Quick NAP - Secure and Efficient Network Access Protocol

Jari Arkko*, Pasi Eronen†, Hannes Tschofenig‡, Seppo Heikkinen§ and Anand Prasad¶

*Ericsson Research NomadicLab, E-Mail: *Jari.Arkko@ericsson.com*
†Nokia Research Center, E-Mail: *Pasi.Eronen@nokia.com*
‡Siemens, E-Mail: *Hannes.Tschofenig@siemens.com*
§Tampere University of Technology, E-Mail: *Seppo.Heikkinen@tut.fi*
¶DoCoMo Euro-Labs, E-Mail: *prasad@docomolab-euro.com*

***Abstract*— Current network access protocol stacks consist of a number of layers and components that are only loosely aware of each other. While this provides flexibility, it also results in a number of limitations, including high signaling latency due to duplicated tasks at multiple layers, security vulnerabilities, and deployment problems when new components and protocols are added. Most of currently ongoing work attempts to improve the network access protocols through enhancements in different parts of the stack, such as network access authentication or mobility protocols. This paper takes a "clean slate" approach by focusing on opportunities that arise when the network access problem is viewed as a whole as opposed to focusing on a single layer. By taking this cross-layer viewpoint, it is possible to design a stack that significantly reduces the number of roundtrips, can be operated securely in ad hoc networks, and allows the secure integration of new features such as firewalls or quality of service signaling.**

I. Introduction

In network access, several steps need to be performed before a device has sufficient end-to-end connectivity for its applications. In IEEE 802.11 networks, for example, these steps include network detection, authentication and association at layer-2, IP address assignment, and router discovery. Additional steps are required for mobile nodes that move between subnets, or in situations where there is a need to interact with quality of service mechanisms or middleboxes such as NATs or firewalls.

Treating these steps independently of each other has shortcomings. Steps that have to be performed in sequence and mandatory delay periods introduce latency. Current protocols also have a number of security vulnerabilities. In addition, different components may require separate security infrastructure and configuration. This can lead to vulnerabilities since actions in different components are not bound together, and the deployment of security for features such as quality of service is often discouraged. These problems are discussed in more detail in Section II.

Ongoing work attempts to optimize and improve this situation through enhancements in different parts of the stack, such as network access authentication or mobility protocols. This follows a common research and engineering approach in networking where designers typically focus on a specific problem at a time.

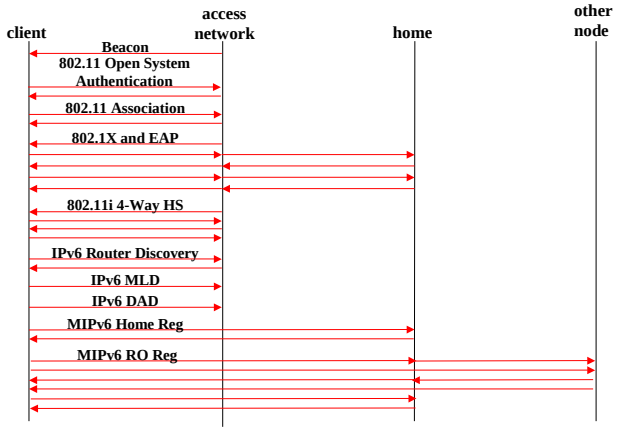

Fig. 1. IPv6 network attachment with existing protocols.

This paper presents a new architecture, Quick Network Access Protocol (or NAP for short), that deviates from current network attachment designs. Instead of focusing on a single layer (such as the link layer) or a single function (such as authentication), this paper analyses problem as a whole: What tasks are necessary in order to have a node attach to a network? How can that node move from one point of attachment to another? Which nodes need to communicate with what other nodes, and when? What is the best order of the tasks so that the number of roundtrips is minimized?

By taking this cross-layer viewpoint the number of roundtrips can be significantly reduced. In addition, the secure integration of new components such as mobility, firewalls, and quality of service signaling becomes possible, and these new facilities can be easily deployed. Sections III and IV describe our proposed architecture and protocol interaction in more detail.

Section V discusses the characteristics of NAP, Section VI discusses some other approaches for solving the same problems, and finally Section VII concludes the findings.

II. Problem Definition

Figure 1 shows an example network attachment message flow from a 802.11 wireless LAN and IPv6 scenario. This flow consists of access point discovery, link layer association, authentication, IP address assignment, router discovery, and mobility tasks. Put together there are 27 messages in the complete flow, along with several mandatory waiting periods (such as waiting up to a second before sending the first IPv6 Neighbor Discovery packet). Assuming that all functions (such as mobility) are needed, this count is still optimistic: in practice there are more messages and larger delays [3]. For instance, many EAP methods have a higher number of roundtrips than what is shown here.

Some of the factors that have led to the current design include sequencing without real causal link between messages, duplicated security at multiple layers, and assumptions that focused on wired networks. But the structure of the standards bodies that developed these protocols is also visible in the end result; no single group has felt responsible for the whole problem.

Current stacks also have security vulnerabilities. Simple examples of these vulnerabilities relate to individual problems within a single protocol. For instance, protocols such as 802.1X, EAP, 802.11, or 802.11i are not very resistant to denial-of-service attacks and are also not very good in providing identity privacy for the participants.

In addition, different components are typically expected to use independent security solutions. This can lead to vulnerabilities since actions in different components are not bound to each other. For instance, network access authentication mechanisms can ensure that a client talks to an authorized access point, and SEcure Neighbor Discovery (SEND) can ensure that the same client talks to an authorized router. However, even with SEND there is no guarantee that the router is authorized to act in this specific access network. In fact, clients will readily accept Router Advertisements from any SEND router as there is no binding between the access network and routers. This is problematic in shared media links such as 802.11. For instance, a compromised SEND router from anywhere in the world may claim to be a local router.

Another reason for binding multiple functions together relates to address ownership. For instance, opening pinholes in a NAT or a firewall, mobility protocol registrations, and quality of service reservations all need to prevent malicious registrations and modifications by outsiders. An ability to show the ownership of an address, such as the validity of your DHCP lease, would make it possible to secure these functions in a convenient manner.

A more serious problem is the expectation to deploy different security infrastructures for different functions of the stack. For economical reasons, it is often feasible to deploy only a single infrastructure and perform a single configuration effort for network access purposes. As a result, security may not be turned on or used even where protocol mechanisms and implementations already exist. For instance, DHCP authentication has been defined but not deployed [15], [14].

This problem affects not only the security of existing services such as DHCP, but also prevents the deployment of new functions. For instance, the FMIP mobility optimization assumes the existence of security associations to local routers [24]. One of the reasons why FMIP is currently not deployed is that configuring such security associations would be costly.

An attachment to a network consists of a transaction between the mobile node, access point, access router, access network, home network, possibly some mediating networks, and possibly also some mobility related nodes such as home agents. Some of these entities, such as access networks, can not be explicitly communicated with in current network architectures. Similarly, the communication mechanisms that are available between these parties are mostly focused on the initial attachment and may not be available during subsequent communications. Even during the initial attachment, current protocols typically achieve secure communications at the very end of the long flow. As a result, the capability of the protocol stack to securely exchange necessary information is limited.

III. The New Architecture

The architecture targets all activities needed for network attachments and movements. NAP operates either in an ad hoc network or uses a single security infrastructure for all of its activities. It also employs a number of techniques for reducing latency, and provides a highly secure operation through employing modern cryptographic protocol design, denial-of-service and privacy protection, and secure identification.

At the network level, the NAP architecture retains the current design where clients communicate with access nodes and with home networks through access nodes. But it introduces a new way to address and communicate securely with other devices in the network (such as DHCP servers or middleboxes). These communications can take place at any time, for handoff guidance or advice of charge purposes, for instance.

The NAP message flow combines link layer and network layer control functions within the same messages, though still enabling a separation between these layers and the devices responsible for them.

NAP operates in one of two security modes, either in the ad hoc or infrastructure modes. The protocols behave very similarly in these two modes, but authorization and payment for network access can occur only in the infrastructure mode. Nevertheless, even the ad hoc mode is capable of protecting on-link communications and signaling with middleboxes and other devices belonging to the access network. This protection is possible through the use of cryptographically generated identifiers at link and network layers. The involved devices are explicitly identified by a hash of their public keys. These hashes replace conventional MAC addresses, and serve as a convenient mechanism to bind the entities to their identities securely. This works well even in the ad hoc mode, even if the trustworthiness or authority of the device represented by its

identifier can not be guaranteed. This method can still provide opportunistic security, however. For instance, communications between a client and an access node are protected from outsiders, and handoffs to another interface of the same access node can be made securely. The public keys of the nodes can be generated by themselves and do not need any security infrastructure.

User identities and IP addresses are kept as they are in current systems. Similarly, the use of legacy credentials through protocols such as EAP [1] needs to be retained.

Once the network attachment and authorization is finished a number of further protocols may need to be executed, including stateless or stateful address configuration procedures, mobility management protocols, QoS signaling protocols, application layer signaling protocols (such as SIP), etc. NAP deals with these protocols in two ways. First, NAP creates keying material, parameters and authorization related information to efficiently secure other protocols. This is similar to what has been proposed in [29] for bootstrapping DHCP, in [35] for bootstrapping of MIPv6, and in [34] for bootstrapping in FMIPv6. Secondly, for performance, tasks can be delegated to the network devices, reducing expensive radio roundtrips. These tasks need not be related to the link layer processing only. For instance, the mobile node can request the access node to allocate an IP address or inform the mobile node's home agent about the currently used care-of address. The mobile node provides the basic information necessary to perform these tasks (such as interface identifier) and, depending on the task, signs a certificate to delegate the right for this specific task to the access node, making various delegated tasks possible (cf. [17]).

A protocol run illustrates the architecture:

1) The access node sends a beacon message, identifying itself with the hash of its public key. It can also send along a small amount of information affecting the attachment decision, such as what payment models it supports, what roaming partnerships it has, what subnets offering fast roaming are provided, etc.
2) The client and the access node initiate an attachment procedure. A Diffie-Hellman exchange is run as early as possible to protect all subsequent communications, including all management operations and negotiations. This also enhances the privacy of the subsequent communications against eavesdroppers on the wireless link. This procedure provides also secure negotiation of capabilities.

   In this phase, the client and the access node also authenticate opportunistically the claimed hash-based identities to ensure that the peer actually knows the private key corresponding to the public key used in the hash (similar to how HIP [28] operates). This can not demonstrate who the peer is, but ensures that it is the same entity all the time.
3) Within the above exchange, NAP also initiates a third party authentication and authorization exchange, if needed. Usually this involves the use of protocols such as EAP and RADIUS to authenticate the client to an existing AAA infrastructure. Note that unlike in some other proposals, it is not assumed that existing AAA can be replaced by new credentials such as a global PKI [17].

   NAP also allows web-based login pages. The use of such pages is explicitly negotiated. In contrast with the existing HTTP hijack approach, NAP makes the client aware of this login requirement, making it possible to use such a mechanism even when the primary application of the user is not web browsing (such as in Wireless LAN phones).
4) The client makes explicit requests for the services that it desires, the main service being IP network connectivity. However, there are typically also a number of other services where the client can depend on the access node. For instance, the client may request the access node to perform IP address allocation on its behalf or set up security associations in order to enable other services, such as opening pinholes in an NSIS-capable firewall [31]. Exactly which services are available depends on the deployed network architecture. Some possible services are discussed later.
5) The client and other nodes can communicate also after access has been granted. For instance, it would be possible to notify the user that his or hers pre-paid balance is running low without making a HTTP hijack necessary.

IV. The New Protocol

A. Basic Exchange

Figure 2 shows the NAP protocol exchange in a scenario that involves EAP, IPv6, SEND, and Mobile IPv6. The first part of the exchange involves the beacon and Diffie-Hellman messages. The beacon carries the hash identity of the access node and some information relating to the services it provides.

The second and third messages carry the Diffie-Hellman values necessary to agree on keying material. In addition, these messages are used to negotiate the security parameters that will be used subsequently. The two messages also carry the public keys associated with the peers' respective hash-based identities, and signatures that show that they possess the private keys associated with the identities.

From this point on, all messages are protected using keys established by Diffie-Hellman, and the parties know each other's hash-based identities.

The next four messages serve two purposes: they perform a third party-assisted authentication and authorization exchange as well as negotiating a set of services that the client gets from the access network.

The example shows a typical password- or shared secret exchange that consists of an identity message, challenge, response, and acknowledgement. Such exchanges are supported by commonly available protocols and infrastructure such as GSM SIM cards and authentication centers [7]. Exchanges involving a larger number of messages are also supported

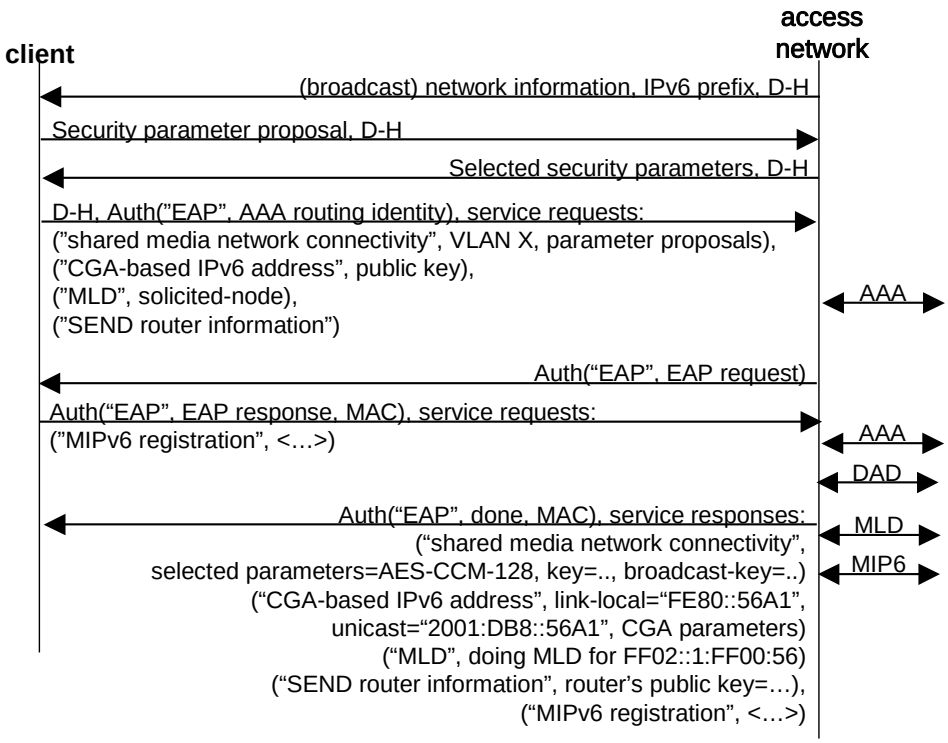

Fig. 2. NAP and IPv6 network attachment.

through the use of standard protocols such as RADIUS and EAP. However, NAP already supports natively some of the features (such as identity privacy) that have led to the development of these more complicated mechanisms.

Unlike traditional network access systems, NAP does not use keys provided in EAP as a basis for subsequent data traffic. However, NAP still needs to prove the possession of these keys in its two last messages in order to thwart man-in-the-middle binding attacks [9].

B. Advanced IPv6 Services

NAP messages carry a number of different information elements designed to ensure secure and efficient IP service. In our example, the Beacon message carries an IPv6 prefix. This helps a moving node to choose an access node that retains its current prefix instead of another access node that does not.

In the fourth message of the protocol, the mobile node requests a number of services from the access node. In the example these were

- Network connectivity over the wireless LAN (and possibly all the way up to a concentrator device).
- Address assignment, including related duplicate address detection (DAD) [30] and multicast listener discovery (MLD) [33]. The interface identifier associated with the mobile node is either chosen by the access node, or, where CGAs [10] are used, generated based on the information provided by the mobile node.
- Information about the SEND [8] router authorized to act in this particular network.
- Performing a Mobile IPv6 [22] home registration on behalf of the mobile node.

In general, these requests fall in three categories: those involving mere information, those involving the creation of security associations with other nodes within the access network, and those involving delegation of the mobile node’s tasks to the access node.

After mutual authentication has been performed, the access node performs the requests and sends information about the results to the mobile node. In the case of SEND, it is sufficient to send a hash of the public key of the authorized router.

In the simplest case address assignment results in an address. DHCP parameters can be necessary too, however, as DNS discovery and other services may depend on it. Also, if CGA-based addresses are used, the access node uses the mobile node’s public key together with its own public key and some other chosen parameters to create a multi-key CGA [23]. The access node’s public key and the other chosen parameters need to be returned to the mobile node.

Mobile IPv6 home registration is performed using a temporary delegation certificate signed by the mobile node, authorizing the access node to establish a suitable security association with the home agent in order to send a Binding Update. The certificate is supplied to the home network along with the authentication transaction. The certificate is considered

invalid until the home network has authenticated the client and authorized the network access for both the client and the access node. This is because this type of delegation involves real-world effects, in this case changing the current location registered at a home agent. Such effects can not be committed to prior to authenticating and authorizing the different parties. Similarly, the freshness of the delegation needs to be ensured by including information from the home network's challenge. Similar designs would also work for other mobility protocols such as HIP [19], but the details are omitted here.

NAP could even be extended to correspondent node registrations in the same manner. For instance, if the mobility protocol employs public keys, a delegation certificate can again be used. However, as discussed in [11], this may be insufficient case due to the lack of a trust or contractual relationship between the mobile and correspondent nodes. To prevent flooding attacks, the claimed care-of address may need to be validated either through assurances made by the access network or another return routability test (see [19]). The former requires a common trusted root for IP address range ownership among the correspondent node and the access network, however. Where such common trust exists, the return routability test can be avoided, making it possible to complete even the correspondent node registrations within the same 7 message NAP exchange.

C. IPv4 Web-Based Login with Firewalls

Another example is shown in Figure 3. It illustrates how NAP works with IPv4, web-based logins and firewalls. The protocol flow has similar structure than in the previous case, but instead of a 4-message handshake the access node requests the mobile node to authenticate through a web page. The URL for this web page is communicated explicitly in the protocol, and a restricted, secure channel is opened for IP access to the indicated server. The explicit indication is necessary in order for the mobile node to bring up a suitable application and alert the user, even if the user normally employs other applications or if the applications on the device are not under human control. This also allows the access network to notify the mobile node when, e.g., paid time is about to be over and a new payment is needed.

Once the authentication with the web server is completed, it becomes necessary for the access node to be told that it can grant access. This can be accomplished in several ways. One common approach is that the URL provided by the access node in message five contains a session identifier and access node's address so that the web server can contact the access node using a pre-configured security association. When the access node learns that the authentication has been completed, it informs the mobile node in message six. This approach is attractive, as it requires no changes to the web browser software in the mobile node. If such changes were possible, then other approaches, such as passing SAML assertions from the web server to the client would also be possible [25].

The second difference to the first example is that DHCP is employed. The access node determines that this network employs DHCP, uses DHCP to allocate an address, and returns this to the mobile node along with other information learned through DHCP. As the mobile node needs to renew its DHCP lease periodically, the access node provides a DHCP authentication key [15].

The addressing properties of the access network are advertised early, in the Beacon message in order to facilitate intelligent decisions about handovers in a manner similar to what was already described for IPv6. In the case of IPv4, it is necessary to advertise both the local and public subnet information, as this can be used to determine whether the local or global address of the mobile node would have to be changed, and whether a global address is available at all.

The example illustrates also how the system can work with firewalls, NATs, or other middleboxes within the access network. The mobile node may request information about a local middlebox and a security association to it. This allows the mobile node to control, for instance, Quality-of-Service settings or firewall pinholes using the NSIS protocol in a secure fashion.

It would also be possible to delegate some of these tasks to the access node in order to reduce the number of roundtrips needed after movements. But it remains to be explored how good tradeoff this is, as it also increases the complexity of the attachment protocol. This may be a viable approach when the access node itself is acting also as a middlebox.

V. Evaluation

This section evaluates NAP against existing designs and other proposed alternatives.

Perhaps the easiest part of the evaluation is looking at performance. The number of roundtrips needed depends on the assumptions, such as which IP version and services are being used. In the scenario that involves EAP, IPv6, SEND, and mobility, NAP completes in 7 messages, compared to the at least 22 messages needed for a similar scenario with the existing protocols. These 22 messages are: 802.11 Beacon, 802.11 Association Request and Response, 802.11 Authentication Request and Response, five 802.1X messages, four 802.11i 4-way handshake messages, IPv6 Router Solicitation and Advertisement, SEND Certificate Path Solicitation and Advertisement, MLD Listener Report, DAD Neighbor Solicitation, and Binding Update and Acknowledgement messages.

While the number of messages by itself is not necessarily a good comparison criterion, there is roughly equivalent difference in roundtrips needed and that roundtrips typically result in specific, radio- and network-dependent delays.

Furthermore, NAP has been constructed in a manner that makes it possible to avoid mandatory waiting periods. For instance, if the access node is the only entity offering this particular IPv6 prefix, it can implement DAD as an internal operation, based on previous transactions and messages from its other mobile nodes.

Another interesting aspect is security. Currently, there are in practice no deployed networks that would employ secure interaction with middleboxes. In NAP, however, securing such

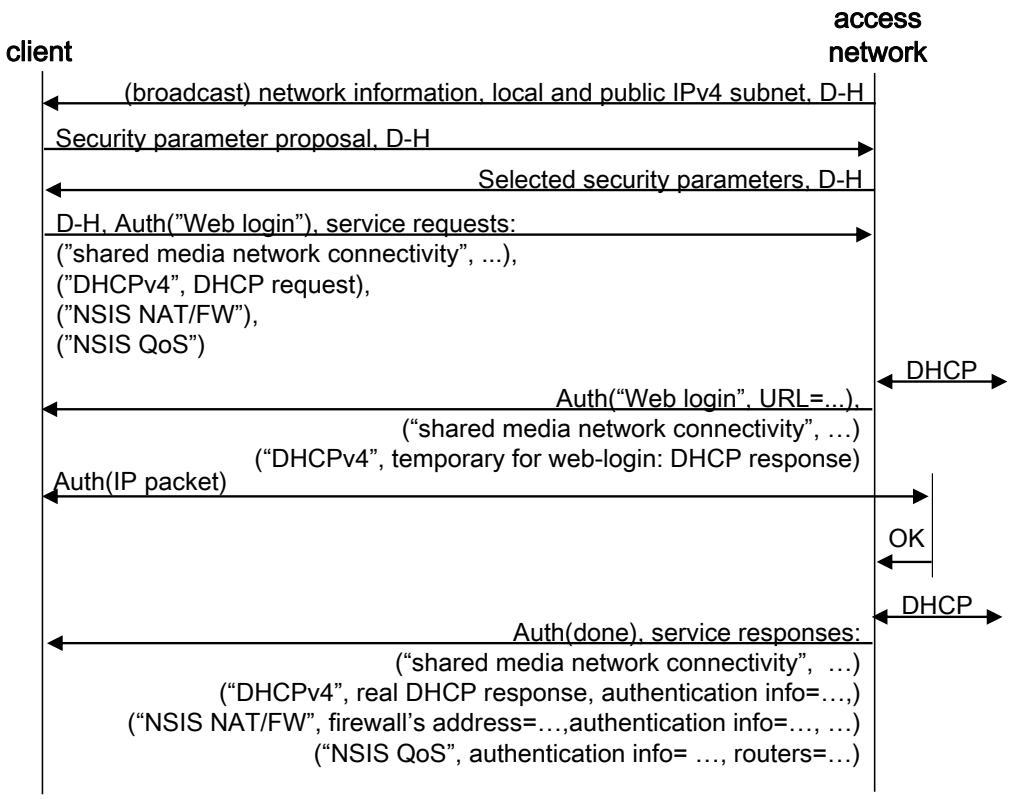

Fig. 3. NAP with IPv4 network attachment.

interactions comes without any additional configuration or deployment effort, as long as support for the new protocols exists in the affected devices. Similarly, NAP can provide secure bindings between independent security mechanisms such as network access and SEND.

NAP also provides a level of privacy protection in the form of turning on protection against passive eavesdroppers at a very early stage. NAP is also capable of operating in an opportunistically secure manner in ad hoc mode, something which is today almost exclusively run without any cryptographic protection.

The early Diffie-Hellman operation makes it possible for NAP to avoid some Denial-of-Service attacks for which other protocols are vulnerable, as subsequent communications are protected by the derived keys. The first three messages, however, are still vulnerable to other types of Denial-of-Service attacks. Adding a cookie- or puzzle-based additional layer of defense to NAP is possible, but cookie-based defenses are not very useful within a radio link, even if they have benefits in a multi-hop Internet environment. Puzzle-based defenses, on the other hand, result in a tradeoff between penalty for legitimate clients and attackers. Heterogeneous devices ranging from sensors and small personal devices to laptops have significantly different computational power. As a result, the ability to protect against laptop-class attackers would probably result in an unacceptable penalty for lower end devices. Adaptive puzzle designs would remain a possibility, however.

It could be argued that as NAP affects multiple layers, it does not provide as clean separation between the layers as the existing protocol stack does. However, NAP separates different tasks within the protocol to different information elements. Even if carried within the same exchange, the processing of these information elements can be implemented in a modular way, much in the same manner as existing stack architecture works.

Can NAP be deployed? It does not require changes to existing user credentials such as SIM cards; nor does it require changes to existing AAA infrastructure; it supports both credit-card based and AAA models; it even supports ad hoc mode. Its IP layer and middle box integration features are designed to be optional, allowing deployment before full support is available (albeit with performance impacts). Nevertheless, it does require a completely new protocol between the mobile nodes and access nodes. Some protocol changes in this interface are required in most other alternative designs as well [17]. In practice, NAP is unlikely to be applied over existing link layers, and is targeted towards new link layers that have a freedom to select a new design for their attachment signaling.

VI. Related Work

A number of attempts are currently being made to improve the performance, security and functionality of network access, particularly in a mobile environment. These attempts

include link-layer enhancements, parameter tuning [32], network selection mechanisms [2], lightweight network access authentication mechanisms with small number of roundtrips and few cryptographic computations (e.g., [12]), fast handover mechanisms [26], [4], and IP layer attachment improvements (such as DNA [21] and Optimistic DAD [27]). Various security improvements address issues, such as spoofing by access nodes [5].

We are aware of only a few previous attempts at looking to the network attachment problem as a whole. Eronen and Arkko analyzed general problems in the network access protocol set in [16]. Arkko et al. [6] was an early problem statement for network attachment and sketch of a solution. Tschofenig and Heikkinen looked into the possibility of employing HIP-like protocols in network attachment and the use of this to secure DHCP [18]. In IETF, the use of network access security for the protection of other services has been discussed for specific tasks such as Mobile IPv6 [35] or DHCP [29]. MobileMan [13] addresses general issues in cross-layer design for ad hoc networks, but does not address the specific problem of network attachments.

New network access control designs, such as those in new IEEE link layers have generally focused on the traditional network access part and have not addressed the security of other functions.

VII. Conclusions

A number of performance and security problems in existing network access stack have been presented. The new design, NAP, addresses these issues using a number of techniques. While some of these techniques are have also been used in other contexts, the approach of solving the whole network attachment problem in one architecturally consistent way is novel. Initial analysis shows that NAP is substantially better than the existing stack in terms of its performance, and solves also many existing security problems.

Further work is, however, required. Work remains in the design of interactions between the access node and the middleboxes. We are also in the process of implementing this approach on a test bed. Such a test bed would allow experimental testing of the impacts of this new design.

Acknowledgment

This document has been produced partially in the context of the Ambient Networks Project. The Ambient Networks Project is part of the European Community's Sixth Framework Program for research and is as such funded by the European Commission. All information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability in respect of this document, which is merely representing the authors view.

References

[1] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H. Extensible Authentication Protocol (EAP). RFC 3748, IETF, June 2004.

[2] Adrangi, F., Lortz, V., Bari, F., and Eronen, P. Identity selection hints for Extensible Authentication Protocol (EAP). RFC 4284, IETF, January 2006.

[3] Alimian, A. and Aboba, B. Analysis of Roaming Techniques. IEEE 802.11 WG, document 802.11-04/0377r1, 2004.

[4] Arbaugh, W. and Aboba, A. Handoff Extension to RADIUS. Internet Draft draft-irtf-aaaarch-handoff-04.txt (Work In Progress), IRTF, October 2003.

[5] Ohba, Y., Partsarathy, M., and Yanagiya, M. Channel Binding Mechanism based on Parameter Binding in Key Derivation. Internet draft draft-ohba-eap-channel-binding-00.txt (Work In Progress), IETF, January 2006.

[6] Arkko, J., Eronen, P., Nikander, P. and Torvinen, V. Secure and Efficient Network Access. Extended abstract presented in the DIMACS workshop, NJ, USA, November 2004.

[7] Haverinen, H. and Salowey, J. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM). RFC 4186, IETF, January 2006.

[8] Arkko, J., Kempf, J., Zill, B., and Nikander, P. SEcure Neighbor Discovery (SEND). RFC 3971, IETF, March 2005.

[9] Asokan, N., Niemi, V. and Nyberg, K. Man-in-the-middle in tunneled authentication. in http://eprint.iacr.org/2002/163/, 2002.

[10] Aura, T. Cryptographically Generated Addresses (CGA). RFC 3972, IETF, March 2005.

[11] Aura, T., Roe, M. and Arkko, J. Security of Internet Location Management. In Proc. 18th Annual Computer Security Applications Conference, pages 78-87, Las Vegas, NV USA, IEEE Press, December 2002.

[12] Clancy, T. and Arbaugh, W. EAP Password Authenticated Exchange Internet Draft draft-clancy-eap-pax-06.txt (Work In Progress), IETF, January 2006.

[13] Conti, M., Maselli, G., Turi, G., and Giordano, S. Cross-layering in mobile ad hoc network design. IEEE Computer, Volume 37, Issue 2, February 2004.

[14] Droms, R. DHCP Security, presentation in the ICOS BoF at IETF-63, IETF, March 2005.

[15] Droms, R. and Arbaugh, W. Authentication for DHCP Messages. RFC 3118, IETF, June 2001.

[16] Eronen, P. and Arkko, J. Role of Authorization in Wireless Network Security. Extended abstract presented in the DIMACS workshop, NJ, USA, November 2004.

[17] Faria, D. and Cheriton, D. DoS and Authentication in Wireless Public Access Networks. ACM Workshop on Wireless Security, 2002.

[18] Heikkinen, S. Tschofenig, H., and Gelbord, B. Network Attachment and Address configuration using HIP Position paper in the Workshop on HIP and Related Architectures, Washington, DC, November 2004.

[19] Henderson, T. End-Host Mobility and Multi-Homing with Host Identity Protocol. Internet Draft draft-ietf-hip-mm-03.txt (Work In Progress), IETF, February 2006.

[20] Kaufman, C. (Ed.) Internet Key Exchange (IKEv2) Protocol. RFC 4306, IETF, December 2005.

[21] Kempf, J., Narayanan, S., Nordmark, E., Pentland, B., and Choi, JH. Detecting Network Attachment in IPv6 Networks (DNAv6). Internet Draft draft-ietf-dna-protocol-00.txt (Work In Progress), IETF, January 2006.

[22] Johnson, D., Perkins, C., and Arkko J. Mobility Support in IPv6. RFC 3775, IETF, June 2004.

[23] Kempf, J. and Gentry, C. Secure IPv6 Address Proxying using Multi-Key Cryptographically Generated Addresses (MCGAs) Internet Draft draft-kempf-mobopts-ringsig-ndproxy-02.txt (Work In Progress), IETF, August 2005.

[24] Koodli, R., Ed. Fast Handovers for Mobile IPv6. RFC 4068, IETF, July 2005.

[25] Maler, E. and J. Hughes. Technical Overview of the OASIS Security Assertion Markup Language (SAML) V1.1. SSTC Working Draft Version 01, SSTC, March 2004.

[26] Mishra, A., Shin, M., Arbaugh, W., Lee, I. and Jang, K. Proactive Key Distribution to support fast and secure roaming. IEEE 802.11 submission IEEE-03-084r1-I, January 2003.

[27] Moore, N. Optimistic Duplicate Address Detection for IPv6. Internet Draft draft-ietf-ipv6-optimistic-dad-07.txt (Work In Progress), IETF, December 2005.
[28] Moskowitz, R., Nikander, P., Jokela, P. and Henderson, T. Host Identity Protocol. Internet Draft draft-ietf-hip-base-05.txt (Work In Progress), IETF, March 2006.
[29] Patel, A. (Ed.) Bootstrapping RFC3118 Delayed DHCP Authentication Using EAP-based Network Access Authentication. Internet Draft draft-yegin-eap-boot-rfc3118-01.txt (Work In Progress), IETF, January 2005.
[30] Thomson, S. and Narten, T. IPv6 Stateless Address Autoconfiguration. RFC 2462. IETF, December 1998.
[31] Tschofenig, H. and Sankhla V. Bootstrapping Kerberos. Internet Draft draft-tschofenig-pana-bootstrap-kerberos-00.txt (Work In Progress), IETF, July 2004.
[32] Velayos, H. and Karlsson, G. Techniques to Reduce IEEE 802.11b MAC Layer Handover Time. Laboratory for Communication Networks, KTH, Royal Institute of Technology, Stockholm, Sweden, TRITA-IMIT-LCN R 03:02, April 2003.
[33] Vida, R. and Costa, L. Multicast Listener Discovery Version 2 (MLDv2) for IPv6. RFC 3810, IETF, June 2004.
[34] Narayanan, V., Venkitaraman, N., Tschofenig, H., Giaretta, G., and Bournelle, J. Handover Keys Using AAA. Internet Draft draft-vidya-mipshop-handover-keys-aaa-01.txt (Work In Progress), IETF, October 2005.
[35] Patel, A. and Giaretta, G. Problem statement for bootstrapping Mobile IPv6. Internet Draft draft-ietf-mip6-bootstrap-ps-04.txt (Work In Progress), IETF, January 2006.