Machine-to-Machine (M2M) Communications in Vehicular Networks

M.J. Booysen[1], J.S. Gilmore[1], S. Zeadally[2], and G.-J.van Rooyen[1]
[1]*MIH Media Lab, Dept. of Electrical and Electronic Engineering, Stellenbosch University, Stellenbosch, 7600, South Africa*
[E-mail: {1, jgilmore,gvrooyen}@sun.ac.za]
[2]*Department of Computer Science and Information Technology, University of the District of Columbia, Washington, DC 2008, USA*
[E-mail:szeadally@udc.edu]

Abstract

To address the need for autonomous control of remote and distributed mobile systems, Machine-to-Machine (M2M) communications are rapidly gaining attention from both academia and industry. M2M communications have recently been deployed in smart grid, home networking, health care, and vehicular networking environments. This paper focuses on M2M communications in the vehicular networking context and investigates areas where M2M principles can improve vehicular networking. Since connected vehicles are essentially a network of machines that are communicating, preferably autonomously, vehicular networks can benefit a lot from M2M communications support. The M2M paradigm enhances vehicular networking by supporting large-scale deployment of devices, cross-platform networking, autonomous monitoring and control, visualization of the system and measurements, and security. We also present some of the challenges that still need to be addressed to fully enable M2M support in the vehicular networking environment. Of these, component standardization and data security management are considered to be the most significant challenges.

Keywords: *M2M, VANET, Protocol, Networking, Security*

Notes.

DOI: 10.3837/tiis.0000.00.000

1. Introduction

When two electronic systems communicate autonomously, that is to say without human intervention, the process is described as Machine-to-Machine (M2M) communications. The main goal of M2M communications is to enable the sharing of information between electronic systems autonomously [1] [2]. Due to the emergence and rapid adoption of wireless technologies, the ubiquity of electronic control systems, and the increasing complexity of software systems, wireless M2M has been attracting a lot of attention from industry and academia [3] [4] [5].

M2M communications include wired communications, but recent interest has focused on wireless M2M communications [4] [6]. Moreover, the number of wireless devices (not including mobile phones) which operate without human interaction (e.g. weather stations, electricity meters, point of sales devices), is expected to grow to 1.5 billion by 2014 [7]. Recent research efforts on M2M communications have investigated areas that include network energy efficiency and green networking, the tradeoff between device power consumption and device intelligence or processing power, standardization of communications, data aggregation and bandwidth, privacy and security, and network scalability [3] [4] [6] [7] [8].

Although "M2M architecture" can technically refer to any number of machines communicating (e.g. based on the fairly broad definition given by the European Telecommunications Standards Institute, ETSI), it is generally accepted that M2M principles apply particularly well to networks where a large number of machines is used, even up to the 1.5 billion wireless devices of the future. This means that when an M2M application is discussed, it is generally presented on a national or global scale with a multitude of sensors that are centrally coordinated. Consequently, when we evaluate a vehicular network as a type of M2M architecture, this evaluation is done for a large-scale network that potentially has many other devices connected to it, some of which may not be related to vehicular networks.

In this work we explore how vehicular networks can leverage the M2M paradigm to support vehicular communications. We present a brief overview of some of the most recent application areas of M2M, namely smart grid technology, home networking, health care, and vehicular networking. The M2M network communication layers in a vehicular network are then explored. We identify five fundamental M2M concepts that have been reported in the literature to address vehicular communication challenges, such as the support for large-scale deployment of devices, cross-platform networking, autonomous monitoring and control, visualization of the system, and security.

The remainder of the paper is organized as follows. Section 2 presents a generic M2M architecture and describes some application areas where M2M support is being used. Section 3 presents the communication layers for vehicular networks and describes how these layers map to the generic architecture presented in section 2. In section 4, we discuss specific M2M design issues that need to be taken into consideration for future M2M-based vehicular networks. Section 5 presents some M2M challenges that still need to be addressed to enable vehicular networks to reap the benefits of M2M support. We make some concluding remarks in section 6.

2. A Generic M2M Architecture and M2M Application Areas

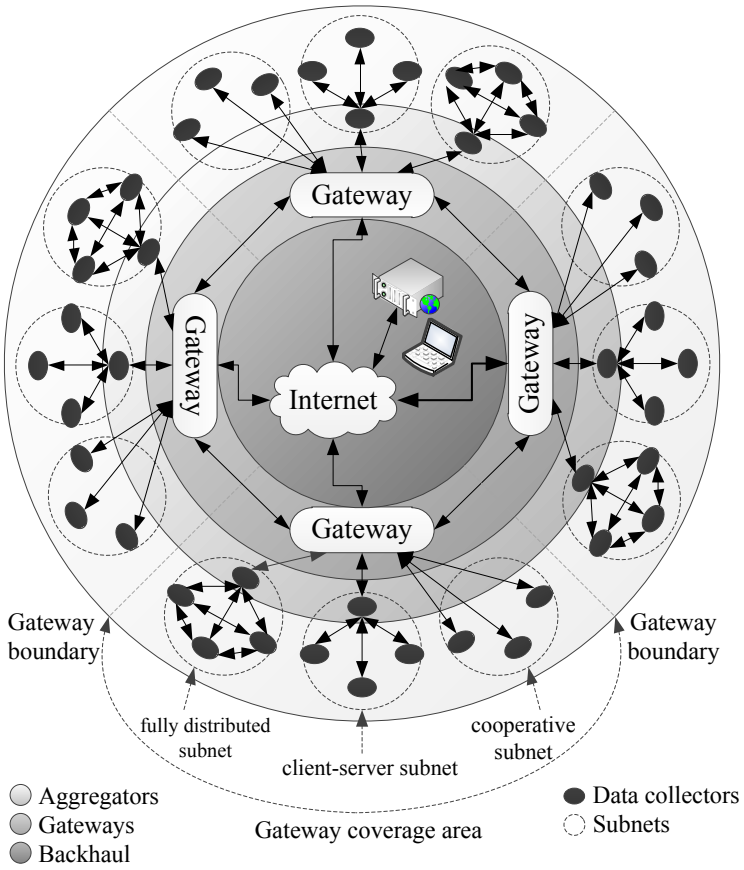

Figure 1.Generic M2M communication architecture.

A generic M2M communication architecture is shown in Figure 1. To support the high number of M2M devices (billions to trillions) that are expected to be part of an M2M network, hierarchical communication architectures have been proposed [4]. At the highest level, the goal of M2M architectures is to aggregate information from data collectors, and to apply some decision-making function to this information to produce decisions which are then executed. Several data collectors (e.g. temperature sensors, location sensors or heart rate monitors) are used to collect information from multiple locations. Data collectors gather data in areas that are small compared to the total area covered by the M2M architecture. The data collectors are usually separated in physical space and can collect information from various types of sources. For example, one data collector could record the ambient temperature in one location, and another could record the current consumed by a television set in another distant physical location.

In M2M architectures, data collectors of the same type are connected to small networks (e.g. Body Area Networks (BANs), Zigbee, and Bluetooth), called subnets. Each subnet uses a network technology appropriate for the type of information to be collected and distributed.

The network technology which is employed determines the subnet architecture. Three types of subnets (fully distributed, client-server and cooperative) are shown in Figure 1. In a *fully distributed* network, all nodes (e.g. various computers on a home Wi-Fi network) are connected as peers and share data amongst themselves. One of the nodes (e.g. a router's Wi-Fi module) acts as a super-peer that has the ability to connect through some gateway (e.g. a router's ADSL connection) to the Internet. In a *client-server* network, all clients only communicate with the server; an example would be portable media players connecting to a media server. The server then relays appropriate information to other clients (e.g. wireless speakers). The server also has the ability to connect to the Internet through some gateway (e.g. a home router). A *cooperative network* is not, strictly speaking, a subnet. None of the nodes (e.g. BAN sensors) communicate directly with each other as is the case on a subnet, but rather via the gateway (e.g. a cellular phone).

The collected data is then aggregated at possibly multiple layers of aggregation points. The number of aggregation layers depends on the expected number of M2M devices and how these devices are logically grouped. At each aggregation layer, data from multiple data collectors can be aggregated by applying some intelligence to the data. This means that the aggregation function is not merely assembling the data, but it can also reduce the amount of data retransmitted. This can be achieved, for example, through filtering data based on relevance, or by extracting higher-level information from aggregated data. Data aggregation is used to allow M2M devices to have low cost, consume little power and have a limited operating area. This is required to enable a system of billions to trillions of these devices.

Multiple local subnets using different communication standards can communicate with each other using some gateway which provides Internet connectivity or a similar backhaul network. The gateway typically interfaces with at least one device on each subnet to which it is connected, and is also connected to other gateways. An end-user can connect to a server to access information collected from the M2M data collectors. This server may be connected to the Internet or some other backhaul network. The function of the M2M server is to perform final processing tasks on the collected data, to store the data, log the transactions that occurred and to make the data available online to the various users of the M2M system.

M2M technology has been deployed in various application areas recently. These include smart power grids, home networking, health care, and vehicular networking. Below, we briefly describe how M2M principles are used to support the selected areas (as depicted in Figure 2 and Figure 3).

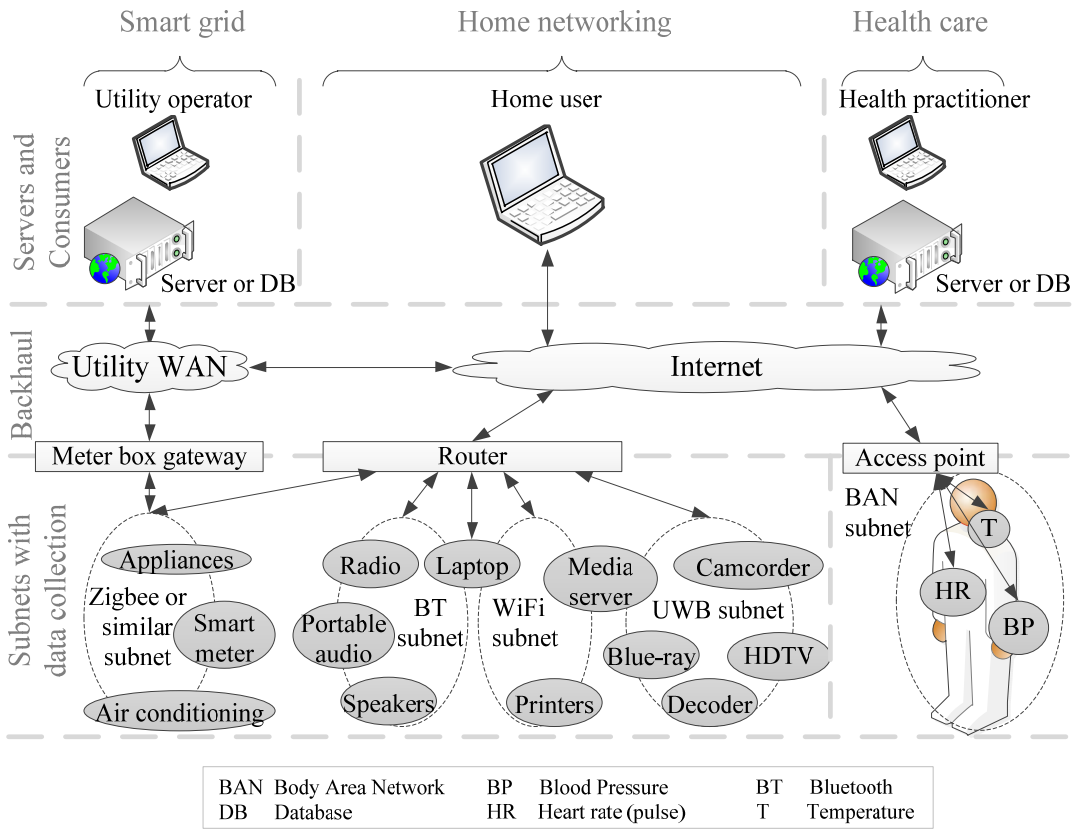

Figure 2 M2M networking applied in smart grid, home networking, and health care.

2.1. Smart Grid

The smart grid is defined as an electrical grid which is specifically designed to improve the efficiency of power transmission, enhance the quality of service to utility users, and to reduce the economic and environmental cost of power generation, distribution and consumption. The smart grid is a combination of a power network and an information network. The distributed nature of an electrical grid, the sensors required to aggregate usage information, and the various tiers of decision making (from home energy management to power generation scheduling) makes M2M principles particularly applicable to the smart grid. For this reason, the smart grid is considered one of the strongest driving forces for M2M communications [1].

In the smart grid, all devices in every home monitor their power consumption, aggregate the data and send it to the servers of the power utility. Multiple aggregators exist in the smart grid. One aggregator is present in each home to aggregate home device data and to optimize local electrical power consumption. Neighborhood aggregators can also exist to aggregate data from multiple homes. After neighborhood aggregators send their collected data to the power utility servers, the power utility company knows how much and when power is consumed by each house and which devices are consuming the power. This allows the utility company to preemptively increase power production to meet transient power requirements, turn off devices that are putting too much strain on the network, monitor the health of all devices in the power network and to improve billing for power usage [7].

2.2. Home Networking

The main purpose of home networking is media distribution, but home networking can also include elements of the smart grid as described earlier. Media distribution systems include media storage (media server), media transportation (Wi-Fi, Bluetooth, Ultra-WideBand (UWB) and media consumption (High Definition TeleVision (HDTV), smart phones, tablet computers, desktop computers). Home networking is currently receiving significant attention as an M2M network [4]. A home network is composed of various smaller home device sub-networks. Each sub-network can contain an aggregator that in turn connects to the Internet gateway (router). Examples of such sub-networks are Zigbee sub-networks (electrical appliances, air conditioner), Wi-Fi sub-networks (laptop, printer, and media server), UWB sub-networks (HDTV, camcorder), smart grid sub-networks (smart meters, smart thermostat, smart switch), body area sub-network (smart phone, monitoring instrument, body sensors) and Bluetooth sub-network (music center, portable audio player) [9]. Possible aggregators include a cellular phone for the BAN subnet and power meters for the smart grid subnet.

Devices exist in the home that can be connected to the Internet to provide extra services to consumers. One example where the M2M paradigm might be employed is where a fridge in a home forms part of an M2M network. The fridge is able to collect data about the number and state of items that it contains, for example the number of eggs that remain and the amount of milk a container has. Many fridges can then be connected, via the Internet and their respective home routers, to report on stock numbers and states. The reporting can be done to a grocery store chain, which can run a dispatch chain that will replenish food items in all the houses that it oversees.

2.3. Health Care

Health care M2M networks are sub-networks within home networks. They are used to monitor peoples' health and inform those being monitored, as well as possibly their doctors, of any abnormal conditions that might occur. Data collectors in a health care network are body sensors to monitor various measures of good health, including blood pressure, temperature, heart rate, and cholesterol. Body sensors are connected to an on-person gateway, such as a smart phone, which also acts as the aggregator for all data collectors. Sensors send data to the smart phone which sends data over the Internet to health monitoring servers. Applications run on the servers that monitor the health of patients.

The M2M paradigm allows for the health of an entire population to be monitored in real time. Ambulances can be immediately dispatched to accident scenes and patients can be monitored at their homes just as effectively as in hospitals. A patient's doctor can also immediately be informed if her patient suffers a heart attack, for example. Health care M2M can also help to track the progression of a virus outbreak by monitoring specific symptoms of the population. Patients that are suspected of being infected by the epidemic can be notified to seek medical care.

2.4. Vehicular Networks

Several research efforts have been investigating M2M communications support for vehicular networks [10] [11] [12]. In a vehicular network, vehicles communicate with other vehicles

(Vehicle-to-Vehicle (V2V)) or with an infrastructure (Vehicle-to-Infrastructure (V2I)). Applications for vehicular networks can be divided into four broad categories, namely safety and collision avoidance, traffic infrastructure management, vehicle telematics, and entertainment services and Internet connectivity [13].

For the most part, previous vehicular network research has focused on point-to-point communications or support for a limited set of vehicles. From a network architecture point of view, this focus constitutes a *bottom-up* approach, where focus is initially placed on developing routing protocols, PHYsical layer (PHY), Medium Access Control (MAC) layer, and broadcasting [13]. M2M networks use centralized and autonomous monitoring, and control of data-collecting devices that are spatially distributed, using a hierarchical *top-down* approach. The M2M paradigm can therefore improve vehicular networks' capacity to support features such as cross-platform networking, autonomous monitoring and control, and visualization of the devices and information in the M2M network. Given the potential that M2M holds for vehicular networks, we focus on M2M communications for vehicular networks in this work.

To explain how vehicular networks are used, and to better understand the benefits of M2M vehicular networks, four application areas for vehicular networking are presented below.

2.4.1. Safety and Collision Avoidance

When driving a non-networked vehicle, a driver makes decisions based only on information within the driver’s Line of Sight (LoS). One of the fundamental reasons for using wireless M2M communication between vehicles is to avoid accidents by overcoming the LoS limitation [13]. In the event of an emergency, information from emergency-detecting sensors (such as accelerometers and the braking system) is sent to other vehicles and to the road-side communication infrastructure within its communication range. To avoid an accident or further accidents, emergencies need to be detected and warning notifications need to be delivered fast enough to allow the driver to respond. Since this message transmission needs to occur in as little as tens of milliseconds, a Quality of Service (QoS) guarantee and low latency is paramount for the communication between the notifying vehicle and the multiple receiving vehicles [13]. Since the messages are only a few bytes, convey only the most critical information [14], and are only sent during emergencies, the required bandwidth is low and continuous connections are optional.

2.4.2. Traffic and Infrastructure Management

Road congestion is a common problem faced by many drivers around the world every day. The number of vehicles on many countries' roads has quickly outgrown the ageing infrastructures. The impact of congestion is not limited to personal discomfort. Congestion leads to increased fuel consumption, which in turn increases costs, and increased emissions, which leads to an increase in pollution [15]. Conversely, a better managed and tightly controlled infrastructure improves productivity and reduces costs and pollution. This provides a strong incentive for society to use road infrastructures more efficiently.

Vehicular networking aims to address this need by providing bidirectional M2M connections between vehicles and the infrastructure that conveys traffic information [11]. Four applications that could be based on traffic information are pay-as-you-drive tolling, real-time

management of the transport infrastructure, law enforcement, and planning of transportation infrastructure. The positional information required to enable these applications does not require sample rates of more than once every few seconds due to the slow rate of change for typical driving [16]. Since only time, coordinates, speed, and car identification need to be captured, only a few bytes are required per sample.

2.4.3. Vehicle Telematics

Vehicle telematics is used to monitor and control vehicles remotely, for example to track or manage vehicle fleets, or to recover stolen vehicles. Physical properties of the vehicle are recorded and transmitted to a central coordinating agent. These properties include Global Positioning System (GPS) information, internal engine parameters such as engine temperature, or video captured by an externally mounted camera. Bandwidth requirements are not high when video capture is not required, and second-generation cellular data services (e.g. General Packet Radio Service (GPRS) and Short Messaging Service (SMS)) are sufficient for simple tracking applications. There is, however, a growing trend to support video telematics. Preliminary studies show that image capture and video streaming is possible from a vehicle with access to a high-bandwidth wireless technology such as WiMAX or Wi-Fi [17].

2.4.4. In-car Entertainment and Internet Services

The ubiquity of wireless area networks (e.g. Wi-Fi), cellular broadband networks (e.g. 3rd-Generation (3G) networks) and metropolitan area networks (e.g. WiMAX) makes it possible to reliably deliver online content and entertainment to vehicles. The wireless network requirements are dependent on the application, which can broadly be categorized as:

- static low-bandwidth (e.g. text-based e-mail, news, RSS feeds, social media);
- static high-bandwidth (e.g. Google Street View, Torrent-based file sharing); and
- streaming video and audio, including videoconferencing (e.g. Skype).

Static content is less susceptible to bandwidth fluctuations and in some cases can be tolerant of substantial transfer delays. Streaming content requires steady high bandwidth with quick handover and a large receiving buffer, but the occasional loss of packets is acceptable.

3. M2M Communication Layers in Vehicular Networks

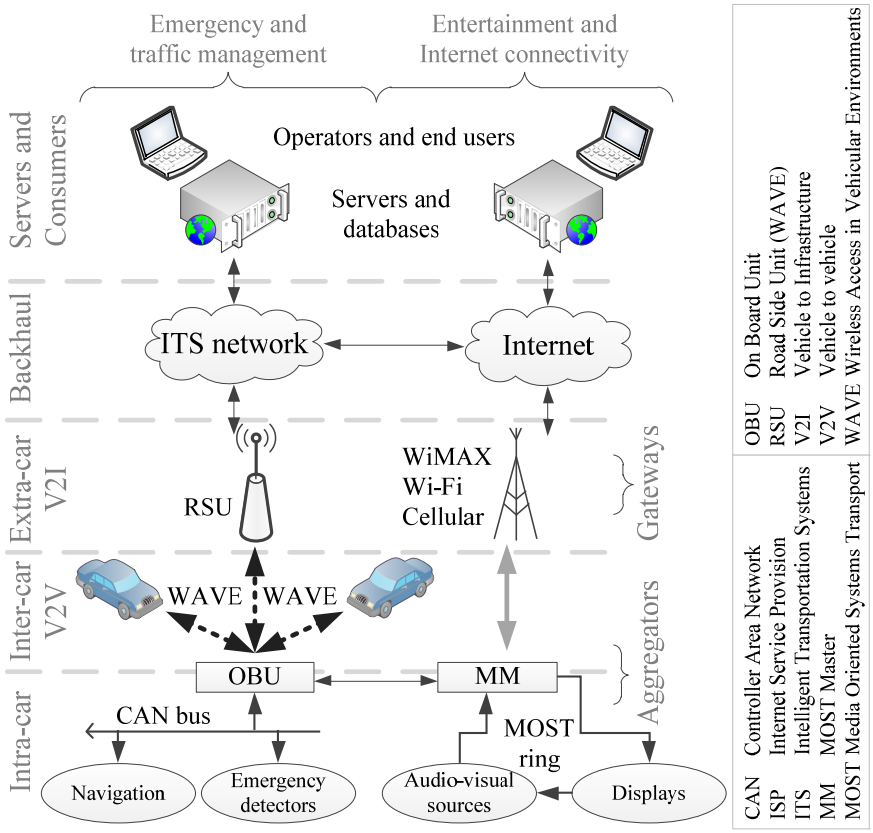

Figure 3 The M2M network architecture in a vehicular context.

Figure 3 shows the M2M network architecture for a vehicular network. Each component in Figure 3 maps to a generic component described in Figure 1.

In a vehicular network, the instruments and sensors in the car are the data collectors. Examples of data collectors are the airbag controller system and the Automatic Braking System (ABS). Communications between instruments in a car is designated as intra-car communications and generally occurs on a wired Controller Area Network (CAN) or fiber-optic Media Oriented Systems Transport (MOST) ring [18]. Non-entertainment components are hosted on the CAN bus and entertainment components are hosted on the MOST ring. An On-Board Unit (OBU) acts as the data aggregator and is connected to the CAN bus. The MOST ring contains a bus master that acts as a media data aggregator.

OBUs of different vehicles connect wirelessly to each other (inter-car) and to RSUs (extra-car) using the Wireless Access in the Vehicular Environment (WAVE) standard, which is the de facto standard for OBU and RSU communications for emergency and traffic management information [19] [20]. The MOST ring master allows media components in the ring to connect to available infrastructure though high-bandwidth wireless technologies (extra-car), such as cellular, WiMAX, and Wi-Fi, to provide video, audio and other entertainment and Internet

connectivity.

The access points of these high-bandwidth wireless technologies and the RSUs act as gateways to the Internet and to an Intelligent Transportation System (ITS) network as backhaul services. ITS networks endeavor to put in place intelligent and cooperative transportation infrastructures that include electronic tolling and traffic monitoring using road-based sensors [21]. The ITS network and the Internet allow all vehicles connected to a gateway to communicate with back-end servers. Although ITS in its broadest sense refers to any communications infrastructure support to transportation networks, this is another use case where the added benefit of applied M2M principles is clear.

Servers and databases connected to the Internet allow end-users to remotely access various services of the vehicular network. The transportation authority or other third party service providers can provide centralized management of the infrastructure and vehicles from servers and databases connected to the ITS network. ITS information can also be uploaded to the Internet to allow wide-spread accessibility for end-users.

Table 1 summarizes the communication areas shown in Figure 3, along with the most popular standards that are currently used in those areas.

Table 1: Popular technologies in vehicular networks

Area	Standard	Description	Ref.
Intra-car (wired)	CAN	The Controller Area Network (CAN) connects the various electronic components of a car, including the display cluster, electronic control unit, accident sensors, GPS and OBU over an electronic wired network. CAN supports high speed transmissions of small amounts of data, which makes it ideally suited for safety applications.	[22] [23]
	MOST	A Media Oriented Systems Transport (MOST) ring is used to connect intra-car media devices. A MOST ring has a high communications cost per node, compared to CAN, but can transmit at higher speeds than CAN (25Mbps compared to 125Kbps).	[24]
V2V and V2I (wireless)	WAVE	The WAVE standard contains a suite of protocols that make up the WAVE communications protocol stack. The WAVE protocol suite contains PHY and MAC layer standards as well as higher level support for IPv6 and the WAVE short message protocol, designed for low-latency transmission of short messages. There are, however, some areas where WAVE is not ideal for V2V communications, such as a short coverage range, the lack of high mobility support, and the lack of support for extreme multipath effects.	[19] [20] [25] [26] [27]
	Wi-Fi	Wi-Fi or IEEE 802.11 is a wireless communications standard that covers a relatively large area (250 m outdoors and 70 m indoors) and is able to transmit at high speeds (54 Mbps for 802.11g to 600 Mbps for 802.11n).	[28] [29] [30]
	WiMAX	WiMAX (IEEE 802.16) covers a much larger area than Wi-Fi (6.5 to 16 km), but at a reduced speed (128 Mbps down and 56 Mbps up). The IEEE 802.16e standard also adds mobility support to WiMAX. The mobility support, high speed and long range makes WiMAX well suited	[31]

		for vehicular communications. A disadvantage of WiMAX is that it is expensive to deploy.	
	Cellular	Cellular data (all 3GPP standards) includes GPRS, Enhanced Data for Global Evolution (EDGE), 3G, High Speed Packet Access (HSPA), Long Term Evolution (LTE) and LTE-Advanced. All these standards have been designed with high mobility and large coverage areas in mind. The latest cellular data standards offer high bandwidth communication capabilities at low latencies. This makes cellular data well suited for media distribution applications. Efforts also exist to add functionality to the 3G standard to allow for ad-hoc operation, which will allow for V2V communications.	[32]

4. M2M Support for Vehicular Networking Environments

Vehicular networks and M2M communications are complementary growing fields of research that have developed independently. However, recent technological trends demonstrate that vehicular communications could significantly benefit from the progress made in M2M communications [16]. The focus of vehicular network research is on the lower layers in the communication stack of point-to-point communications. M2M research focuses on centralized and autonomous monitoring, with a spatially-distributed multitude of devices in a hierarchical network [33] [34] [35] [36] [37].

The working group on communication patterns of the Dagstuhl Seminar recently presented a report evaluating future trends in vehicular communication patterns [38]. This report recognized that vehicular networks are a part of the emerging field of M2M communications research. The group suggested that existing vehicular technologies, such as IEEE 802.11p could also be adapted for the purpose of M2M communications.

In this section we review recent research efforts which have focused on leveraging M2M support to improve communications and information transfer for vehicular networking. A few of the goals of these recent projects are listed in Table 2 to provide some context of the works discussed in the rest of this paper.

Table 2 Literature relevant to M2M and vehicular networking.

Goals of the project	Ref
Greenwood et al. applied an M2M approach to develop a method for real-time road transportation optimization. The goal of the research is to improve transportation time and transportation costs in real-time.	[16]
Kapsalis et al. described an M2M networking platform designed to support real-time monitoring and autonomous control of a vehicle fleet used in the transportation of flammable and dangerous goods.	[10]
Lequerica et al. extended the features introduced by M2M to enable social networking services and media distribution with vehicles as the network nodes.	[11]
In the project from [39], not limited to vehicles, the goal is to provide a complete M2M asset management system through highly visual and embeddable middleware called	[39]

SMART.	
Cha et al. explored ways to ensure trust and security in a vehicular M2M environment.	[12]
Galetić et al. described a generic M2M architecture and presented examples of different M2M architectures. Amongst these examples, the Ericsson CoCar project is presented.	[37]

4.1. M2M Support for Diversity and Multitude of Devices

Due to the number of vehicles on the road (255 million registered vehicles in the USA in 2011 [40]), and the variety of devices present in each, a vehicular network will have to be able to sustain a large number of devices. Moreover, the vehicular network is not fixed in size; it needs to be scalable to adapt to the continuously changing network topology due to the nodes' high mobility [13]. The variety of communications and sensing devices further compounds the challenge for vehicular networks. Since the challenges of multitude and variety of devices and communication standards are a common problem in M2M networks [37], other authors [16] [10] [11] have proposed M2M solutions for vehicular communications. M2M supports diversity and multitude of devices [35] [36] [33] in a vehicular network at the Intra-car level of the network architecture illustrated in Figure 3.

In [16], the problem of multiple devices is addressed with a solution from the M2M paradigm, by using the On-Board Units (OBUs) to aggregate, consolidate and filter measurements from the multiple sensors in a vehicle, including the toll collection units, tachographs, on-board management units, and load-status sensors. The consolidated information is stored in the OBU to be transmitted only when required. The approach effectively reduces the number of devices in the M2M network by substituting the devices in the vehicle with one representative OBU aggregator, which consolidates information from the devices it represents in the vehicular M2M hierarchy.

To address the challenges associated with heterogeneity and the large number of end-user devices and communication buses on which these units reside, the vehicular M2M in [10] connects to the devices through an Object Linking and Embedding (OLE) for Process Control (OPC) server that provides a generic Application Programming Interface (API) to all components. The server is set up to use an extended set of generic Input and Output (IO) channels that are made available for end-user devices. The approach in [10] therefore ensures a generic access method for different devices in the vehicular M2M network, and also simplifies management of a large number of devices through the dedicated server.

To overcome the problems associated with the heterogeneity of communications and sensing devices, to keep devices simple, and to keep device power consumption low, the authors of [11] re-allocate as much as possible of the intelligence traditionally found in the device itself, to higher tiers of the vehicular M2M network. Moreover, applications are executed as remote services on the M2M server, rather than on the device. Software modules are developed to provide standard APIs to the devices, which further support diverse device types. This M2M-based approach facilitates easy software porting between devices, simplifies management across the range of devices, and enables the authors to use a single communication stack to access all devices in the same way.

4.2. M2M Support for Autonomy and System Management

The vehicular networking applications considered in this paper, namely safety and collision avoidance, traffic infrastructure management, and vehicle telematics, require autonomous data collection, aggregation of collected data, transmission and distribution of aggregated data, and storing and reporting of information. Although autonomy is fundamental to vehicular networking applications (for example, it is essential for collision avoidance), autonomy has received little attention in the literature on vehicular networking. System autonomy is one of the distinguishing features of an M2M network [33], and is important in several areas of the vehicular M2M architecture illustrated in Figure 3, including the centralized management system, connectivity, security, and sensing devices. We now investigate how system autonomy can be achieved by exploring recent vehicular M2M networking literature.

The system in [16] applies M2M principles to a vehicular network by implementing rules-based autonomy on all layers of the architecture shown in Figure 3. To autonomously select between available communication connections (cellular, WiMAX or WAVE), the vehicles (nodes) follow a rule-based system that uses information such as the vehicle's location, connection availability and signal strength, transmission cost, and the priority and size of the task to execute (e.g. whether new firmware must be downloaded, or whether GPS location information must be transmitted). The authors hypothesize that this approach could reduce communications costs for vehicles in the network. A similar rule-based Event Control Action (ECA) mechanism is introduced in [10] to support autonomous control of vehicle routes and early detection of critical situations in a vehicular M2M network. These configurable rules are deployed in either the centralized control center or in the vehicles, or in both, to provide adaptable autonomy.

In the vehicle-based M2M network described in [11], social networking information is generated by drivers and other information is automatically logged by the sensing devices in the vehicles. To support autonomous data acquisition and processing by the management software, the vehicles are polled with a data query and the information is stored in the centralized database. The system operator configures reports (traffic flow, road loading, etc.) to be automatically generated periodically. Anomalies (accidents, breakdowns, etc.) are defined by the operator as events, which are automatically flagged, and, more importantly, autonomously distributed to and shared with other vehicles.

4.3. M2M Support for Visualization and Reporting

In a large and complex system which is managed centrally, such as a vehicular network, it is beneficial to simplify visual representation of the entities, make device control easy, and to automate reporting. We describe below how the M2M networking concept supports visualization and reporting for vehicular communications at the Servers and Consumers level of the network architecture illustrated in Figure 3.

To improve the interpretation and visualization of measurements obtained from the wide range of sensing devices and nodes in the vehicular M2M network discussed in [10], a generic visual presentation is used for all devices. This presentation is created with a representative graphical visualization of the vehicle-based sensing devices (e.g. speedometer, OBU, etc.). A user-configurable model is constructed for every type of entity in the vehicular M2M network. For example, a model could be built for a generic airbag system and another model for a

generic wheel pressure gauge. To provide easy interpretation of information, the authors of [39] propose highly visual data models with configurable dials and controls built in. For example, a generic model for a location device (e.g. a GPS navigation device) is built to indicate where the node is on a map, and to plot its speed. When speed control is required for fleet management, this generic model can then be configured for individual vehicles to also plot the speed limit, to report when this limit is exceeded and to control actuators (e.g. an alarm) on the vehicle. The software is built on Google's OpenSocial Applications Programming Interface (API), which can be embedded into a web page to provide ubiquitous access [41] to the vehicle-based devices in the M2M network. Similar approaches are presented in [42] and [43]; however, these works do not provide APIs that can be embedded into a web page, and their visualization tools are not user-configurable, but predefined.

4.4. M2M Support for Cross-platform Networking and Connectivity

Vehicles are mobile by definition and the positional distribution of vehicles is variable. Wireless communications, which is central to vehicular communications, has limited coverage, and a variety of wireless technologies may be required to interoperate. Connectivity, of vehicles to infrastructure and to other vehicles, and cross-platform networking are therefore challenges for vehicular networking environments. A fundamental aspect of M2M communications is the underlying network it uses, and the associated connectivity of remote devices to this network. M2M supports the cross-platform networking and connectivity for vehicular communication at the inter-car and extra-car levels of the network architecture illustrated in Figure 3.

To support virtually ubiquitous backhaul connectivity and location information in a vehicular M2M network, the vehicles described in [10] are equipped with GPRS cellular modems and GPS devices. The CoCar project referenced in [37] investigates the feasibility of using only existing 3rd-Generation (3G) cellular technology in an M2M network, to enable both vehicle-to-vehicle and vehicle-to-infrastructure networks. The project envisions a fully-connected vehicular network, where all vehicles are connected via road infrastructures to support safety and media distribution applications. Cellular communication (HSPA) is also used by SMART in [39]. SMART provides a network-agnostic interface to support devices (without connectivity to the Internet) on any cellular network. To do this, cellular providers were co-opted to make an access point available and host services for the project. The mobile service providers were willing to do this because of the potential data revenue. Coverage of cellular networks is near ubiquitous for the transportation infrastructure, which makes it suited for connectivity in a vehicular M2M network with a distributed multitude of devices.

In [16], an M2M network is used for remote navigation and vehicle-routing by using various mobile-technology modems that include WAVE, Wi-Fi, cellular connections and satellite services. The same connections are used to disseminate routing instructions back to the vehicles. Selection of the appropriate connection is based on the vehicles' location, the local connection availability and signal strength, transmission cost, and the task to be executed.

4.5. M2M Support for Security and Privacy

Many applications envisaged for vehicular networks require secure and private communications [12]. In collision-avoidance applications, for example, data tampering could

be fatal, while privacy is important when considering vehicle tracking and electronic tolling. Security in a VANET can be compromised by four types of attacks: unauthorized access, malicious modification, denial of service, and repudiation [45]. Several conventional approaches have been proposed to protect VANETs against these security attacks; a detailed analysis of the threats and proposed solutions can be found in [46]. The conventional centralized network security model is too rigid and is therefore unsuitable for vehicular M2M architectures. Decentralized and scalable security models are therefore required in a vehicular network, where the components are dispersed and often unguarded [12]. We explain how the M2M concept supports security and privacy for vehicular communications at all levels of the network architecture illustrated in Figure 3. M2M support for security in VANET stems from the strong architectural definition of M2M networks.

In [11], third-party software, called Identity Provider (IdP), runs on the centralized server of the vehicular M2M network. IdP is used to obscure the identity of the drivers in shared information (e.g. location information) and to hide secure information (e.g. bank details) from other users. The software works by requiring every node to sign in to IdP from a remote location in the vehicular network in order to be authenticated. After authentication IdP registers the identity information on a Drive and Share (DaS) server. After the identity registration the vehicle sends encrypted information to the DaS via the M2M network without compromising its own identity.

The authors of [12] evaluate autonomous, remote and semi-autonomous validation and security enforcement in a vehicular M2M framework. Autonomous validation is beneficial because of the ability to establish assurance in a device independent of the network, thus overcoming the problem of unreliable connectivity. The drawback of autonomous validation is the need for the M2M network to keep track of the state of every device, and always keep the security components of the whole network synchronized. Remote validation overcomes the requirement of state awareness, but makes security dependent on network coverage. The vehicular network described in [12], uses semi-autonomous validation. This approach balances device-centric trust and traditional security enforcement by relegating key security functions to the individual vehicles. The vehicular network described in [12] uses an M2M approach to ensure a secure system, based on the concept of a trust boundary. To implement a distributed trust system, every device on the vehicle is equipped with a logically separate entity called the TRust Environment (TRE). The TRE hides sensitive data and software (e.g. encryption functions and keys, TRE identification, security policy functions etc.) from untrusted access. The TRE forms a trust boundary upon a secure boot and is able to communicate this trust to other devices and expand the trust boundary to other devices in the vehicle, and to other vehicles using validation of expected TRE states. Hardware security measures are centered on a Root of Trust (RoT) set of fundamentally trusted functions, which are used to protect the trust anchor and to prevent tampering with it. The RoT secures internal operations of its device and is able to convey sensitive information to external entities. A configurable set of security functions is kept centrally in the M2M network.

5. M2M Challenges and Issues for Vehicular Networking

In this section we discuss some of the remaining challenges that need to be addressed to enable the deployment of M2M-based vehicular networks.

5.1. Diversity and Multitude of Devices

Although progress has been made to overcome problems associated with the broad range of devices in a vehicular M2M network, Lequerica et al. report that more work needs to be done to adequately address technical limitations and cost ineffectiveness of the existing solutions [11]. This concern relates to the rapid rate of change of consumer electronics that must be integrated into vehicular networks, such as smart phones, tablets, and navigation devices.

5.2. Autonomy, System Management, and Applications

Autonomy is required at several layers of the M2M architecture, namely centralized management systems, dynamic connectivity, security, and sensing devices. However, substantial research is still needed to apply M2M autonomy in vehicular networks [10] [16]. For example, Greenwood et al. [16] state that legacy sensing-device and OBU technology have limited processing capability. This limits such devices' ability to be used as autonomous data sources and aggregators in a vehicular M2M networks. They recommend that further research should be undertaken to make vehicular M2M systems more autonomous by including presence-announcing and auto-negotiating features on the OBUs and combining this with RFID technology [16].

Another anticipated M2M-related contribution to vehicular networks, is the use of centralized intelligence to more efficiently share information in the network. The usefulness of inter-vehicular communication is hamstrung by the apparent random behavior of neighboring nodes. A central agent which is in contact with all vehicles, and aware of their locations and headings, could use knowledge of data supply and demand to improve the coordination and management of information transfer among nodes. For example, a centralized agent could use a cellular or WiMAX network to orchestrate inter-vehicle information sharing, which in turn uses Wi-Fi or WAVE technologies.

5.3. Security and Privacy

Innovative solutions are needed to ensure the privacy of drivers and passengers in a vehicular M2M network, especially in applications where vehicles are tracked or driver behavior is monitored (e.g. for fleet management and traffic reporting). Cha et al. [12] highlight other security challenges that relate to the method employed to validate the state of the TRE during autonomous node validation. For example, when using autonomous node validation, the labeling of rogue devices is impossible and remote management is difficult. Also, the network needs to be aware of the maintenance state of every device, which is not practically feasible [12]. Further work needs to be done to address these shortcomings [12].

In [11], Lequerica et al. note that more work needs to be done to address privacy concerns. Users need to be able to set levels of anonymity for different types of shared information. Security in general is also highlighted as a remaining challenge in [10].

6. Conclusion

In this paper we described concepts key to the development of M2M communications systems. We gave a brief overview of four prominent M2M applications, namely health care, home

networking, smart grid, and vehicular networking. We then focused on vehicular networking, introducing an M2M perspective on vehicular communications, and highlighted the specific applications, requirements and protocols relating to M2M-based vehicular networks. To establish where M2M communications could add value to vehicular networks, we provided a thorough survey of research and development projects that intersect both technologies. Five areas were identified: Multiplicity, Autonomy, Connectivity, Visualization and Security.

Finally, we performed an analysis of the remaining challenges faced by vehicular M2M systems. The most significant challenge is the standardization of communication interfaces in a network with exceedingly high mobility and variability of components. Managing security and privacy in such a dynamic network requires further attention.

7. Acknowledgements

We thank the anonymous reviewers for their constructive feedback which greatly helped us to improve the quality and presentation of this paper. This research was partially funded by MIH Holdings through the Media Lab at Stellenbosch University. Sherali Zeadally was partly funded by a District of Columbia NASA Space grant.

8. References

[1] D. Niyato, Lu Xiao, and Wang Ping, "Machine-to-machine communications for home energy management system in smart grid," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 53-59.
Article (CrossRef Link)

[2] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K.D. Johnson, "M2M: From mobile to embedded internet," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 36 – 43, 2011.
Article (CrossRef Link)

[3] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 28 – 35, 2011.
Article (CrossRef Link)

[4] Y. Zhang et al., "Home M2M networks: Architectures, standards, and QoS improvement," *IEEE Communciations Magazine*, vol. 49, no. 4, pp. 44 – 52, 2011.
Article (CrossRef Link)

[5] C.-Y. Chan, "Connected vehicles in a connected world," in *VLSI Technology, Systems and Applications (VLSI-TSA), 2011 International Symposium on* , Hsinchu, Taiwan, 25-27 April 2011 , pp. 1 – 4.
Article (CrossRef Link)

[6] Y. Chen and W. Wang, "Machine-to-Machine Communication in LTE-A," in *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*, Ottawa, ON, Canada, 6 – 9 Sept 2010, pp. 1 – 4.
Article (CrossRef Link)

[7] Z.M. Fadlullah et al., "Toward intelligent machine-to-machine communications in smart grid," *IEEE Communications Magazine*, vol. 49, no. 4, pp. 60-65, 2011.

Article (CrossRef Link)

[8] S.-Y. Lien, K.-C. Chen, and Y. Lin, "Toward ubiquitous massive accesses in 3GPP machine-to-machine communications," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 66 -74, 2011.
Article (CrossRef Link)

[9] M. Starsinic, "System architecture challenges in the home M2M network," in *Applications and Technology Conference (LISAT), 2010 Long Island Systems* , Farmingdale, 2010, pp. 1 – 7.
Article (CrossRef Link)

[10] V. Kapsalis et al., "A networking platform for real-time monitoring and rule-based control of transport fleets and transferred goods," in *Intelligent Transportation Systems (ITSC), 2010 13th International IEEE Conference on* , Madeira Island, Portugal, Sept. 2010, pp. 295 – 300.
Article (CrossRef Link)

[11] I. Lequerica, M. García Longaron, and P.M. Ruiz, "Drive and share: efficient provisioning of social networks in vehicular scenarios," *Communications Magazine, IEEE* , vol. 48, no. 11, pp. 90 – 97, 2010.
Article (CrossRef Link)

[12] I. Cha, Y. Shah, A.U. Schmidt, A. Leicher, and M.V. Meyerstein, "Trust in M2M communication," *Vehicular Technology Magazine, IEEE* , vol. 4, no. 3, pp. 69 – 75, Sept. 2009.
Article (CrossRef Link)

[13] M.J. Booysen, S Zeadally, and G.-J. van Rooyen, "Survey of media access control protocols for," *IET Communications*, vol. 5, no. 11, pp. 1619–1631, 22 July 2011.
Article (CrossRef Link)

[14] K Bilstrup, E. Uhlemann, E.G. Ström, and U. Bilstrup, "On the ability of the 802.11p MAC method and STDMA to support real-time vehicle-to-vehicle communication," *EURASIP Journal on Wireless Communications and Networking*, vol. Vol. 2009, no. Article ID 902414, March 2009.
Article (CrossRef Link)

[15] H. Li, "Calculation of additional pollutant gas emissions and their social cost from transport congestion," in *Mechanic Automation and Control Engineering (MACE), 2011 Second International Conference on* , Inner Mongolia, China , 15-17 July 2011 , pp. 5639 – 5641.
Article (CrossRef Link)

[16] D. Greenwood, C. Dannegger, K. Dorer, and M. Calisti, "Dynamic Dispatching and Transport Optimization – Real-World Experience with Perspectives on Pervasive Technology Integration," in *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on* , Hawaii , 2009, pp. 1 – 9.
Article (CrossRef Link)

[17] M. Aguado, J. Matias, E. Jacob and M. Berbineau, "The WiMAX ASN Network in the V2I scenario," *IEEE 68th Vehicular Technology Conference, 2008*. VTC 2008-Fall., Sept 2008, pp. 1 - 5.
Article (CrossRef Link)

[18] N. Navet, Y. Song, F. Simonot-Lion, and C. Wilwert, "Trends in Automotive Communication Systems," *Proceedings of the IEEE* , vol. 93, no. 6, pp. 1204 – 1223 ,

June 2005.
Article (CrossRef Link)

[19] IEEE 802.11p, "IEEE Standard for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements, Part 11, Amendment 6: Wireless Access in Vehicular Environments," IEEE Std doi: 10.1109/IEEESTD.2010.5514475, 2010.
Article (CrossRef Link)

[20] IEEE 1609.2, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages," IEEE Std doi:
Article (CrossRef Link).

[21] M.D. Nuri and H.H. Nuri, "Strategy for efficient routing in VANET," in *Information Technology (ITSim), 2010 International Symposium in*, Kuala Lumpur , June 2010, pp. 903 – 908.
Article (CrossRef Link)

[22] ISO 11898, "Road vehicles – Controller area network (CAN)," Internation Organisation for Standardisation, Standard 2007.

[23] ISO 11519, "Road vehicles – Low-speed serial data communication," International Organisation for Standardisation, Standard 1994.
http://dx.doi.org

[24] MOST Cooperation, "MOST Specification [CP/DK]," MOST Cooperation, Karlsruhe, Germany, 2008.

[25] IEEE 1609.3, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services," IEEE Std doi: 10.1109/IEEESTD.2010.5680697, 2010.
Article (CrossRef Link)

[26] IEEE 1609.4, "IEEE Standard for Wireless Access in Vehicular Environments (WAVE)–Multi-channel Operation," IEEE Std doi: 10.1109/IEEESTD.2011.5712769, 2011.
Article (CrossRef Link)

[27] IEEE P1609.1, "IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) – Resource Manager," IEEE Std doi: 10.1109/IEEESTD.2006.246485, 2006.
Article (CrossRef Link)

[28] IEEE 802.11n, "IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirments – Part 11, Amendment 5," IEEE computer society, Standard 2009.

[29] M. Wellens, B. Westphal, and P. Mahonen, "Performance Evaluation of IEEE 8002.11-based WLANs in Vehicular Scenarios," in *IEEE VTC*, Baltimore, USA, 2007, pp. 1167-1171.
Article (CrossRef Link)

[30] C. Chou, C. Li, W. Chien, and K. Lan, "A Feasibility Study on Vehicle-to-Infrastructure Communication: Wi-Fi vs. WiMAX," in *MDM '09 Proceedings of the 2009 Tenth International Conference on Mobile Data Management*, Washington DC, USA, 2009, pp. 397–398.
Article (CrossRef Link)

[31] IEEE 802.16, "IEEE Standard for Local and metropolitan area networks – Part 16: Air

Interface for Broadband Wireless Access Systems," IEEE computer society and the IEEE Microwave Theory and Techniques Society, Standard 2009.
Article (CrossRef Link)

[32] Third Generation Partnership Project 2 (3GPP2). (Accessed 10 Aug 2011) The Third Generation Partnership Project 2. (Accessed: 2 Aug 2011]. http://www.3gpp2.org/

[33] IEEE, "IEEE 802.16p Machine to Machine (M2M) System Requirements Document (SRD)", IEEE, IEEE 802.16p-10/0004 (draft), 2011.

[34] IEEE, "Machine to Machine (M2M) Communications Technical Report," IEEE, IEEE 802.16p-10/0005, 2010.

[35] ETSI, "Machine to Machine Communications (M2M); M2M definitions," ETSI, DTR/M2M-00004 (draft), 2011.

[36] ETSI, "Machine to Machine Communications (M2M); M2M functional architecture," ETSI, TS 102 690 (draft), 2011.

[37] V. Galetić et al., "Basic principles of Machine-to-Machine communication and its impact on telecommunications industry," in *Proceedings of 34th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO*, 2011, pp. 89-94.

[38] C. Casetti et al., "10402 Report – Working Group on Communication Patterns," in *Inter-Vehicular Communication at Dagstuhl Seminar Proceedings*, 2011.

[39] Trinity Telecommunications. (Accessed 2 August 2011) Trinity SMART sense for remotedevice management. [Online].

[40] Research and Innovative Technology Administration (RITA) – U.S. Department of Transportation (US DOT), "National Transportation Statistics," U.S. Department of Transportation (US DOT), 2011.

[41] Open Social. OpenSocial 2.0. (Accessed: 2 Aug 2011). http://opensocial.org

[42] BITX. (Accessed: 2 Aug 2011) BITX for Automotive. [Online]. http://www.bitx.com/sites/bitx.mediagrouptv.com/files/attachments_public/BITX_APPWARE_AUTOMOTIVE_ENG_1.0.pdf

[43] mtelematics. (Accessed: 2 Aug 2011) Next Generation M2M Middleware. [Online]. http://www.mtelematics.com/mtelematics_middleware.php

[44] R. Uzcategui and G. Acosta-Marum, "Wave: A tutorial," *Communications Magazine, IEEE*, vol. 47, no. 5, pp. 126-133, 2009.
Article (CrossRef Link)

[45] M. Al-Qutayri, C. Yeun, F. Al-Hawi, "Security and Privacy of Intelligent VANETs," Chapter 13, *Computational Intelligence and Modern Heuristics,* ISBN 978-953-7619-28-2, InTech, February 2010
Article (CrossRef Link)

[46] J.T. Isaac, S. Zeadally, J.S. Camara, "Security attacks and solutions for vehicular ad hoc networks," *IET Communications*, vol. 4, no. 7, pp. 894 – 903, 2010.
Article (CrossRef Link)

Marthinus J Booysen is currently pursuing a PhD at the MIH Media Lab, and is a Lecturer at the Electrical & Electronic Engineering Department at Stellenbosch University, South Africa. He is a Member of the Institution of Engineering Technology (MIET) and a Chartered Engineer (CEng) at the Engineering Council, UK. He has ten years' experience in the aerospace and automotive industries with companies that include SunSpace, Rolls-Royce, Boeing, BMW, and Jaguar Land Rover.

John S Gilmore obtained his Bachelor's and Master's degrees in Electrical & Electronic Engineering with Computer Science from Stellenbosch University in 2007 and 2010 respectively. He is currently pursuing his PhD at the MIH Media Lab at Stellenbosch University. His research interests include peer-to-peer massively multiuser virtual environments, computer networks, distributed systems and communication protocols.

Sherali Zeadally is an Associate Professor in the Department of Computer Science and Information Technology at the University of the District of Columbia, Washington DC, USA. He currently serves on the editorial boards of over 15 peer-reviewed scholarly journals. He has Guest-edited over 15 special issues of refereed scholarly journals. He is a Fellow of the British Computer Society (FBCS) and a Fellow of the Institution of Engineering Technology (FIET).

Gert-Jan van Rooyen is Senior Lecturer in Telecommunications at Stellenbosch University, and holds a PhD in Electronic Engineering from the same institution. He is the director of the MIH Media Lab, an interdisciplinary research laboratory that focuses on the broad application of emerging communications media. His research interests include software radio, digital signal processing and vehicular networks.