SYSTEM FOR AUTHENTICATING AND AUTHORIZING ACCESS TO AND ACCOUNTING FOR WIRELESS ACCESS VEHICULAR ENVIRONMENT CONSUMPTION BY CLIENT DEVICES

Background

[01] In January, 2016, the United States Secretary of Transportation announced that the USDOT was proceeding with the federal motor vehicle safety standard (FMVSS) 150 based on vehicle-to-vehicle (V2V) communications technology called Dedicated Short-Range Communications (DSRC). DSRC operates over a 75 MHz frequency band centered at 5.9 GHz, which had previously been allocated by the FCC to support a broad range of intelligent transportation systems (ITS) applications. During the period 2002-2009, the IEEE developed the 1609 suite of protocol specifications governing the use of the band, which is divided into 7 channels, each with 10 MHz width. Four of the channels support an IPv6 (Internet Protocol Version 6) interface, which means that UDP/IPv6 or TCP/IPv6-based application software can operate over these channels.

[02] The protocol specifications contained in the IEEE 1609 suite, commonly known as Wireless Access Vehicle Environment (WAVE) and incorporated herein by reference, incorporate security provisions to ensure authentication of WAVE-enabled on-board equipment (OBE) attempting to communicate with roadside equipment (RSE). The terminology OBE and RSE is commonly interchanged with OBU (On-board unit) and RSU (roadside unit). OBU typically includes, but is not limited to, a mobile computing device enabled for DSRC communications, meeting the requirements for V2V specified in SAE J2945/1 and SAE J2945/2, or the requirements for V2P, to be specified in future variants of SAE J2945. RSU typically includes, but is not limited to, a stationary or quasi-stationary computing device enabled for DSRC communications, compliant with the IEEE 802.11p specification for the DSRC MAC and PHY layers, the WAVE

protocol stack and capable of broadcasting WAVE Service Advertisements (WSAs) on the DSRC Control Channel (CCH). OBU devices without valid security credentials can be effectively denied the WSAs of the RSU, which is typically accomplished by simply discarding transmissions sent by the OBU. WSA are periodic messages defined by the IEEE 1609 protocol suite that identifiers services available on the network.

[03] These aforementioned security provisions present in the IEEE 1609 protocol are aimed at controlling access to services resident in the RSU or accessible to the RSU through dedicated application software in the RSU; i.e. services of which the RSU is "aware" and for which the RSU has the policy responsibility to control access. Examples of such services include, but are not limited to, traveler information, in-vehicle signage, navigation, traffic management, weather information, safety, electronic payment, network services, configuration management, and the like.

[04] In the case of IPv6 communications, the role of the RSU is to route IPv6 datagrams towards their destination address. The WAVE architecture provides for authentication of an OBU based on a digital signature in the headers of WAVE Short Message Protocol (WSMP) messages originating from the OBU. The digital signature is generated by the OBU according to an asymmetrical encryption technique and the message transmitted also includes the certificate containing the public key so that the receiving RSU can decrypt the signature. A DSRC infrastructure authority ("infrastructure authority") may propagate the Certificate Revocation List to the RSUs, which identifies OBU devices for which the security credentials are no longer valid. This can be used by the RSU as a criterion for discarding OBU messages sent using WSMP.

[05] In US Patent Application 14/151,035, incorporated herein by reference, discloses a system which enables a user-interface device, such as a Smartphone or tablet, to establish

connectivity to the Internet by using the mechanism defined in RFC 4861 for Router Discovery. This mechanism allows a user device to attach itself to an OBU using Stateless Address Auto-configuration (SLAAC), for example through a WiFiPeertoPeer (WiFiDirect) interface. The OBU acts as an IPv6 router for the user device to connect with the Internet through any RSU which advertises the availability of one or more WAVE Service Channels for this purpose. The system also provides the foundation of the methods for authentication of the user device.

Summary

[06] In one aspect, a system and method are disclosed which performs Authentication, Authorization and Accounting (AAA) functions necessary to enable an RSU infrastructure operator to quantify wireless bandwidth consumption by in-vehicle devices using the WAVE Service Channels, on a per-device basis.

[07] Another aspect provides a AAA server operated by, or on behalf of a DSRC infrastructure authority, comprising at least one processor running at least one computer program adapted to communicate through the Internet with a plurality of mobile devices and/or an OBU operating a subnet for one or more mobile devices, with a plurality of RSUs, in order to carry out the authentication, authorization, and accounting (AAA), thereby enabling the authority to account for WAVE service channel bandwidth consumption by each of the mobile devices having been duly provisioned by the AAA server.

[08] Another aspect provides a plurality of AAA servers operated by, or on behalf of a DSRC infrastructure authority, each server comprising at least one processor running at least one computer program adapted to communicate through the Internet with a plurality of mobile devices and with a plurality of RSUs in order to carry out the authentication, authorization and accounting, the plurality of AAA servers being arrayed for load balancing of inbound Internet traffic and

enabling the authority to account for WAVE service channel bandwidth consumption by each of the mobile devices and/or by an OBU operating a subnet for one or more of the mobile devices, which have been duly provisioned in a single database, access to the database being synchronized among the plurality of AAA servers.

[09] Another aspect provides a RSU configured with an extended IPv6 Management Information Base (MIB) operable to determine packet and byte count statistics for WAVE service channel usage per client device. The client device may be an OBU, a non-DSRC mobile device that is IPv6-reachable through an OBU, or a DSRC-enabled user device. The IPv6 MIB is also operable to retrieve, for each datagram received from an IPv6 node operating in the route optimization mode of Mobile IPv6, the fixed "home address" of the mobile node carried in the Mobile IPv6 routing header of the datagram. The RSU is operable to accumulate, in Non-Volatile Random Access Memory (NOVRAM), the packet and byte count statistics for WAVE service channel usage per client device and periodically sends the statistics to the AAA server, encapsulated in a UDP/IP message, only refreshing the NOVRAM table when the AAA server has acknowledged reception of the UDP/IP message.

[010] Another aspect provides an OBU, compliant with WAVE and IEEE 802.11p and configurable with dual-radio capability, running at least one application level computer program adapted to request authentication and authorization from the AAA server, for IPv6 connectivity to the Internet, either on behalf of a neighboring non-DSRC mobile device or for itself, and configured with an extended IPv6 MIB operable to retrieve the addresses of neighboring devices when a new entry is inserted in a routing table, using either a synchronous method based on SNMP GET to retrieve the routing table periodically, or an asynchronous method based on SNMP TRAP

to report "real-time" changes in the routing table. It is to be appreciated that other methods may be practiced for updating the routing table without deviating from the subject invention.

[011] Another aspect provides a non-DSRC mobile device, operable to request "Internet Subscription" credentials from the AAA server, using a symmetrically encrypted communications channel established with SSL or a similar handshaking protocol for mutual authentication and key exchange, and operable to use the “Internet Subscription” credentials when responding to authentication challenge messages received from the AAA server as defined by one or more exemplary embodiments or aspects herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[012] Other objects, features, and advantages of the present invention will be readily appreciated as the same becomes better understood after reading the subsequent description taken in connection with the accompanying drawing wherein:

[013] Figure 1 is a system block diagram illustrating an authorization process and an authentication process between a user device and a AAA server according to the subject invention;

[014] Figure 1b is system block diagram illustrating one method for retrieval of an IP source address from a routing table using Simple Network Management Protocol;

[015] Figure 1c is system block diagram illustrating another method for retrieval of an IP source address from a routing table using Simple Network Management Protocol;

[016] Figure 2 is a system block diagram illustrating another embodiment of an authorization and authentication process between an On-board Unit and a AAA server;

[017] Figure 3 is a system block diagram illustrating an embodiment of an authentication process according to the subject invention;

[018] Figure 4 is a system block diagram illustrating an authentication process for foreign devices according to the subject invention;

[019] Figure 5 is a block diagram illustrating a protocol stack above Wireless Access Vehicular Environment utilizing a Border Gateway Protocol;

[020] Figure 6 is a system block diagram illustrating a process for distribution of security credentials according to another embodiment of the subject invention;

[021] Figure 7 is a system block diagram illustrating yet another authentication and authorization process for foreign devices according to the subject invention;

[022] Figure 8 is a system block diagram illustrating communication between an AAA server and a plurality of Roadside Units;

[023] Figure 9 is a flowchart illustrating the authorization process according to the subject invention;

[024] Figure 10 is a system block diagram and flowchart illustrating a blocking and an unblocking of a client device, such as an On-board Unit, at a AAA server;

[025] Figure 11 is a system block diagram and flowchart illustrating an accounting process according to the subject invention; and

[026] Figure 12 is a schematic view of a Handshaking protocol enabling key distribution for multi-cast message encryption; and

[027] Figure 13 is a schematic view of a Multicast Message Registration process.

Detailed Disclosure

[028] It is to be understood that the invention is not limited in its application to the details of construction or to the arrangements of the components set forth in the following description of exemplary embodiments, or illustrated in the drawings. The invention is capable of other

embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of the description and should not be regarded as limiting. The use of "including," "comprising," or "having" and variations thereof herein is meant to encompass the items listed thereafter and equivalents thereof as well as additional items. In addition, the terms "connected", "coupled", "de-coupled" and variations thereof are not restricted to physical, mechanical or electrical connections or couplings. Furthermore, and as described in subsequent paragraphs, the specific mechanical and/or other configurations illustrated in the drawings are intended to exemplify embodiments of the invention. However, other alternative configurations are possible which are considered to be within the teachings of the instant disclosure.

[029] In relation to some exemplary embodiments, due to the WAVE security requirements, all nodes (both mobile and stationary) are required to have credentials using the encryption methods specified in IEEE 1609.2. The credentials are issued when the device is provisioned and are used to create digital signatures allowing devices to authenticate themselves, as in the case where mobile devices broadcast a Basic Safety Message (BSM) which carries a digital signature based on the issued credentials. However when a device is provisioned, there is no explicit authorization to use a service channel for general-purpose IPv6 communications. Whether the service channel can be used should depend on whether there is a Provider Service Identification (PSID) for this, duly registered according to the procedure defined in IEEE 1609.12. It is generally assumed that DSRC infrastructure will be deployed and managed using various forms of public-private partnership, all sharing the attributes of an "infrastructure authority", which will address the question of spectrum monetization within the framework of their business models. Provided that an OBU complies with the functional requirements established in the NHTSA safety

standard, the decision as to whether the OBU, or a third party user device connected to the OBU, can be granted IPv6 connectivity over the WAVE Service Channels, and whether the bandwidth usage is billed, may become discretionary choices for the infrastructure authority. Therefore, some exemplary embodiments may enable an infrastructure authority to grant or deny IPv6 connectivity to individual devices and to measure the service channel bandwidth consumption associated with each device. This is accomplished by implementation of the subject invention as described herein.

[030] The first step is "Authentication". This is based on a "logon" procedure executed by a client device, which includes user device (e.g. a Smartphone) or alternatively by the OBU acting on behalf of the user device. The distinction between these two scenarios is a function of the business models available from an infrastructure operator and the choice made by an owner of the OBU, which could be an OEM-manufactured device or an aftermarket retrofit. For example, if the owner of the OBU absorbs all of the costs associated with IPv6 bandwidth consumption, regardless of which third party user device is the communications end point, the logon is to emanate from the OBU device. If the costs are attributable to a neighboring third party user device, the accounting for bandwidth is applicable to the user device, which should therefore be the originator of the logon.

[031] The logon is essentially a request for IPv6 connectivity through a neighboring RSU. The user device or the OBU acting on behalf of the user device described above is a requesting device and may be referred to as a "client" or “client device”. A logon message is digitally signed using an encryption key obtained from a digital certificate issued by, or on behalf of, the infrastructure operator. The digital certificate is encapsulated in the logon message, enabling the receiver to decrypt the signature and to verify the credentials presented in the certificate. The logon message is encapsulated in a UDP/IP packet addressed to the "Roadway Authorization Server"

(RAS), a separate host maintained by the infrastructure operator. As disclosed in Application No. 14/151,035, when a specific RSU is prepared to offer IPv6 connectivity services to passing OBUs, it broadcasts the IP address and application port of the RAS service in a WAVE Service Advertisement (WSA). Since the verification of credentials constitutes the Authentication step and since some exemplary embodiments herein define the complementary functions of authorization and accounting, the RAS in some exemplary embodiments is designated as a AAA server, as will be described in more detail below.

[032] The Authentication step is supported by an external system capable of verifying the credentials identified in the logon message. Such a system has been defined as part of the Federal Motor Vehicle Safety Standard (FMVSS) 150, called the Security Credentials and Management System (SCMS). SCMS is based on a Public Key Infrastructure (PKI) architecture, wherein asymmetrical encryption keys are generated by a "root" certificate authority and encapsulated in digital certificates which constitute the credentials of the client device. The technical architecture of SCMS has evolved from a cooperative effort by the USDOT and the automotive industry, as represented by the Collision Avoidance Metrics Partnership (CAMP). A detailed description of SCMS can be found at http://federalregister.gov/a/2014-24482, which is incorporated herein by reference. The primary purpose of SCMS is to ensure that devices participating in the vehicle-to-vehicle (V2V) communications defined by the FMVSS 150 are duly certified and that their operation does not compromise consumer privacy. Through a secure link between the AAA server and the SCMS, the AAA server is enabled to request assistance from SCMS components in validating the security credentials of a specific device. The validation process is based on the digital signature, the certificate information and an encrypted unique identifier for the device, all of which is encapsulated in the logon received from that device. It is to be appreciated that the

digital signature, the certificate information and the encrypted unique identifier could be transmitted separately in a secure manner.

[033] The next step is "Authorization", to which there are two aspects. The first is the verification that the credentials of the client device have not been revoked by the credentialing authority. This is done using the Certificate Revocation List, which is maintained by the SCMS. The current specification for SCMS calls for distribution of the Certificate Revocation List only to OBUs and RSUs. However, the Certificate Revocation List is also to be distributed to the AAA server, in order to enable the latter for the aforementioned verification. The second aspect is that the account associated with the client is in good standing, which is determined according to the policy of the infrastructure operator.

[034] The Authorization step may only be required when the Authentication step passes. A Boolean result of "fail" for the first step, or the logical conjunction of both steps, becomes an input to a mechanism which enables the AAA server to manage an IPv6 routing table of the RSU currently providing the connectivity to the client. Implementation of this capability is based on harnessing existing methods specified in IETF RFCs. Specifically, by adding the functionality of Border Gateway Protocol (BGP) to both the AAA server and the RSU, the AAA server is enabled for Remotely Triggered Black Hole (RTBH) filtering within the RSU, whereby IPv6 traffic from the client can be either blocked or unblocked based on whether the client passed the Authentication and Authorization steps. This methodology provides an efficient, standards-based means of controlling access to the mobile Internet services which infrastructure operators may want to offer, and links the duly authorized credentials of the client device requesting the service to the IPv6 routing table of the RSU, without the need to alter the WAVE suite of specifications.

[035] The final step is Accounting. The RSU is configured to keep track of the service channel bandwidth consumption by each device, when using the IPv6 interface, and periodically send reports to the AAA server. To accomplish this, the Management Information Base (MIB) of the IPv6 layer may be extended to acquire packet and byte count statistics per client. The consumption data is retrieved using a standard SNMP interface and periodically transmitted to the AAA server, for example through a TCP connection.

[036] In relation to some exemplary embodiments, a DSRC RSU routes IPv6 datagrams received from, or transmitted to, an OBU via a WAVE Service Channel. If the owner of the RSU, which may be the "infrastructure authority", adopts a policy to control and manage service channel bandwidth usage by individual OBUs, and devices connected to OBUs, then mechanisms are required to authenticate these devices, authorize their use of service channel and account for the amount of bandwidth consumed by each device. The subject invention provides a server which supports these mechanisms, which is typically called AAA (authentication, authorization and accounting).

[037] A single-radio OBU device which adheres to the required duty cycle for monitoring both the safety or "V2V" channel, (which is now specified at CH 172 at the "bottom" of the DSRC band) and the Control Channel (CCH or CH 178), may not be suitable for providing IPv6 connectivity services, since, at a minimum, its receiver would have to divide its time even further between the safety channel, CCH and the designated service channel. The incremental cost of dual-radio devices is sufficiently low to warrant vendors configuring an OBU product, either an Aftermarket Safety Device (ASD) or Retrofit Safety Device (RSD), as defined in the "V2V Readiness Report", incorporated herein by reference, as a dual-radio device. It is therefore assumed throughout this disclosure that an OBU providing access to service channel bandwidth is

configured as a dual-radio device. However, it is to be appreciated that the subject invention could also be implemented with the single radio device.

[038] Since the WAVE standard allows IPv6 datagrams to be transmitted on the service channel without any restriction, the RSU which receives the datagram will automatically route it towards its destination. However, if the administrative policy for the RSU calls for IPv6 traffic to be subject to AAA, then authorization for over-the-air IPv6 communications is to be requested on behalf of either the OBU or one or more devices connected to it.

[039] Figure 1 illustrates the authorization process and an authentication process between the user device and the AAA server according to the subject invention. The notification from the RSU indicating the requirement for authorization is embodied in the WAVE Service Advertisement (WSA) 35. WSAs, which are broadcast on the WAVE CCH by RSUs, constitute the method, required by the WAVE standard, with which the RSU informs the OBUs what services are accessible through the RSU broadcasting the WSA.

[040] RSU 30 is configured by the infrastructure operator to issue a WSA which includes the IP address and port of the AAA service to which the OBU can send an authorization request. As disclosed in US Patent Application 14/151,035, the WSA has previously been used to identify only the address where the OBU should send an authorization request. The subject invention utilizes the WSA to also include channel availability information which the OBU should use for channel configuration, as described further below. WSA 35 encapsulates both the IP address and port for the AAA server. WSA 35 also encapsulates a Provider Service Identification (PSID) signifying that this RSU supports the availability of general-purpose IPv6 connectivity subject to AAA management, as well as the identifiers of the available service channels. Different PSIDs are established in order to allow the OBU to differentiate between a service which applies billing

charges to the OBU for any neighboring user devices and one for which each user device is associated with its own billing account. The utility of this differentiation is explained further below. Otherwise, as previously indicated, if there is no requirement for AAA, WSA 35 is not required because access to the service channel may be automatic or not restricted. As used herein, automatic means real-time or near real-time automated processing by one or more processors, non-manually and without human intervention. However, it is to be appreciated that manual involvement may be required without deviating from the subject invention. The payload of WSA 35 must also contain cryptographic keying material, associated with a digital certificate issued to the AAA server and which is needed by the OBU to encrypt data included in its authorization requests sent to the AAA server, as explained further below.

[041] The content of WSA 35 is reported to Process 21, which is generally a user application running in OBU 20, through the WSMP interface. Process 21 is implemented by and executed by a processor resident in the OBU 20. It is to be appreciated that the processor may be any readily available device capable of performing the processes as described herein. The process steps or instructions, which execute via the processor of OBU 20 or user device 10, implement the functions/acts specified in the flowchart and/or diagram shown throughout the Figures and discussed herein. Process 21 then registers a "transmitter profile" with the MAC Layer Management Entity (MLME) which specifies the service channel number specified in the WSA. This registration of the transmitter profile ensures that the MLME is always updated whenever a policy change results in a change to the services advertised in a WSA. If IPv6 connectivity services are deactivated at a specific time or location (i.e. specific RSU or cluster of RSUs), the PSIDs corresponding to these services are not present in the WSA and process 21 registers a new transmitter profile which does not include the corresponding service channel number. As explained

in IEEE 1609.4, when the Channel Router function of the IEEE 802.11p MAC layer (not shown in Figure 1) cannot find this service channel number, packets intended for transmission using this channel are discarded.

[042] The authorization function involves a request sent by OBU 20 to the AAA server 40, illustrated in Figure 1 by authorization request, or message, 25. An example of such messages 25 are disclosed in US Patent Application 14/151,035, wherein it takes the form of a UDP/IPv6 message. This message 25 is initiated by process 21, and process 21 listens for WSA 35. If the request has not already been granted by the AAA server 40, process 21 queues the message 25 for transmission through the IPv6 interface. WSA 35 indicates that the service advertised is billed to an individual account for a third party user device and therefore the authorization request is from the OBU "on behalf of" the third party device, for example a neighboring Smartphone or tablet, the interface between the OBU and the third party device being, in some exemplary embodiments, a wireless link such as WiFi Direct (also called WiFi Peer to Peer). In this instance the UDP payload of message 25 contains the IP source address of the user device.

[043] The mechanism whereby user device 10 attaches itself to OBU 20 requires that the latter is configured to support the IPv6 "neighbor discovery" specification in RFC 4861, incorporated herein by reference. In this specification, a network node notifies its neighbors of its routing capabilities through periodic broadcasts of a "router advertisement" (RA) over the interface through which the neighbors may wish to join the network. The router advertisement is shown in Figure 1 as RA 100. US Patent Application 14/151,035 discloses the process of attachment in terms of the mechanism of Stateless Address Auto-Configuration (SLAAC) specified in RFC 4862 which is also incorporated herein by reference.

[044] Prior systems, such as that disclosed in US Patent Application 14/151,035, did not disclose the method by which the IP source addresses contained in the authorization requests exemplified by message 25 is obtained. When the user device attaches itself to the OBU, the latter may discover the IP source address, in some exemplary embodiments, due to a reception of a Router Solicitation message from the user device, which, as defined in RFC 4861, results in the address of the user device being added to the OBUs routing table. Acquisition of this information requires implementation of SNMP in the OBU. There are two alternative methods that would then be possible, illustrated in Figures 1b and 1c, respectively, which illustrate well-known protocol layers. The simplest method (Figure 1b) is to configure process 21 to periodically issue an SNMP GET to the localhost to retrieve the ipv6RouteTable object in the IPv6 MIB. The second method (Figure 1c) is computationally more efficient but requires an extension to the standard IPv6 MIB which defines a new object corresponding to a change in the routing table. When this is detected, a TRAP message is generated which can be received by a handler function 25, registered with the SNMP layer by process 21.

[045] Using WAVE as a platform for mobile Internet services which rely on TCP at the transport layer is frequently discouraged because the OBU address changes as the device moves from one RSU to another. As a result, the user device attaching itself to the OBU will always discover a change in its own IPv6 address with each transition between RSUs, which will disrupt TCP sessions and in turn degrade the quality of any connection-oriented streaming services above the transport layer. The subject invention overcomes these problems by enabling the user device for Mobile IPv6, which is specified in RFC 6275 and incorporated herein by reference, and configured for the "route optimization" (section 11.3.1) mode. According to one aspect of the subject invention, the OBU 20 becomes the primary "care-of address" for the neighboring user

device. In the "route optimization" mode, the "home address" is carried in the IPv6 Destination Option header. This address is fixed and used as a substitute for the IP source address and destination addresses, since the latter, in the route optimization mode of Mobile IPv6, are the mobile node's "care-of address" address, which is the OBU itself, or, in the case of a DSRC-enabled user device, such as a Smartphone incorporating a DSRC interface, is the RSU. The substitution is therefore required to ensure the granular accumulation of traffic statistics per individual user device, implemented by the Accounting function described below, rather than an aggregate for the OBU to which they are attached. Similarly to the mechanisms explained above in connection with the OBU obtaining the IP source address shown in Figures 1b and 1c, the "home address" information required can be acquired by process 31 running in the RSU 30 using an SNMP GET call to retrieve it from the Mobile IPv6 MIB or by processing a TRAP generated for each datagram routed by the RSU.

[046] In some exemplary embodiments, the OBU includes authentication information in the request message 25, which enables both authorization and authentication to be combined in a single step. This procedure is used in the case where the accounting of service channel bandwidth consumption is aggregated for all devices neighboring the OBU 20 and billed to a single account associated with the OBU 20. As shown in Figure 2, the WSA 36 uses a distinct PSID reflecting the nature of the service. In this instance, AAA server 40 receives message 24 containing information required to authenticate the client, and therefore does not need to respond with an authentication challenge. The information required for authentication is well known, and may include, but is not limited to, International Mobile Equipment Identity for Smartphones or vehicle identification number, or other such Personal Identifying Information. The method of authentication is described below. The path segments 28 and 29 in Figure 2 are functionally

equivalent to the path segments 27 and 26 in Figure 1. Also in, in some exemplary embodiments, in order to facilitate the Accounting process, the payload in message 24 should contain the OBU's IP address in lieu of the actual source IP address. Subsequent IPv6 datagrams originating from the user device will contain this address in the routing header. This enables the RSU to accumulate the datagram byte count for active OBUs as explained in more detail below.

[047] Referring back to Figure 1, RSU 30 is the first IPv6 hop for the authorization request 25, which is transmitted over a service channel. RSU 30 then routes the datagram towards its destination. The routing is illustrated by the path segments 26 and 27 in Figure 1, which are respectively, the inbound IEEE 802.11p MAC frame received from the service channel and the outbound frame on whatever medium is deployed for backhaul to the Internet. In order to account for service channel bandwidth consumption by individual user devices, RSU 30 caches the source IP address of the datagram in a non-volatile random-access memory (NOVRAM) table of such addresses. In the accounting process of the subject invention, the source IP of inbound datagrams, and the destination IP address of outbound datagrams, are matched against the entries in this table and the datagram byte counts are accumulated in the NOVRAM table for the entry corresponding to the correct match. If the RSU is configured for accounting of aggregated service channel bandwidth consumption for all devices neighboring the OBU, then the entry in the NOVRAM table must be the address of the OBU, which can be parsed from the IPv6 header.

[048] Upon receipt of the authorization request 25, AAA server 40 is configured to authenticate the client. Figure 1 depicts the AAA server 40 sending an UDP/IP authentication challenge message 105 (or Authentication Challenge) to the IP source address associated with the request, which is the user device 10. The response mechanism is shown in Figure 1 as Authentication Challenge Response 103. The challenge response 103 serves to verify the

credentials of the sender, so it requires a secure encryption methodology allowing the sender to prove its authenticity to the infrastructure authority. Since the DSRC cyber-security provisions are specified in IEEE 1609.2, and since the encryption keying material is contained in digital certificates produced and distributed by certificate authorities operated by, or in collaboration with, the infrastructure authority, it follows that these certificate authorities can also provide the same kind of certificates (i.e. compliant with IEEE 1609.2 specifications) to user devices as will be provided to OBUs and RSUs.

[049] User device 10 assembles the Authentication Challenge Response 103, involving the encryption keying material (basically the public key of the certificate issued to the user device) and an encrypted payload including some unique identifying information, such as its International Mobile Equipment Identifier (IMEI). Successful decryption enables the receiver to authenticate the user device according to the asymmetrical encryption technology specified in the IEEE 1609.2. Upon receipt of Authentication Challenge Response 103, AAA Server 40 performs a search through a database for the IP source address. This database includes a table, of which the row entries may contain, at a minimum, a unique device identifier, an IPv6 address, security credentials issued to the device by a duly authorized certificate authority and the accumulated WAVE service channel bandwidth consumption within the current reporting period. If a match is found for the IP source address, this means that this address has been previously encountered and will have already been authenticated. However, in the event that this address is a duplicate of another IPv6 address, formulated according to SLAAC, at a previous time with an entirely different OBU, then the least amount of time it would take for an OBU to leave and then return to the coverage area of an RSU may define the point at which the source IPv6 may be a possible duplicate address, therefore requiring that AAA server 40 authenticate the client.

[050] The ability of the AAA server 40 to authenticate a client and to authorize its use of an service channel is dependent on whether it implements the encryption/decryption process specified in the request. The preferred mechanism for authentication is illustrated in Figure 3, which depicts the process of issuing, to the client device 10, the security credentials which it employs when it needs to be authenticated by the receivers of its messages. The security credentials are issued by an entity called the Enrollment Certificate Authority (ECA) which is one of the Certificate Management Entities (CMEs) defined within the SCMS.

[051] The issuance of security credentials by the ECA 70 to the OBU 20 is shown in Figure 3 by the operation 71. However, the functional specifications for the issuance of security certificates are part of the bootstrapping process defined by the SCMS whereby the ECA assigns a long-term enrollment certificate or similar to each OBU, which is well-known and beyond the scope of the present disclosure. The enrollment certificate provides, in one possible form, the credentials needed by the OBU for authentication during subsequent procedures defined within the scope of the SCMS. These procedures have been designed so that the digital signatures accompanying the basic safety messages serve the dual purpose of preserving the anonymity of individual vehicles while ensuring that the signatures are authentic, in the sense that the encryption keying material used to create them was duly issued by an authorized certificate management entity.

[052] The design criteria for the SCMS architecture have, as a primary objective, the protection of consumer anonymity, and do not include requirements for "monetizing" WAVE service channels based on bandwidth consumption per device. As the subject invention provides for accounting procedures, the ability to associate bandwidth consumption with a specific device requires that the security credentials, i.e. the certificates issued by the CMEs, include unique

Personal Identifying Information (PII). Generally, the SCMS design ensures that no PII will be available in any certificates used by OBUs to digitally sign messages, such as basic safety messages. This ensures that while the security credentials of a transmitting device can be validated, its anonymity is protected because it is not possible to identify a device. Therefore, an infrastructure authority requiring AAA functionality cannot rely on enrollment certificates alone to associate bandwidth consumption with any specific OBU or third-party device.

[053] However, the use of WAVE bandwidth to provide mobile Internet services is based on a consumer discretionary choice. Hence, when the infrastructure authority requests some form of PII in order to register for the service, there is no violation of privacy. One example of PII that can be automatically acquired and delivered to the AAA server is the Vehicle Identification Number (VIN), which can be acquired by an OBU with a CAN-bus connection to the Engine Control Module (ECM) using protocols defined in the SAE standard J-1979 or similar protocols. This is the preferred PII in the case of a billing applied to the aggregate traffic through the OBU, since aftermarket OBU devices can be moved from one vehicle to another.

[054] The preferred mechanism for establishing the association between the SCMS-issued credentials encapsulated in the enrollment certificate and the PII which can be linked directly to a billing account, is shown in Figure 3. Process 22 is an application-level software module running in the OBU 20 with two principal functional responsibilities. First, it maintains a listener to receive the credential certificate, as shown by the operation 71, which delivers the certificate from the ECA, and an acknowledgement 72, which confirms (or rejects) reception of the certificate. It is to be appreciated that the certificate that is received in operation 71 may be, separately or together, an enrollment certificate, an identification certificate, or other certifying credential used for the authentication function. For simplicity, the following discussion will

describe the authentication with the enrollment certificate, without limiting the subject invention thereto. Utilizing the other credential certificates in the same manner is envisioned within this disclosure. To this extent, process 22 is a required component of OBU application software. Second, when operating within range of an RSU that advertises billable IPv6 connectivity services, process 22 has the responsibility of triggering a request 25 from OBU 20 to the AAA server 40, which combines both the authorization and authentication functions in one step. Process 22 encrypts the VIN, acquired by interrogating the ECM using standard protocols defined in SAE J-1979. It is noteworthy that in the asymmetrical encryption methodology specified in IEEE 1609.2, the private key is used only for decryption, whereas encryption of data must be performed using a symmetrical key derived from the public key. Therefore, in order to encrypt data which can only be decrypted by the AAA server, the OBU must acquire a public key published by the AAA server itself. This public key is associated with an enrollment certificate issued to the AAA server and is propagated to OBUs through the WSAs broadcast by RSUs operating within the same domain as the AAA server, as previously described. Process 22 then encapsulates the encrypted VIN as part of the payload of authorization request 25, which should also include the OBU's enrollment certificate information, consisting of a digital signature and the public key required for its validation. Process 22 then sends the authorization request 25 to the receiver of the AAA server 40 (which is process 41) and which owns the private key required to decrypt the VIN. For simplicity of presentation, the two software functions described above are implemented within the single process 22. In another embodiment, these two functions could be decoupled so as to yield two separate processes.

[055] The SCMS specifications define the ECA as responsible for enrollment of DSRC devices which, by definition, comply with all the standards (IEEE 1609.x, IEEE 802.11p, SAE J-

2735 and SAE J-2945) required for these devices to be certified. However, when IPv6 traffic using the WAVE service channel originates from non-DSRC mobile devices, and it is the policy of the infrastructure authority to create billing accounts for individual non-DSRC mobile devices, these devices require the same kind of credentials if their traffic is to be authorized by the AAA system. To issue such credentials, the AAA server is enabled as a certificate management entity only for non-DSRC mobile devices neighboring OBUs and whose IP traffic can be offloaded onto the WAVE service channel. The certificates produced are "Internet Subscription Certificates" in order to distinguish them from OBU enrollment certificates or the like. Operations 73 and 74 in Figure 3 illustrate the issuance of such credentials. In some exemplary embodiments, the communications path for the distribution of these credentials is based on an SSL session between the non-DSRC mobile device and the AAA server.

[056] In some exemplary embodiments, there are three conditions to be satisfied in order for the AAA server 40 to authorize OBU 20 for access to the IPv6 connectivity service of RSU 30. First, the security credentials of OBU 20 are validated. This is accomplished by successful decryption of the PII encapsulated in the request 25 and received by process 41, using the public key of the enrollment certificate sent in the request. The decryption algorithm is implemented as software module 42 running in AAA server 40, and invoked through a synchronous call from process 41, as shown in Figure 3. Second, a database 43 of subscribers registered in the AAA server 40 is queried by the search 45 to determine if the PII is found. This constitutes authentication of OBU 20.

[057] In addition, the flow chart in Figure 9 summarizes these steps. The AAA server 40 receives the authentication and/or authorization request in step 101. Next, the OBU 20 digital signature is decrypted in step 110. The digital signature is then validated in step 120 and if the

signature is not validated, notification is returned to the OBU 20. If the signature if validated, in step 130, the database 43 is queried for the PII. If the PII is found in step 140, notification is returned to the OBU 20. Otherwise, the request is forwarded to the ECA in step 150.

[058] Typically, user registration is carried out through a Web User or Web Services interface offered by the DSRC infrastructure operator. The actual registration method(s) is (are) outside the scope of this disclosure. Whatever method is used, it is to enable the infrastructure operator to create an account associated with unique identifying information (PII), for example the VIN of the vehicle.

[059] It is a fundamental tenet of USDOT policy that operation of DSRC infrastructure will be decentralized across the United States. It is envisioned that local jurisdictions, whether they are cities, counties, regional municipal authorities or state DOTs, will establish, or oversee the establishment of, independent DSRC infrastructure operators. Whereas it is expected that in many or perhaps all cases, these operating entities will take the form of public-private partnerships, the corporate structure, the roles and responsibilities of the partners and the procedures for establishing policies which are implemented using the DSRC technology itself, may vary. With particular reference to the present disclosure, there is no technical reason why the policy with respect to mobile Internet service has to be standardized across all jurisdictions. Each jurisdiction has the option of enabling a mobile Internet service through whichever RSUs are deployed within its territory and subject to its management, and to apply whatever schedule of charges for bandwidth consumption of the WAVE service channels that it deems appropriate.

[060] The last of the three steps for authentication arises when there is no local database match for the PII, which requires additional procedures set forth below. To ensure inter-operability across regions for mobile Internet services, each infrastructure authority is to maintain a AAA

server in which vehicles associated with that territory can be registered. An example of the need for this arises in the following scenario. A vehicle is registered (with the DMV) as having an address within a region where the policy of the infrastructure authority is for free mobile Internet service. The vehicle is currently travelling in another region which applies charges for bandwidth consumption and operates the administrative tools (AAA server) for this purpose. Each RSU in this region will advertise the IP address and UDP port number only of the AAA server which is owned and operated by the local authority. The OBU in the vehicle requests authorization to access the service. If the request comes from a non-DSRC mobile device, the AAA server attempts to validate the credentials. Otherwise it requests validation from the ECA for the enrollment certificate used by the OBU. But since the decrypted PII (e.g. the VIN) will not appear in the AAA database, the infrastructure authority could assert its right to deny the vehicle access to the mobile Internet services. The mechanisms for enabling or prohibiting access to the mobile Internet services are described below. However, if a "foreign" vehicle is not registered in its AAA server, an infrastructure authority is operable to interrogate the entire population of AAA servers wherever they have been deployed throughout the jurisdiction governed by the SCMS. If the infrastructure authority prohibits access to a "foreign" vehicle (i.e. one that is not registered in its AAA server) it is operable to forego the revenue that could otherwise be generated from an account associated with the PII registered in a "remote" AAA server.

[061] In short, if mobile Internet services are to be accessible wherever a vehicle operates, a mechanism is necessary to enable the operator providing the service to authenticate a "foreign" vehicle operating in its territory and to reconcile the charges for bandwidth consumption with the AAA server in the home territory.

[062] Figure 4 illustrates the sequence of steps needed to find a "foreign" vehicle. As discussed above, the role of the ECA with respect to issuance of credentials to mobile devices is defined within the scope of the SCMS specifications. However, the ECA encompasses an additional role for authentication of devices which request mobile Internet services but cannot be found in local AAA server databases. This new role requires that the AAA server be integrated into the Public Key Infrastructure (PKI) architecture of the SCMS.

[063] PKI systems are commonly used in Internet transactions for computing devices to present security credentials to any other device that needs proof of authenticity. Security credentials can be derived from a trust "chain" or "hierarchy", whereby a digital certificate containing the credential(s), itself, is to be authenticated according to the digital signature of the issuer of the certificate. Authentication of a device based on the certificate it presents may require several iterations before reaching a "root" certificate authority which does not derive its trustworthiness from another entity above it in the "trust hierarchy".

[064] The role for the ECA is to incorporate the requisite functionality to support the various procedures or functions of exemplary embodiments herein. In particular, it is configured to issue a certificate to any AAA server that an infrastructure authority wishes to deploy. By doing so, it extends the trust hierarchy of the SCMS into the AAA servers that infrastructure authorities need to manage the monetization of the WAVE service channel spectrum. Furthermore, it is to maintain a NOVRAM table of the IP addresses of each AAA server to which it has issued certificates. This ensures that when the PII for the client cannot be found in the database of the local AAA server, the ECA can interrogate all of the duly certified AAA servers operating under the jurisdiction of the SCMS, in order to determine whether the vehicle in question is registered somewhere, as illustrated in step 150 of the flow chart in Figure 9.

[065] The interrogation of "remote" AAA servers by the ECA is exemplified in Figure 4 by the interaction between the ECA 70 and the AAA servers 50 and 60. This representation is intended solely for the purpose of simplifying the diagram and is not intended to imply that the interrogation process is restricted to only two AAA servers. In the first case, ECA 70 sends a request 75 to a specified listener 56 running in AAA server 50, which in turn issues the query 55 to the database 53 for the VIN. A binary result (found/not found) is returned to the ECA with the response 76. Similarly, request 77 to listener 66 in AAA server 60, encompassing listener 66 and database 63 which are functionally equivalent to listener 40 and database 43, will trigger query 65 and the same type of binary result in response 78. Since the AAA servers are integrated in the PKI architecture of the SCMS system, the security provisions exist to ensure the confidentiality of the VIN information transmitted by the ECA.

[066] Alternatively, and in order to decouple the credentialing responsibilities of the ECA as currently specified in the SCMS, from the credentialing requirements for any device associated with a mobile IP billing account, the AAA server is configured to issue "Internet Subscription" certificates to DSRC OBUs, as well as to non-DSRC mobile devices, as previously described. In this case, the communications path for distribution of "Internet Subscription" certificates to OBUs is over DSRC, instead of cellular, and the certificate information is, in some exemplary embodiments, secured by asymmetrical encryption using the enrollment certificate. The authorization request 25 from an OBU 20 uses its Internet Subscription certificate (in lieu of the enrollment certificate) to request authentication from the AAA server 40. This is illustrated in Figure 6. The sequence of steps required to obtain an Internet Subscription certificate is as follows:

- process 80 is spawned by process 21 (Figure 1), running in OBU 20, the first time the WSA 35 (or 36) is received.

- OBU 20 sends UPD/IP message 81 to the process 82, running in the AAA server 40, to request an Internet Subscription certificate. This request includes the OBU's enrollment certificate information.
- process 82 sends a request/response exchange 83 to the ECA 70 to validate that the enrollment certificate has not been revoked.
- process 82 sends request/response exchange 84 to module 85 to generate an asymmetrical encryption key pair for OBU 20 and an Internet Subscription certificate containing this information.
- Process 82 encrypts the information generated by module 85, using the public key of the enrollment certificate received in message 81, and returns this, as the payload of message 86, to process 80 of the OBU 20.
- OBU 20 acknowledges receipt with message 87.

[067] The additional advantage of "Internet Subscription" certificates for OBUs is that it eliminates the need for interrogation, by the ECA, of multiple AAA servers in order to search for a "foreign" vehicle. Internet Subscription certificates should include the domain name of the AAA server that issues them, which is included in the authorization request from OBUs (or in the authorization challenge response from non-DSRC mobile devices). The AAA server receiving the request can therefore resolve the domain name to an IP address. In turn, rather than scanning all remote servers until a match is found (requests 75, 77 and responses 76, 78 in Figure 4), only a single UDP/IP request/response is required. Also included in the request or authorization challenge response from the OBU, is the public key of the enrollment certificate of the AAA server which issued the Internet Subscription, which can be used for re-encryption of the VIN in the event that the request/response has to be forwarded to a remote AAA server, as described below.

[068] This alternative path of authorization/authentication of a "foreign" device is shown in Figure 7. Process 41 running in AAA server 40 uses a DNS address resolution request 47 to a DNS server 90 to acquire the IP address of a remote AAA server 60, and then forwards the request 79 to AAA server 60. To ensure confidentiality of the PII in the payload of request 79, AAA server 40 re-encrypts the PII using a symmetric key derived from the public key of remote AAA server 60, and uses its own credentials obtained from the ECA to digitally sign the request 79 and sending both its certificate information and the re-encrypted PII in request 79, so that remote AAA server 60 can both validate its signature and decrypt the PII in the request. Since the credentials of AAA server 40 are obtained from the ECA, this both protects the private information included in request 79, and enables the remote AAA server 60 to authenticate the sender as being linked to the SCMS chain of trust and provide a response 88.

[069] The third condition for authorization is to ensure that the enrollment certificate itself is confirmed as not having expired or been revoked for some reason. Some exemplary embodiments of a mechanism for accomplishing the authorization may involve constructing the request 46 such that its primary objective is verification that the enrollment certificate does not appear is the latest Certificate Revocation List maintained and disseminated by the SCMS. However, if the Certificate Revocation List is propagated by the SCMS to the AAA Server, there is no longer a requirement for request 46 to ask the ECA to verify the received certificate against the Certificate Revocation List. Secondarily, and only if the enrollment certificate is valid and the method described above, of directly interrogating the AAA server identified in the "Internet Subscription" certificate, is not used, request 46 can specify whether the PII in the request (i.e. the VIN) was not found in the local database and needs to be searched in the remote AAA servers.

[070] AAA server 40 may respond to the sender of the request for authorization. If the security credentials are invalid or have been revoked, the billing account is delinquent or simply non-existent; the governing policy may call for the request to be denied. However, in order to ensure that IPv6 traffic is blocked, it is not sufficient for the AAA server 40 to send the client a notification of denial. Since the process of granting authorization for IPv6 connectivity falls outside the scope of the IEEE 1609 specifications, it follows that any device requesting such authorization is doing so "voluntarily" and that, if it is denied the authorization, it is not "obligated" to abide by this decision. WAVE specifications do not prohibit it from routing IPv6 traffic towards the destination addresses specified in the datagram headers and there are no provisions within WAVE for the RSU to block this traffic. It follows that a mechanism is required that enables the AAA server 40 to cause IPv6 traffic originating from a specific OBU to be filtered and, conversely, to cause the removal of a filter that has been applied to a specific OBU once it has been authenticated and authorized.

[071] The preferred methodology for such a mechanism is one which can be implemented in an RSU certified to comply with USDOT recommendations, which implies that the protocol stack above WAVE, illustrated in Figure 5, is fully implemented. A filtering mechanism operates as application layer software using an API provided by the RSU vendor which exposes the transport layer of the protocol stack. The requirement for a router to discard traffic, based on the point of origin of the traffic, arises in the case of Denial of Service (DOS) attacks. One of the methods used by ISPs to protect against these attacks is called Remote Triggered Black Hole (RTBH) filtering. RTBH filtering can be applied to both source and destination addresses but in the specific case of DOS, the filtering is applied to the source address. This methodology is described in the informational RFC 5635, incorporated herein by reference, which specifies the

use of internal Border Gateway Protocol to deliver RTBH filtering instructions to a router. Border Gateway Protocol as specified in RFC 4271, incorporated herein by reference, operates as a peer-to-peer session over a TCP connection on a well-known port (179), allowing for the propagation of routing information between pairs of routers.

[072] An infrastructure operator would normally have a plurality of RSUs and a very limited number, if not a single, AAA server, all operating within the same Autonomous System. This topology is illustrated in Figure 8, where the AAA server 40 executes multiple instances of the BGP Finite State Machine defined in RFC 4271, each with a TCP connection to an individual RSU 30. As shown in Figure 10, the RTBH filtering instructions are sent as UPDATE messages, which are defined in RFC 4271 and which specify the addresses to be blocked (filtered) or unblocked by the receiving RSU 30. Figure 5 illustrates use of BGP by a software application, in contrast to the more conventional scenario in which the BGP services are invoked by a network administrator through a command line interface. In other words, the use of BGP in the context of this disclosure is a completely automated process, defined by the flow chart in Figure 10, which can be described in terms of the following algorithmic steps:

- An authorization request 25 from an OBU 20 is received by the AAA server 40.
- Authentication and authorization are carried out in step 200 according to the mechanisms already described in the present disclosure.
- In step 210, the request is validated. If the request is invalidated (either because authentication fails or authorization is not granted), a "denial notification" can be returned to the OBU in the form of UDP message 92.
- If the request is authorized, a "grant notification" 94 can be returned to the OBU.

- In both cases of the preceding cases, a response 96 to the OBU is shown as a dotted line to signify that it is optional. The request for authorization is not part of the WAVE standard and therefore, as previously indicated, the OBU is neither obligated to send this request nor to listen for, or take any action with respect to, a response. Hence implementation of the response message in the AAA Server is not a requirement.
- In both cases, the result of the authentication/authorization process becomes an input 98 to the invocation of the BGP service that sends an UPDATE message to the RSU through which the OBU request was routed to the AAA Server. Depending on the result, this message will instruct the peer BGP entity running in the RSU to either block or unblock traffic originating from the requesting OBU. The TCP connection is chosen according to the IPv6 address of the RSU, which is obtained by parsing the global prefix and subnet ID from the IPv6 address of the OBU (see RFC 4291 IP Version 6 Addressing Architecture, incorporated herein by reference).
- An alternative methodology for instructing the RSU block mobile-terminated traffic to a specified mobile destination address would be to send an SNMP SET command instructing the RSU to set to either TRUE or FALSE the MIB object ipv6RouteValid corresponding to the ipv6RouteTable entry for the specified mobile destination address. This approach would not be applicable to blocking (or unblocking) the routing of mobile-originated traffic.

[073] Accounting

[074] Since one goal of the subject invention is the monetization of radio spectrum, the RSU, in some exemplary embodiments, is configured to keep track of the service channel bandwidth consumption by each device, when using the IPv6 interface, and periodically send

reports to the AAA server. To accomplish this, the Management Information Base (MIB) of the IPv6 layer is extended to acquire packet and byte count statistics per client, the data is retrieved using a standard SNMP interface and periodically transmitted to the AAA server, in some exemplary embodiments through a TCP connection. The preferred implementation is illustrated in Figure 11. Process 31 running in the RSU invokes the TRAP handler registration 33 to register TRAP handler 32 with the SNMP, so that per client byte count statistics are reported asynchronously. Whenever a packet is sent to, or received from, the WAVE IPv6 interface, the extended MIB provides the statistics on per client basis (Ipv6ByteRxorTxPacketByteCount), which generates TRAP message 34. TRAP handler 32 processes the TRAP and informs process 31 using a callback procedure 37. Process 31 accumulates the per client statistic in a NOVRAM table and periodically sends a UDP/IP report (message 38) to the AAA server which is persistent (i.e. requiring an acknowledgement). Before sending the acknowledgement, process 41 running in AAA server 40 invokes the database procedures 43 in order to store the information received in the report.

[075] Multicast Push Notifications

[076] In relation to some exemplary embodiments, some I-V (infrastructure-to-vehicle) WAVE applications use multicast techniques in a “one-to-many” configuration which delivers “push notifications” to mobile devices. There are two basic categories for such applications:

(1) Geo-temporal commercial advertisements; e.g. promotions for discounted products or services at specific retail locations for specific dates/times.

(2) Roadside Alerts (RAs). These are advisory messages from the road network operator which correspond to the types of information currently provided as a telephone service by many state and provincial jurisdictions in North America. They include, but are not limited to,

accident notifications, lane closures, travel time advisories, and other road network operational events. They can also include quasi-static navigational information such as speed limits, distances to destinations, parking restrictions, school or construction zone warnings, and so on. RAs are structured according to a standardized format defined in the SAE J-2735 message set, incorporated herein by reference.

[077] Due to the "one-to-many" communications topology for multicast WAVE services, the task of deriving revenue from mobile subscriptions for these services requires a slightly different approach than in the instances described herein.

[078] Business Models

[079] In some exemplary embodiments, there are two models for generating revenue from push notifications: "advertising" and "subscription". With the "advertising" model, the originator of the push notification compensates the network operator in some fashion in consideration for the delivery of the message. In this context, "advertising" is not limited to purely commercial applications but may also apply to public services announcements such as accident notifications, lane closures, travel time advisories, and other road network operational events reported according to the standardized format for Roadside Alerts (RAs) defined in the SAE J-2735 message set.

[080] In the "subscription" model of some exemplary embodiments, messages should be received only by devices associated with a paid subscription account. In both models, efficient utilization of network resources (i.e. bandwidth) is achieved by using a multicast, or "one-to-many", method of message delivery. A client device which joins a multicast group can receive messages sent to the multicast address associated with that group, which means that it is technically feasible to implement software enabling any device to receive multicast messages, regardless of whether it has a valid subscription.

[081] Differentiation of Client Devices in the “Subscription” Model

[082] In the case of the “advertising” model, in some exemplary embodiments, since revenue comes from the source of the messages, there is no need, from a business perspective, to restrict access to the messages for different categories of client devices. However if the “subscription” model is to be effective, where the source of revenue is associated with individual client devices, it is necessary to restrict access only to those client devices with valid subscriptions.

[083] In some exemplary embodiments, such restricted access may be provided by encrypting the payloads of multicast messages. Such exemplary embodiments are not necessarily limited to any particular encryption methodology for this, and concerned exclusively with the task of ensuring that all receivers authorized to receive these messages are in possession of the keying material necessary for decryption. The focus here to establish a method to ensure that the key(s) required for decryption can be distributed to authorized devices in a secure manner.

[084] In some exemplary embodiments, a reliable and secure mechanism to support the “subscription model” for multicast messaging is illustrated in Figure 12, whereby client devices may request authentication/authorization from the AAA Server for access to services based on unicast Internet messaging. Figure 12 shows that a Roadside Unit (RSU) 30 may use WSA 37 to advertise a multicast service with a PSID (Provider Service Identifier) associated with the “subscription model”. As described in Figures 1 and 2, the OBU (On-board unit) 20 may send a request 25 to the AAA Server 40, identifying the IPv6 address of the client (user) device which is connected to it. AAA Server 40 then issues the authentication challenge 105 to Client device 10 which responds with the authentication challenge response 106 encapsulating the digital credentials necessary for access to the multicast service, including an ECDSA signature and the parameters for its verification provided by an SCMS Identification Certificate (ID Cert) for

multicast service, consisting of the public key and the elliptic curve domain parameters. As already specified, AAA Server 40 verifies the signature and the account status to determine whether authorization should be granted to the client device 10. When authorization is granted, AAA Server 40 employs ECIES (Elliptic Curve Integrated Encryption Scheme) 107 to derive a symmetric key using the parameters published in the ID Cert, and then to encrypt the payload of ECIES message 108. The plaintext version of the payload in ECIES message 108 encapsulates the keying material required by any and all client devices granted authorization to decrypt multicast messages 110. Client device 10 decrypts the payload of ECIES message 108 by executing ECIES step 109. Different embodiments of AAA Server 40 may use different algorithms for symmetric encryption/decryption of the payloads of multicast messages 110.

[085] The services advertised by RSU 30 are preferably administered by AAA Server 40, since it is the AAA Server which is responsible for validation of the subscription accounts associated with the client devices. Furthermore, only the AAA Server 40 is able to map the geo-temporal parameters specified by the business or governmental authority from which the multicast messages originate ("multi-caster"), into a correct selection of RSU target addresses. This process is illustrated in Figure 13. For each instance in which the message content for a particular target geographic area is changed, the multi-caster 300 sends the AAA Server 40 the new message content and geo-temporal parameters, using message 301. AAA Server 40 then executes process 302 to assemble a new set of multicast messages targeted at the appropriate RSUs and schedule their transmission. AAA Server 40 also may change the keying material for encryption of the multicast message payload, delivered using the ECIES mechanism already described, as client devices submit authentication/authorization requests on encountering new RSUs. The result of

these steps of selecting the RSUs, scheduling the transmissions and encrypting the payload, are multicast messages 303.

[086] While the AAA server as described in some exemplary embodiments enable an authority to account for Wireless Access Vehicular Environment service channel bandwidth consumption, the capability provided by the AAA server in some exemplary embodiments may be utilized for other processes, applications, services or the like, for which an OBU and/or one or more user devices associated therewith may have a valid account therefor, or be a subscriber thereto, which requires an SCMS certificate in order to support its authentication. For instance, in the case of traffic signal pre-emption, the authority may validate to a traffic management center responsible for controlling a traffic signal co-located with an RSU, that the authenticated OBU in an approaching vehicle is authorized for priority signaling at the designated intersection. Other exemplary embodiments may include vehicles licensed to operate in lanes dedicated for use only by vehicles of specific vehicle types.

[087] Thus, in some exemplary embodiments, the OBU may be configured to request authentication and authorization from a AAA server, for access to any service subscribed thereby, either on behalf of a neighboring non-DSRC mobile device or for itself.

[088] The individual components shown in outline or designated by blocks in the attached Drawings are all well-known in the injection molding arts, and their specific construction and operation are not critical to the operation or best mode for carrying out the invention.

[089] While the present invention has been described with respect to what is presently considered to be the preferred embodiments, it is to be understood that the invention is not limited to the disclosed embodiments. To the contrary, the invention is intended to cover various modifications and equivalent arrangements included within the scope of the appended claims. The

scope of the following claims is to be accorded the broadest interpretation so as to encompass all such modifications and equivalent structures and functions.

[090] CLAUSES:

[091] Exemplary embodiments as described herein, including RSU's, OBUs, AAA servers and/or client or remote devices, are described in the following clauses:

1. An AAA server operated by, or on behalf of a Dedicated Short-Range Communications infrastructure authority, transmitting messages among and between On-board Units (OBU) and Roadside Units (RSU), said AAA server comprising at least one processor running at least one computer program adapted to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, with a plurality of RSUs, in order to carry out the functions of Authentication, Authorization and Accounting (AAA), enabling the authority to account for Wireless Access Vehicular Environment service channel bandwidth consumption by each of said user devices having been duly provisioned by said AAA server.
2. An AAA server operated by, or on behalf of a Dedicated Short-Range Communications infrastructure authority, transmitting messages among and between On-board Units (OBU) and Roadside Units (RSU), said AAA server comprising at least one processor running at least one computer program adapted to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, with a plurality of RSUs, in order to carry out the functions of Authentication, Authorization and Accounting (AAA), enabling the authority to authenticate said user devices and/or said

OBU, and to authorize said user devices and/or said OBU for access to any service subscribed thereby.

3. An AAA server as defined in any of the preceding or following clauses, configured as a Certificate Management Entity and operable to issue Internet Subscription digital certificates for IPv6-addressable user devices and to transmit said certificates to said user devices over a secure communications channel, said certificates including the domain name of said AAA server.
4. An AAA server as defined in any of the preceding or following clauses, linked to a PKI chain of trust between components of a Security Credentials and Management System (SCMS), operable to process requests from DSRC OBUs for said digital certificates, said requests encapsulating Personal Identifying Information (PII) for said OBUs and secured by the asymmetrical encryption algorithm specified in IEEE 1609.2, using an enrollment certificate issued to said OBUs by the SCMS and operable to establish said secure communications channel for sending said certificate to said OBU using the encryption key of said enrollment certificate.
5. An AAA server as defined in any of the preceding or following clauses, operable to process requests from non-DSRC mobile devices for said digital certificates, said requests encapsulating PII for said mobile device, each mobile device initiating a handshaking protocol to establish a secure, symmetrically encrypted communications channel with said AAA server.
6. An AAA server as defined in any of the preceding or following clauses, operable to receive combined authorization and authentication requests from OBUs, said requests incorporating credentials in the form of digital signatures generated using keys from said

Internet Subscription certificates issued to said OBUs by said AAA server; operable to receive said combined authorization and authentication requests forwarded from one or more remote AAA servers on behalf of OBUs that have received said Internet Subscription certificates from said remote AAA servers; operable to process requests from both said OBUs and said remote AAA servers by cryptographic validation of the credentials presented correspondingly by said OBUs and said remote AAA servers, for each request querying a non-remote AAA database for a match with PII contained in the request, and returning a message to the requesting OBU or remote AAA, either granting or denying authorization with a code representing a reason for denial.

7. An AAA server as defined in any of the preceding or following clauses, operable to receive authorization requests from said OBUs on behalf of non-DSRC mobile devices, to send UDP/IP authentication challenge messages directly or indirectly to IPv6 address of said non-DSRC mobile devices; to process responses to said authentication challenges which incorporate credentials in the form of digital signatures generated using keys from said Internet Subscription certificates issued to said non-DSRC mobile devices by said AAA server; and operable to receive said authorization requests forwarded from a remote AAA server on behalf of non-DSRC mobile devices that have received Internet Subscription credentials from said AAA server; operable to process said requests from both non-DSRC mobile devices and remote AAA servers by cryptographic validation of the credentials presented, querying the local AAA database for a match with PII contained in the request, and returning a message to the requester either granting or denying authorization with a code explaining the reason for denial.

8. An AAA server as defined in any of the preceding or following clauses, operable, in the case where the domain name of the Certificate Management Entity having issued credentials used by a user device to request authentication and authorization, identifies a remote AAA server, to forward said request to said remote AAA server, using credentials obtained from said SCMS chain of trust to secure communications with said remote server.
9. An AAA server as defined in any of the preceding or following clauses, operable, in the case where the domain name of the Certificate Management Entity having issued the credentials used by a user device to respond to an authentication challenge from said AAA server, identifies a remote AAA server, to forward said request to said remote AAA server, using credentials obtained from said SCMS chain of trust to secure communications with said remote AAA server.
10. An AAA server as defined in any of the preceding or following clauses, operable to use Remotely Triggered Black Hole (RTBH) filtering with internal bBorder Ggateway Protocol to send UPDATE messages to RSUs within a same Autonomous System, said UPDATE messages being triggered by, and encapsulating the results of an authentication and authorization request for Internet Subscription services received from a user device, said results being either the failure to authenticate said mobile device, or the granting or denial of authorization to said user device.
11. An AAA server as defined in any of the preceding or following clauses, wherein, on receipt of an authorization request with SCMS credentials issued for a multicast service, as identified by the PSID encapsulated in the request, ECIES is used to encrypt, and to transmit to the requesting device, the necessary parameters and keying material for

symmetric encryption of the payload of the multicast “push notifications” provided by said multicast service.

12. A Roadside Unit (RSU) configured with an extended IPv6 Management Information Base (MIB) operable to determine packet and byte count statistics for Wireless Access Vehicular Vehicle (WAVE) service channel usage per client device, said client device being either an On-board Unit (OBU), a non-DSRC mobile device that is IPv6-reachable through an OBU, or a DSRC-enabled user device; said IPv6 MIB being also operable to retrieve, for each datagram received from an IPv6 node operating in a route optimization mode of Mobile IPv6, a fixed "home address" of the mobile node carried in the Mobile IPv6 routing header of said datagram; said RSU being operable to accumulate, in Non-volatile Random Access Memory (NOVRAM), said packet and byte count statistics for WAVE service channel usage per client device and periodically to send said statistics to a AAA server, encapsulated in a UDP/IP message, only refreshing said NOVRAM table when the AAA server has acknowledged reception of said UDP/IP message.
13. An RSU as defined in any of the preceding or following clauses, compliant with the USDOT specifications found in http://docplayer.net/11087167-Dsrc-roadside-unit-rsu-specifications-document.html or a functional equivalent thereof.
14. An RSU as defined in any of the preceding or following clauses, operable to process RTBH filtering instructions from a AAA server within a same Autonomous System.
15. A RSU, compliant with the USDOT specifications found in http://docplayer.net/11087167-Dsrc-roadside-unit-rsu-specifications-document.html or a functional equivalent thereof, operable to broadcast Service Announcements (WSAs) which encapsulate the public key

of the Security Credential and Management System (SCMS) enrollment certificate issued to the AAA server operating in the same domain as said RSU.

16. An OBU, compliant with WAVE and IEEE 802.11p and configurable with dual-radio capability, running at least one application level computer program adapted to request authentication and authorization from a AAA server, for IPv6 connectivity to the Internet, either on behalf of a neighboring non-DSRC mobile device or for itself, and configured with an extended IPv6 MIB operable to retrieve the addresses of neighboring devices when a new entry is inserted in a routing table, using either a synchronous method based on SNMP GET to retrieve the routing table periodically, or an asynchronous method based on SNMP TRAP to report "real-time" changes in the routing table.
17. An OBU, compliant with WAVE and IEEE 802.11p and configurable with dual-radio capability, running at least one application level computer program adapted to request authentication and authorization from a AAA server, for access to any service subscribed thereby, either on behalf of a neighboring non-DSRC mobile device or for itself, and configured with an extended IPv6 MIB operable to retrieve the addresses of neighboring devices when a new entry is inserted in a routing table, using either a synchronous method based on SNMP GET to retrieve the routing table periodically, or an asynchronous method based on SNMP TRAP to report "real-time" changes in the routing table.
18. An OBU, as defined in any of the preceding or following clauses, operable to request "Internet Subscription" credentials from a AAA server, using its SCMS enrollment certificate from encryption of the request to, and decryption of the response from, said AAA server, and operable to use said credentials when requesting authentication and authorization from said AAA server for said IPv6 connectivity to the Internet.

19. An OBU as defined in any of the preceding or following clauses, wherein, following transmission of an authorization request with SCMS credentials issued for a multicast service, as identified by the PSID encapsulated in the request, ECIES decryption is used to decrypt ECIES-encrypted parameters and keying material necessary for symmetric decryption of a payload of multicast "push notifications" provided by said multicast service.

20. A mobile device, configured to communicate with an OBU for IPv6 connectivity to the Internet, as defined in any of the preceding or following clauses, wherein, following transmission of an authorization request with SCMS credentials issued for a multicast service, as identified by the PSID encapsulated in the request, ECIES decryption is used to decrypt ECIES-encrypted parameters and keying material necessary for symmetric decryption of a payload of multicast "push notifications" provided by said multicast service.

21. A system facilitating communication between and among On-board Units (OBU) and Roadside Units (RSU) utilizing Dedicated Short-Range Communications (DSRC) to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, said system comprising a server transmitting messages among and between the OBU and the RSU, said server comprising at least one processor running at least one computer program adapted to authenticate the user device, authorize the user device to have access to Wireless Access Vehicular Environment (WAVE) service channels, and account for bandwidth consumption by each of said user devices having been duly authenticated and authorized by said AAA server.

22. A system as defined in any of the preceding clauses, comprising a plurality of servers operated by, or on behalf of a Dedicated Short-Range Communications (DSRC) infrastructure authority.

23. A system defined in any of the preceding clauses.

[092] The present disclosure, clauses, claims and figures are to be considered to support any claim reciting any element, feature, structure, function, and/or step, of any aspect and/or exemplary embodiment described in the present disclosure including the figures, clauses and/or claims herein, either alone or combined with any one or more elements, features, structures, functions, and/or steps from the same or any other aspects or exemplary embodiments described in the present disclosure including the figures, clauses and/or claims herein.

[093] The following references are herein incorporated by reference:

[094] WAVE: IEEE WIRELESS ACCESS IN VEHICULAR ENVIRONMENTS (WAVE) - IEEE 1609 SERIES, available at http://www.techstreet.com/standards/ieee-wireless-access-in-vehicular-environments-wave-ieee-1609-series?sid=goog&gclid=Clbc_ZfFxs0CFQ6naQodjolKlg&product_id=1893147.

[095] IEEE 802.11p: IEEE STANDARD 802.11p-2010 - IEEE Standard for Information technology- Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments, available at: https://standards.ieee.org/findstds/standard/802.11p-2010.html

[096] US Patent Application 14/151,035, available at http://www.google.com/patents/US20140195102

[097] SCMS Vehicle-to-Vehicle Security Credential Management System; Request for Information, A Notice by the National Highway Traffic Safety Administration on 10/15/2014, available at http://federalregister.gov/a/2014-24482

[098] Request For Comments (RFC) 4861 (Neighbor Discovery for IPv6) September 2007, available at https://tools.ietf.org/html/rfc4861

[099] RFC 4862 (Stateless Address Autoconfiguration) September 2007, available at https://tools.ietf.org/html/rfc4862

[0100] RFC 6275 (Mobility Support in IPv6) July 2011, available at https://tools.ietf.org/html/rfc6275

[0101] RFC 5635 (Remote Triggered Black Hole Filtering) August 2009, available at https://tools.ietf.org/html/rfc5635

[0102] RFC 4271 (Border Gateway Protocol 4) January 2006, available at https://tools.ietf.org/html/rfc4271

[0103] RFC 4291 (IPv6 Addressing Architecture) February 2006, available at https://tools.ietf.org/html/rfc4291

[0104] V2V Readiness Report DOT HS 812 014 August 2014. Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application, available at http://docplayer.net/13180-Dot-hs-812-014-august-2014-vehicle-to-vehicle-communications-readiness-of-v2v-technology-for-application.html

[0105] All U.S. patents and patent applications discussed above, as well as all articles, documents, papers, specifications, etc., referenced above are hereby incorporated by reference herein.

What is claimed is:

1. A Roadside Unit (RSU) configured with an extended IPv6 Management Information Base (MIB) operable to determine packet and byte count statistics for usage per client device, said client device being either an On-board Unit (OBU), a non-DSRC mobile device that is IPv6-reachable through an OBU, or a DSRC-enabled user device; said IPv6 MIB being also operable to retrieve, for each datagram received from an IPv6 node operating in a route optimization mode of Mobile IPv6, a fixed "home address" of the mobile node carried in the Mobile IPv6 routing header of said datagram; said RSU being operable to accumulate, in Non-volatile Random Access Memory (NOVRAM), said packet and byte count statistics for usage per client device and periodically to send said statistics to a AAA server, encapsulated in a UDP/IP message, only refreshing said NOVRAM table when the AAA server has acknowledged reception of said UDP/IP message.

2. An RSU as defined in claim 1, compliant with the USDOT specifications found in http://docplayer.net/11087167-Dsrc-roadside-unit-rsu-specifications-document.html or a functional equivalent thereof.

3. An RSU as defined in claim 1 or claim 2, operable to process RTBH filtering instructions from a AAA server within a same Autonomous System.

4. An RSU, compliant with the USDOT specifications found in http://docplayer.net/11087167-Dsrc-roadside-unit-rsu-specifications-document.html or a functional equivalent thereof, operable to broadcast Service Announcements (WSAs) which encapsulate the public key of the Security Credential and Management System (SCMS) enrollment certificate identification certificate or other certifying credential issued to the AAA server operating in the same domain as said RSU.

5. An OBU, compliant with WAVE and configurable with dual-radio capability, running at least one application level computer program adapted to request authentication and authorization from a AAA server, for IPv6 connectivity to the Internet, either on behalf of a neighboring non-DSRC mobile device or for itself, and configured with an extended IPv6 MIB operable to retrieve the addresses of neighboring devices when a new entry is inserted in a routing table, using either a synchronous method based on SNMP GET to retrieve the routing table periodically, or an asynchronous method based on SNMP TRAP to report "real-time" changes in the routing table.

6. An OBU, compliant with WAVE and configurable with dual-radio capability, running at least one application level computer program adapted to request authentication and authorization from a AAA server, for access to any service subscribed thereby.

7. An OBU, as defined in claim 6, operable to request authentication and authorization from a AAA server on behalf of a neighboring non-DSRC mobile device and configured with an extended IPv6 MIB operable to retrieve the addresses of neighboring devices when a new entry is inserted in a routing table, using either a synchronous method based on SNMP GET to retrieve the routing table periodically, or an asynchronous method based on SNMP TRAP to report "real-time" changes in the routing table.

8. An OBU as defined in claim 5 or claim 6, operable to request "Internet Subscription" credentials from a AAA server, using its SCMS enrollment certificate, an identification certificate or other certifying credential to digitally sign the request to said AAA server, said request including the public key of said enrollment certificate, identification certificate or other certifying credential, which enables said AAA server to encrypt the response, and operable

to use said credentials when requesting authentication and authorization from said AAA server for said IPv6 connectivity to the Internet.

9. An OBU as defined in any of claims 5 to 7, wherein, following transmission of an authorization request with SCMS credentials issued for a multicast service, as identified by the PSID encapsulated in the request, ECIES decryption is used to decrypt ECIES-encrypted parameters and keying material necessary for symmetric decryption of a payload of multicast "push notifications" provided by said multicast service.

10. A mobile device, configured to communicate with an OBU for IPv6 connectivity to the Internet, as defined in any of the claims 5-9, wherein, following transmission of an authorization request with SCMS credentials issued for a multicast service, as identified by the PSID encapsulated in the request, ECIES decryption is used to decrypt ECIES-encrypted parameters and keying material necessary for symmetric decryption of a payload of multicast "push notifications" provided by said multicast service.

11. A system facilitating communication between and among On-board Units (OBU) and Roadside Units (RSU) utilizing Dedicated Short-Range Communications (DSRC) to communicate through the Internet with a plurality of user devices and/or an OBU operating a subnet for one or more user devices, said system comprising:

a server transmitting messages among and between the OBU and the RSU, said server comprising at least one processor running at least one computer program adapted to authenticate the user device, authorize the user device to have access to Wireless Access Vehicular Environment (WAVE) channels, and account for bandwidth consumption by each of said user devices having been duly authenticated and authorized by said AAA server.

12. A system as defined in claim 11, comprising a plurality of servers operated by, or on behalf of a Dedicated Short-Range Communications (DSRC) infrastructure authority.

13. A system comprising an RSU, an OBU and/or a mobile device as defined in any of claims 1 to 9.