, the master node is responsible to collect the services provided within the personal cluster and present them to the outside world such as other personal clusters or even foreign clusters.

In addition, personal clusters are not in isolation, they can connect to the outside world either via infrastructure based networks such as the Internet or through ad-hoc networks. Normally, infrastructure access is preferable if it is available. However, there may be some situations where infrastructure access is not available or not convenient. In these cases, personal clusters can also be extended in an ad-hoc fashion. A hierarchical structure is adopted for PN ad-hoc communication in order to improve the scalability and reduce the control packet overhead. Personal clusters belonging to different PNs automatically form the first level clusters and they are managed by their own master nodes. At the second level, personal clusters belonging to different PNs, which are in close vicinity of each other, form an extended cluster. A cluster head can further be elected; and routing information can be exchanged between the cluster head and master nodes

0-7803-9792-4/06/$20.00 ©2006 IEEE

of different first-level clusters. At the third level, extended cluster heads could further exchange their routing information with each other. In this way, ad-hoc routing for PN communications can be well established even though the ad-hoc network might be large in size.

Providing security for communication of PN devices is a challenge. The limited computational and energy resources of many PN devices indicates that any proposed solution must be simple and lightweight so that it does not create a performance bottleneck. As energy is the scarcest resource in our system, security mechanisms must be selected based on their power consumption. We believe that it is sufficient for PN devices to demonstrate group membership of a cluster rather than their individual identity. This reduces key management overhead. A symmetric group key known as the cluster key is used to guard against unauthorized access that can degrade the QoS for PN users. All intra-cluster traffic is protected using message authentication codes derived from the cluster key shared by all cluster members. Consequently any other device receiving this traffic can verify that it was generated by another cluster member and not modified in transit by any un-trusted device. Unauthenticated traffic is not forwarded into the cluster. Once an un-clustered device is recognized as part of the PN, it receives the cluster key, enabling it to take part in secure communication. This cluster key is then periodically refreshed at an interval that depends on the security level required and the need to forcibly evict cluster members.

Cluster discovery is done by listening for cluster advertisements, which are generated by the master node. These advertisements are forwarded by other cluster members and thus propagate to the edges of the cluster, quite like a ripple on a pond. Un-clustered devices periodically wake up to listen for such advertisements. When an un-clustered device receives a cluster advertisement from a cluster belonging to its own PN, it will attempt to authenticate itself and to join that cluster. Besides authenticated cluster traffic (i.e. traffic protected with the cluster key), cluster members also accept unauthenticated EAP requests which are forwarded to the master node for authentication. EAP is an extensible protocol that can carry a variety of authentication mechanisms like shared keys, digital certificates etc. Predictably, devices that are not part of a cluster do not accept EAP requests.

The EAP mechanisms we propose for use have some important differences with IEEE 802.1X. For instance, after a successful authentication the supplicant no longer maintains any relationship with the authenticator and can communicate through any other cluster device. We also propose an extension which allows complete clusters to merge instead of just permitting individual devices to join a cluster. For more details on the security architecture refer to [2].

III. Service discovery framework

A personal network consists of several nodes that self-organize into clusters. For this self-organization we need a service discovery mechanism to find what is available in the neighborhood. We consider the case where one or both of the clients and services are mobile devices, connected in an ad-hoc fashion to other nodes. First, we distinguish the case where the client and server are located in each others vicinity, either in the same PN, in separate PNs or not in any PN at all. Here, the client wants to locate the nearest server with the best matching service. Second, we need a global service discovery, where any client in anybody's PN can find any service located anywhere in the world. The client and server can be connected through Infrastructure, like the Internet. In the following paragraphs, we will discuss local service discovery and how the local service discovery is applied in a PN context and used for global service discovery.

Local Service Discovery: For service discovery in PNs, where we want to discover services located nearby, we need a fully distributed system, suitable for multi-hop wireless networks. Furthermore the system should work as soon as a new node joins, without the need to pre-establish a personal cluster. Note that not necessarily all nodes in the vicinity are part of the same PN. For local service discovery in ad-hoc networks we propose to use attenuated Bloom filters. Bloom filters are used to represent several strings in one set of bits by using hash coding techniques. An attenuated Bloom filter is an array of standard Bloom filters of depth d. Every row in the filter represents objects at a different distance, indicated by the number of hops. For each neighbor a node will receive and store a separate attenuated Bloom filter. This enables to select a neighbor with more information about where an object most likely can be found. Periodically broadcast packets are sent to all direct neighbors. The packets contain Bloom filters that represent the services reachable through the sending node up to *d* hops away. Advantages of using Bloom filters are the simple computations and efficiency with space and bandwidth. For details on the service discovery protocol, refer to [3].

Service discovery in PNs: The local service discovery mechanism lets nodes located in the same local area distribute the services they know of among each other. There is no need yet for setting up routes or forming clusters. The system can be used to get information about the nodes nearby to form a personal cluster. Another use is to find other clusters, belonging to other persons/organizations so we can form an extended cluster, see Section II. Nodes will advertise services they consider to be public to all neighbors. When a cluster is formed, nodes in this cluster can communicate securely, and all services are advertised within the cluster. In order to locate other clusters, a directory server can be established at home or at an Internet service provider, where all services available for the PN will be stored. Anybody trying to find a service in the PN will contact the directory server that will give the location the personal cluster containing the requested service. When the query arrives in the personal cluster, it will be handled as if it was a query for a local service.

IV. QoS aspects of PNs

The ad-hoc nature of PN brings many difficulties for QoS provisioning, needed for real time and broadband applications. The main issues complicating QoS provisioning in PNs are:

- *Unpredictable link properties*: Interference and signal fading make the media unpredictable.

- *Limited battery life:* Mobile devices have limited resources, so QoS must be power aware and efficient.
- *Hidden and exposed terminal problem:* Nodes may cause collisions because they do not sense each other, or may unnecessarily block each other.
- *Node mobility:* The network topology can be dynamic, changing the links between nodes as they move in and out of each others transmission range.
- *Route maintenance:* Maintenance of state information is very difficult. Routes may break during data transfer, which calls for route recovery.

In mobile ad-hoc networks, due to the issues stated above, guaranteed QoS can not really be achieved; it can, at most, be 'approximated' by applying appropriate packet handling and resource management at the MAC layer in conjunction with sophisticated routing at the network layer.

QoS at the MAC layer: The MAC layer plays an important role in QoS provisioning. For achieving differentiated QoS, priority levels are assigned to packets from different applications. This differentiation is on a hop-by-hop basis, not end-to-end. More stringent QoS requirements can be met when, in addition, all nodes between sender and destination reserve resources for a (real-time) traffic flow. Obviously, this is more complex and requires appropriate cooperation with routing at the network layer.

One of the most well-known MAC protocols is the IEEE 802.11 MAC protocol, which uses the Distributed Coordination Function (DCF) as the basic access mechanism. DCF utilizes CSMA/CA where all nodes sense if the channel is idle. Each node holds a contention window (CW), from which a random backoff time is taken. After the channel has been idle for a distributed interframe space (DIFS), the backoff timer is decremented and when it expires, transmission is initiated. Some proposals have been made to extend the protocol with service differentiation. The IEEE 802.11e MAC protocol is the standardized packet scheduling approach to QoS provisioning in ad-hoc networks. IEEE 802.11e stations have different queues (access categories, or ACs) for packets originating from applications with different service requirements. For all ACs different DCF parameter settings can be used, for instance a smaller contention window, DIFS size and allowing multiple packets to be sent after winning the contention.

Other approaches use a more explicit differentiation between the traffic classes in different nodes by exchanging information about the rank of their highest priority packet to synchronize their scheduling parameters. An out of band approach is also possible to make fast reservations for the high priority traffic. A centralized approach is possible as well where some nodes are chosen to coordinate access to the channel of the other nodes in their neighborhood. This could for instance be done by the cluster heads in a PN. A polling scheme like the Point Coordination Function (PCF) from IEEE 802.11b can then be used.

QoS Routing in PNs: Much work has been done in the areas of QoS routing for static networks, i.e., the networks with non-varying topology and ad-hoc routing. For example, SAMCRA is proposed as an exact QoS routing algorithm for static networks and can be considered as sufficiently useful in practice. But the solutions proposed for QoS routing in static networks are not straightforwardly extended to ad-hoc networks due to the changing topology and non-uniform propagation characteristics of wireless transmissions. Most of the QoS algorithms for static networks assume the availability of precise state information (e.g., the probability distribution for link delay) besides the topology of the network. In ad-hoc networks, the topology and the link parameters e.g., available bandwidth are changing, although, the topology is changing on a slower time scale. Moreover, if the topology of an ad-hoc network changes too fast, QoS routing may become impossible. Due to the inherent characteristics of the wireless medium in ad-hoc networks, the available bandwidth is shared between the neighboring nodes. Thus, QoS routing in ad-hoc networks is heavily dependent on how well the resources are managed at the MAC layer.

Most of the current ad-hoc routing protocols such as AODV, OLSR and ZRP are best-effort. They are targeted at finding a feasible route from the source to the destination without considering current network traffic or application requirements. Since hard QoS, i.e. guaranteed constant bit rate and delay, is difficult to achieve for ad-hoc networks, the aim of many QoS ad-hoc routing protocols has been to develop soft QoS or better than best-effort services.

An alternative solution to the problem of QoS routing is the AntNet algorithm [4]. In AntNet, the network topology and the end-to-end delays for different paths are represented by probabilistic routing tables. The probabilistic routing tables are updated by the mobile agents (control packets) depending on the end-to-end delay. The data packets travel using probabilistic routing tables leading to load-balancing or multi-path routing. AntNet has been shown to provide load balancing and it performs well under heavy traffic conditions as well as small static networks with sparse topologies. But the performance of the AntNet algorithm for ad-hoc networks is an open issue and needs further investigation.

V. Conclusion

This paper discussed the architectural and QoS aspects of a self-organized personal network taking into consideration security issues. Solutions for a secure PN architecture, service discovery framework, and QoS support for PNs at both the MAC layer and the network layer are presented briefly.

References

[1] I. G. Niemegeers and S. M. Heemstra de Groot, "Research issues in ad-hoc distributed personal networking", Wireless Personal Communications, vol. 26, no. 2-3, August 2003.

[2] A. Jehangir, and S.M. Heemstra de Groot, "A Security Architecture for Personal Networks", First International Workshop on Personalized Networks, San Jose, U.S.A, 2006.

[3] P. Goering and G. Heijenk, "Service Discovery Using Bloom Filters", Proc. Twelfth Annual Conference of the Advanced School for Computing and Imaging, Belgium, June 14-16, 2006.

[4] G. Di Caro, and M. Dorigo, "AntNet: Distributed Stigmergetic Control for Communication Networks", Journal of Artificial Intelligence Research 9, 1998.