Providing Authentication and Access Control in Vehicular Network Environment

Hasnaa Moustafa[1], Gilles Bourdon[1], and Yvon Gourhant[2]

France Telecom R&D
38-40 rue de General Leclerc, 92794 Issy Les Moulineaux, France[1]
2 avenue Pierre Marzin, F-22307 Lannion, France[2]
{hassnaa.moustafa, gilles.bourdon, yvon.gourhant}@francetelecom.com

Abstract In this paper we make use of the recent advances in 802.11 technologies and the new perspectives for ad hoc networks to provide a novel architecture for Inter-Vehicular communication on highways. This architecture provides authentication and access control for mobile clients on highways and ensures network transparency to mobile clients in their vehicles. We propose an integrated solution considering the service provider as the core entity for all authentication and access control operations. We develop an AAA (Authentication, Authorization, and Accounting) mechanism to authenticate mobile clients with respect to service providers authorizing them to services' access, and ensuring a confidential data transfer between each communicating parties. Our mechanism adapts 802.11i standard to the vehicular environment setting up secure links, in layer 2, that guarantee confidential data transfer. To achieve a reliable transfer, we propose a routing approach based on the Optimized Link State Routing (OLSR) protocol that is expected to provide a reliable routing infrastructure in such a hybrid scalable wireless environment. Also, we present a simple and appropriate scheme for assigning IP addresses to mobile clients. Finally, we give a brief analysis and discuss the advantages and limitations of the proposed architecture.

1 Introduction

Due to the great advances in wireless technologies over the last years, ad hoc networks are reaching a stage where they can support the mixing of different services in order to provide an infrastructure useful for the mobile users. The 62nd IETF meeting described three scenarios for these networks: ad hoc networks as standalone networks that are not connected to any external network, ad hoc networks at the edge of an infrastructure network, which are standalone networks connected to the Internet via one or more Internet gateways, and ad hoc networks as intermittent networks that may be standalone for most of the time but temporarily connected to an infrastructure network e.g. mobile users in cars or trains.

Currently, Inter-Vehicle Communication Systems (IVCS) are attracting considerable attention from the research community as well as the automotive industry [1]. The new ad hoc networks trend and the recent advances in wireless technology, allow several possible vehicular network architectures. Three alternatives

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

include [2]: a pure wireless vehicle-to-vehicle ad hoc network (V2V), a wired backbone with wireless last hops, or a hybrid architecture using V2V communications that does not rely on a fixed infrastructure, but can exploit it for improving performance and functionality when it is available.

An important research and development aspect in vehicular networks concerns the usage of standardized transmission systems like 802.11 in ad hoc mode, the development of protocols and security mechanisms for trusted ad hoc communications, with geographical addressing and reliable routing. Several ad hoc network functionalities and integration strategies are required for services' delivery to users in vehicular networks. Essential features like information routing, security, authentication, authorization and charging should be considered. The routing of information should be reliable and scalable, minimising resources' consumption and delay. The security mechanisms must guarantee that only authorized users can access the ad hoc network resources and services offered by the provider. Also, eavesdropping as well as modification of the transmitted data must be prevented.

In this paper, we propose a novel architecture intended for vehicular networks on highways and present some potential services that aim at assisting drivers as well as passengers. An authentication, authorization and accounting (AAA) scheme is developed for convenient and secure communication between mobile users, authorizing only subscribed users to access the services offered by the provider. Our proposed architecture introduces the concept of ad hoc networking for mobile users' communication. In this context, we propose an approach that adapts Optimized Link State Routing (OLSR) protocol [3] to the vehicular environment aiming to provide reliable data transfer. Also, we give a preliminary solution for the lack of IP addressing within the vehicular environment. The remainder of this paper is organized as follows. Section 2 reviews the relevant literature and contributions, highlighting the motivation to our architecture. The proposed architecture is described in Section 3. In Section 4, we give a brief analysis. Finally, we conclude the paper with Section 5.

2 Literature Review and Related Contributions

Significant parts of the research work in vehicular communication have been supported by the German federal Ministry of Education and Research (BMBF) within the *FleetNet-Internet on the road* project [4] and the *Network on Wheels: NoW* project [5]. The basic goal of these projects is to develop a platform for inter-vehicle and vehicle-to-roadside communication allowing Internet access, based on wireless multi-hop communication. In fact, a close cooperation between the European Car-2-Car Communication Consortium (C2C CC) [6] and the NoW project is being established in order to promote the project results towards European standardization. The *InternetCar* project [7] in Japan is working to develop and deploy a system that provides the Internet connectivity to automobiles, and the EU DAIDALOS project [8] addresses the main aspects of integrating heterogeneous networks technologies including ad hoc networks.

Several approaches employ broadcast to provide intelligent transportation system (ITS) services in vehicular environments, including traffic monitoring, congestion

avoidance and safety messages' transfer. A driver assistant is proposed in [9] exploiting upstream traffic information with the assumption that traffic information is sensed by each individual vehicle and analyzed with other vehicles information, and then it is broadcasted. A location-based broadcast communication protocol is proposed in [10], using the information concerning nearby vehicles, aiming to provide highway safety message transfer. Also, a safety-oriented model is designed in [11] based on the concept of ad hoc peer-to-peer (P2P) networking to support the exchange of safety-related data on highways. As an alternative to broadcast dependent approaches, a mobility-centric data dissemination algorithm intended for vehicular networks is presented in [2] exploiting the broadcast nature of wireless transmission but combining opportunistic and geographical forwarding, and a new efficient IEEE 802.11 based multihop broadcast protocol is proposed in [12] that is designed to address the broadcast storm and reliability problems.

In the context of hybrid ad hoc networks applications, ad hoc networks integration in vehicular communication is highly expected. Thus, some ad hoc routing propositions are suggested as solutions for data dissemination on highways. The approach presented in [13] multicast messages among highly mobile hosts in ad hoc networks, with the assumption that the source is stationary and the receivers move at high speeds, mostly towards the source. An extension to this approach is proposed in [14], which considers source and receivers sets that change dynamically based on the content of the transmitted information and the mobility of the receivers and the source. This model introduces sensors to generate the required information, and then pass it to a central node in each region.

From our investigation to the relevant contributions, we noticed that they mostly tackle the problem from an application view and are assumption based. Several propositions focus on providing ITS services in vehicular environment that is especially useful on highways. These propositions provide solutions in terms of message dissemination among mobile clients that are mostly broadcast dependent, and ad hoc routing has emerged as one of the solutions to provide safety and/or traffic situation messages' transfer. Recently, Internet connectivity becomes one of the target services due to the great advances in 802.11 technologies. This approach is highly promoted by many large projects working towards providing Internet connectivity to mobile users in their vehicles, which led to the emergence of new design trends by automotive industry for future cars. In this paper, we focus on vehicular communication on highways addressing one of the promising applications of hybrid ad hoc networks. We follow a realistic approach, considering the benefit of both mobile clients on highways and service providers. We propose a novel architecture providing an integrated solution that achieves: services provision ranging from ITS to Internet connectivity, constructing a virtual infrastructure for vehicular communication, mobile clients' authentication, confidentiality in data transfer and reliability in routing the information.

3 The Proposed Architecture

We start by defining the services offered by the service provider, and then we propose an appropriate architecture design considering vehicular-to- vehicular and vehicular-

to-road communication in order to achieve the offered services. We develop an AAA scheme based on 802.11i [15] for authenticating mobile clients with respect to the service provider at the entry points of highways , authorizing them to access the offered services according to their subscription. This scheme also assures the confidentiality and the integrity in data transfer between each two parties. For information routing, we benefit from the ad hoc networks that are randomly constructed between mobile clients, proposing an approach that adapts OLSR to the vehicular communication environment as well as a suitable and simple mechanism to provide mobile clients with the required IP addresses achieving appropriate routing.

3.1 Architecture Design Overview

The general objective of this architecture is to support communication and data transfer between mobile clients (moving vehicles) as well as mobile clients' access to some offered services on highways. These services include (vehicular network access enabling inter-vehicles communication and data transfer, safety and traffic condition messages' transfer, speed limit reminder messages, and mobile clients' Internet access) and they are provided by the network operator, the ISP (Internet Service Provider) or the WISP (Wireless Internet Service Provider). We propose two possible business models that are discussed in Section 3.2. The proposed architecture is not limited to these defined services and is quite general to support services' extension. It combines a fixed network infrastructure and a virtual infrastructure constituted by mobile ad hoc networks comprising three core entities as shown in Figure 1: a) Access network, which is the fixed network infrastructure and forms the back-end of the architecture. b) Wireless mobile ad hoc networks, constructed by the moving vehicles and form the architecture front-end. c) 802.11 WLAN infrastructure in the form of access points (APs), providing a limited wireless infrastructure and is connected to the backbone access network infrastructure, and thus forming the interface between the architecture front and back ends. These APs are installed on highways entry points and are scattered at gas stations and rest houses areas along the highways.

The APs have three important roles: they are considered as Area Border Routers (ABRs) for mobile clients, linking them to the access network. They play a role in routing the information among mobile clients and constructing the virtual routing infrastructure, this is discussed in Section 3.4. Furthermore, they play an important role in authenticating mobile clients at the entry points at the beginning; this is detailed in Section 3.3. Ad hoc network chains are constructed among mobile clients; these chains may be separated or temporally linked. We define an ad hoc network chain as a group of geographical dynamic clusters, continuously reconfiguring among mobile nodes. Each cluster is composed of mobile nodes having the same proximity, the same movement direction, and the same average speed. We assume that there is a fixed cluster that always exists in the coverage area of each AP, which can be considered as a geographical virtual cluster.

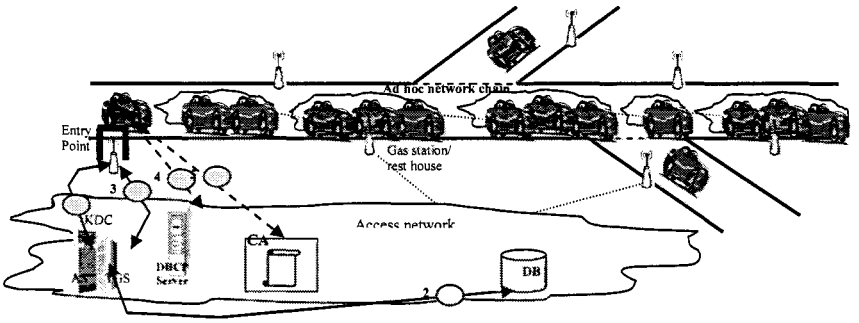

Fig. 1. Architecture design.

3.2 Business Model

We assume two possible business models, each of which is associated to the clients' Internet subscription or telephone subscription (fix or mobile telephone): *pure package* (pay before use), where the billing is monthly fixed whether the client will use the services or not. *On-use package* (use before pay) in which the billing is associated to the network access authorization (discussed in Section 3.3), which is obtained at the entry points of highways.

3.3 The Authentication, Authorization, and Accounting (AAA) Mechanism

We propose a solution that uses the mobile users' service providers as the core entity for all AAA processes [16], adapting the 802.11i standard to ad hoc networking environment. This allows each two communicating parties to properly authenticate and encrypt the data transfer between themselves. To provide a stronger encryption mechanism, we assume that 802.11i employs the Advanced Encryption Standard (AES) promoted by the WPA2 [17] for 802.11 devices. The Business model in Section 3.2, discusses the mobile clients billing process. The developed authentication and authorization processes are presented in this section. In our approach, we treat three issues: a) client/service provider mutual authentication at the entry point, b) client/client authentication and secure communication, c) AP/client authentication and secure data transfer. A successful client/service provider mutual authentication authorizes each client to access the required services during his voyage. The client/client and AP/client mutual authentication are carried out between each two nodes sharing the same proximity, which are authenticated and authorized by the service provider at the entry point. This allows links to be setup in layer 2 among authenticated and authorized nodes. Although 802.11i considers the RADIUS server as the default authentication server (AS) employing it in conjunction with Extensible Authentication Protocol (EAP) [18], RADIUS does not outfit our previously discussed issues as it does not provide authorization for special services but rather provides authorization for channel access. Accordingly, we apply a Kerberos

authentication model [19] authenticating clients at the entry point and authorizing them to services' access.

In Kerberos model, every service requires some credentials for the client in the form of a ticket. There are two types of tickets: *Ticket Granting Ticket* (TGT) and *Ticket Granting Service* (TGS). The TGT allows the client to obtain service tickets (TGSs), while the TGS is the ticket that grants the clients the services' access. So the client must first obtain a TGT, then requests a TGS for each service that he needs. A Kerberos server contains a Key Distribution Center (KDC), which encompasses two parts: an authentication service part that plays the role of an AS and grants the TGT after each successful authentication, and a TGS part for granting TGS tickets for each authenticated client having a valid TGT. To apply Kerberos authentication model in our architecture, each client at the entry point authenticates via the AS in the Kerberos KDC and obtains a TGT. The TGT indicates mutual authentication between the client and the service provider. Then, the client uses the obtained TGT to request a TGS for each service he needs. We assume that two services are requested at the entry point: 1) a network access service, by which each authenticated client is assigned an IP address. 2) a public key certificate service, by which each authenticated client obtains a certificate that he uses later for authentication and secure communication with other clients.

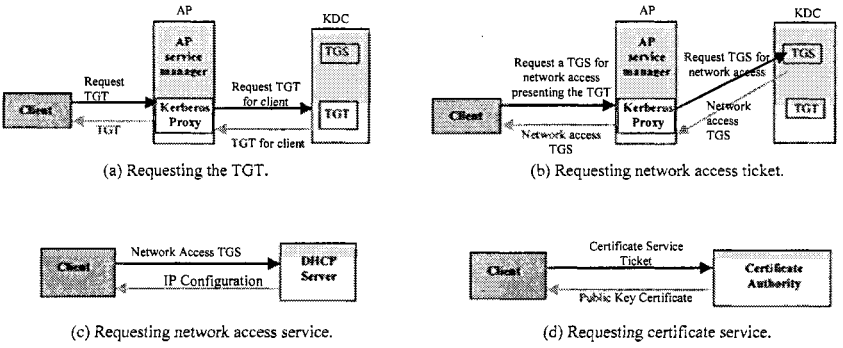

Fig. 2. Kerberos authentication model.

Figure 2, describes the message flow for applying the Kerberos model. Since 802.11i requires the client to initially authenticate to an AP in order to gain access to the network, via employing IEEE/802.1x, we introduce the notion of Kerberos proxy [20]. The AP at the entry point is a Kerberos proxy and at the same time plays the role of the authenticator that authenticates each client after consulting the Kerberos AS. Then, it provides the client with network access through TGS grants. Figure 2(a) shows the process of client's authentication, obtaining the TGT from the AS. In Figure 2(b), the client presents the TGT and requests a TGS for network access (any other service can be requested). Figure 2(c), shows the client IP configuration through communicating a DHCP server and presenting the network access TGS (the process of IP configuration is detailed in Section 3.5). In Figure 2(d), the client obtains the public key certificate, presenting the corresponding TGS that is assumed to be obtained in a similar way to Figure 2(b). Figure 3, illustrates the authentication

messages' exchange, where we employ EAP-Kerberos [20, 21] since the AS is not directly accessible to the client. The client exchanges the authentication messages with the AP (Kerberos proxy) using EAP, and the AP consults the AS through a Kerberos request to authenticate the client. Then the AP sends a TGS request to the TGS center, granting the client the requested services' tickets. To this end, mutual authentication with the service provider and services' authorization are achieved for each client. As no actual data transfer takes place at this phase, we are restricted to mutual authentication and services' authorization and do not involve the 802.11i encryption key generation phase. As seen in Figure 3, the AS generates a session key after obtaining a password proof for the client. This session key is contained in the TGT and is received by both the client and the AP, providing also mutual authentication between them. Then, each client is granted a network access and a public key certificate TGSs, through which he respectively obtains an IP configuration and a certificate that, is used afterwards for setting up links in layer 2 with other vehicles during the voyage. EAPoL protocol (EAP over LAN), which is defined as a part of the 802.1X specification, runs between the client and the authenticator encapsulating EAP-Kerberos. The corresponding messages exchange is shown in Figure 3.

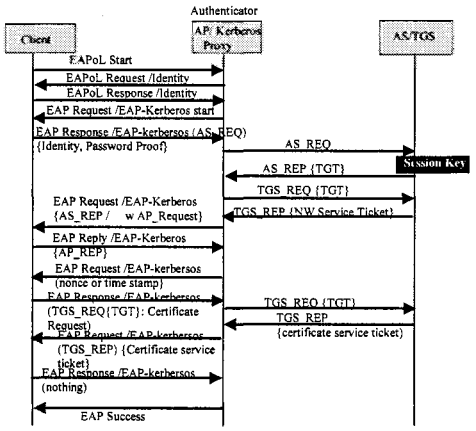

Fig. 3. EAP-Kerberos messages exchange.

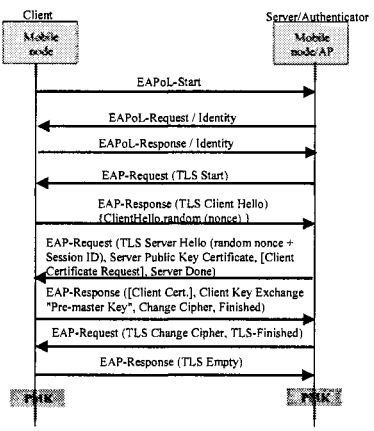

Fig. 4. EAP-TLS messages exchange.

The second step is to setup secure links in layer 2 between each two communicating parties that are authenticated. In this case, we employ 802.11i in an ad hoc mode, without introducing an AS. Authentication is completely carried out by each two communicating nodes, making use of the previously obtained certificates. Firstly, we employ EAP-TLS [22] between each nodes pair that fall in the same proximity, and wants to communicate. A *public key client-server* approach is used, where each authenticating pair acts as a client-server pair using the obtained certificates at the initial Kerberos authentication and service-granting phase. This saves the overhead of certificates' generation during authentication. We assume that the client does not send the TLS *certificate verification* signal as it has already a certificate signed by the CA. Figure 4, illustrates the corresponding messages' exchange. The client generates a pre-master key, when it receives the server

certificate. This is in the form of a 48 bytes random number encrypted with the server public key, then decrypted by the server using the server private key. The client and server use a *Hash {Pre-master key, Server nonce, Client nonce}* to generate a Pairwise Master Key (PMK), providing mutual authentication between the client-server pair. We assume that TLS session resumption [23] may take place if each client is capable of storing a copy of the PMK, thus minimizing layer 2 delays with clients' mobility. Secondly, to obtain an increased security on each authenticated link, we introduce the 802.11i encryption phase via employing the 4-way Handshake between the client and the server. In this case EAPoL-Key messages are used in the messages' exchange, which are intended to allow secret key information exchange. Firstly, PMK is used to generate a Pairwise Temporal Key (PTK) for encrypting unicast data transfer on the link. Then, a Group Temporal Key (GTK) is generated for encrypting broadcast and multicast data transfer on the link. Thereby, all upcoming data transfer on the authenticated link will be encrypted using the generated keys ensuring communication privacy and secure data transfer. We follow the WPA2 proposed key exchange message [24], reducing latency and overhead.

3.4 Routing

To provide appropriate routing infrastructure among the authenticated links in layer 2, an appropriate ad hoc routing protocol is required to be employed at layer 3. We tend to apply a proactive routing approach to ensure the continuous existence of a routing infrastructure among vehicles, proposing a solution that remediates the proactive approach overhead. This solution uses the OLSR protocol and adapts it to the vehicular environment. OLSR protocol is chosen as it is a proactive protocol that minimizes the control packets flooding and is suitable for large and dense networks when communicating over a large subset of nodes. Moreover, OLSR auxiliary functions support communication with external networks. This is useful in providing Internet connectivity service in our architecture.

Adapting OLSR to the Proposed Architecture: we extend OLSR to include the notion of *Local Scope (LS)*. We define the LS as the logical subnet constructed among each group of nodes sharing the same geographical area. Each LS is dynamic and continuously re-configurable. The former is due to the nodes' mobility changing their geographical area, and the latter is due to the nodes membership change (joining or leaving different LSs) according to their connectivity. An Ad hoc chain is formed by a group of connected LSs that may be temporally linked to an AP through one LS of the chain. The whole vehicle-vehicle network is the collection of ad hoc chains that may be temporally connected or separated. The classical OLSR protocol executes in each LS "*Intra LS routing*", where each LS member node stores in its routing table routes to all possible destinations in its LS. While routing between different LSs "*Inter LS routing*" takes place through *gateway nodes*, which we define as the border nodes at each LS.

LS Construction and Intra LS Routing: each LS is constructed by a *root node* that may be fix or mobile (AP or client), using the ad hoc IP flooding protocol presented in [25]. A new multicast group is specified for flooding, given the name "ALL_IPv4_MANET_NODES". Each root node floods an *LS-construct* packet with a multicast address associated to the group, and a pre-defined maximum hop count

(*TTL*) to limit the flooding radius to the local geographical scope. The maximum hop value is selected in terms of the desired LS size and the density of vehicles on highways. The *LS-construct* packet has a unique identifier (*LS-ID*), identifying the LS that is being constructed. Each node receiving the packet, if it is not already a member in other LS, stores a copy of the *LS-ID* and becomes an LS member. The reception redundancy is detected and each node receives each flooded packet only once. This phase takes place in a periodic manner for continuous LS construction and maintenance, allowing *LS-ID* soft state storage at each LS member. A node elects it self as a root node following the *first declaration win* (FDW) rule, used in passive clustering construction in ad hoc networks [26], where the node that sends the *LS-construct* packet first becomes the root node. We add the condition that this node should be granted the network access at the entry point and it does not receive any *LS-construct* packets for a timeout period. Using the LS mechanism, OLSR provides routing within a limited geographical scope. All transmitted OLSR packets by each node carry the corresponding *LS-ID* as well as the node's type (gateway, non gateway), and are only received by the same LS member nodes. This introduces fewer overheads in transmission size and routing tables' storage and maintenance, allowing scalability of the protocol's operation among numerous nodes that may constitute the vehicular network.

Inter LS Routing: *gateway nodes* in each LS are last nodes receiving the *LS-construct* packet during the LS construction. They are nodes that have neighbors in its range belonging to different LSs, we call these neighbors *Inter LS neighbors*. Gateway nodes are responsible for Inter LS routing through proactively maintaining routing paths, in their routing tables, to their one hop Inter LS neighbors. A root node having only Inter neighbors in its one hop neighbor table understands that it is separated from its LS and accepts the first *LS-Construct* packet coming from another root node. Thus it joins the announced LS.

Data Structures: a new record (*node-info*) is created at each node, storing the node's type (gateway, no gateway) with respect to its LS as well as the *LS-ID*. Otherwise, no additional data structure is needed compared to OLSR as we assume that each node announces its type in all transmitted control packets during the Intra LS routing. Thus, all member nodes of each LS are aware of their gateway nodes and store the type of each destination in their routing tables. Section 4, gives the required implementation consideration.

Data Transfer: we distinguish between two types of data transfer: regular transfer, including inter-vehicles communication for routing data between defined pair(s) as well as Internet access. And emergency transfer, including safety and traffic condition messages' dissemination. In regular transfer, the adapted-OLSR routing protocol proceeds employing classical OLSR for Intra LS routing and using gateway nodes for Inter LS routing. A node that does not find a route for the destination in its Intra LS routing table, transfers the data packet to its gateway nodes that forward it to their Inter LS neighbors, until the destination is localized. We assume that reception redundancy is detected and discarded. In emergency transfer, data is locally disseminated within the LS. In this case, routing switches to flooding to the previously defined multicast group, following the same approach of *LS-construct* packet propagation. If dissemination extension (including more than LS) is desired, gateway nodes are employed to forward the packets to their Inter LS neighbors.

Connection to Access Network: We assume that APs are equipped with multiple interfaces, including non OLSR interfaces connected to the access network. Each AP is then charged with injecting routing information of this external network to the OLSR VANET nodes, via employing the OLSR *Host and Network Association (HNA)* message. The HNA messages periodically inject external networks information to ad hoc network nodes, including the external network address and the net mask. We thus assume that each AP along the highway periodically diffuses this message in its virtual fixed cluster. Each mobile vehicle falling in this cluster (i.e. member nodes of a given LS that fall in this cluster) will receive this diffused access network information and creates/updates its association set repository with the recent access network information as well as the corresponding AP. Consequently, each node requesting an Internet connectivity service utilizes this stored information.

3.5 IP Addressing

Mobile clients construct dynamic ad hoc network chains during their continuous movements, at the same time the problem of IP address configuration is not yet resolved in such a dynamic environment devoid of any fixed infrastructure or centralized administration. As a simple solution, we make use of the existing infrastructure at the entry points of highways in order to provide each mobile client with an IP configuration. Our solution is based on using a Dynamic Host Configuration Protocol (DHCP) server with IPv4, considering the following assumptions: a) after the authentication of each mobile client (obtaining TGT ticket), it requests a network access TGS. b) a DHCP server exists at the entry point of each highway, using the dynamic allocation mechanism [27], where each client having a network access TGS can directly communicate with the DHCP server and achieve the IP configuration service. c) each address assigned by the DHCP server to the client has a fixed *lease* decided by the server, and the client is not allowed to require *lease* extension. d) IP address release is carried out by the server, when an IP address *lease* is expired the server gets back the IP address and reallocates it to another client. Thus, *DHCPRELEASE* message is not used. Although this proposed scheme provides a simple solution, it partially solves the clients' IP configuration problem as it limits the size of services' access (this is discussed in Section 5).

4 Brief Analysis

In our AAA scheme, Kerberos authentication combines authentication and services' authorization embedding clients' credentials in tickets. We succeed in authenticating clients through contacting the AS only once, minimizing the load on the AS and reducing the delay imposed by layer 2. Applying 802.11i in ad hoc mode ensures continuous authentication for communication parties and secure links setup. This employs EAP-TLS, avoiding the shared secret weakness of the PSK authentication proposed by the standard for ad hoc mode. Moreover, TLS session resumption possibility allows a fast roam back between authenticated clients and reduces disconnection latency. In our routing approach, introducing local scopes is expected

to reduce routing overhead caused by high nodal density while involving only one extra control packet. OLSR support for sleep mode and external networks helps respectively in saving equipments' batteries and providing a partial solution for Internet connectivity.

5 Conclusion and Limitations

In this paper we propose a new architecture for vehicular communication and diverse services' access on highways, integrating ad hoc networking with 802.11 technologies. Our architecture is extensible to any services, it does not require any changes in the 802.11i standard, and it does not involve new wireless technologies develop a novel AAA mechanism independent of layer 3 routing protocol and particularly suitable for vehicular environment. To the best of our knowledge, ours is among the primary schemes integrating 802.11i security in an ad hoc environment and introducing Kerberos model and EAP-Kerberos in 802.11i WLAN environment. We make use of the ad hoc networks construction among mobile clients to achieve reliable information dissemination, via proposing a mechanism that adapts OLSR to the scalable vehicular environment. This scheme benefits from OLSR proactive approach in the sense of providing continuous routing infrastructure while proposing a remedy for its limited scalability due to the continuous propagation of routing messages among all nodes. For realistic routing environment, we present a simple IP configuration scheme based on DHCP and IPv4. The limitation of this architecture is the lack of continuous Internet connectivity among mobile clients as they change their IP domain. Also, this architecture does not support IPv6. A next step is to integrate micro/macro mobility management along the vehicular network and between vehicular networks in different highway branches. We also intend to provide an IPv6 support, based on the existing OLSR IPv6 solutions.

6 References

1. Hartenstein H. et al.: Position-Aware Ad Hoc Wireless Networks for Inter-vehicle Communications: The Fleetnet Project, ACM symposium on Mobile Ad Hoc Networking and Computing, MobiHoc, 2001
2. Wu J. et al.: MDDV: A Mobility-Centric Data Dissemination Algorithm for Vehicular Networks, first ACM VANET Workshop, Philadelphia, PA, USA, 2004
3. Clausen T. and Jacquet P.: Optimized Link State Routing Protocol (OLSR), RFC 3626, October 2003.
4. The FleetNet Project http://www.Fleetnet.de/
5. The Network on Wheels Project http://www.informatik.unimannheim.de/pi4/lib/projects/NoW
6. The Car 2 Car Communication Consortium http://www.car-2-car.org
7. The InternetCAR Project http://www.sfc.wide.ad.jp/InternetCAR/
8. The EU Project DAIDALOS http://www.ist-daidalos.org
9. Wischhof L. et al.: Adaptive Broadcast for Travel and Traffic Information Distribution Based on Inter-Vehicle Communication, IEEE IV'2003, 2003
10. Xu Q. et al.: Design and Analysis of Highway Safety Communication Protocol in 5.9 GHz Dedicated Short Range Communication Spectrum, IEEE VTC'03, 2003

11. Chisalita I. and Shahmehri N.: A Peer-to-Peer Approach to Vehicular Communication for the Support of Traffic Safety Applications, 5th IEEE Intelligent Transportation System Conference (ITS), 2002
12. Korkmaz G. et al.: Urban Multi-Hop Broadcast Protocol for Inter-Vehicle Communication Systems, first ACM VANET Workshop, Philadelphia, PA, USA, 2004
13. Briesemeister L., and Homel G.: Role-Based Multicast in Highly Mobile but Sparsely Connected Ad Hoc Networks, in IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), 2000
14. Zhou H. and Singh S.: Content based multicast (CBM) in ad hoc networks, in IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC), 2000
15. IEEE Std. 802.11i: Medium Access Control Security Enhancements July 2004
16. Moustafa H., Bourdon G., Gourhant Y.: AAA in vehicular communication on highways with ad hoc networking support: a proposed architecture, proceeding of the VANET ACM workshop in conjunction with MobiCom 2005, Germany, September 2005
17. WiFi Alliance http://www.wi-fi.org/OpenSection/protected_access.asp
18. Aboba B. and Calhoun P., RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication protocol (EAP), RFC 3579, September 2003
19. Kohl J. and Neuman B. C.: The Kerberos Network Authentication Service (Version 5), RFC 1510, September 1993
20. Trostle J. et al.: Initial and Pass Through Authentication Using Kerberos V5 and the GSS-API (IAKERB), IETF Internet Draft, draft-ietf-cat-iakerb-09.txt, October 2002
21. N/A: EAP-Kerberos, IETF Internet Draft, draft-someoneeapkerberos-00.txt, February 2005
22. Aboba B., Simon D.: PPP EAP TLS Authentication Protocol, RFC 2716, October 1999
23. Salowey J. et al.: TLS Session Resumption without Server-Side State, IETF Internet Draft, draft-salowey-tls-ticket-02.txt, February 2005
24. AiroSpace : White Paper http://www.airospace.com/technolog/technote_auth_enc_wlan.php
25. Perkins C., Belding-Royer E. M., Das S.: IP Flooding in Ad hoc mobile Networks, IETF Internet Draft, draft-ietf-manet-bcast-02.txt, November 2001
26. Gerla M., Kwon T. J., and Pei G.: On Demand Routing in Large Ad hoc Wireless Networks with Passive Clustering, IEEE WCNC 2000, September 2000
27. Droms R.: Dynamic Host Configuration Protocol, RFC 2131, March 1997