SELF-MANAGEMENT IN AMBIENT NETWORKS FOR SERVICE COMPOSITION

Lawrence Cheng[1], Roel Ocampo[1], Alex Galis[1], Robert Szabo[2], Csaba Simon[2], Peter Kersch[2]

[1] *University College London, Electrical Engineering Department, Torrington Place, London, WC1E 7JE, UK {l.cheng, r.ocampo, a.galis}@ee.ucl.ac.uk:*

[2] *Budapest University of Technology and Economics, Department of Telecommunication and Media Informatics, Magyar Tudosok krt. 2., 1117, Budapest, Hungary {szabo, simon, kersch}@tmit.bme.hu*

Abstract: This paper describes the concepts and challenges of self-managing management-layer network composition and service composition in Ambient Networks. A set of requirements are identified. This paper describes the concept of Ambient Virtual Pipe (AVP), which is an autonomic, secure, QoS-assured, self-adapted context aware management service overlay network that provides a secure and QoS-assured environment for AN service composition. The AVP is supported through a programmable platform, and is capable of dynamic deployment of new management services.

Key words: Ambient networks; context-awareness; programmable techniques; self-management; service composition.

1. INTRODUCTION

The EU-IST Ambient Networks (AN) project [4] focuses on the development of novel networking concepts and systems that support a wide range of user and business communication scenarios beyond today's fixed, 3rd generation mobile and IP standards. The concept of Ambient Control Space (ACS) [5] is the centre of the project. The ACS is responsible for the management of the underlying data transmission capabilities. A complex set of interdependent control functions form the ACS. The management of AN

is conducted by the Domain Manager Control Function. This management function works consistently and autonomically with other control functions being developed in the AN project. Details of ACS and Domain Manager Control Function can be found in [4][5].

AN management systems support the *composition* and *cooperation* of heterogeneous networks, on demand and transparently. Composition and cooperation must be achieved without the need of manual (pre or re)-configuration or off-line negotiations between network operators. Thus, AN management systems must be dynamic, distributed, self-managing and responsive to the network and its ambience [6]. The composition of heterogeneous ANs means an Ambient Network is able to dynamically compose with several other Ambient Networks. Co-operations between Ambient Networks could potentially belong to separate administrative or economic entities. Hence, Ambient Network composition provides network services across a set of ANs which were originally independent of each other in a cooperative way. The Ambient Network Interface (ANI) provides the facility of co-operation across different Ambient Networks. It is through the ANI that different management systems and network elements of ANs may communicate and co-operate with each other. A composed and cooperating AN(s) enable a user to access transparently the services offered by other Ambient Networks (that are previously independent of each other) via the Ambient Service Interfaces (ASI). Figure 1 shows the concept of composition and co-operation, and the logical location of ANI and ASI in AN(s) [5].

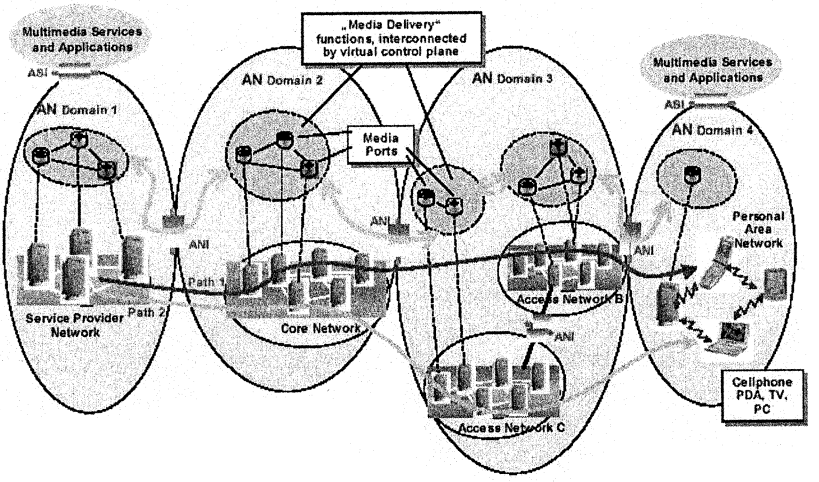


Figure 1. ASI and ANI in AN(s)

This paper starts with the discussion on the requirements of AN network composition in management point of view; followed by a description on a solution towards self-managing management-layer network composition and service composition in ANs. The proposed solution is known as the *Ambient Virtual Pipe (AVP),* which creates a management service overlay network for dynamic deployment of new management service over composed AN.

2. AN COMPOSITION REQUIREMENTS

Network composition is one of the major concepts of Ambient Networks. An AN may consist of many individual smaller ANs. The smaller ANs were composed through network composition. Through network composition, the sharing of network resource such as inter-network connectivity or network storage are negotiated during network composition according to policies. Note that because ANs are mobile, they may compose and decompose dynamically. As a result of network composition, end users are capable of being connected, and connecting to any network instantly. This is known as network-layer composition in this paper. From management point of view, AN network composition refers to the instant negotiation and enforcement of a new Service Level Agreement (SLA) between network resources under composition for the provisioning of an IP service. From a business point of view, network composition can be viewed as a temporary agreement among independent networks. A common business goal is achieved by the collaboration of agreements. The diversity and complexity of the market are matched by the temporary agreement. Thus the capability of rapid reaction to the dynamically-changing demands of today's markets is improved. It is obvious that for scalability and performance issue, the process of network composition should be as transparent as possible. One of the major challenges of compositions is currently there is a lack of support for automatic creation and administration of composed/composing service networks. Automatic service composition refers to the discovery of adequate ANs and their services, negotiation among them, the definition of business relations, the collection of configuration information and requirements, and the reservation of appropriate resources in the network infrastructure. AN network-layer composition is discussed in details in [8].

The management challenge of AN network composition is that the management systems of individual networks must also be composed during network composition for the purpose of consistency. This is known as management-layer network (de)composition in this paper. The requirements for AN management-layer network composition is as follow. Detail discussions on AN management challenges can be found in [5]:

a) The composition mechanism should be *performance-wise low cost,*

robust and *scalable*. Performance and scalability are concerned because potentially a large number of ANs may compose and decompose at a given time (so as their management systems). Robustness is needed because the underlying ANs may compose and decompose dynamically as the ANs join and leave arbitrarily (so as the management-layer).

b) The network management systems of the underlying ANs that are composing or decomposing may be heterogeneous. The composition mechanism should be *flexible* to overcome heterogeneity.

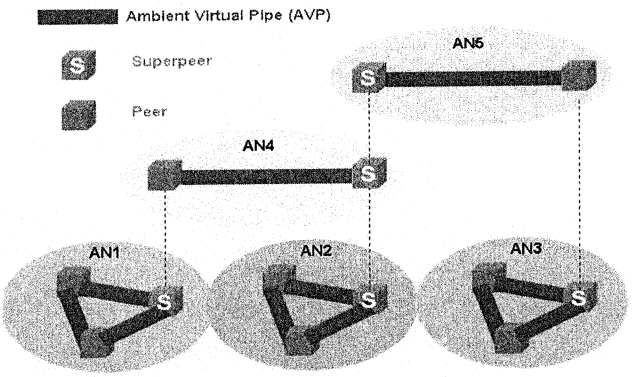
c) *Service-oriented* composition mechanism is needed in order to support new management services running in the composed management system.

d) Due to the potential large number of AN composition and decomposition (due to AN nodes joining or leaving the AN arbitrarily), the composition mechanism should be *autonomic*.

Conclusively, a self-managed management system is needed in AN to support autonomic management-layer composition and service composition for dynamic deployment of AN services across heterogeneous composed/composing ANs.

3. AMBIENT VIRTUAL PIPE (AVP)

It was discussed in early section that the AVP is an autonomic, secure, self-adapted, and context aware management service overlay network across composed AN nodes. This management service overlay network is self-adapted according to change in underlying network context information in order to support the dynamic deployment and execution of new AN (management) services in the composed management system, thus provides a dynamic, secure and QoS assured channel for P2P management traffic. A highly dynamic and flexible information infrastructure is needed in order to support new management service deployment over a composed AN management domain. This information infrastructure must be capable of providing secure and reliable connectivity across heterogeneous networks with guaranteed quality on demand. It may be arguable that conventional solutions like the currently available Virtual Private Networks (VPNs) may be used to provide QoS guarantees to networks. However, the major drawback of the today's VPNs is their low flexibility to quickly adapt to the changing requirements. A programmable [11], flexible, and network contextaware information infrastructure is therefore needed with guaranteed QoS in the composed AN management domain. This infrastructure is the AVP.



The AVPs are shown in Figure 2. The AVP provides a secure and QoS-assured channel for protecting P2P management information exchanged between distributed AN management entities in composed ANs, and the AVP creates an environment where new AN management services to be launched and executed i.e. service composition across heterogeneous ANs.

This secure, QoS-assured, management service network overlay is essential for both management-layer composition in AN as well as new AN management service deployment and execution. As discussed earlier, AN network composition is carried out through negotiation, AN management systems composition is also carried out through negotiation between heterogeneous management systems. Superpeer election is conducted through negotiations between peers. Distributed management information must be shared securely and in a QoS-assured fashion to enable negotiation to take place (hence management-layer and service composition). The AVP provides a suitable environment in which all these management negotiations may take place. Traditionally, a network domain administrator is capable of managing the administrative tasks within its own administrative domain. End users within a particular administrative domain may request for services that are served with some level of service guarantee from its own network domain administrator. However, inter-domain service management is complex, this is due to the heterogeneity of the administrative environment and the underlying network elements of different administrative domains. The idea of AN management-layer network composition through the P2P management system and the creation of a management service overlay network among the peers provides a mean to achieve inter-domain service

management in a secure, QoS-assured, and self-adaptable environment. The network context aware capability of AVPs provide the necessary QoS and resource assurance and security for protecting the management traffic within the management service overlay network in a *dynamic* fashion. The creation of AVPs and its capabilities (such as security and contextawareness) are supported by a flexible and programmable infrastructure (see later section on implementation).

Note that AVPs are not restricted to provide a secure and QoS assured management service overlay network for management services. The capabilities of AVPs make it potentially ideal for the dynamic deployment of user specific services across heterogeneous ANs. For instance, with the existence of AVP, it is possible for a management entity in a particular AN to deploy its own services (that are not available in other ANs) in another (composed) AN. As discussed, the capabilities of AVPs are supported through a programmable platform. A set of requirements for AN programmability were defined in [5][7]: rapid development of new management services replaces slow manual configuration; customisation of existing management service features; scalability and cost reduction in AN network and service management; independence of AN network equipment manufacturers; information AN network context and service integration. The dynamic creation of AVP is achieved by dynamically injecting active code to desired peers in order to instantiate AVPs. The active code carries executable programs which result in security association implementation between peers. QoS in AVP is assured through the injection of active code to dynamically prioritising AVP traffic flow. DINA [2] is used as a programmable platform in AN to support AVP provisioning. Figure 3 shows the actual deployment of AVP through a programmable network. Details of the AVP implementation are discussed in the next section.

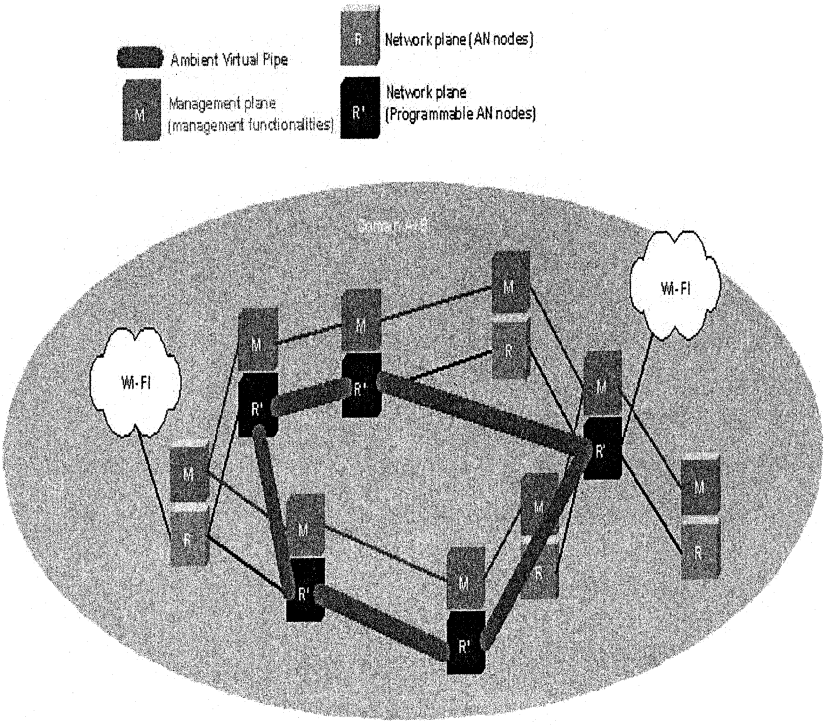


Figure 3. AVP Support through a Programmable Structure

4. IMPLEMENTATION OF AVP

The *AVP Managers* are responsible for managing AVPs .The AVP Managers are distributed across desired participating AN nodes in the composed AN network. The ContextWare components of AVP i.e. CMSs are responsible for monitoring real-time network context information, and are responsible for providing pointers to the distributed network context information that can be retrieved by the AVP Manager. Details of the ContextWare components of AVP are presented in [9]. Retrieving network context information by the AVP Managers subsequently triggers SNMP traps. The traps are then processed by sub-components of the AVP Manager according to pre-defined policies. The traps indicate the type of dynamic provisioning and self-adaptation to be deployed on the management service overlay network.

As discussed earlier, the autonomic establishment of AVP is done by

using DINA [2][11] active packets. Active packets are also used for security provisioning and QoS provisioning of AVPs. The AVP QoS provisioning is an example of its capability of self-adaptation. An interface is provided between the AVP Manager and the Linux iptables and tc mechanisms for AVP internal flow marking and classification. This interface causes the AVP flow to be internally marked within the node using iptables. The flows are then classified by tc into specific classids. Bandwidth is allocated to each flow by setting the bandwidth of the associated queuing discipline (qdisc) of the tc classid. AVP security provisioning is needed in order to protect the authenticity, integrity and confidentiality of the management data transmitted in the AVPs, and also the active control packets that are transmitted and executed across AN nodes. The AVP Manager currently uses Freeswan IPSec and therefore supports IKE and IPSec. AVP supports hop-to-hop protection, which is needed for protecting the authenticity, integrity and confidentiality of active packets. The discussion and implementation of hop-to-hop protection for active packets is discussed in details in another paper [3] written by the author of this paper. Note that in the current implementation, as a proof of concept, a unicast IPSec structure is assumed. The security of multicast traffic is being investigated in [10]. The context awareness and capability of self-adaptation of AVP were demonstrated through various aspects. Firstly, when two (or more) ANs compose, AVP will be automatically established between the peers (of the two composing ANs). As soon as a composed AN is formed, a Superpeer is elected by the P2P management system (of the peers within the AN). Note that AN nodes are regarded as peers in AN. Peers are organised by a P2P management system in a hierarchical structure for scalable management [1]. A Superpeer is an elected peer of which is responsible for inter-AN communications. The election process of Superpeer is described in [1]. The establishment of AVP between Superpeers results in a new overlay network on top of the other peers. The selection of new Superpeer of this new overlay is done by negotiation between the two Superpeers' P2P management system, which is conducted securely and in a QoS assured fashion through the AVP. The activation of the secure channel is done by active packets. It should be note that the AVP Manager (through the use of IKE) is responsible for negotiating with peers on security associations (SAs) establishment. As soon as the CMSs detects a new peer has joint the AN, SAs are negotiated automatically. The CMSs also reports when an AN (Superpeers and/or peers) has left, the AVP will adapt itself when decomposing i.e. obsolete the established SA. This is an example of network contextawareness. Another example of self-adaptation is that once a new overlay is created, the AVP Managers retrieves network context information from the CMSs for QoS self-adaptation. For instance, when an AN composes with another AN, and the latter AN generates a large amount of management traffic, then the AVP

Manager will self-adapt the AVP bandwidth (in the original AN) through the use of active technologies as described in [9]. In this way, the QoS of the AVP in the original AN is assured.

5. CONCLUSION & FUTURE WORK

In this paper we presented the architecture and the key concept of Ambient Networks namely the management-layer network composition for service composition. A set of requirements were listed. We have identified the management challenges of network composition and service composition. A solution was then presented.

AN nodes are organised in peer groups and are placed in a hierarchical order, through a P2P management platform. The operations of P2P management system results in a hierarchically structured management overlay network aligned with the physical network structure. The hierarchy of management overlays is developed in accordance with network composition strategies. This can be viewed as a topological resource composition which structures the network resources and their topology according to dynamic composition rules/policies.

We then presented the concept of AVP which is an autonomic, secure, QoS-assured, self-adaptable, and contextaware management service overlay network that is needed to overcome the service composition challenges. This management service overlay network is created dynamically between AN management entities in order to provide a secure and QoS assured means of communication channels between management entities in composed ANs, as well as a secure and QoS-assured environment in which new AN (management) services may be deployed and executed. The instantiation of AVPs is supported through a flexible, scalable, and programmable infrastructure deployed among the peers. Through AVPs, it is now possible to transport management traffic and carry out negotiations between the management entities in the P2P management system in a secure and QoS assured way. The AVP also provides a secure and QoS-assured environment in which new services across heterogeneous ANs may be deployed. The AVP is self-adapted and contextaware, that it may automatically adjust its behaviour according to changing network context. Lastly, the implementation of AVP and its deployment were presented. The next stage of implementation is to refine the current implementation of the AVP Manager. Instead of unicast IPSec, a multicast alternative should be deployed should the management traffic is multicast. The SA establishment between peers must also be refined. This is because there may be a lack of a trusted third party in wireless domains. Performance results will be analyzed to prove the practicability of the presented solution.

ACKNOWLEDGEMENT

This paper describes work undertaken in the context of the Ambient Networks - Information Society Technologies project, which is partially funded by the Commission of the European Union.

REFERENCES

1 C. Simon, et al., Peer-to-peer management in Ambient Networks, poster in 14th IST Mobile & Wireless Communications Summit (2005).
2 D. Raz, et al., An Active Network Approach for Efficient Network Management, Lecture Notes in Computer Science 1653 Springer (1999), ISBN 3-540-66238-3.
3 L. Cheng, et al., Strong Authentication for Active Networks, IEEE-Softcom (2003).
4 Ambient Networks (2005), http://www.ambient-networks.org.
5 Brunner, M., et al., Ambient Networks Management Challenges and Approaches, ISBN 3-540-23423-3, Springer- Verlag Lecture Notes in Computer Science - IEEE MATA (2004).
6 Galis A., et al, Ambient Network Management – Technologies and Strategies, AN Deliverable 8.1 (2005), http://www.ambient-networks.org.
7 Jorge Andres, et al., R8-2 Report: Description of concept and scenarios for network composition management and self-management, (unpublished), Ambient Networks project internal report, 2004.
8 C. Kappler, et al., A Framework for Self-organising Network Composition, WAC (2004).
9 R. Ocampo, et al., ContextWare Support for Network and Service Composition and Self-Adaptation, to appear in IEEE-MATA (2005).
10 G. Selander, et al., Ambient Networks Intermediate Security Architecture, (2005), Deliverable 7.1, http://www.ambient-networks.org.
11 Galis A., et al., Programmable Networks for IP Service Deployment, Artech House Books, ISBN 1-58053-745-6; pp.450.