ATHABASCA UNIVERSITY

PRIVATE CARS, PUBLIC CLOUD:
VEHICULAR CLOUD COMPUTING CHALLENGES AND FUTURE

BY

PAUL MAGUIRE

A project submitted in partial fulfillment

of the requirements for the degree of

MASTER OF SCIENCE in INFORMATION SYSTEMS

Athabasca, Alberta

December 2015

DEDICATION

As with every aspect of my life, I dedicate this paper to my children, Erin and Chris, in the hope that they will recognize it as a symbol of determination and perseverance. From this effort, I hope they find inspiration to pursue their own dreams with relentless fervour, and refuse to surrender without challenge when obstacles are encountered. Something given can be valued and simultaneously hold only little worth; something earned can cost little, yet be priceless.

ABSTRACT

From the observation that modern road vehicles are equipped with significant computing capacity that is largely underused came the notion of Vehicular Cloud Computing (VCC). While moving, a cloud of vehicular nodes faces networking challenges to form a cohesive whole from a body of highly volatile component parts. While parked, that cloud must not render the vehicles immobile; their batteries must retain sufficient power to start their motors. Many candidate application areas impose various requirements on VCC. This paper reviews literature that proposes solutions to matters of ensuring security and privacy, effective networking, efficient communications, operational concerns, and motivating participation. On balance, it appears that VCC can, at best, serve niche markets.

ACKOWLEDGEMENTS

The journey that culminates with this essay was eased by the excellent support of various individuals from Athabasca University's School of Computing and Information Systems. Over the years, I appreciated the ongoing support from Linda Gray in particular, as well as the rest of the departmental team. In this final effort, the patience and indulgence of my supervisor, Dr. Mahmoud Abaza, was critical to my success. At the end of all, my wife Patricia voiced not a single negative thought over the several years' long pursuit, and offered help and support in every way she could. I cannot imagine another person showing such tolerance. Thank you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I

INTRODUCTION

Statement of purpose

Today's road vehicles are built with significant computing capacity that is largely unused, especially when the vehicles are parked. Vehicular Cloud Computing (VCC) was conceived as a use for that surplus computing power (Eltoweissy, Olariu, & Younis, 2010). By layering a Cloud Computing (CC) architecture on top of Vehicular Ad Hoc Networking (VANET), powerful new opportunities become available. Where VANET offers inter-vehicle communication for shared information, aggregating the vehicular computing resources into a cloud creates computational ability on a larger scale. Suggested application areas include traffic management, asset management and third-party value-added infotainment. But VCC is not widely implemented. This paper will assess the state of VCC and factors contributing to, and challenging, its long term viability.

Research problem

Various efforts have contributed to enabling and realizing VCC. Industrial and government involvement in Europe, Asia and North America led to the establishment of the Dedicated Short Range Communication (DSRC) suite of standards for rapid transfer of secure messages between vehicles and the allocation of enabling bandwidth (Morgan, 2010), and the evaluation of safety applications that use it (NHTSA, 2005). Conventional cloud computing has matured and is a commercial reality offered by many large vendors, such as Amazon,

Google and Microsoft. Academic and industrial attention has looked for solutions to various aspects of growing the marriage between VANET and CC into a viable platform.

VCC has been discussed in different forms. One differentiation is between static and dynamic models (Olariu, Eltoweissy, & Younis, 2011). The static VCC model takes advantage of vehicles parked together in a single lot, either for moderate durations such as at a mall or the workplace, or for longer periods such as at an airport (Arif et al., 2012). Dynamic VCC creates a cloud from mobile vehicular resources and must deal with much more volatile networking than static VCC.

In essence, VCC was conceived as a merging of VANET and CC. VANET provides the underlying communication infrastructure. Cloud computing is in effect a new service provided on the VANET framework. Mobile Ad Hoc Networks (MANETs) and Mobile Cloud Computing (MCC) can be seen as precursors to VANET and VCC, or as the superclasses from which VANET and VCC are derived. MANETs were conceived as a network of handheld devices, typically military, decades before the smartphone became commonplace (Hubaux, Gross, Le Boudec, & Vetterli, 2001). In an oversimplified sense, MCC is less volatile and dynamic than VCC, typically with pedestrian nodes rather than vehicular. Indeed, VCC can be seen as the solution to MCC's key problem, which is battery life. Both MCC and VCC are aggregations of mobile devices that form, and then might make use of, a volatile cloud where the node population is in constant flux. The MCC cloud offers potential to undertake computationally intensive efforts such as speech recognition, natural language processing, computer vision and graphics, augmented reality, searching, and data

mining (Satyanarayanan, Bahl, Caceres, & Davies, 2009) (D. Huang, Zhou, Xu, Xing, & Zhong, 2011). The evolution of MANET to a vehicular base was motivated by the notion of enabling traffic-event detection systems (Eltoweissy et al., 2010). With huge financial stakes forecasted for MCC (Perez, 2010), it seems likely there will be significant drive for VCC as well.

Dynamic VCC networks must allow for transient network membership as vehicles will remain in range of each other for limited time. Node mobility inevitably produces network gaps (Bhoi & Khilar, 2015). Effective network establishment and maintenance is critical.

With any public network, security and privacy are major concerns. Cloud computing can increase the risk by placing data outside the corporate domain (Armbrust et al., 2010) (Ren, Wang, & Wang, 2012), which requires extending some trust to a third party provider. With VCC, the cloud provider is no longer a single, third-party entity, but a faceless, nameless amalgamation. Any procedural weakness in anonymizing data for cloud processing becomes increasingly important (Mershad & Artail, 2013). Privacy concerns are more severe in VCC than in conventional CC as cloud data is shared on private sector vehicles, and as the vehicles must be protected against various identity disclosure threats. Securing VCC must address many threat vectors (Yan, Wen, Olariu, & Weigle, 2013).

Even if the technological challenges are overcome, it is unreasonable to assume that car owners will willingly offer their vehicles without sufficient incentive. The cost of the incentive must maintain economic viability for the VCC service. In some cases, self-interest

will sufficiently motivate vehicle owners to participate in creating a network to support traffic remediation efforts (Eltoweissy et al., 2010). Where no direct benefit exists, vehicle owners will require other compensation.

Various challenges have been enumerated in the literature, some more extensively than others. Communications must happen in near real-time. Routing models must address the high network volatility created by nodes that are in motion. Security and privacy are major concerns, sufficient to prevent realization of VCC. Motivating participation has not been studied in depth. Cost of equipment has been discussed, but no business model has been presented that would compare incentive costs with the benefits generated by VCC. Benefits can conceivably be accrued by a third party agency managing the VCC as data centre, and/or by the contributing participants. Consumer psychology must be addressed in order to assess the likelihood of adoption.

Organization of the remaining chapters

The remaining sections of this paper are set out as follows. Chapter II presents a review of pertinent literature, organized so as to identify chief areas of interest. Chapter III offers commentary on those interest areas. Chapter IV offers an analysis and review of remaining issues and challenges. Chapter V draws conclusions about the likely future for VCC.

CHAPTER II

LITERATURE REVIEW

It is clear that today's cars have significant computing power. One 2014 car might be built with 75 sensors and 100 computers running 60 million lines of code (Public Works and Government Services Canada, 2015). Its wireless capabilities offer connection to other devices such as smartphones and tablets (Boutilier, 2015). Connecting and exploiting all these underused resources may prove inevitable.

To more clearly define VCC, it is necessary to look at its component parts. VCC is in essence the addition of a cloud computing application atop a VANET infrastructure. The promise of VANET in application areas such as traffic safety and management, and Intelligent Transportation Systems (ITS), are only strengthened within a VCC environment (Kang, Lee, Jeong, & Park, 2015). In describing VANET services under VCC or discussing various service models, the literature can muddy this characterization. This paper includes VANET and MCC in the VCC discussion because of their close relationships. VANET is an enabling technology for VCC, and VCC is a special case of MCC.

VANETs

VANET was born of a desire to share road safety and traffic congestion information among drivers (Eltoweissy et al., 2010) (Bilal, Bernardos, & Guerrero, 2013). The cooperation between vehicles that creates the conceptual VANET is akin to a sensor network that feeds

some processing mechanism. VANET communications are either Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I). VANETs that are exclusively V2V require that each vehicle draws its own inferences from incoming messages (Eltoweissy et al., 2010) (Ghafoor, Bakar, Mohammed, & Lloret, 2013). V2V computing is local to the vehicle; V2I computing incorporates a controller entity.

VANET has been well supported internationally by government, manufacturers and standards organizations (Eltoweissy et al., 2010). ITS and VANET could lead to a sophisticated computing environment that will support a safer driving experience. Governments supported this development by legislating dedication of bandwidth. The excess bandwidth capacity will entice third party providers to add services beyond the safety model, including entertainment. The only inter-vehicle cooperation in VANET is the sharing of knowledge. In a sensor net environment, VANET assumes no handshaking protocol. Applications would typically broadcast messages (Hartenstein & Laberteaux, 2008).

Cloud computing

Cloud computing can be considered the abstracting of a "large-scale resource provisioning and programming problem" (Nurmi et al., 2009). Cloud computing comprises several delivery models. Infrastructure elements include hardware and systems software, while software elements include applications accessed over a network, typically the Internet (Armbrust et al., 2010). Differentiations are made between low-level infrastructure elements, generally called "Infrastructure-as-a-Service" (IaaS) and higher-level "Platform-as-a-

Service" (PaaS) elements. At the top of the service hierarchy is "Software-as-a-Service" (SaaS). Key defining aspects of CC are the seemingly unlimited capacity, the ability for on-demand provisioning to smart small and grow when needed, and the pay-per-use model. Shared data centre operations through CC led to a decrease in energy, hardware and operations costs by a factor of five to seven. Security and privacy are uniformly considered among the top obstacles to adoption (Ren et al., 2012). Security threats are recognized from inside and outside the cloud. Within the cloud, virtualization is key to isolation of computing environments, but it can't always be successfully achieved (Armbrust et al., 2010). The final security concern is the service provider's unavoidable access to cloud hardware. At this ultimate level, protection might come not from software, but legal repercussions and courtrooms.

Four different CC models are observed. Public clouds are for sale by some third party, private clouds are exclusively internal to some organization, community clouds are owned and operated by some group of organizations based on common benefits, and hybridized clouds combine public and private (Gupta, Seetharaman, & Raj, 2013). VCC further hybridizes, creating a public or private community cloud. The benefit might be not shared, but symbiotic: the various parties to the VC can all realize gains.

VCC Models

VCC builds upon CC in different ways (Yan et al., 2013). VCC can seamlessly extend the consumer's networked experience outside the home. The "infotainment" possibilities

presented by VCC include location-specific services and online gaming. Specific development for the new VCC platform will be necessary to advance these infotainment offerings beyond what is already commonly available through smartphones in order to attract customers. The volatility and dynamism of the nodes add significant networking and security challenges.

VANET's two characteristic communication models, V2I and V2V, contributed to differing early views on Vehicular Clouds. Autonomous Vehicular Clouds (AVC) were conceived as a V2V phenomenon that aggregated autonomous nodes so as to address traffic management and asset management scenarios (Eltoweissy et al., 2010). Vehicular Cloud Computing, first named VC2, was the same product, but with a clearer attachment to its VANET underpinnings (Abuelela & Olariu, 2010). Both describe on-the-fly clouds built on autonomous and mobile nodes, providing both traffic and third party services. AVC's claimed differentiation by virtue of "autonomous cooperation among vehicular resources" (Eltoweissy et al., 2010) does not distinguish it from VC2. AVC was presented as eventually integrating with road-side infrastructure to enhance services. This independence from infrastructure led to the conclusion that a second type of VC called infrastructure-based VC should be identified (Yan et al., 2013). This differentiation offers no real value. Both V2I and V2V features can be considered part of VCC.

The features that distinguish VCC as a subclass of conventional cloud computing are the autonomy and mobility of the nodes (Abuelela & Olariu, 2010). Consequently, VCC node availability is volatile, unlike CC (Ghazizadeh, Mukkamala, & El-Tawab, 2014).

Proprietorship is another distinguishing feature between VCC and conventional CC, and impacts how VCCs operate. Conventional clouds are owned by single organizations, while VCCs are crowd-sourced, with several privately owned nodes belonging to different participants. The ownership perspective affects trust and hinders adoption. Legislative requirements such as *Sarbanes-Oxley* and *Health and Human Services Health Insurance Portability and Accountability Act* (HIPAA) may influence the requirements customers place on the location and protection of their data (Armbrust et al., 2010).

Static VCC models focus on cars parked, either for shorter durations as at a mall or company parking lot, or longer durations as at an airport (Arif et al., 2012) (Abuelela & Olariu, 2010) (Whaiduzzaman, Sookhak, Gani, & Buyya, 2014). At some computing level, power drain will threaten battery capacity in parked vehicles. Adding standard external power supply hardware to maintain vehicular battery charge, coupled with some form of Ethernet wired access, has been proposed as a solution (Arif et al., 2012). Implementation would call for material infrastructure change. Parking lots will require a system to deliver power to individual vehicles. Vehicles will need modification in order to make use of the provided power. Wired networking capability will require modifications for both the parking lot and the vehicles. Significant cost would be incurred in order to create and maintain the environment that could supply the power and network connectivity. Enabling vehicular power recharging could create new data security hazards. As parking lots are not secure physical locations, some form of juice jacking, where shared power and data lines permit data theft, could develop (InfoTransec, 2014) (Lau et al., 2013).

A pseudo-static VCC model exists wherein traffic-bound vehicles form a localized VCC that contributes to solving their own problem (Eltoweissy et al., 2010). The VCC could be used by transit authorities to run simulations that seek improved street traffic routing and signal timings.

VCC is often lauded for offering solutions to traffic management and enhancing road safety (Whaiduzzaman et al., 2014). These features are promised by VANET, without explicit reference to cloud computing as a delivery mechanism. As mentioned above, the V2V VANET solution requires that each vehicle examine messages received from neighbours and calculate appropriate responses. The VCC layer enables calculation at a different, higher level. More sophisticated traffic modeling can be undertaken when using cloud resources, and direction offered to participating vehicles.

It is important to differentiate between VCC as opposed to conventional CC that involves vehicles when the vehicles are not shared computing nodes. A taxonomy has been introduced to label the disparate groups as Vehicular Clouds (VC), where vehicles are computational nodes at the basis of a cloud, and Vehicles using Clouds (VuC), where static infrastructure hardware called Road Side Units (RSUs) becomes gateways to cloud services that are then accessed by vehicles (Hussain, Son, Eun, Kim, & Oh, 2012) (Gu, Zeng, & Guo, 2013). Hybrid Clouds (HC) are a combination of the two, where the vehicles make use of the cloud they are part of – that is, vehicles act as both service provider and consumer. This taxonomy provides clarity when the literature refers to VCC rather loosely, blurring the boundary between VC and VuC. VCs are recognized as divisible into static and dynamic classes. Static

VCs are suitable for Infrastructure-as-a-Service (IaaS) and data storage functions. Dynamic VCs can also offer Network-as-a-Service (NaaS) to neighbouring vehicles, as well as application-level services such as traffic support and infotainment. Hussain et al. specifically exclude Platform-as-a-Service VC offerings, but the case for PaaS is made elsewhere. A cooperating community of VCs creates an information and service bundle that serves as a platform that can be packaged and sold as a PaaS offering (He, Yan, & Xu, 2014). Another perspective holds that components and services such as web and email servers can be configured as PaaS services (Yan, Rawat, & Bista, 2012). Beyond data centre capability, which can be called Computing-as-a-Service (Bhoi & Khilar, 2015), the IaaS layer offers Network-as-a-Service (NaaS), where vehicles can communicate with other vehicles to share connections to external networks, and Storage-as-a-Service (StaaS), which provides extra storage capacity on demand (Bravo-Torres, Ordonez-Morales, Lopez-Nores, Blanco-Fernandez, & Pazos-Arias, 2014). SaaS provides pay-as-you-go access to traffic news, VANET apps, infotainment, P2P, and other Entertainment-as-a-Service or Information-as-a-Service offerings (Bhoi & Khilar, 2015). An overarching perspective looks at services such as NaaS as part of a larger whole that can be called Collaboration-as-a-Service (CaaS) (Mousannif, Khalil, & al Moatassime, 2011) (Arif et al., 2012). Ultimately, these classifications can have fuzzy borders and distinguishing between then might not bring great value (Armbrust et al., 2010). Even when the cloud itself is not vehicle-based, cars can form a contributing sensor net to build a platform ultimately for vehicular use (Bernstein, Vidovic, & Modi, 2010). VehiCloud is a VuC example where the vehicles send waypoint information to infrastructure that uses a cloud architecture layer separate from the vehicles to calculate optimal communication network routing (Qin, Huang, & Zhang, 2012).

Various papers present architectures with an Internet-based cloud, augmented by a local vehicular cloud (Satyanarayanan et al., 2009) (Mario Gerla, 2012) (Fernando, Loke, & Rahayu, 2013). Compared with a strictly Internet-based cloud VuC system, performance gains can be realized when querying a local cloud's large data store for traffic applications. In such a solution, only persistent data would be transferred to the Internet, thereby reducing communication and data costs. Short-lived data is delegated to the mobile cloud. This outlines a hybrid system that uses CC at the Internet level and VCC locally (Mario Gerla, 2012).

VCC has been seen as a network of sensing and communicating computing devices that extend the Internet of Things (IoT) (He et al., 2014), and as a component of a larger ubiquitous computing cloud that provides application level support such as spatio-temporal calendaring (Khalifa, Hassan, & Eltoweissy, 2011).

Motivation for VCC development

VANET offered the promise of improved traffic safety and routing by using shared information gathered from contributing vehicles. Economic benefits were anticipated in saved time, fuel and lives, and reduced environmental impact attributable to traffic, in a wireless environment that would cost less to build and operate than ITS with its significant roadside hardware requirements (C.-L. Huang, Fallah, Sengupta, & Krishnan, 2010). By pooling the computing power of moving vehicles, the identified possible VCC benefits include High-Performance Computing (HPC) ability to solve difficult traffic optimization

problems, coordinate emergency management efforts and augment small business computing ability, while adding entertainment and other value-added applications (Eltoweissy et al., 2010).

Architecture

With VCC, a typical public cloud is built on private vehicles. The vehicles provide private crowd-sourced computing hardware capabilities in exactly the way any provider would offer conventional cloud computing services. Services such as emergency management and traffic remediation that had been suggested for VANET can be improved and offered as VCC services (Olariu et al., 2011).

Prior to the creation of the DSRC standards, a unified V2V and V2I communication system using cellular networks was proposed (Santa, Gómez-Skarmeta, & Sánchez-Artigas, 2008). Cellular costs are higher than other wireless options, but the existing cellular infrastructure offered the opportunity to launch VCC relatively immediately. General Motors announced intentions to add a 4G LTE cellular connection that would be "turning [a car] into a smartphone with four wheels" (Harris, 2013). Several lower-cost communications alternatives, such as DSRC, are available today. It is unlikely that cellular will play a major role in VCC development or deployment, but cellular will likely be part of a contributing suite of communications protocols that includes WiFi, IEEE 802.11p DSRC and Wireless Access in Vehicular Environments (WAVE), and Worldwide Interoperability for Microwave Access (WiMAX) as well (Ghafoor et al., 2013).

VCC will take advantage of allocated wireless bandwidth left unused by VANET traffic applications, and will be built upon the VANET communication infrastructure (Hussain et al., 2012). Stakeholders jointly created the DSRC standard to support wireless network communications (NHTSA, 2005). DSRC allocates 75 MHz of bandwidth, an amount that far exceeds VANET's anticipated need of 10 to 20 MHz (Hartenstein & Laberteaux, 2008). A successful VCC architecture will have sufficient communication throughput capacity, but still must address issues regarding communication, network design and maintenance, security and privacy, and highly mobile nodes.

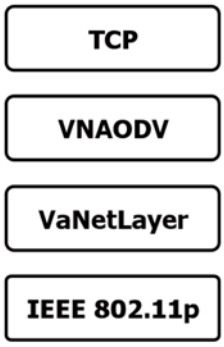

Figure 1 - VaNetLayer protocol stack

The driving notion behind VCC is capitalizing on available excess vehicular computing capacity. Developing a major supportive infrastructure is not only expensive, but not strictly necessary (Ghafoor et al., 2013). While V2V may be the more feasible near term solution, some of the VCC promise will be difficult to deliver until sufficiently inexpensive network access is prevalent. Network-as-a-Service will not be offered for a price below the cost incurred by the source vehicle(s) as profitability will be a driving factor.

Layered network architectures such as the ISO OSI model, or TCP/IP stack, are familiar and popular. Development similar to the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) model (ISO, 1994) is a comfortable first step when devising a new protocol stack. One proposed protocol stack to support NaaS suggests a design derived from OSI (see Figure 1) to build a network of static Virtual Nodes (VNs) able to function with irregular vehicular traffic and packet loss. The design places IEEE 802.11p

at the physical (lowest) layer, VaNetLayer, VNAODV (slightly modified Ad hoc On-demand Distance Vector (AODV) routing algorithm – see (Perkins, Belding-Royer, & Das, 2003)), then TCP at transport layer (Bravo-Torres et al., 2014). VaNetLayer enables virtualization by defining procedures that allow physical nodes (vehicles) to be managed as virtual nodes (VNs) within a defined geographical region. VaNetLayer nominates group leaders that function cooperatively to avoid single point of failure and service bottlenecks. Selected regular non-leader nodes function as backups, able to transition to leaders as needed. VaNetLayer outperforms other vehicle-based approaches in simulated time for downloading. This design creates a static network of VNs for use among a fixed network of third party wireless access points which the authors describe as "increasingly common". Until more wireless access is available, the infrastructure requirement will constrain usefulness and development of any similar design.

V-Cloud claims to be a novel vehicle cloud architecture (Wang, Cho, Lee, & Ma, 2011). The proposed 3-tier architecture has a device layer that incorporates smartphone and vehicular Cyber-Physical Systems, V2V inter-vehicle communications and V2I access to cloud-based services. The physical nature of the cloud and its underlying computing nodes is not discussed, but it is identified as provider of non-specified application services, with one exception. The authors propose a cloud-based system for monitoring driver activity to assess well-being. It is not clear whether the vehicles are cloud nodes, which would be HC, or only consumers, data providers (and sensors), which would be VuC.

There is concern that a traditional layered network architecture like TCP/IP might not perform well enough for VCC. Communication overhead can certainly interfere with timely receipt of real-time information, such as collision avoidance warnings. There is some preference for Service Oriented Architectures (SOAs) and modular, component-based architecture as basis for VCC (Eltoweissy et al., 2010) (He et al., 2014).

Hardware requirements

VCC was born of the realization that increasingly excessive computing capacity was in place already. Much total computing and sensing capacity is assumed. Several major automobile manufacturers have plans to further extend vehicular computational ability. As of 2014, all Ford vehicles include SYNC, its integrated in-vehicle communication and entertainment capability (Ford.ca, 2015) ("Ford Sync," 2015) (Whaiduzzaman et al., 2014). Toyota and Microsoft partnered to turn automobiles into "information terminals", intending to access CC service providers for entertainment, news and vehicle care (Squatriglia, 2011), while also enhancing driver and traffic safety (Gayomali, 2011). General Motors announced an intended "wireless safety net" which is built on Google's Android operating system that would collect data from other vehicles (i.e., V2V) and infrastructure (i.e., V2I) so as to enhance driver safety by providing warnings of possible road hazards (Stone, 2010) (Quick, 2011). Each of these elements is an enabling step toward VCC. Vehicles are already manufactured with various capacities, including sonar, GPS, computer, communications, tamper-proof devices (TPD), event data recorder (EDR), small-scale collision radars, and cameras, in effect

becoming “networked computing centres on wheels” (Whaiduzzaman et al., 2014) (Olariu & Weigle, 2009).

On-board computing must be supported by a CPU that is “virtualizable” (Ghazizadeh, Olariu, Zadeh, & El-Tawab, 2015). Certain traffic applications such as accident reporting may require a tamper-proof EDR that logs vehicle records data for position, speed, time, etc. EDRs are already present in some vehicles, and U.S. legislation to require EDRs in all vehicles may be forthcoming (Abuelela & Olariu, 2010) (“U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety | National Highway Traffic Safety Administration (NHTSA),” 2012). Securing vehicular communication calls for specialized hardware. Although the EDR provides tamper-proof storage, a second, specialist TPD can add cryptographic processing ability (Raya, Papadimitratos, & Hubaux, 2006).

Infrastructure hardware could be needed as VCC moves closer to commonplace reality. Earlier traffic support efforts saw installation of Inductive Loop Detectors (ILDs), y embedding into roadways a piece of hardware that detects passing vehicles, and the very expensive optical fibre that connects ILDs (Eltoweissy et al., 2010). Future development may see corporate placement of wireless access points, possibly reducing the consumer cost for infrastructure (Bravo-Torres et al., 2014) (Sun, Zhang, Zhang, & Fang, 2010).

Network approaches

High vehicular mobility makes connections tenuous and ephemeral, and creates the network gap generation problem and link disruption (Yan, Olariu, & Weigle, 2009) (Bhoi & Khilar, 2015). Fault tolerance is a crucial VCC issue (Ghazizadeh et al., 2015) that must be solved at the underlying VANET level. DSRC's effective range for inter-vehicle communications is limited to about 300m-1000m (Yan et al., 2013). As vehicles go out of range, ongoing network reconfiguration risks consuming large amounts of available communication time. Various efforts to support VCC and mitigate the impact of high node mobility have been documented. A representative sample is presented below.

Various methods have been considered for enabling inter-vehicle communication with sufficiently low latency to serve the public safety needs, and sufficiently low cost so that infotainment and other third-party value-added applications can be delivered on a wide enough scale. Consortia of industry, government and other interested parties outlined Dedicated Short Range Communications, "a two-way short-to-medium-range wireless communications capability that permits very high data transmission" (United States Department of Transportation, 2015) (NHTSA, 2005).

Routing proposals are sometimes built on instantaneous data which fails to adequately consider the duration of proposed communication links. To address this, Yan et al. (Yan et al., 2009) offer a probabilistic multihop path model that estimates link duration based on an assumption that the instantaneous gap between vehicles obeys a log-normal distribution.

VehiCloud uses conventional CC to determine the routing for inter-vehicle communications, a VuC approach (Qin et al., 2012). Vehicular waypoint messages describe vehicle "trajectory", which is used to predict vehicles' future locations. The messages are aggregated and a centralized decision maker can generate optimal network routing. If effective, transitioning from VuC to VC should be considered.

RVCloud is a proposed protocol that uses RSUs to upload vehicle beacon information into an Internet-based cloud which returns the determination of optimal RSU for network formation and maintenance (Bhoi & Khilar, 2015). Although simulation results show better performance than other commercial routing options, cost information is not available. The added architecture to support Internet-based CC suggests increased expense. An underlying premise is limitations of available on-board computing ability restrict vehicular computation of routing information – i.e., that individual vehicles cannot calculate their own optimal routing, and that the external cloud is needed for that purpose. This may underestimate rapid growth of on-board computing ability and the potential of VCC.

Service provision is often governed by Service Level Agreements. For simple services, Quality of Services (QoS) guarantees are fairly straightforward. Compound services are more challenging (Mazloom, Mohadesipour, & Babaei, 2015). The component simple services can be aggregated into a single service tree. Then a QoS for the tree as an atomic element can be determined and delivered efficiently by moving the computing burden from the RSU to an infrastructure-based cloud. It is not unreasonable to speculate that service providers will eventually create more complex offerings, in effect offering as a single service that which

presently can be done only by compounding simple services. The long term impact of compound service QoS support may be minimal. Although the authors trial a Genetic Algorithm approach against a Greedy algorithm, genetic algorithms are processing-intensive and might prove impractical in a real-world environment.

To form a dynamic VC, a network group leader vehicle is first identified according to some strategy. Infrastructure controllers can select among volunteers that may be aspiring service providers. For example, from a candidate pool, it might nominate a vehicle with the lowest mobility relative to neighbouring vehicles in order to maximally prolong cloud and network life (Ghafoor et al., 2013). Alternatively, a broker could be elected from prospective members and tasked with obtaining permission to form a network from an infrastructure-based authority and then inviting candidate vehicle nodes to join (Olariu et al., 2011). Self-appointed managers can also issue a broadcast invitation to prospective group members. In V2V situations, the cell leader can be monitored by peer vehicles that will challenge and blacklist the leader if problems are detected (Yan et al., 2013).

CROWN is a service brokerage model for VCC that employs RSUs as cloud directories with distributed dynamic indexes of servers (Mershad & Artail, 2013). The vehicles volunteer to act as server (called a STAR in this model), specifying to each encountered RSU their offered services and costs. The RSU determines each STAR's "area of influence" based on distance traveled between beacons in order to notify area RSUs and properly inform client vehicles. The authors suggest mobile nodes offer higher network Quality of Service (QoS) than RSUs would, which is defensible as the workload would be spread wider and

connection distance between vehicles might be less than from vehicle to RSU. CROWN includes a manual service inquiry provision that could allow a client to map estimated locations of area service providers and further inquire about each server's offerings, which raises privacy concerns. CROWN was evaluated in simulated testing against the authors' B-CROWN cloud service discovery protocol, which replaces the RSU directory function by having STARs broadcast to neighbouring potential clients that in turn cache-and-forward the STAR service list. Results indicate that traffic conditions are significant determinants regarding which approach will perform better. Certainly under B-CROWN the load is somewhat greater on the various vehicles, and data traffic will be increased. The "Consuming Delay", or elapsed time between sending a service packet and exchanging the first data packet, varies from four seconds in the best of all simulated scenarios to 11 seconds. In both CROWN and B-CROWN, the client specifies certain requested parameters, such as maximum delay and minimum access bandwidth. The simulation's randomness for request generation might not model real-world behaviour particularly well. A random choice from a set of logical parameter configurations consistent with real-world vehicle capabilities, rather than randomly selecting on each parameter, should be considerably more realistic. The simulation would be more interesting if negotiation on price were incorporated in service brokerage.

Security

Wireless communications offer convenience at the cost of increased exposure. VCC risks leakage of vehicular sensor information and personal information belonging to the vehicle's

occupants. As financial information may be exchanged between provider and consumer, the risk becomes more serious (Kang et al., 2015).

Depending on the nature of the specific VC, information may or may not need to be concealed. Messages supporting a public service cloud that advises on traffic alternatives can be left unencrypted, although the sender will need to be authenticated before the information is deemed reliable. The secure exchange of information between two parties in a VC requires that the vehicle owner's information remains private, as should data belonging to customers who use the VCC resources (Abuelela & Olariu, 2010). This requires that the source of information can be trusted and that a message in transit will arrive unmodified (Hartenstein & Laberteaux, 2008).

VCC calls for a two-tiered security approach (Hussain et al., 2012). At the network communications level, it is necessary to guarantee the successful exchange of data. The transmission must be private and free from interference from malefactors. Identification of both participants in a communication must be provable. At the application level, cloud operations must be reliable. This is especially true as data can be dispersed among many unknown public sector vehicles. Even for CC, security concerns, sometimes caused by legislative requirements, are among the most common obstacles to adoption (Armbrust et al., 2010).

There are several considerations to address in VCC security. Ongoing network reconfiguration risks consuming large amounts of available connection time. Node mobility

and network dynamism require efficient processes for node authentication (Yan et al., 2013). Key elements also include integrity, confidentiality, privacy, and availability (Raya & Hubaux, 2005) (Sun et al., 2010) (Yan et al., 2013) (Kang et al., 2015) (Whaiduzzaman et al., 2014). Various proposals have been offered. A representative sample is discussed.

Yan et al. (Yan et al., 2013) (Yan et al., 2012) outline security challenges that face VCC, and propose a scheme that addresses several of those challenges. The STRIDE threat model (Microsoft, 2005) is used to identify and categorize security needs. Several concerns specific to VCC are itemized. Although some VC applications will rely on accurate location information, authentication of high mobility nodes using geographical position is difficult. Privacy is ensured through a trusted Pseudonymization Service Center that is charged with assigning temporary pseudonyms to conceal vehicle identification. The argument is offered that security effort should be somewhat proportional to volume of traffic, citing examples such as enhanced police presence at large public gatherings. It is not clear that the security effort per capita increases in this example, nor that some lesser effort at VCC security can be justified by limited traffic. Throttling is offered as a solution to network attacks. By limiting the ability of an attacking node to connect to other nodes, the negative effect of a single problem node can be mitigated. However, that type of solution has shown limited success against large scale Internet botnet attacks. In some circumstances, VCs have higher risk than conventional clouds in that attacker and target can be physically co-located. The malefactor can have proximate access to location and incident records and may attempt to subvert an investigation by erasing information. Trust relationships are supported by a tamper-proof Certificate Authority (CA), which is presumably the local traffic authority. At manufacture,

vehicles receive a key pair that must be periodically renewed. The CA architecture is difficult to manage, in part because key information and Certificate Revocation Lists (CRLs) must migrate between neighbouring authorities in a time-sensitive manner. Aside from performance issues, the CA model also imposes privacy risks. “[T]he problem of privacy in public” (Zimmer, 2005) is encountered because vehicles send out pings with ID, location and speed 10 times per second, and they might be tracked and monitored by their unique identifiers. Other identified challenges include node heterogeneity, which is manageable by imposing minimum hardware requirements for participants in the VCC; scalability; and provision of a single-user interface, which is a relatively straightforward development effort. The authors acknowledge this model cannot guarantee non-repudiation, which is a requirement of some application areas.

In discussing VANET security, Raya et al. point out that VANET safety messages can be transmitted in plaintext as long as the sender can be authenticated (Raya & Hubaux, 2005). Many of the requirements for VANET communications, such as authentication, integrity and privacy, apply equally to VCC. Some, such as non-repudiation, can be less important for VCC. Presuming that the underlying VANET traffic support applications will exist in a VCC environment, two message types (encrypted and unencrypted) can reasonably co-exist in a somewhat more complicated configuration. It becomes necessary to ensure that plaintext VANET messages do not provide a vector through which VCC security, or especially privacy, can be breached. Plaintext messages that can be tracked to an identifiable source could violate privacy. Therefore, anonymity is necessary in all transmissions. VANET support requires near real-time performance for traffic safety applications. This impacts

authentication procedures because verification of a digital signature requires a decryption step for each message. Although it is faster than asymmetric encryption, a symmetric approach requires a handshake to establish a shared key. The efficiency necessary to support VANET's urgent messages suggests the handshake step takes too much time. The authors argue in favour of a Public Key Infrastructure (PKI) under which anonymous key pairs could be established. Public keys could be exchanged in advance, saving time later during decryption. Elliptic Curve Cryptography (ECC) has a shorter key than RSA and is favoured by the authors. However, while ECC performs better for signing messages, RSA is faster at verification. Verification is the more common procedure as some VANET messages are broadcast. The system would be built upon vehicular identification enabled by an Electronic Licence Plate (ELP) or Electronic Chassis Number (ECN). However, PKI will require an infrastructure-based solution that might be expensive and not readily or widely available. In addition, privacy risks are incurred as vehicular information might be retrieved by government agencies without proper authorization.

Sun et al. recognized that certain VANET application scenarios would call for confidentiality (Sun et al., 2010). Their proposed system guarantees authentication, non-repudiation, message integrity, and confidentiality. All communications are anonymized using pseudonyms generated, assigned and periodically replenished by a Regional Transportation Authority (RTA). The proposed infrastructure includes two types of RSU. Regular RSUs are presumed to be operated by third party service providers and provide access to infrastructure and network services. RSUs have no pre-established trust relationship with the RTA. RSUs and vehicles register with RTA and are assigned a key pair. Outsourcing RSUs to corporate

partners could lower costs for initial implementation and operations. Border RSUs are a special case, operated by the RTA and with exclusive responsibility for pseudonym management. Border RSUs are the only infrastructure elements that are aware of the real identity of participating vehicles. The authors identify ID-Based Cryptography (IBC) as a building block for their proposed system, suggesting that the public key can be derived from the pseudonym while avoiding use of a CA. By avoiding PKI certificates for key verification and exchange, computational and communication gains can be achieved. Message verification and session key establishment can be achieved with no interaction beyond issuance and receipt of a single signed message. This is a low overhead solution for dealing with highly dynamic networks of nodes that are frequently new and unknown. Privacy is protected by a role-based authentication system that requires cooperative approval from two authorized parties before identifying information can be retrieved from the infrastructure RSU that issued the pseudonym. A signature-based threshold scheme based on the ∑-protocol for zero knowledge proof provides nonframeability. This approach provides the mechanism to split control over the retrieval of information between two or more authorities, protecting against malfeasance by a corrupt authority. Excessive authentication attempts result in the member's revocation at the group level and notification to RTA, which decides whether to revoke the vehicle's credential. The threshold authentication enables a selective process that permits some low-frequency bad behaviours, such as might happen with malfunctioning hardware, without automatically revoking the offending unit's credentials. This process would without doubt be targeted by malefactors exploring vulnerabilities.

A proposed Service-oriented Security Framework for Vehicular Cloud Computing (VCC-SSF) takes a service-oriented view of VCC (Kang et al., 2015). Its layered architecture includes two application-level service offerings. Accident Management Service provides accident avoidance and reporting functions. Payment Service enables advance, in-vehicle payment for goods and services. The security layer identifies the need for the typical functions, including authentication, message integrity, authorization and privacy protection. Vehicle authentication is handled differently for moving and stationary vehicles. This is justified by allowing only limiting access to Storage-as-a-Service and Computing-as-a-Service capabilities to parked vehicles. VCC-SSF proposes a CA-based, pseudonymized approach, but the differentiation between stationary and moving vehicle authentication procedures is not clarified. Message integrity is ensured using a digital signature under an asymmetric PKI. In-vehicle data is encrypted for protection against malicious outside access using a symmetric key generated using a static, manufacturer-supplied key that is XORed with a randomized temporary key. The short lifetime for this session key should, in general, ensure its sufficiency against attack. The authors do not discuss key exchange between internal systems. Encrypted communications with external infrastructure rely on a pseudonymized vehicular ID, but no explanation is offered to describe the procedure to generate or refresh the pseudonyms. A complex, time-sensitive

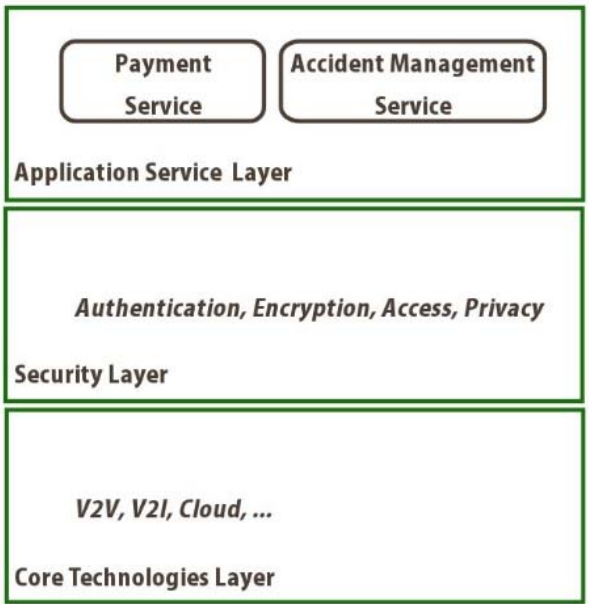

Figure 2 - VCC-SSF architecture

role-based access control system restricts access to vehicular information. For example, it appears that a vehicle's mechanical maintenance might not be possible between midnight and 06:00. Clearly this requires both that the vehicle's clock is tamper-proof, and protection against spoofing of roles.

Of the various issues in successfully implementing cryptographic services within VCC, key management poses the greatest challenge within a Vehicular Public Key Infrastructure (VPKI) (Whaiduzzaman et al., 2014). Assignment, authentication and revocation each present difficulties. Trust between the vehicle and authority are necessary for key assignment because the authority has the information necessary to reveal true identities and will necessarily be secured against inappropriate access. Authentication must achieve service levels that will accommodate security sufficient to protect confidential information, but performance that will adequately serve application needs. Revocation must manage significant lists of expired temporary pseudonymous identification IDs. And the whole system must support inter-jurisdictional communication as vehicles transition between jurisdictions.

VCC-specific issues

VCC inherits security and privacy concerns from its VANET and CC components. It has been suggested that, in addressing VANET and CC security issues, those communities will resolve all or most VCC security issues (Hussain et al., 2012). As conventional CC is a viable commercial product, its security protections have reached some level of acceptance.

Others identify challenges specific to VCs that include tangled identities, establishing trust relationships in a volatile environment, and authentication of high-mobility nodes (Yan et al., 2013). Tangled identities occur when vehicle and driver identities are correlated, which can intrude on driver privacy. Pseudonym management in a high mobility environment is also challenging. Many privacy concerns remain open (D. Huang, Misra, Verma, & Xue, 2011).

Location-based encryption

Security can be enhanced by making message decryption dependent on physical location, with the option to further constrain decryption by time of day as well, through geo-encryption (Scott & Denning, 2003). The vehicle must be location aware. In order to protect against tampering or bypassing the geographic process, encryption / decryption keys are built using the positional information. This also protects against revealing the location of the decrypting vehicle, which is important in the original military context. Depending on location granularity, or the size of the zone within which a message can be decrypted, a brute force attack might have a manageable number of candidate positions to test. The system is built on a static, 3-dimensional (latitude, longitude, time) table of GeoLock keys that are XORed with asymmetric encryption and decryption keys. It is unclear whether the authors allowed for the possibility that the XOR process would weaken the keys. The table's granularity is aligned with the sensitivity of the GPS devices. It is possible to bypass the requirement for a static, preloaded table of coordinates by applying a hashing function to the location information (Yan et al., 2009). The authors also remove the asymmetry from inter-vehicle communications, instead using RSUs to assist with establishment of a symmetric key to be

shared between participating vehicles. Problems with geolocation can arise when GPS reception is weak.

Cloud operational concerns

In an environment where computational nodes have non-guaranteed availability, Refaat et al. argue that Virtual Machine Migration (VMM) is one of the most crucial issues to resolve (Refaat, Kantarci, & Mouftah, 2014). VCC's dynamism and malleable network topology add emphasis to the importance of effective and efficient VMM. The authors consider three models for Vehicular Virtual Machine Migration (VVMM). Simulated tests compared a baseline VVMM-U (Uniform) model with no intelligence for selecting the node to receive a migrated VM against two heuristic models: VVMM-LW (Least Work) selected the least busy network node as recipient, and VVMM-MA (Mobilty Aware) added to VVMM-LW by also considering candidate target vehicles' trajectory – that is, estimated time remaining local to the VC. Both heuristic models performed better than VVMM-U, with VVMM-MA achieving top results. The simulation used a simple traffic grid, considered congestion scenarios and had essentially homogenous nodes. The drop rates, or frequency with which no migration is possible, remained quite high, with a best-case result showing almost 32% of migrations failing to find a target.

In order to manage large processing jobs in the static VCC-as-data-centre model, task scheduling must still address the transient nature of the computing nodes in order to prevent premature job termination when the vehicle leaves the parking lot. Various approaches have

been assessed. One VCC job scheduling approach employs mixed integer linear programming to determine optimal job assignment (Ghazizadeh et al., 2014). Tasks are assigned redundantly to several parallel identical computation nodes. Live transfer of the Virtual Machine from a departing node to another node that remains is minimized. Simulations report optimal or near-optimal results. The simulation is restrictive and presumes identical computational ability at each node, and requires that the duration of computation is known for each job. This deterministic model does not allow for random arrival and departure.

To add fault tolerance, Ghazizadeh et al. introduced a modified checkpointing strategy to VCC task assignment (Ghazizadeh et al., 2015). As checkpointing can incorporate significant overhead, it is minimized. No central checkpoint server is required. Each task is assigned to two randomly selected nodes. If one of the vehicles leaves, a checkpoint is taken and transferred to a third vehicle. The second and third vehicles restart from the checkpoint. Two sets of simulations were undertaken. In the first, vehicles were not able to leave during checkpointing. In the second, departure during checkpointing was permitted, allowing system failures that require job restart from initial state. Simulated results matched analytical results.

A cost minimizing model for task scheduling makes estimates regarding the lifetime of the dynamic vehicle cloud and assigns non-preemptible jobs under the supposition that sufficient time exists to achieve job completion before the cloud dissolves (when vehicles go out of range) (Aminizadeh & Yousefi, 2014). A Binary Integer Programming approach is applied to various constraints to determine the optimal job scheduling strategy. Roadside infrastructure

operates a cloud directory/application repository (CDAR) that manages task allocation. Participating vehicles share trajectory data to help build effective networks. The broker forms a cloud of heterogeneous nodes. No discussion is offered to describe how the cloud/network broker is initiated. Once a task starts, it cannot be migrated to another node. This requires reliable estimates of node availability before assigning a task. The simulation uses Gaussian stochastic rates for various parameters, including node availability (with WAVE-based communications) between 30 minutes and 3 hours. It is unclear whether the simulation randomizations could end up with an unlikely vehicle instance type such as a car with high end computing and low end communication ability. It is also unclear whether modeling considered the possibility that a single vehicle could offer both a more expensive cellular and a less expensive WAVE/DSRC communication channel options, which could affect the cost of services. As communication can be the dominant component of the cost, real-world scenarios will require different service offerings from individual heterogeneous vehicles. Within the imposed constraints, the model does successfully choose lower cost options.

ITS-cloud, a CC model for Intelligent Transportation Systems, considers load balancing as an NP-complete allocation problem (Bitam & Mellouk, 2012). The static ITS-cloud model is conventional CC. The dynamic ITS-cloud model builds a temporary VC. A Bee Algorithm identifies candidate task allocations. Simulated tests found total run time required to complete several tasks in ITS-cloud to be slightly better with conventional CC. Underlying assumptions such as a homogenous task execution time of eight milliseconds, the use of a Manhattan mobility model, and limited node mobility mitigate the applicability of this simulation to real world scenarios. Computational Intelligence approaches such as Bee

Algorithm tend to be computationally expensive and might be impractical in a VCC environment.

Some research models time-varying arrival and departure rates in order to predict parking lot occupancy. Arif et al. propose an architecture that includes a resource manager tasked with, among other duties, predicting resource availability based on stochastic modelling (Arif et al., 2012). This model produced a probability distribution for parking lot occupancy as a function of time. Task assignment and migration is out of their scope. Their simulation outcomes are consistent with empirical results, suggesting their model is viable.

Yu et al. consider resource pricing in a game-theoretical resource allocation model (Yu, Zhang, Gjessing, Xia, & Yang, 2013). Their proposed architecture consists of three cooperating clouds: a V2V VC, an RSU cloud, and a central cloud made of dedicated Internet servers. They offer two customization strategies for the VC. The Generalized Vehicular Cloud Customization (GVCC) adds a central controller responsible for VC creation and management. Under the Specialized Vehicular Cloud Customization (SVCC), VC management responsibilities fall to the vehicles. In the game model, VMs are selfish players trying to obtain all their desired resources. The cloud allocates the resources based on requests. Resource pricing avoids waste. Utility function weighting factors allow for model adaptability. The VM resource allocation game achieves a Nash equilibrium over fast-converging iterations.

CHAPTER III

DISCUSSION

Though a marriage between VANET and MCC, VCC has its own challenges. The representative literature reveals inroads in the major areas, as well as issues that remain outstanding. Security and privacy are paramount in any network that exposes private data to public access. Managing volatility both from a network perspective and as a cloud-supportive platform are major operational challenges. The business case that supports VCC development serves, at best, a small niche market. Motivating participation for service providers, consumers and participants will be difficult for different reasons that are explored below.

Potential VCC uses

VC types can be differentiated into two very broad categories. General purpose VCs are comparable to conventional public clouds. Both represent large scale, on-demand provisioning capability made available to third party consumers. Purpose-built vehicular clouds, or Mission Oriented Mobile Clouds (Mario Gerla, 2012), are more like conventional private clouds. Conventional private clouds are built to serve a single purpose, which is to address the needs of their owners. Similarly, purpose-built VCs are built for some single purpose. Neither conventional private clouds nor purpose-built VCs are sold to third party consumers for ad hoc use. Purpose-built PaaS VCs, such as data collectors and aggregators that form platforms on which various applications can be built, can be considered exceptions. MobEyes was conceived as a purpose-built urban surveillance middleware tool for support of

proactive monitoring applications (Mario Gerla, 2012). Pics-On-Wheels, a purpose-built VC tool similar to MobEyes but with centralized support, provides on-demand surveillance and image sharing capability (M. Gerla, Weng, & Pau, 2013) (Weng, 2013). ITS-Cloud's dynamic model is one of several proposed VCC approaches that supports traffic management. General purpose VCs can serve many needs simultaneously, just as a conventional CC public cloud does. Suggested application areas for general purpose VCs include asset management (Eltoweissy et al., 2010).

The crowd-sourced nature of VCC presents another interesting development opportunity. By layering an open-source cloud computing software framework on top of the crowd-sourced vehicular cloud, the potential for a minimal or zero cost cloud platform becomes real. Eucalyptus is an example of an open-source product that implements IaaS, creating operational control for distributed VM instances (Nurmi et al., 2009). Layered over VCC, Eucalyptus or a similar tool could create a free or low-cost cloud. Not-For-Profit and school organizations are obvious candidate clients for a free or low-cost cloud.

See *APPENDIX A - Anticipated VANET and VCC application areas* for a list of potential VANET and VCC application areas.

Motivation for using VCC

VCC nodes can ultimately be any mobile device with computational ability – chiefly, any vehicle on the road and the portable smart devices therein. It has been suggested that large

organizations have vehicular fleets that might provide private services to their own organizations (Eltoweissy et al., 2010). To provide general purpose services, an infrastructure-based management layer will likely be required. The quickest and most likely model for establishing VCC will see private sector interests develop a framework and provide necessary infrastructure equipment (Eltoweissy et al., 2010). The dynamic, mobile VC will not serve dedicated asset management requirements efficiently. That model will probably require a stationary infrastructure base.

User models should be considered in assessing implementation approaches and the expectation of success in developing VCC. The various VCC proposals indirectly outline different roles for which the following basic taxonomy is offered. The *consumer* can be either public or private sector. Public sector consumers are likely to use services such as infotainment and traffic remediation. Private sector consumers can purchase IaaS functionality, either for in-house use or to provide consumable VCC services. The *service provider* is a middleware tier that aggregates the vehicular computing capabilities and reformats them into a useable cloud. The service provider might package VC services for purchase either as cloud capability (as private cloud) or as cloud-enabled add-on services. The service provider, either governmental or a private sector entity, would provide physical road-side infrastructure elements as well, as anticpated by Eltoweissy et al. (Eltoweissy et al., 2010). And the *participants* are the vehicles and their owner/operators that provide the base computing ability. The participants may or may not have the ability to choose whether they participate, depending on the cloud model. It is conceivable that manufacturers will develop some collaborative platform in which their vehicles automatically participate. It is also

possible that, in some jurisdictions, governmental transportation authorities will mandate participation to support traffic and emergency management applications, or driverless vehicles.

The literature does little to address the willingness of a community to participate in, or take advantage of, VCC. Some assertions are offered regarding the participants' willingness to form a VC. Referring to dynamically synchronizing signals to relieve traffic, Abuelele et al. wrote "[w]e anticipate that the drivers will be only too willing to let the municipality use the computing power of their cars for the public good" (Abuelela & Olariu, 2010). This may be culturally or geographically specific. In some communities and nations, observable acts of public interest are rare. People are unwilling to risk their own privacy. Government-mandated participation might be necessary in order to enable VCC. Others point out that incentive might motivate participation. Eltoweissy et al. wrote "a company may … seek formation of a static AVC by providing appropriate incentives to its employees" (Eltoweissy et al., 2010). Whaiduzzaman et al. wrote "[s]ome vehicle owners may agree to rent out excess on board resources" (Whaiduzzaman et al., 2014). Arif et al. wrote "[i]t is very likely that, given the right incentives, the owner of a vehicle will decide to rent out their on-board capabilities on-demand or on a per-hour or per-day basis" (Arif et al., 2012). It is a certainty that people will rent out excess vehicular computing capacity given the right incentive. The question is whether the right incentive will be cost effective. In busy urban centres, offering valuable free parking in exchange for VCC participation can represent a huge net revenue loss.

Some minimal participation rate is necessary, at least for some applications. NAVOPT, a tool for vehicular navigation, demonstrates the ability to improve traffic flow with only 10% market penetration, and yields near-optimal results at a 40% participation rate (Mario Gerla, 2012) (Kim & Gerla, 2011). The problem will be motivating participation to levels that support both profitability and the applications.

Consumers of public VCC services may be difficult to find unless some consumer need is addressed. Purpose-built clouds that alleviate traffic will be desirable, dependent on price. If the purchase price is participation, vehicle owner/operators may be sufficiently motivated to participate in a VC.

Work has been done to assess the factors that determine the adoption of cloud computing. Some of the material has relevance, or can be projected, to VCC. This is discussed below.

Economic motivational factors

For any product or service, it is important to assess whether there is a reasonable expectation that it can be produced in a cost-effective manner, and whether there will be a consumer, before investing too much. Certainly if profitability is anticipated, service providers will appear.

Various economic benefits of VCC and VANET have been discussed (Abid, Phuong, Wang, Lee, & Qaisar, 2011) (Abuelela & Olariu, 2010). Government and business see value in traffic applications that can support vehicular routing. Safety improvements have the potential to mitigate the estimated billions of dollars spent annually on medical treatment for crash victims. Lost worker productivity can be reduced. Less fuel will be wasted waiting in stalled traffic. VCC can easily circumvent the power constraints on a projected billion dollar MCC industry (Perez, 2010). Cloud computing vendors anticipated and realize profitable operation. Very large economies of scale enable cost reduction by "factors of 5 to 7" for electricity costs, network bandwidth, and other equipment when compared to a traditional data centre (Armbrust et al., 2010). This suggests VCC can offer cost-effective services as well. However, the ability of VCC to enable entertainment and added-value information services might be effectively outpaced by the decreasing costs and increasing services made available by ever faster data communication options. Vehicle manufacturers continue to expand and improve product and service offerings. VCC penetration into the public cloud market will be hampered by marketplace competition from widely available and inexpensive conventional CC (Amazon Web Services, 2015a) (Amazon Web Services, 2015b) (Google Cloud Platform, 2015) (Microsoft Azure, 2015).

Human motivational considerations

Yan et al. observed that VCC offers great benefit to vehicles, especially those that are less well equipped (Yan et al., 2012). The implication is that the greater part of the VCC burden

will be imposed on those who need it less. It cannot be assumed that the wealthy will offer their resources to serve the less financially well off.

The difficulties facing VCC adoption include the same elements that challenged the adoption of conventional cloud computing. Complexity is increased by superimposing a new model on CC, loss of infrastructure control in a crowd-sourced platform, and the uncertainty of high volatility networks. Participants will be concerned about leasing their resources to unknown entities. Consumers will be concerned about placing their data in an unknown vehicle. Even in a trusted car, an unknown mobile device may appear (Fernando et al., 2013). Because customer data goes into the hands of many unknown members of the public, VCC provides a greater data privacy risk. In some circumstances, that data risk would be unacceptable. This suggests that some CC concerns become increasingly important for VCC. Adoption studies can give a perspective on corporate decision making in a CC context, which can be projected to VCC.

Oliveira et al. used a combination of Diffusion of Innovation (DOI) and Technology-Organization-Environment (TOE) models in applying a statistical analysis to a collection of previous studies that examined the determinants of organizational adoption of cloud computing across different industry sectors (Oliveira, Thomas, & Espadanal, 2014). (See *APPENDIX B – Innovation adoption models* for a very brief review of pertinent innovation adoption models.) The work is justified by the overlap between DOI and TOE models, and a persistent call from researchers to better model IT technology adoption by combining multiple perspectives. The study found relative advantage, compatibility, technological

readiness and top management support as positive influencers in innovation adoption, at least in some industries. Manufacturing sectors are less likely than other industries to adopt innovation in certain situations, possibly consistent with membership among late majority or laggard groups. Competitive pressure and regulatory support are not seen to influence innovation adoption. Security matters were not seen to impede adoption of CC, either in the study as a whole or in its subsections. The authors posit that confidence in evolving security and privacy technology and/or faith in regulatory protection explain the lack of concern. However, the regulatory protection that constrains the actions of a single conventional CC service provider will be more difficult to impose upon a community of vehicle owners. Illicit data access is frequently reported in the media. Dozens of known incidents have compromised hundreds of millions of people (Information is Beautiful, 2015). Security can be expected to arise as the major concern in a VCC environment.

Lian et al. undertook a study to discover the factors of major influence regarding adoption of CC technology, specifically in a Taiwanese hospital environment (Lian, Yen, & Wang, 2014). The authors integrated TOE and Human, Organization, Technology-fit (HOT-fit) models to create a framework for this effort. The five areas of greatest influence were determined to be security, technical competence, cost, top management support, and complexity. Technical competence and complexity were deemed important in large part because of the specific Health Care industry application and are therefore not germane to VCC in the general case. The top management support factor is consistent with Oliveira et al. Cost is a driver in all corporate decision making. The authors described security as important not only in the specific Health Industry case, but also in general, which seems to contradict

Oliveira et al. It is conceivable that the supporting data is influenced by cultural factors owing to its Taiwan-centric nature, but it is not known whether this would strengthen or weaken the argument that security is a prime determining consideration when assessing willingness to adopt innovative technology.

Gupta et al. surveyed micro and small businesses, predominantly in Asia-Pacific, to assess the relative importance of several known variables on willingness to adopt cloud computing (Gupta et al., 2013). Their findings showed ease of use to be the most influential factor among micro and small businesses (SMBs, having 1-99 employees) and medium businesses (SMEs, having 100-200 employees). Security and privacy ranked second, followed by cost considerations. Reliability was found to be the fourth most important influencer. However, the authors claim that SMEs do not consider CC to be reliable, and so did not consider reliability in their study. As VCC must be less reliable than CC, this indicates a major roadblock for VCC penetration into the SME market. The fifth determinant was a lack of willingness on the part of SMEs to use cloud technology. The implications of this study for VCC are enhanced by its focus on smaller organizations. In general, VCC seems likely to appeal to smaller organizations as consumers because their computing needs would more easily fit into a smaller “data centre” built on vehicular resources. Larger organizations capable of developing their own private conventional cloud would be less impacted by potential cost savings realized in switching to a commercial cloud service, whether vehicular or conventional.

Making VCC function

For any VCC job, the computing effort required relates inversely to the ideal vehicular dynamism. Consider a private sector organization that uses VCC for its batch processing. In a volatile environment, jobs that run longer will encounter more disruptions. More time will be lost in repeatedly migrating a virtual machine from a departing node to one that remains. This is a low efficiency model. A stationary fleet with less dynamism is better suited to large batch job applications. The dynamic VC is more appropriate for short term jobs such as traffic data collection and processing. Slow moving traffic that will remain local to its area will require fewer VM migrations and can therefore support tasks of intermediate duration.

The challenges of making VCC work have been carefully examined. As a final architecture design has not been established, researchers are challenged to anticipate future decisions. Past developments in consumer technology products have shown that effective marketing is likely to be a contributing factor in determining a successful design. Operational matters define steps necessary to make VCC work. Security matters address securing a working VCC model.

Operations

Although the extreme dynamism of moving traffic creates network topology challenges, the essential high-level operations are unchanged. Dynamic VCC will require effective, near real-time communication between nodes of potentially high mobility. Nodes must be

identifiable and addressable; information exchange must be secure. Node mobility mandates novel approaches that diverge from the static network solutions to these problems.

Static VCC will have to manage power drain on parked vehicles. Power drain must not disable the vehicle's ability to start the motor. Appropriate vehicular sensors and software that monitor and manage power drain could be necessary in the future if static VCC is to be possible.

Task allocation must be appropriate to the network volatility. Refaat et al.'s best case 32% drop rate for VVMM-MA (Refaat et al., 2014) will not support effective VCC. Non-preemptive task allocation approaches are more straightforward simply by avoiding the significant task of migrating the virtual machine. But a non-preemptive approach is inflexible and likely to achieve only limited success in real-world situations. If Aminizadeh et al.'s Binary Integer Programming task allocation algorithm is proven unsuccessful, it cannot be used, as its alternative solution requires impractical compensatory improvement in the communication hardware (Aminizadeh & Yousefi, 2014). VMM is a problem that requires a solution on a scale different than CC, where node location is not volatile.

Concerns at the application level will impose constraints on communication speeds. Accident avoidance solutions must be effective in no more than a few seconds, and possibly faster. Dynamic VCC communications must be efficient; perhaps more than those under a typical OSI model and TCP/IP stack. The Service-Oriented solution may prove more effective.

However, sender authentication will continue to be a security and efficiency problem under any model.

At the vehicle level, computing hardware must be amenable to virtualization. Baseline standards may prove necessary for establishing cooperation among heterogeneous nodes. Basic communication capability will be prime in a list of minimal qualifying criteria. Task allocation can be made appropriate for the available processing power. Older vehicles lacking minimal requirements will be unable to participate in forming or using VCs.

Very little has been written on payment options for VCC. Several sorts of transactions are possible. VCC services can be purchased by entities external to the VC, and vehicles can purchase value-added services that would be delivered through the vehicular network. Services may be exchanged for considerations that are not financial. A secure and fraud-proof model to manage the exchange of value is necessary, whether that value is represented by currency, contra services, credit or some other medium. The exchange system will need to accurately identify parties to a transaction, which may rely on a vehicle ID, driver's license, or some other form of identification.

Vehicular Security

In addition to inter-vehicle communications, vehicles' on-board data must be secured. Hackers will attack whatever opportunity they identify.

Parked cars have less need for the high communications efficiency required by dynamic VCs. Establishment of effective trust relationships will, in all cases, be critical. But parked vehicles have dimished urgency in their communications, and benefit from having familiar neighbours (Eltoweissy et al., 2010). Increasingly durable trust between VC elements is possible when vehicles meet in the same parking lot on a regular basis.

Opinions differ on whether VCCs exacerbate classical security problems sufficiently to create VCC-specific problem subclasses. Integration of two systems to seamlessly produce a third is difficult to achieve perfectly and has the potential to create new exposures. Consequently, although the issues at present appear to be compartmentalized, a dedicated VCC security effort is necessary. In conventional CC, the client trusts a single provider. That trust comes in part from legal protections. However, when building a cloud on a public infrastructure, legal protections will be more difficult to enforce. Therefore, VCC requires a greater trust threshold than CC.

Without knowing which exposures can become major problems, all exploits must be considered serious. VCC presents real world security challenges. The breadth of the exposure vectors is cause for concern. Various vehicular security issues have already been exposed, and, in some cases, exploited. A disgruntled laid-off former employee in Austin, Texas, accessed an add-on hardware feature called WebTech Plus, intended for use as an alternative to repossessing vehicles, to activate dozens of customers' car horns overnight (Poulsen, 2010). The only immediate remedy was to remove the car battery, effectively bricking the vehicle. In a proof-of-concept test, researchers exploited a car's Bluetooth connection and

cellular radio to take control of a vehicle using an app on their Android cellular phone from within the car (Greenberg, 2014). They were able to wirelessly access the car's electronic control unit and override operator commands. In another proof-of-concept test, researchers remotely hacked a 2014 Jeep Cherokee over the Internet (Greenberg, 2015) (Wayland, 2015). Access was gained through an exploit of a vulnerability in the hardware used to connect to networks and through the UConnect infotainment system. The test gained control over engine functions and interior features. This exploit also gained access to vehicle GPS information, enabling remote surveillance.

North American military took interest in the vehicle exploits. USA's Defence Advanced Research Projects Agency (DARPA) gave researchers a grant to explore vehicular vulnerabilities (Greenberg, 2013). Defence Research and Development Canada (DRDC) issued a Request for Proposal (RFP) titled "Cyber Security of Automotive System" to investigate vehicular systems' security to identify exposures (Public Works and Government Services Canada, 2015). The stated intent is defensive (Boutilier, 2015), but the weaponization of remote vehicles might be a side effect of the project. The possibility exists that vehicles will be turned into blunt, guided missiles.

In addition to network-accessible vulnerabilities, smart phones and in-car CDs can also create exposure (Shepardson, 2015). Security measures such as ID numbers and radio frequencies can be altered or bypassed. Vehicular systems like the well-known OnStar rely on built-in cellular capability. This creates a possible exposure. These and other wireless technologies such as Bluetooth make location tracking, in-vehicle eavesdropping, and data

theft possible for a remote hacker (Markoff, 2011). The computerization of vehicles began before widespread wireless vehicular communications abilities were also considered (Pagliery, 2014). Protection against external access was not a priority for a closed box.

The problem grows. The flawed UConnect hardware, for example, could allow a hacker to gain control of several units which would, in turn, scan for still more vehicles to infect, worming its way through a network of vehicles and creating a large-scale botnet (Greenberg, 2015). Because characteristics such as operating system and installed software are exploited by malefactors, vehicular computing nodes might be at greater risk than home computers because manufacturer details are more readily visible to anybody who can see the cars. If all Fords use common systems, a remote wireless attack on Fords can be targeted quickly at roadside or in a parking lot.

Citing studies where hackers were able to gain access to control and geographical position systems, USA legislators introduced a bill to establish federal standards for vehicle security and driver privacy (Shepardson, 2015). In framing their bill, US legislators surveyed 20 vehicle manufacturers. Almost every vehicle sold has some form of wireless communication capacity. But only seven of the respondents hired external security specialists, and only two reported that their vehicles monitor internal data bus traffic for illicit activity (Greenberg, 2015). A key element of the proposed protection mandate would be isolation of vehicle control function from the wirelessly accessible systems.

Systems require security updates and retrofits for protection against malicious access. As is common with many computing devices, vehicles will require data and software updates. Online updates in the form familiar to users of computers and smart phones are one possible delivery method. If a wireless update can not be delivered securely, a manual system and/or some form of vehicle recall will be necessary. To correct the UConnect vulnerability, Fiat-Chrysler issued a major vehicle recall (FCA US LLC, 2015a) (FCA US LLC, 2015b). Uconnect also made a manual software update available to vehicle owners. Software can be downloaded to a USB flash drive and then used to update the vehicle (Uconnect, 2015).

Essentially, VCC security challenges mirror those of any network environment. Private data must be encrypted before transmission, and the receiver must be able to decrypt it. Authentication, authorization and accountability must be managed. VCC-specific issues stem from high node mobility, which creates problems for authentication of moving vehicles, and establishing and managing trust relationships (Yan et al., 2012). With VCC, the consequences are higher. Data and privacy risks as comparable, but, when vehicular control is seized, lives are also at risk.

Securing communications

Securing wireless communications is a well explored field. VCC divergences from routine range from establishment of a trust mechanism that parallels the familiar CA model to authenticating messages so that parties can verify message legitimacy. These elements have been mentioned elsewhere.

Obstacles to VCC realization

Obstacle categories are fairly clearly defined. Chief challenge areas are: network operations, such as network establishment and maintenance in a highly volatile environment; security and privacy strategy creation and establishment, including establishing trust relationships, authentication, authorization, accountability, etc.; infrastructure creation must be financed and managed; market entry and penetration after a competing model has already been successfully established; and motivation of consumers and participants.

Confidence issues will impede VCC implementation. Corporate VCC engagement will be hampered by perceived data risk from putting private data on unattributable third party hardware. This differs from conventional CC where a single provider would be seen as more reliable than the multiple providers in VCC. Reliability is more challenging in VCC than it is in conventional CC. Public awareness of hacking exploits and failures such as the T-Mobile Sidekick server failure that caused loss of personal data (Shiels, 2009) will impede participation of individuals.

VCC might be able to mirror CC's savings in power consumption and network bandwidth. But that comparison also emphasizes that a successful competing model was first to market. Creating a viable product when a successful alternative is already available is a challenge in any industry. Product differentiation is normally necessary in order to compete. VCC's ability to offer something novel appears limited.

The increased complexity of dynamic VCC, coupled with its greater fragility, makes it unlikely to see useful outcomes. However, the power issues inherent in capitalizing on static VCC provide their own challenge.

CHAPTER IV

ANALYSIS OF ISSUES AND CHALLENGES

This paper examines the VCC literature and discusses some of its ramifications. A more quantitative analysis will assist with an evaluation of VCC viability. The underlying premise that excess computing resources exist must be examined. The two VCC classes, dynamic and static, are considered separately. Product viability from a business perspective is also considered.

On viability of dynamic VCC

Dynamic-class VCC creates networks of moving vehicles that are in full operational mode. Onboard computing resources are therefore in use to operate vehicular systems such as fuel injection, exhaust gas control, braking, etc. (Ziegenbein & Hamann, 2015). Without manufacturer-level input, determining whether excess capacity exists would require a thorough mechanical analysis. Such an investigation is beyond the scope of this paper. However, certain assumptions can be made. Vehicle manufacturers design and build to serve some existing need, and, to keep costs low, will not add superfluous capacity in anticipation of a possible future demand. If excess capacity exists, it might be intended as a safety buffer that should not be compromised. Unused capacity at any moment is likely attributable to a momentary resting state for some mechanical component. This is the space in which dynamic VCC must be built.

For each vehicle, some traffic or usage situation will create the maximum demand for its computing resources. If a vehicle is cooperating in a VC when this demand occurs, the VC must be pre-empted by the operating environment in order to satisfy resource demand. Safety authorities are likely to impose certain constraints on the allocation of resources from vehicular operations to external matters. Jurisdictional or practical restrictions may make it infeasible or impossible to allocate resources to VC. The discussion on excess capacity remains speculative without operational information on computational hardware and usage levels.

As self-driving cars become a reality, the availability of excess onboard computing resources seems likely to diminish. It would be dangerous if computing power were unavailable to the vehicle when most needed. The trend toward hybrid and electric cars might also mean fewer vehicles will be able to afford to spend electricity to participate in a VC. The ability to recharge the batteries in an electric vehicle while it is operational is not yet in place. Increasing the power load on an electric car decreases its range.

Dynamic VCs might be possible, but the high network volatility can be exacerbated by a similar volatility at the vehicular level. Each car can contribute, but only its resting state excess capacity. VC processing will be subject to interruption by pressing vehicular concerns. With security, safe vehicular operation is a top concern for dynamic VCC.

On viability of static VCC

Assertions and assumptions have been made on the ability to operate vehicular clouds using parked vehicles with no external power support, for example at a mall or office. An analysis of power requirements and its availability is necessary. Creation of a power infrastructure for parked cars that also supplies wired Ethernet is likely cost-prohibitive and more expensive thaN the benefit.

Scarcity of vehicle manufacturing detail requires certain assumptions. Table 1 shows a summary of assumptions related to assessment of static VC power issues.

Assumptions

# of CPUs per vehicle	50
Battery voltage	12v
Power capacity of typical car battery	60 Ah
Power draw for one conventional CPU (TDP)	40 W
Power draw for one conventional CPU (real - idle)	60 W
Power draw for one conventional CPU (real - peak)	140 W
Power draw for one vehicular CPU/MCU	118 mW
Power demand for engine start	2 kW
Crank time required for engine start	3 s

Table 1 - Assumptions for static VCC power analysis

Several sources speak to the number of computers that operate within a single new vehicle (Pagliery, 2014) (Boutilier, 2015) (Public Works and Government Services Canada, 2015) (PT&C|LWG, 2015). Estimates range from 20 to 100. For illustrative purposes, this paper assumes 50 CPUs per vehicle.

The power supply in most of the vehicles owned by the general public, at least in North America, is 12 volts.

Data on 105 vehicle batteries from three manufacturers shows a range of power storage capacity from 5 to 110 amp-hours (Ah), with an average of 52 Ah and a median 50 Ah. For convenience of calculation and conservativeness of estimate, 60 Ah is assumed as typical. (See *APPENDIX C – Projected power draws and vehicle battery capacity* for information on battery capacity and calculation.)

Data for 873 standard desktop and laptop CPUs were examined. Out-of-service CPUs are included in this analysis as many vehicular applications will not require the performance levels of high-end desktop computers. A processing speed ranging from 56 MHz to 4096 MHz, with an average of 1949 MHz and median of 1946 MHz, was identified. The Thermal Design Power (TDP) ratings for these CPUs ranges from 0.5 watts (W) to 240 W, with average 49 W and median 37 W. TDP is a value used for cooling system design, and refers to maximum heat generated by a CPU under normal loads. Peak CPU power has been estimated at 150% of TDP ("Thermal design power," 2015). As only a portion of the consumed power will be converted to heat (the rest being dedicated to processing), TDP offers a conservative estimate of the total power draw. The W/MHz for these CPUs ranges from 0.0008 to 0.2, with average 0.03 and median 0.02. Intel's Atom processors, designed for energy-efficient use in netbook computers, are the top performers by this metric, with 14 different Atom processors using less than 0.002 W/MHz.

A second study that measured actual power consumption by desktop and laptop CPUs was also considered ("Power Consumption - CPU Charts 2012," 2012). The idle (60 W) and peak (140 W) power draws are also included in Table 1, and are consistent with the data from

APPENDIX D – Power draw for desktop/laptop CPUs.

At 60 W per idle CPU, 50 CPUs consume at least 3000 W. Amperage draw for conventional CPUs is shown in Equation 1.

[1] $$Amps_{CONV} = 3000\,W \div 12\,V = 250\,A$$

[*2* shows that a typical 60 Ah battery can support 50 idle conventional CPUs for fewer than 15 minutes without recharging (showing 14.4 amp minutes). Battery power is insufficient to operate static VCC using desktop or laptop processors.

[2] $$Capacity_{TIME} = 60\,Ah \div 250\,A = 0.24\,Ah = 14.4\,Am$$

It is possible that these CPU numbers are not representative of most of the computing hardware used in consumer vehicles.

Specifications on examples of CPUs used in real-world automotive environments are not readily available in the public domain.

A low-power microcontroller (MCU) offers significant energy savings. Like all processors, typical use often puts a MCU in a sleep or idle state and drawing little power. It reaches

active, or peak, power state only sporadically (Fukuda et al., 2014). Demand on the on-board computing resources is dependent upon how the vehicle is asked to perform.

MCUs designed for low-power consumption are presumed more common for general vehicular operations that require much less computational power. ARM is a supplier that develops and licenses enhanced RISC processors for embedded applications, including automotive ("Cortex-R Series - ARM," 2015). Specifications on a representative sample of ARM processors used in automotive applications is shown in Table 2. The clock frequency,

	Cortex-R4	**Cortex-R5**	**Cortex-R7**
Maximum clock frequency	Above 1.4GHz	Above 1.4GHz	Above 1.5 GHz
Performance (deep sleep/idle/peak)	1.68 / 2.03 / 2.45 DMIPS/MHz	1.67 / 2.02 / 2.45 DMIPS/MHz	2.50 / 2.90 / 3.77 DMIPS/MHz
Efficiency	From 62 DMIPS/mW	From 62 DMIPS/mW	From 46 DMIPS/mW
Peak DMIPS	3512	3512	5405
Peak power draw	57 mW	57 mW	118 mW

Table 2 - ARM processor specs

performance and efficiency are given by the manufacturer. Peak Dhrystone MIPS (DMIPS) is calculated as shown in Equation 3:

[3] $$DMIPS_{PEAK} = Perf_{PEAK} \times 1024 \frac{MHz}{GHz} \times Clock$$

where $DMIPS_{PEAK}$ is the DMIPS at the hypothetical maximum clock frequency; $Perf_{PEAK}$ is the peak performance rating (from Table 2); and *Clock* is the maximum clock frequency (from Table 2). Peak Power Draw is calculated as shown in Equation 4:

[4] $$Power_{PEAK} = \frac{DMIPS_{PEAK}}{Efficiency}$$

where *Efficiency* is provided by the manufacturer. These calculations show MCU peak power draws from 57 mW to 118 mW, orders of magnitude better than traditional desktop and laptop CPUs of comparable clock speed. Among the 13 energy-efficient conventional Atom processors with speeds between 1.5 GHz and 1.7 GHz, TDP ranges from 2 W up to 13 W, with average and median of 5.9 W and 5.5 W, respectively. Actual power draw will be significantly higher than TDP.

With 100 Cortex-R7 processors all operating at their individual peak power draw rating of 118 mW, less than 12 W are required. A typical battery could supply that draw for several hours. Assuming the 12 W demand for a 12 V battery rated at 60 Ah, the required amperage is calculated in Equation 5:

[5] $$Amps\ required\ (A) = \frac{12\ W}{12\ V} = 1\ A$$

A 60 Ah battery can deliver 1 A for 60 hours and can therefore power the 100 on-board MCUs for 60 hours before its charge is depleted.

Examples of extremely high-end components used for 3D rendering in navigational systems are available in promotional and anecdotal form ("Introducing The Tegra X1 Super Chip from NVIDIA," 2015) ("Everything you need to know about Nvidia's new Tegra X1 chip," 2015). The Tegra X1 is an example of a System-on-a-Chip (SoC). It comprises 8 ARM processing cores, a 256-core GPU, and more. Its peak power draw is reported at 10 W. Such super-powered chips will be uncommon among a vehicle's CPU cohort, and reserved for complex, interactive, integrated navigation and infotainment systems. However, at least one should be expected and accommodated. NVIDIA is a niche player in the automotive market, with realized 9-digit revenues and a 10-fold increase scheduled ("US processor company," 2015). Budgets at this level show that the automotive computing market can afford dedication to researching low-power computing. NVIDIA promotes those gains in its advertising, claiming 40% efficiency gains and doubled performance per watt when compared with Tegra K1, NVIDIA's previous offering in this product line ("NVIDIA Tegra X1 Preview & Architecture Analysis," 2015).

Adding a powerful navigation chip such as the NVIDIA Tegra X1, rated at 10 W, roughly doubles the power draw and halves the battery's service time to 33.3 hours, as shown in Equation 6 and Equation 7.

[6] $$Amps_{50\ MCUs+Tegra\ X1} = \frac{12\ W + 10\ W}{12\ V} = 1.8\ A$$

[7] $$Service\ Time_{50\ CPUs+Tegra\ X1} = \frac{60\ Ah}{1.8\ A} = 33.3\ h$$

Even with top tier vehicles carrying as many as 100 MCUs, conservative estimates still show sufficient battery service time to sustain computation for a working day, as shown in Equation 8 and Equation 9.

[8] $$Amps_{100\ CPUs+Tegra\ X1} = \frac{24\ W + 10\ W}{12\ V} = \ 2.8\ A$$

[9] $$Service\ Time_{100\ CPUs+Tegra\ X1} = \frac{60\ Ah}{2.8\ A} = \ 21.4\ h$$

However, a fully depleted battery will not allow the vehicle to start its motor. *APPENDIX E – Car starter ratings* has data on 44 car starters, including the rated power for each. The starters' rated power ranges from 0.7 kW to 2.4 kW, with an average 1.6 kW and a median 1.8 kw. The mode is 2 kW, occurring for 11 of the 44 starters. This value (2 kW) is selected as representative and conservative. Of the remaining 33 starters, 26 have a rated power below 2 kW.

Assuming the vehicle starter will demand 2 kW, it is possible to make an estimate of the power required to start the vehicle. The required amperage is calculated in Equation 10:

[10] $$Amps_{STARTER} = \frac{2000\ W}{12\ V} = 167\ A$$

As Equation 10 shows, the typical starter will draw approximately 167 A. This is consistent with anecdotal reports that suggest starter power draw ranging between 80 and 200 amps ("Starter Motor. Amps?," 2008) ("electricity - Calculating engine starter's energy use - Physics Stack Exchange," 2013). The large amperage is required for only a short time. Usually no more than a few seconds spent cranking an engine are sufficient to start it. The Ah requirement calculation is shown in Equation 11. This assumes 3 seconds cranking time in order to start the engine:

[11] $$Ah_{STARTER} = 167\ A\ \times\ 3\ s \div 3600 \frac{s}{h} = 0.14\ Ah$$

The Ah available will depend on battery health and charge. The engine crank time required for starting is temperature dependent. Even with these constraints, a typical 60 Ah battery supporting a vehicle with a full slate of 100 MCUs on board and 1 high end navigational system SoC will draw about 34 W. That load can be supported longer than the typical office work day or shopping trip. Static VCC is therefore shown to be feasible when built upon parked vehicles with as many as 100 MCUs on board.

Vehicular cohort

Having established that some vehicles have sufficient hardware to support VC, at least in some circumstances, it becomes appropriate to assess the road traffic for sufficient numbers of capable vehicles.

Anecdotal citation of 2001 data survey suggests that almost 40% of the cars on American roads were more than ten years old ("Passenger vehicles in the United States," 2015). In some other nations, vehicles will be older. The target 10%-40% participation rate for successfully enabling traffic routing applications (Kim & Gerla, 2011) will be difficult to achieve in many locations (see Figure 3). A survey of on-road vehicles is necessary as part of the business case that determines when to undertake a VCC development project. Communities with a vehicular population that can support VCC are likely to be more affluent. It has been suggested that developing countries might reap greatest benefit from vehicular clouds (Eltoweissy et al., 2010). It is not apparent that those nations can achieve VCC. Cars cost more than cell phones.

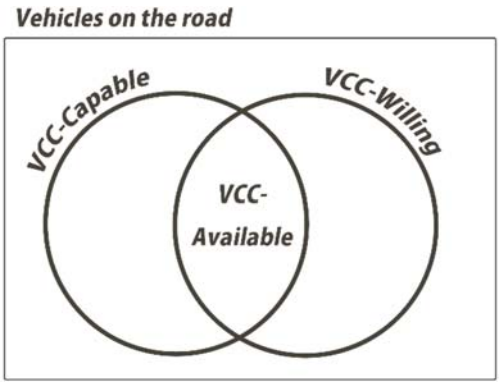

Figure 3 - Vehicular VCC cohort

Proprietorship

Different VCC ownership models are possible. The participants can be privately owned vehicles or proprietary fleet vehicles. Service provider models have more options. Open

source VCs with no clear ownership are possible. The Mozilla model, where open source software is effectively owned by a NFP foundation, is conceivable in VCC. Open source models may experience difficulties financing infrastructure development. Government involvement is possible, and, in cases such as accident surveillance and reporting, may be necessary. Transportation authorities can provide RSUs that serve as the root of a trust system. Private sector involvement is certain if profitability is anticipated. It is conceivable that vehicle manufacturers will extend their current products and services, creating a VCC infrastructure beyond the cellular connections used by in-vehicle systems like OnStar. Any of a number of major technology companies, from customer-centric companies like Apple, Microsoft and Google to major hardware firms such as Hitachi, Samsung and Toshiba, might get involved. The most likely third party involvement in infrastructure development is from existing communications companies and ISPs because they have industry experience and already build wireless networks that might be extended. It is likely that application services will operate on top of the new communication infrastructure, whoever builds it. In other words, the communication service will be separate from the application services, and will be developed by different organizations. The car will be like a smart phone: the cellular or WiFi connection will be supplied by a communication company; and the apps by various vendors. The VC will enable some applications, and can be the mechanism for application delivery in some cases where vehicle communications are shared between cars.

Support from manufacturers and government has already been established and is evidenced by the various consortia that have worked to develop VCC communication standards such as DSRC (Ghafoor et al., 2013).

Manufacturers are building increasing capability into the vehicles that can support VCC, often in partnership with major IT companies. Ford SYNC offers cloud based services ("Ford Sync," 2015); Microsoft and Toyota partnered to use cloud services to inform vehicles (Squatriglia, 2011) while also creating safer traffic environments and providing enhanced protection for drivers (Gayomali, 2011); GM is using Google's Android O/S to collect information from surrounding vehicles and infrastructure to enable advanced hazard warning (Stone, 2010) (Quick, 2011). These VuC manufacturer models create the groundwork for evolution to VCC, which would lower the infrastructure demands and accelerate inter-vehicle communication.

On feasibility and business case

Practical considerations still need to be addressed. First, it must be possible to protect battery charge to ensure engine start. VC participation must be opt-in, at least for parked vehicles. And it should be location-specific, or a car parked at home might be co-opted into a VC without the owner's knowledge, possibly draining battery reserves. Second, vehicles will require a supportive VCC software control layer that accesses the computing hardware and communicates with the VC. Manufacturers must use virtualizable computation units or the onboard resources will not be able to participate in a VC. A mechanism within each vehicle's VCC layer to enable inter-vehicle VC coordination and cooperation is necessary. The communication channels exist already, but a software layer must enable the VCC process in each car.

It is possible that battery life may be detrimentally affected by VC participation. Frequent short drives are known to deplete batteries without properly recharging, and have been identified as a cause for shorter battery life. This will be exacerbated with participation in either static or dynamic VCs.

Traffic VCs are among the most likely application areas for dynamic VCC. But traffic applications must compete with other offerings such as traffic-aware GPS. Google Maps is readily available on smart devices and incorporates Waze, a leading crowd-sourced tool for traffic and navigation support ("Free Community-based Mapping, Traffic & Navigation App," 2015). Audi, for example, already incorporates Google Maps into their on-board navigation system ("Audi connect® Help & Support | Audi USA," 2015). Each manufacturer's dedication to profit will see them pursue their own independent solutions. However, some commitment to a common operating system for automotive control systems ("OSEK VDX Portal - Home," 2015) might indicate a willingness to work together on some issues, such as enabling VCC.

Static VCC power issues have been largely satisfied. In parking lots that are private property, infrastructure will be pursued by private sector entities. The well-defined geographical space will reduce VCC infrastructure costs. Motivation of participants and consumers remains a challenge. Enabling software is still must be provided.

Dynamic VCC differs from conventional CC in that the multi-tasking CPUs are burdened with a purpose that takes precedence over all cloud operations. Virtualization procedures

must be altered to ensure primacy of vehicular operations. Use of resting state capacity may be possible, but may be fragmented by the vehicle's demands. Participation of vehicular nodes will not participate as robust or reliable as dedicated conventional CC servers. Public exposure of wireless transmissions, placing private data in public hands, and protection against unwanted access are major issues that must be resolved.

CHAPTER V

CONCLUSIONS AND RECOMMENDATIONS

Today's vehicles appear to have the computing power and battery reserves to start the engine after operating a vehicular cloud while parked outside the office for the working day, or at the mall while drivers shop. The power draw on operational vehicles is low enough that a VC is feasible, but it will be subject to interruption so that vehicular operations can be sustained. The primary remaining obstacles are security, network mobility, infrastructure, motivation, and operational factors.

Security for wireless VCs must protect cloud data from inappropriate external and internal access, and must prevent interference with VC operations. Authentication, authorization and accountability must be satisfied in a highly volatile network environment. A key protective element will be isolation of vehicle control functions from the wirelessly accessible systems. However, some vehicular safety systems specifically use external feedback to trigger operational effect, such as slowing a vehicle when the driver is not reacting to a detected problem ahead. The greatest challenge might be in opening a channel, albeit as securely as possible, into operating vehicles. If they can be remotely accessed and controlled, VCC will be completely untenable.

Networks of mobile vehicles need new protocols for rapid, authenticated communication between highly dynamic nodes. Effective and efficient algorithms for deciding and managing network membership and virtual machine migration are required.

Certain scenarios will require a ground-based infrastructure. Collaborators who will undertake financing, construction and maintenance of RSUs must be identified. Profit will provide incentive, but will also add cost to the VCC system.

Attracting and motivating collaborators will be difficult. Driver/owners will need to see participation's benefits that outweigh fear of data loss, privacy invasion, and other vehicular attacks. The novelty of VCC will appeal to early adopters. Green community advocates of low energy expenditure might support VCC regardless of cost, just as some will pay an extra fee for recycled paper. Most candidate participants will require incentive, the costs of which must not exceed service value. Continual advances in the technology world will quickly devalue most of VCC's possible benefits. The greatest gain VCC can offer participants is their own time, made possible through traffic relief in a dynamic VC environment. Access to control systems such as signal lights to optimize traffic flow will shorten driving time. Traffic VCC systems will operate in competition with publicly available navigation systems that are intelligent and traffic-aware. But dynamic VCC is more difficult than static because of network volatility.

VCC will require that manufacturers provide capable vehicles. Although VCC represents a convergence of technologies, manufacturers will diverge from a common purpose in individual pursuits of profit. Their early support of DSRC might easily transform into a quest for some new revenue stream. Manufacturing sector competition might be sufficient to kill VCC. The various manufacturers each have their own projects underway that may never converge.

Government will have a role to play, but that role is not yet clearly defined. Authorities may operate RSUs for authentication of vehicles and drivers, or may legislate participation in public service VCs.

Consumers will not have many familiar conventional CC offerings available through VCC. For example, PaaS would be specific to certain niche markets such as travel and navigation. Whether attractive service offerings can be made in a cost effective manner remains to be seen.

The implications of the capacities and obstacles suggest that VCC is a hard target to reach. It might not be achieved on a real-world scale before landscape changes make it impossible. Growing numbers of electric cars may be unable to share their battery power without impeding range of travel. Self-driving vehicles may be unable to share their computing power without compromising safety – or a VCC-like infrastructure might be used for autonomous vehicles, specifically enabling safety applications. Driverless cars, which are already on the horizons and roads, could contribute fairly soon to a world where vehicular computing demands are significantly different from today. Government could legislate against VCC for safety reasons, but will be likely to support manufacturers and income streams.

This paper was constrained by lack of specific information on vehicular power consumption. The academic aspects of VCC are addressed: research into dynamic node networking, cloud operations, and security. Practical economic considerations should also be addressed. VCC

will not be developed without private sector involvement. Careful business analysis will be required to determine whether a market for VCC exists, whether the vehicular cohort can provide the support, whether the driver/owners will be willing to participate, what form of VC is operationally viable at what level of infrastructure investment, and whether VCC can be offered at a price that is competitive with established conventional CC.

VCC is an interesting idea as an academic study, but seems unlikely to overcome its challenges before technology outpaces VCC's potential benefits. Its time may have already passed thanks to continual advances in communication technologies, wireless coverages, CC market inroads, and lower hardware costs. Given the evolving landscape, with 4G cellular communications and increasingly enabled vehicles and other portable computing devices, VCC most likely can hope to serve only a few niche markets. Dynamic urban surveillance, both routine and emergency traffic management applications, and green static data centre are the leading possibilities. It has been suggested that VCC might be of greatest advantage to developing nations, but VCC is a first world solution to a third world problem.

REFERENCES

Abid, H., Phuong, L. T. T., Wang, J., Lee, S., & Qaisar, S. (2011). V-Cloud: Vehicular Cyber-physical Systems and Cloud Computing. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies* (pp. 165:1–165:5). New York, NY, USA: ACM. http://doi.org/10.1145/2093698.2093863

Abuelela, M., & Olariu, S. (2010). Taking VANET to the Clouds. In *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia* (pp. 6–13). New York, NY, USA: ACM. http://doi.org/10.1145/1971519.1971522

Amazon Web Services. (2015a). Amazon S3 Pricing | AWS Cloud Storage Pricing. Retrieved October 11, 2015, from //aws.amazon.com/s3/pricing/

Amazon Web Services. (2015b). AWS | Amazon EC2 | Pricing. Retrieved October 11, 2015, from //aws.amazon.com/ec2/pricing/

Aminizadeh, L., & Yousefi, S. (2014). Cost minimization scheduling for deadline constrained applications on vehicular cloud infrastructure. In *2014 4th International eConference on Computer and Knowledge Engineering (ICCKE)* (pp. 358–363). http://doi.org/10.1109/ICCKE.2014.6993446

Arif, S., Olariu, S., Wang, J., Yan, G., Yang, W., & Khalil, I. (2012). Datacenter at the Airport: Reasoning about Time-Dependent Parking Lot Occupancy. *IEEE Transactions on Parallel and Distributed Systems*, *23*(11), 2067–2080. http://doi.org/10.1109/TPDS.2012.47

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., … Zaharia, M. (2010). A View of Cloud Computing. *Commun. ACM*, *53*(4), 50–58. http://doi.org/10.1145/1721654.1721672

Audi connect® Help & Support | Audi USA. (2015). Retrieved December 18, 2015, from https://www.audiusa.com/help/audi-connect

Bernstein, D., Vidovic, N., & Modi, S. (2010). A Cloud PAAS for High Scale, Function, and Velocity Mobile Applications - With Reference Application as the Fully Connected Car. In *2010 Fifth International Conference on Systems and Networks Communications (ICSNC)* (pp. 117–123). http://doi.org/10.1109/ICSNC.2010.24

Bhoi, S. K., & Khilar, P. M. (2015). RVCloud: a routing protocol for vehicular ad hoc network in city environment using cloud computing. *Wireless Networks*, 1–13. http://doi.org/10.1007/s11276-015-1035-8

Bilal, S. M., Bernardos, C. J., & Guerrero, C. (2013). Position-based routing in vehicular networks: A survey. *Journal of Network and Computer Applications*, *36*(2), 685–697. http://doi.org/10.1016/j.jnca.2012.12.023

Bitam, S., & Mellouk, A. (2012). ITS-cloud: Cloud computing for Intelligent transportation system. In *2012 IEEE Global Communications Conference (GLOBECOM)* (pp. 2054–2059). http://doi.org/10.1109/GLOCOM.2012.6503418

Boston University School of Public Health. (2015). Diffusion of Innovation Theory. Retrieved October 14, 2015, from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/SB721-Models/SB721-Models4.html

Boutilier, A. (2015, October 6). Military research branch looking for hackers to develop exploits for motor vehicles, come up with defences against cyber attacks. *The Toronto*

Star. Retrieved from http://www.thestar.com/news/canada/2015/10/06/canadian-military-to-study-hacking-cars.html

Bravo-Torres, J. F., Ordonez-Morales, E. F., Lopez-Nores, M., Blanco-Fernandez, Y., & Pazos-Arias, J. J. (2014). Virtualization in VANETs to support the vehicular cloud - Experiments with the network as a service model. In *2014 Third International Conference on Future Generation Communication Technology (FGCT)* (pp. 1–6). http://doi.org/10.1109/FGCT.2014.6933225

CAR PARTS from Mister Auto - Your Parts at discount prices. (2015). Retrieved December 18, 2015, from http://www.mister-auto.ie/en/

Cortex-R Series - ARM. (2015). Retrieved December 16, 2015, from http://www.arm.com/products/processors/cortex-r

Edutech Wiki. (2015). Technology-organization-environment framework - EduTech Wiki. Retrieved December 4, 2015, from http://edutechwiki.unige.ch/en/Technology-organization-environment_framework

electricity - Calculating engine starter's energy use - Physics Stack Exchange. (2013, August 29). Retrieved December 15, 2015, from http://physics.stackexchange.com/questions/57794/calculating-engine-starter-s-energy-use

Eltoweissy, M., Olariu, S., & Younis, M. (2010). Towards Autonomous Vehicular Clouds. In J. Zheng, D. Simplot-Ryl, & V. C. M. Leung (Eds.), *Ad Hoc Networks* (pp. 1–16). Springer Berlin Heidelberg. Retrieved from http://0-link.springer.com.aupac.lib.athabascau.ca/chapter/10.1007/978-3-642-17994-5_1

Everything you need to know about Nvidia's new Tegra X1 chip. (2015, February 4). Retrieved December 19, 2015, from http://www.greenbot.com/article/2879437/everything-you-need-to-know-about-nvidias-new-tegra-x1-chip.html

FCA US LLC. (2015a, 24). FCA US LLC (via noodls) / Statement: Software Update. Retrieved August 25, 2015, from http://www.noodls.com/view/C56FE6141D26447D3680AF5D98678AA4E8F983E2?8863xxx1437757981

FCA US LLC. (2015b, July 16). FCA US LLC (via noodls) / FCA US LLC Releases Software Update to Improve Vehicle Electronic Security and Communications System Enhancements. Retrieved August 25, 2015, from http://www.noodls.com/view/44A8A1CD92C87BDEAB4AF146044E1F35350F6BED?3851xxx1437066711

Fernando, N., Loke, S. W., & Rahayu, W. (2013). Mobile cloud computing: A survey. *Future Generation Computer Systems*, *29*(1), 84–106. http://doi.org/10.1016/j.future.2012.05.023

Ford.ca. (2015). Ford SYNC | SYNC Support, Phone Compatibility, Updates, Manuals, Voice Guides, Instructions & More | Ford.ca. Retrieved November 26, 2015, from http://www.ford.ca/technology/sync/

Ford Sync. (2015, January 30). In *Wikipedia, the free encyclopedia*. Retrieved from http://en.wikipedia.org/w/index.php?title=Ford_Sync&oldid=639534788

Free Community-based Mapping, Traffic & Navigation App. (2015). Retrieved December 10, 2015, from https://www.waze.com/

Frequently Asked Questions (FAQ) - DC Battery Specialists. (2015). Retrieved December 14, 2015, from http://www.dcbattery.com/faq.html

Fukuda, T., Kohara, K., Dozaka, T., Takeyama, Y., Midorikawa, T., Hashimoto, K., … Hojo, T. (2014). 13.4 A 7ns-access-time 25 #x03BC;W/MHz 128kb SRAM for low-power fast wake-up MCU in 65nm CMOS with 27fA/b retention current. In *Solid-State Circuits Conference Digest of Technical Papers (ISSCC), 2014 IEEE International* (pp. 236–237). http://doi.org/10.1109/ISSCC.2014.6757415

Gayomali, C. (2011, April 7). Toyota and Microsoft Team Up to Bring Cloud Computing On the Road. *Time*. Retrieved from http://techland.time.com/2011/04/07/toyota-and-microsoft-team-up-to-bring-cloud-computing-on-the-road/

Gerla, M. (2012). Vehicular cloud computing. In *Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean* (pp. 152–155). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6257116

Gerla, M., Weng, J.-T., & Pau, G. (2013). Pics-on-wheels: Photo surveillance in the vehicular cloud. In *2013 International Conference on Computing, Networking and Communications (ICNC)* (pp. 1123–1127). http://doi.org/10.1109/ICCNC.2013.6504250

Ghafoor, K. Z., Bakar, K. A., Mohammed, M. A., & Lloret, J. (2013). Vehicular cloud computing: trends and challenges. *Mobile Networks and Cloud Computing Convergence for Progressive Services and Applications*, 262.

Ghazizadeh, P., Mukkamala, R., & El-Tawab, S. (2014). Scheduling in vehicular cloud using mixed integer linear programming. In *Proceedings of the first international workshop*

on Mobile sensing, computing and communication (pp. 7–12). ACM. Retrieved from http://dl.acm.org/citation.cfm?id=2633681

Ghazizadeh, P., Olariu, S., Zadeh, A. G., & El-Tawab, S. (2015). Towards Fault-Tolerant Job Assignment in Vehicular Cloud. In *2015 IEEE International Conference on Services Computing (SCC)* (pp. 17–24). http://doi.org/10.1109/SCC.2015.13

Google Cloud Platform. (2015). Pricing. Retrieved December 4, 2015, from https://cloud.google.com/pricing/

Greenberg, A. (2013, 24). Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video). Retrieved August 25, 2015, from http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/

Greenberg, A. (2014, August 6). How Hackable Is Your Car? Consult This Handy Chart. Retrieved August 25, 2015, from http://www.wired.com/2014/08/car-hacking-chart/

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Retrieved August 25, 2015, from http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Gu, L., Zeng, D., & Guo, S. (2013). Vehicular cloud computing: A survey. In *2013 IEEE Globecom Workshops (GC Wkshps)* (pp. 403–407). http://doi.org/10.1109/GLOCOMW.2013.6825021

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, *33*(5), 861–874. http://doi.org/10.1016/j.ijinfomgt.2013.07.001

Harris, C. (2013, March 25). General Motors Connects Cars to 4G LTE. Retrieved from http://en.techpageone.co.uk/technology/general-motors-connects-cars-to-4g-lte/

Hartenstein, H., & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine*, *46*(6), 164–171. http://doi.org/10.1109/MCOM.2008.4539481

He, W., Yan, G., & Xu, L. D. (2014). Developing Vehicular Data Cloud Services in the IoT Environment. *IEEE Transactions on Industrial Informatics*, *10*(2), 1587–1595. http://doi.org/10.1109/TII.2014.2299233

How Car Computers Work. (n.d.). Retrieved December 9, 2015, from http://auto.howstuffworks.com/under-the-hood/trends-innovations/car-computer.htm

Huang, C.-L., Fallah, Y. P., Sengupta, R., & Krishnan, H. (2010). Adaptive intervehicle communication control for cooperative safety systems. *IEEE Network*, *24*(1), 6–13. http://doi.org/10.1109/MNET.2010.5395777

Huang, D., Misra, S., Verma, M., & Xue, G. (2011). Pacp: An efficient pseudonymous authentication-based conditional privacy protocol for vanets. *Intelligent Transportation Systems, IEEE Transactions on*, *12*(3), 736–746.

Huang, D., Zhou, Z., Xu, L., Xing, T., & Zhong, Y. (2011). Secure data processing framework for mobile cloud computing. In *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 614–618). http://doi.org/10.1109/INFCOMW.2011.5928886

Hubaux, J.-P., Gross, T., Le Boudec, J.-Y., & Vetterli, M. (2001). Toward self-organized mobile ad hoc networks: the terminodes project. *IEEE Communications Magazine*, *39*(1), 118–124. http://doi.org/10.1109/35.894385

Hussain, R., Son, J., Eun, H., Kim, S., & Oh, H. (2012). Rethinking Vehicular Communications: Merging VANET with cloud computing. In *2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 606–609). http://doi.org/10.1109/CloudCom.2012.6427481

IGI Global. (2015). What is Technology Organization Environment (TOE) | IGI Global. Retrieved October 14, 2015, from http://www.igi-global.com/dictionary/technology-organization-environment-toe/29534

Information is Beautiful. (2015, October 2). World's Biggest Data Breaches & Hacks | Information is Beautiful. Retrieved from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

InfoTransec. (2014). Juice Jacking Vulnerability for iOS | InfoTransec.com. Retrieved September 29, 2015, from https://www.infotransec.com/news/juice-jacking-vulnerability-ios

Introducing The Tegra X1 Super Chip from NVIDIA. (2015). Retrieved December 14, 2015, from http://www.nvidia.com/object/tegra-x1-processor.html

ISO. (1994). ISO - ISO Standards - ICS 35.100: Open systems interconnection (OSI). Retrieved October 26, 2015, from http://www.iso.org/iso/iso_catalogue/catalogue_ics/catalogue_ics_browse.htm?ICS1=35&ICS2=100

Kang, W. M., Lee, J. D., Jeong, Y.-S. . . ., & Park, J. H. (2015). VCC-SSF: Service-Oriented Security Framework for Vehicular Cloud Computing. *Sustainability*, *7*(2), 2028–2044.

Khalifa, A., Hassan, R., & Eltoweissy, M. (2011). Towards ubiquitous computing clouds. In *FUTURE COMPUTING 2011, The Third International Conference on Future Computational Technologies and Applications* (pp. 52–56). Retrieved from http://trafficlight.bitdefender.com/info?url=http%3A//www.thinkmind.org/index.php%3Fview%3Darticle%26articleid%3Dfuture_computing_2011_2_40_30128&language=en_US

Kim, W., & Gerla, M. (2011). NAVOPT: navigator assisted vehicular route optimizer. In *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2011 Fifth International Conference on* (pp. 450–455). IEEE. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5976214

Lau, B., Jang, Y., Song, C., Wang, T., Chung, P. H., & Royal, P. (2013). Mactans: Injecting malware into iOS devices via malicious chargers. *Proceedings of Black Hat USA*. Retrieved from http://www.securitylearn.net/wp-content/uploads/iOS%20Resources/Injecting%20Malware%20into%20iOS%20Devices%20via%20Malicious%20Chargers%20WP.pdf

Lian, J.-W., Yen, D. C., & Wang, Y.-T. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management*, *34*(1), 28–36. http://doi.org/10.1016/j.ijinfomgt.2013.09.004

List of CPU power dissipation figures. (2015, November 19). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=List_of_CPU_power_dissipation_figures&oldid=691362751

Markoff, J. (2011, March 9). Researchers Hack Into Cars' Electronics. *The New York Times*. Retrieved from http://www.nytimes.com/2011/03/10/business/10hack.html

Mazloom, S., Mohadesipour, M., & Babaei, H. (2015). An Ontology-Based Approach for Optimal Resource Allocation in Vehicular Cloud Computing. Retrieved from http://www.ijcsmc.com/docs/papers/February2015/V4I2201552.pdf

Mershad, K., & Artail, H. (2013). CROWN: Discovering and consuming services in vehicular clouds. In *2013 Third International Conference on Communications and Information Technology (ICCIT)* (pp. 98–102). http://doi.org/10.1109/ICCITechnology.2013.6579530

Microsoft. (2005). The STRIDE Threat Model. Retrieved October 16, 2015, from https://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

Microsoft Azure. (2015). Pricing Overview - How Azure pricing works | Microsoft Azure. Retrieved December 4, 2015, from https://azure.microsoft.com/en-us/pricing/

Morgan, Y. L. (2010). Notes on DSRC amp; WAVE Standards Suite: Its Architecture, Design, and Characteristics. *IEEE Communications Surveys Tutorials*, *12*(4), 504–518. http://doi.org/10.1109/SURV.2010.033010.00024

Mousannif, H. (1), Khalil, I. (2), & al Moatassime, H. (3). (2011). Cooperation as a service in VANETs. *Journal of Universal Computer Science*, *17*(8), 1202–1218.

NHTSA. (2005, March). Vehicle Safety Communications Project Task 3 Final Report. Retrieved September 30, 2015, from http://www.its.dot.gov/research_docs/pdf/59vehicle-safety.pdf

Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2009). The Eucalyptus Open-Source Cloud-Computing System. In

9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009. CCGRID '09 (pp. 124–131). http://doi.org/10.1109/CCGRID.2009.93

NVIDIA Tegra X1 Preview & Architecture Analysis. (2015). Retrieved December 17, 2015, from http://www.anandtech.com/show/8811/nvidia-tegra-x1-preview

Olariu, S., Eltoweissy, M., & Younis, M. (2011). Towards autonomous vehicular clouds. *ICST Transactions on Mobile Communications and Applications*, *11*(7–9), e2. http://doi.org/10.4108/icst.trans.mca.2011.e2

Olariu, S., & Weigle, M. C. (Eds.). (2009). *Vehicular Networks: From Theory to Practice* (1 edition). Chapman and Hall/CRC.

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, *51*(5), 497–510. http://doi.org/10.1016/j.im.2014.03.006

OSEK VDX Portal - Home. (2015). Retrieved December 19, 2015, from http://www.osek-vdx.org/

Pagliery, J. (2014, June 1). Your car is a giant computer - and it can be hacked. Retrieved December 16, 2015, from http://money.cnn.com/2014/06/01/technology/security/car-hack/index.html

Passenger vehicles in the United States. (2015, November 25). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Passenger_vehicles_in_the_United_States&oldid=692406810

Perez, S. (2010, February 23). Mobile Cloud Computing: $9.5 Billion by 2014. Retrieved October 14, 2015, from http://readwrite.com/2010/02/23/mobile_cloud_computing_95_billion_by_2014

Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc On-Demand Distance Vector (AODV) Routing* (No. RFC3561). RFC Editor. Retrieved from https://www.rfc-editor.org/info/rfc3561

Poulsen, K. (2010, March 17). Hacker Disables More Than 100 Cars Remotely. Retrieved August 25, 2015, from http://www.wired.com/2010/03/hacker-bricks-cars/

Power Consumption - CPU Charts 2012: 86 Processors From AMD And Intel, Tested. (2012, December 23). Retrieved December 17, 2015, from http://www.tomshardware.com/reviews/cpu-performance-comparison,3370-17.html

PT&C|LWG. (2015, August 19). Car Hacking, The Most Hackable Cars | PT&C|LWG. Retrieved December 8, 2015, from http://www.ptclwg.com/news/the-most-hackable-cars-on-the-road-1

Public Works and Government Services Canada. (2015, October 5). CYBER SECURITY OF AUTOMOTIVE SYSTEM. Retrieved from https://buyandsell.gc.ca/cds/public/2015/10/05/e831fd26bafe14946e25602502281f2a/ABES.PROD.PW_QCL.B018.E16558.EBSU000.PDF

Qin, Y., Huang, D., & Zhang, X. (2012). VehiCloud: Cloud Computing Facilitating Routing in Vehicular Networks. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1438–1445). http://doi.org/10.1109/TrustCom.2012.16

Quick, D. (2011, October 17). GM developing vehicle-to-vehicle and vehicle-to-infrastructure communications systems. Retrieved January 31, 2015, from http://www.gizmag.com/gm-vehicle-communications/20187/

Raya, M., & Hubaux, J.-P. (2005). The Security of Vehicular Ad Hoc Networks. In *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks* (pp. 11–21). New York, NY, USA: ACM. http://doi.org/10.1145/1102219.1102223

Raya, M., Papadimitratos, P., & Hubaux, J.-P. (2006). Securing vehicular communications. *IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications*, *13*(LCA-ARTICLE-2006-015), 8–15.

Refaat, T. K., Kantarci, B., & Mouftah, H. T. (2014). Dynamic Virtual Machine Migration in a vehicular cloud. In *2014 IEEE Symposium on Computers and Communication (ISCC)* (Vol. Workshops, pp. 1–6). http://doi.org/10.1109/ISCC.2014.6912651

Ren, K., Wang, C., & Wang, Q. (2012). Security Challenges for the Public Cloud. *IEEE Internet Computing*, *16*(1), 69–73. http://doi.org/10.1109/MIC.2012.14

Santa, J., Gómez-Skarmeta, A. F., & Sánchez-Artigas, M. (2008). Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks. *Computer Communications*, *31*(12), 2850–2861. http://doi.org/10.1016/j.comcom.2007.12.008

Satyanarayanan, M., Bahl, P., Caceres, R., & Davies, N. (2009). The Case for VM-Based Cloudlets in Mobile Computing. *IEEE Pervasive Computing*, *8*(4), 14–23. http://doi.org/10.1109/MPRV.2009.82

Scott, L., & Denning, D. E. (2003). A Location Based Encryption Technique and Some of Its Applications. Retrieved from https://calhoun.nps.edu/handle/10945/37173

Shepardson, D. (2015, 22). Senators introduce auto cyberhacking bill. Retrieved August 25, 2015, from http://www.detroitnews.com/story/business/autos/2015/07/21/senators-introduce-auto-cyberhacking-bill/30463153/

Shiels, M. (2009, October 13). Phone sales hit by Sidekick loss. *BBC*. Retrieved from http://news.bbc.co.uk/2/hi/technology/8303952.stm

Squatriglia, C. (2011, April 6). Toyota, Microsoft to Bring the Cloud to Cars. Retrieved January 31, 2015, from http://www.wired.com/2011/04/toyota-microsoft-to-bring-the-cloud-to-cars/

Starter Motor. Amps? (2008). Retrieved December 18, 2015, from http://www.electro-tech-online.com/threads/starter-motor-amps.36783/

Stone, J. J. (2010, May 19). Google's Android OS Headed to the Chevy Volt [UPDATED]. Retrieved January 31, 2015, from http://www.treehugger.com/cars/googles-android-os-headed-to-the-chevy-volt-updated.html

Sun, J., Zhang, C., Zhang, Y., & Fang, Y. (2010). An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks. *IEEE Transactions on Parallel and Distributed Systems*, *21*(9), 1227–1239. http://doi.org/10.1109/TPDS.2010.14

Thermal design power. (2015, September 6). In *Wikipedia, the free encyclopedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Thermal_design_power&oldid=679685093

Uconnect. (2015). Uconnect® Software Update - Update your Uconnect® System. Retrieved August 25, 2015, from http://www.driveuconnect.com/software-update/

United States Department of Transportation. (2015, 27). RITA - Intelligent Transportation Systems - DSRC: The Future of Safer Driving Fact Sheet. Retrieved November 3, 2015, from http://www.its.dot.gov/factsheets/dsrc_factsheet.htm

U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety | National Highway Traffic Safety Administration (NHTSA). (2012, December 7). Retrieved December 23, 2015, from http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety

US processor company: The car of the future is the most powerful computer you will ever own. (2015, May 17). Retrieved December 14, 2015, from http://www.businessinsider.com/us-processor-company-the-car-of-the-future-is-the-most-powerful-computer-you-will-ever-own-2015-5

Wang, J., Cho, J., Lee, S., & Ma, T. (2011). Real time services for future cloud computing enabled vehicle networks. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 1–5). http://doi.org/10.1109/WCSP.2011.6096957

Wayland, M. (2015, 21). Jeep hack a red flag for industry. Retrieved August 25, 2015, from http://www.detroitnews.com/story/business/autos/chrysler/2015/07/21/hackers-fca-communications-hacked-jeep/30486307/

Weng, J.-T. (2013). On Demand Surveillance Service in Vehicular Cloud. *eScholarship*. Retrieved from http://escholarship.org/uc/item/7sc0b7rb

Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R. (2014). A survey on vehicular cloud computing. *Journal of Network and Computer Applications*, *40*, 325–344. http://doi.org/10.1016/j.jnca.2013.08.004

Yan, G., Olariu, S., & Weigle, M. C. (2009). Providing location security in vehicular Ad Hoc networks. *IEEE Wireless Communications*, *16*(6), 48–55. http://doi.org/10.1109/MWC.2009.5361178

Yan, G., Rawat, D. B., & Bista, B. B. (2012). Towards Secure Vehicular Clouds. In *2012 Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS)* (pp. 370–375). http://doi.org/10.1109/CISIS.2012.96

Yan, G., Wen, D., Olariu, S., & Weigle, M. C. (2013). Security challenges in vehicular cloud computing. *IEEE Transactions on Intelligent Transportation Systems*, *14*(1), 284–294. http://doi.org/10.1109/TITS.2012.2211870

Yu, R., Zhang, Y., Gjessing, S., Xia, W., & Yang, K. (2013). Toward cloud-based vehicular networks with efficient resource management. *Network, IEEE*, *27*(5), 48–55.

Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., & Stergioulas, L. K. (2008). An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). *International Journal of Medical Informatics*, *77*(6), 386–398. http://doi.org/10.1016/j.ijmedinf.2007.08.011

Ziegenbein, D., & Hamann, A. (2015). Timing-aware control software design for automotive systems. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1–6). http://doi.org/10.1145/2744769.2747947

Zimmer, M. T. (2005). Personal information and the design of vehicle safety communication technologies: An application of privacy as contextual integrity. *AAAS Science and*

Technology in Society. Retrieved from

http://crypto.stanford.edu/portia/papers/Zimmer.pdf

APPENDIX A - Anticipated VANET and VCC application areas

This is a collection of lists of application areas considered for VANET or VCC.

From U.S. National Highway Traffic Safety Administration (NHTSA, 2005):

Safety Applications

Intersection Collision Avoidance
Traffic Signal Violation Warning

Stop Sign Violation Warning

Left Turn Assistant

Stop Sign Movement Assistance

Intersection Collision Warning

Blind Merge Warning

Pedestrian Crossing Information at Designated Intersections

Public Safety
Approaching Emergency Vehicle Warning

Emergency Vehicle Signal Preemption

SOS Services

Post-Crash Warning

Sign Extension
In-Vehicle Signage

Curve Speed Warning

Low Parking Structure Warning

Wrong Way Driver Warning

Low Bridge Warning

Work Zone Warning

In-Vehicle Amber Alert

Vehicle Diagnostics and Maintenance
Safety Recall Notice

Just-In-Time Repair Notification

Information from Other Vehicles
Cooperative Forward Collision Warning

Vehicle-Based Road Condition Warning

Emergency Electronic Brake Lights

Lane Change Warning

Blind Spot Warning

Highway Merge Assistant

Visibility Enhancer

Cooperative Collision Warning

Cooperative Vehicle-Highway Automation System (Platoon)

Cooperative Adaptive Cruise Control

Road Condition Warning

Pre-Crash Sensing

Highway/Rail Collision Warning

Vehicle-To-Vehicle Road Feature Notification

Non-Safety Applications
Traffic Management

Intelligent On-Ramp Metering

Intelligent Traffic Flow Control

Tolling

Free-Flow Tolling

Information from Other Vehicles

Cooperative Glare Reduction

Instant Messaging

Adaptive Headlamp Aiming

Adaptive Drivetrain Management

Enhanced Route Guidance and Navigation

Point of Interest Notification

Map Downloads and Updates

GPS Correction

Other potential applications:

Green light optimal speed advisory

Infrastructure-based traffic management – probes

Traffic information

Transit vehicle data transfer

Emergency vehicle video relay

Border clearance

On-board safety data transfer

Vehicle safety inspection

Driver's daily log

Access control

Drive-thru payment

Parking lot payment

Data transfer / Info-fueling

Vehicle computer program updates

Video downloads

Vehicle sensing alt

Transmitter for bicycle/pedestrian/blind person (in-vicinity advisory)

On-call mechanic

SOS environmental

Overhead storage reminder (height clearance)

Drowsy driver advisory

Distracted driver advisory

Beacon for child left in vehicle

Peer voting of driving patterns (commercial vehicle)

Dynamic emissions tests

Speed limit assistant

Parking spot locator

Electronic license plate

Electronic driver's license

Vehicle lock-down* (disable a vehicle remotely)

All-points bulletin* (request vehicle with particular identity to respond)

APPENDIX B – Innovation adoption models

The *Diffusion of Innovation* (DOI) theory describes the advancement of an idea or product by discussing how behaviour changes for people in five different adopter categories (Boston University School of Public Health, 2015). Innovators want to be first to try something new; Early Adopters are opinion leaders and comfortable with change; Early Majority are at the head of the pack of followers and need proof before adopting change; Late Majority are skeptics who join after the majority has decided; and Laggards need to be pushed. The different categories require different persuasive strategies in order to motivate action. Most people fall into the middle categories.

The DOI model offers 5 traits for consideration in describing organizational adoption of innovation (Oliveira et al., 2014). Relative Advantage quantifies the improvement over the previous state; Compatibility addresses the ease of merging the innovation into the organization; Complexity discusses ease of use of the innovation; Observability characterizes how noticeable the change is to others; and Trialability measures ease of testing the new change.

From Oliveira et al.:

> *DOI is predominantly based on the characteristics of the technology and the users' perceptions of the innovation…. Rogers suggests that innovation is a communication process using the various channels within the social system. Three factors influence the adoption of innovation in organizations. They are individual (leadership attitude toward change), internal organizational structure (centralization, complexity,*

interconnectedness, the number of employees, and organizational slack), and external characteristics (system openness) of the organization.

The Technology-Organization-Environment (TOE) framework describes traits that influence technology adoption by assessing context from three perspectives. TOE considers the characteristics of the technology, the organization's readiness, and environmental factors as key drivers of technology adoption" (IGI Global, 2015) (Edutech Wiki, 2015).

The Human, Organization, Technology-fit (HOT-fit) model was built in response to a perceived need for specialization with Health Information Systems (Yusof, Kuljis, Papazafeiropoulou, & Stergioulas, 2008). It extends two earlier IS models by considering in greater depth the relationships between the model's dimensions. The Information Systems Success Model assesses the relationships between information quality, system quality, service quality, information use, user satisfaction, and net benefits. The IT-Organization Fit model considers relationships between strategy, structure, information technology, roles and skills, and management process.

APPENDIX C – Projected power draws and vehicle battery capacity

"A modern ECU might contain a 32-bit, 40-MHz processor " ("How Car Computers Work," n.d.). Using 40-MHz as a baseline to find power draw for a representative CPU, as a rough estimate we project a 4.8 W power draw for a hypothetical conventional desktop Pentium 40 MHz CPU (see Table 3).

Model	MHz	W	W/MHz	
	40MHz	*4.8 W*	*0.12*	*projected*
Pentium	75 MHz	8.1 W	0.11	
Pentium	90 MHz	9.0 W	0.10	
Pentium	100 MHz	10.1 W	0.10	
Pentium	120 MHz	11.9 W	0.10	
Pentium	133 MHz	11.2 W	0.08	
Pentium	150 MHz	11.6 W	0.08	
Pentium	166 MHz	14.5 W	0.09	
Pentium	200 MHz	15.5 W	0.08	

Table 3 - 40MHz CPU power draw projection

source:
https://en.wikipedia.org/wiki/List_of_CPU_power_dissipation_figures#Pentium

alternate source:
http://www.intel.com/content/dam/support/us/en/documents/processors/pentium/sb/24199710.pdf, p.31

Table 4 shows the calculation of the amperage draw on a 12-volt battery by 50 CPUs at 4.8 watts/CPU (from Table 3) and at 37 watts/CPU (median TDP from Table 6).

# CPUs	Watts/CPU	Total wattage (W)	Battery voltage (V)	Amperage required (A = W/V)

50	4.8	240	12	20
50	37	1850	12	154

Table 4 - Amperage calculation

The Amperage Required shown in Table 4 identifies to the power draw for 50 CPUs that demand, on average, either 4.8 watts or 37 watts.

The capacity of a battery to deliver power is measured in amp hours (Ah). This is a measure of the length of time an amperage can be provided by the battery ("Frequently Asked Questions (FAQ) - DC Battery Specialists," 2015). The amp hour rating is the product of the amperage and the length of time the amperage can be sustained. For example, an 80 Ah battery will provide 4 amps for 20 hours.

Table 5 shows specifications for over 100 12-volt vehicular batteries. Amp-Hour ratings and voltage are provided by the vendors. The hours of service give a rough estimate of how long a vehicle battery might support operation of vehicular CPUs, excluding all other power draws and without recharging, before complete power drain. Hours of service is calculated using the batteries' manufacturers' amp-hour ratings (shown in Table 5) and the Amperage Required from Table 4 as shown in Equation 12.

[12]
$$Hours\ of\ service = \frac{Ah}{Amperage\ Required}$$

Table 5 - Vehicular battery specifications
Sources:
http://www.puretyre.co.uk/car-battery-specification-chart/
http://www.optimabatteries.com/
http://www.interstatebatteries.com/

Vendor	Yuasa Battery code / model	Amp - Hours	Hours of service (4.8W/CPU)	Hours of service (37W/CPU)
Pure Tyre	4	50	**2.5**	**0.32**
Pure Tyre	5	60	**3**	**0.39**
Pure Tyre	8	50	**2.5**	**0.32**
Pure Tyre	9	30	**1.5**	**0.19**
Pure Tyre	12	45	**2.25**	**0.29**
Pure Tyre	012T	55	**2.75**	**0.36**
Pure Tyre	14	60	**3**	**0.39**
Pure Tyre	17	88	**4.4**	**0.57**
Pure Tyre	19	95	**4.75**	**0.62**
Pure Tyre	019T	100	**5**	**0.65**
Pure Tyre	20	110	**5.5**	**0.71**
Pure Tyre	24	90	**4.5**	**0.58**
Pure Tyre	27	60	**3**	**0.39**
Pure Tyre	027T	62	**3.1**	**0.40**
Pure Tyre	30	70	**3.5**	**0.45**
Pure Tyre	31	70	**3.5**	**0.45**
Pure Tyre	37	35	**1.75**	**0.23**
Pure Tyre	38	35	**1.75**	**0.23**
Pure Tyre	48	45	**2.25**	**0.29**
Pure Tyre	49	45	**2.25**	**0.29**
Pure Tyre	53	45	**2.25**	**0.29**
Pure Tyre	54	33	**1.65**	**0.21**
Pure Tyre	55	33	**1.65**	**0.21**
Pure Tyre	56	36	**1.8**	**0.23**
Pure Tyre	57	45	**2.25**	**0.29**
Pure Tyre	63	45	**2.25**	**0.29**
Pure Tyre	063T	47	**2.35**	**0.30**
Pure Tyre	65	54	**2.7**	**0.35**
Pure Tyre	69	70	**3.5**	**0.45**
Pure Tyre	72	70	**3.5**	**0.45**
Pure Tyre	75	60	**3**	**0.39**
Pure Tyre	075T	60	**3**	**0.39**
Pure Tyre	77	45	**2.25**	**0.29**
Pure Tyre	78	59	**2.95**	**0.38**

Pure Tyre	85	45	**2.25**	**0.29**
Pure Tyre	86	75	**3.75**	**0.49**
Pure Tyre	93	48	**2.4**	**0.31**
Pure Tyre	95	68	**3.4**	**0.44**
Pure Tyre	96	75	**3.75**	**0.49**
Pure Tyre	096T	80	**4**	**0.52**
Pure Tyre	97	59	**2.95**	**0.38**
Pure Tyre	100	70	**3.5**	**0.45**
Pure Tyre	100T	70	**3.5**	**0.45**
Pure Tyre	102	38	**1.9**	**0.25**
Pure Tyre	110	75	**3.75**	**0.49**
Pure Tyre	110T	80	**4**	**0.52**
Pure Tyre	111	50	**2.5**	**0.32**
Pure Tyre	113	50	**2.5**	**0.32**
Pure Tyre	156	45	**2.25**	**0.29**
Pure Tyre	202	38	**1.9**	**0.25**
Pure Tyre	334	95	**4.75**	**0.62**
Pure Tyre	335	95	**4.75**	**0.62**
Pure Tyre	012T	55	**2.75**	**0.36**
Pure Tyre	895	26	**1.3**	**0.17**
Pure Tyre	896	26	**1.3**	**0.17**
Pure Tyre	12N5-3B	5	**0.25**	**0.03**
Pure Tyre	12N5-4B	5	**0.25**	**0.03**
Pure Tyre	12N5.5-3B	6	**0.275**	**0.04**
Pure Tyre	12N5.5-4A	6	**0.275**	**0.04**
Pure Tyre	12N5.5A-3B	6	**0.275**	**0.04**
Pure Tyre	12N7-3B	7	**0.35**	**0.05**
Pure Tyre	12N7-4A	7	**0.35**	**0.05**
Pure Tyre	12N7D-3B	7	**0.35**	**0.05**
Pure Tyre	12N9-3A-1	9	**0.45**	**0.06**
Pure Tyre	12N9-3B	9	**0.45**	**0.06**
Pure Tyre	12N9-4B-1	9	**0.45**	**0.06**
Pure Tyre	12N10-3A-2	10	**0.5**	**0.06**
Pure Tyre	12N10-3B	10	**0.5**	**0.06**
Pure Tyre	12N12A-4A-1	12	**0.6**	**0.08**
Pure Tyre	12N14-3A	14	**0.7**	**0.09**
Pure Tyre	12N16-3B	16	**0.8**	**0.10**
Pure Tyre	12N16-4B	16	**0.8**	**0.10**
Pure Tyre	12N24-3	24	**1.2**	**0.16**
Pure Tyre	CHD4-12	28	**1.4**	**0.18**
Optima	D31A	75	**3.75**	**0.49**

Optima	D31T	75	**3.75**	**0.49**
Optima	D34	55	**2.75**	**0.36**
Optima	D34/78	55	**2.75**	**0.36**
Optima	D35	48	**2.4**	**0.31**
Optima	D51	38	**1.9**	**0.25**
Optima	D25/75	48	**2.4**	**0.31**
Optima	25	44	**2.2**	**0.29**
Optima	34	50	**2.5**	**0.32**
Optima	34/78	50	**2.5**	**0.32**
Optima	75/25	44	**2.2**	**0.29**
Optima	78	50	**2.5**	**0.32**
Interstate	MT-47/H5	53	**2.65**	**0.34**
Interstate	PF-47/H5-6	53	**2.65**	**0.34**
Interstate	MT7-48/H6	70	**3.5**	**0.45**
Interstate	MT5-48/H6	70	**3.5**	**0.45**
Interstate	MTP-48	70	**3.5**	**0.45**
Interstate	MT-48	50	**2.5**	**0.32**
Interstate	PF-48	50	**2.5**	**0.32**
Interstate	MT5-94R	80	**4**	**0.52**
Interstate	MTP-94R	80	**4**	**0.52**
Interstate	PF-94R	80	**4**	**0.52**
Interstate	MT5-49	95	**4.75**	**0.62**
Interstate	MTP-49	100	**5**	**0.65**
Interstate	MT-49	80	**4**	**0.52**
Interstate	PF-49	80	**4**	**0.52**
Interstate	MTP-95R	110	**5.5**	**0.71**
Interstate	MTP-90	56	**2.8**	**0.36**
Interstate	MTP-91	60	**3**	**0.39**
Interstate	MTP-92	80	**4**	**0.52**
Interstate	MTP-93	90	**4.5**	**0.58**

APPENDIX D – Power draw for desktop/laptop CPUs

This information is provided as a basic guideline. Sources have not been thoroughly authenticated, but small samples have been verified against manufacturers' web sites. Data should be considered anecdotal but representative. The low granularity of the subject matter and data does not call for more rigorous treatment at this time.

Table 8 shows power information for over 800 different CPUs from various manufacturers. The CPUs in this data sample are predominantly intended for use in desktop or laptop computers and were designed and built at various times since 2000. The data is extracted from ("List of CPU power dissipation figures," 2015). VCore, where supplied, refers to the voltage required by the CPU core.

Metric	Value
Average MHz	1949
Median MHz	1946
Average W (TDP)	48.7
Median W (TDP)	37.0
Average MHz/W	66.71
Median MHz/W	40.83
CPU count in study	873

Table 6 - CPU power summary (TDP)

Several of the chips are obsolete. The data shows that the Intel Atom processors, designed for netbook use, are on average significantly more energy efficient than other processors.

Table 6 summarizes the CPU power information from Table 8. The summary shows the power draw for an average CPU as approximately 40-45 watts.

Metric	Value
Average W (idle)	60
Median W (idle)	61
Average W (peak)	74
Median W (peak)	210
CPU count in study	57

Table 7 - Real CPU power draw

A 2012 survey of 57 contemporary desktop and laptop processors and their real power draws ("Power Consumption - CPU Charts 2012," 2012) shows a range from 38 W to 83 W when idle, with average 60 W and median 61 W. At peak use, the draw ranges from 74 W to 210 W, with average 145 W and median 136 W. This information is illustrated in Table 7.

Table 8 - CPU power requirements (TDP)
source: https://en.wikipedia.org/wiki/List_of_CPU_power_dissipation_figures

CPU ID	Clock speed	Thermal design power	Vcore	Amperage (12V)	W/MHz	MHz/W	MHz/A
Atom Z500	800 MHz	0.65 W		0.054	0.0008	1230.77	14769
Atom Z515	1.2 GHz	1.4 W		0.117	0.0011	877.71	10533
Atom Z560	2.13 GHz	2.5 W		0.208	0.0011	872.45	10469
Atom Z550	2 GHz	2.4 W		0.200	0.0012	853.33	10240
Atom Z530	1.6 GHz	2 W		0.167	0.0012	819.20	9830
Atom Z540	1.86 GHz	2.4 W		0.200	0.0013	793.60	9523
Atom Z530P	1.6 GHz	2.2 W		0.183	0.0013	744.73	8937
Atom N280	1.67 GHz	2.5 W		0.208	0.0015	684.03	8208
Atom Z520	1.33 GHz	2 W		0.167	0.0015	680.96	8172
Atom N270	1.6 GHz	2.5 W		0.208	0.0015	655.36	7864
Atom Z520PT	1.33 GHz	2.2 W		0.183	0.0016	619.05	7429
Atom Z510	1.1 GHz	2 W		0.167	0.0018	563.20	6758
Atom Z510P	1.1 GHz	2.2 W		0.183	0.0020	512.00	6144
Atom Z510PT	1.1 GHz	2.2 W		0.183	0.0020	512.00	6144
Atom N2600 (Dual-Core)	1.6 GHz	3.5 W		0.292	0.0021	468.11	5617
Atom 230	1.6 GHz	4 W		0.333	0.0024	409.60	4915
Windsor F3 Athlon 64 X2	2800 MHz	89W	1.30-1.35 V	0.667	0.0029	350.00	4200
Atom N450	1.67 GHz	5.5 W		0.458	0.0032	310.92	3731
Atom N2800 (Dual-Core)	1.87 GHz	6.5 W		0.542	0.0034	294.60	3535
Atom N470	1.83 GHz	6.5 W		0.542	0.0035	288.30	3460
Atom N475	1.83 GHz	6.5 W		0.542	0.0035	288.30	3460
Pentium M ULV 773	1.3 GHz	5 W		0.417	0.0038	266.24	3195
Atom N455	1.67 GHz	6.5 W		0.542	0.0038	263.09	3157

Core 2 Solo SU3500	1.4 GHz	5.5 W		0.458	0.0038	260.65	3128
PowerPC 750FX	900 MHz	3.6 W	1.2 V	0.300	0.0040	250.00	3000
Core Solo U1500	1.33 GHz	5.5 W		0.458	0.0040	247.62	2971
Pentium M ULV 753	1.2 GHz	5 W		0.417	0.0041	245.76	2949
Pentium M ULV 733	1.1 GHz	5 W		0.417	0.0044	225.28	2703
Pentium M ULV 733J	1.1 GHz	5 W		0.417	0.0044	225.28	2703
Core 2 Solo U2200	1.2 GHz	5.5 W		0.458	0.0045	223.42	2681
Core 2 Solo SU3300	1.2 GHz	5.5 W		0.458	0.0045	223.42	2681
Atom D2700 (Dual-Core)	2.13 GHz	10 W		0.833	0.0046	218.11	2617
Atom 330 (Dual-Core)	1.6 GHz	8 W		0.667	0.0049	204.80	2458
Pentium M ULV 723	1 GHz	5 W		0.417	0.0049	204.80	2458
Core Solo U1400	1.2 GHz	6 W		0.500	0.0049	204.80	2458
Atom N570 (Dual-Core)	1.66 GHz	8.5 W		0.708	0.0050	199.98	2400
Core 2 Solo U2100	1.06 GHz	5.5 W		0.458	0.0051	197.35	2368
Atom D2500 (Dual-Core)	1.87 GHz	10 W		0.833	0.0052	191.49	2298
Atom D2550 (Dual-Core)	1.87 GHz	10 W		0.833	0.0052	191.49	2298
Celeron M 373	1 GHz	5.5 W		0.458	0.0054	186.18	2234
Celeron M 383	1 GHz	5.5 W		0.458	0.0054	186.18	2234
Core Solo U1300	1.06 GHz	6 W		0.500	0.0055	180.91	2171
Atom N550 (Dual-Core)	1.5 GHz	8.5 W		0.708	0.0055	180.71	2168
Celeron M 353	900 MHz	5 W		0.417	0.0056	180.00	2160
PowerPC 440GX	800 MHz	4.5 W		0.375	0.0056	177.78	2133
Atom D410	1.66 GHz	10 W		0.833	0.0059	169.98	2040
Pentium M LV 778	1.6 GHz	10 W		0.833	0.0061	163.84	1966
Core 2 Duo SU9600	1.6 GHz	10 W		0.833	0.0061	163.84	1966
Pentium M ULV 713	1.1 GHz	7 W		0.583	0.0062	160.91	1931
Pentium M LV 758	1.5 GHz	10 W		0.833	0.0065	153.60	1843
Core i7-4610Y	1.70 GHz	11.5 W		0.958	0.0066	151.37	1816
Pentium M ULV 1.0	1 GHz	7 W		0.583	0.0068	146.29	1755

Core i7-4600U	2.10 GHz	15 W		1.250	0.0070	143.36	1720
Pentium M LV 738	1.4 GHz	10 W		0.833	0.0070	143.36	1720
Core 2 Duo SU9400	1.4 GHz	10 W		0.833	0.0070	143.36	1720
Core i5-4202Y	1.60 GHz	11.5 W		0.958	0.0070	142.47	1710
Core i5-4300Y	1.60 GHz	11.5 W		0.958	0.0070	142.47	1710
Core i5-4302Y	1.60 GHz	11.5 W		0.958	0.0070	142.47	1710
Atom D525 (Dual-Core)	1.8 GHz	13 W		1.083	0.0071	141.78	1701
Core Duo U2500	1.2 GHz	9 W		0.750	0.0073	136.53	1638
Core 2 Duo U7700	1.33 GHz	10 W		0.833	0.0073	136.19	1634
Core i3-4012Y	1.5 GHz	11.5 W		0.958	0.0075	133.57	1603
Core i3-4020Y	1.5 GHz	11.5 W		0.958	0.0075	133.57	1603
Core i5-4210Y	1.50 GHz	11.5 W		0.958	0.0075	133.57	1603
Pentium III-M ULV 933	933 MHz	7 W		0.583	0.0075	133.29	1599
Core 2 Duo SU7300	1.3 GHz	10 W		0.833	0.0075	133.12	1597
Pentium SU2700	1.3 GHz	10 W		0.833	0.0075	133.12	1597
Pentium SU4100	1.3 GHz	10 W		0.833	0.0075	133.12	1597
Atom D510 (Dual-Core)	1.66 GHz	13 W		1.083	0.0076	130.76	1569
Core i5-4300U	1.90 GHz	15 W		1.250	0.0077	129.71	1556
Pentium III-M ULV 900	900 MHz	7 W		0.583	0.0078	128.57	1543
Pentium M ULV 900	900 MHz	7 W		0.583	0.0078	128.57	1543
Core 2 Duo SL9600	2.13 GHz	17 W		1.417	0.0078	128.30	1540
Core Duo L2500	1.83 GHz	15 W		1.250	0.0080	124.93	1499
Core i5-4200Y	1.40 GHz	11.5 W		0.958	0.0080	124.66	1496
Pentium III-M ULV 866	866 MHz	7 W		0.583	0.0081	123.71	1485
Core 2 Duo U7600	1.2 GHz	10 W		0.833	0.0081	122.88	1475
Core 2 Duo SU9300	1.2 GHz	10 W		0.833	0.0081	122.88	1475
Celeron M 723	1.2 GHz	10 W		0.833	0.0081	122.88	1475
Core i3-4100U	1.8 GHz	15 W		1.250	0.0081	122.88	1475

Core i7-4500U	1.80 GHz	15 W		1.250	0.0081	122.88	1475
Pentium III-M ULV 850	850 MHz	7 W		0.583	0.0082	121.43	1457
Core Duo U2400	1.06 GHz	9 W		0.750	0.0083	120.60	1447
Core i7-3667U	2.00 GHz	17 W		1.417	0.0083	120.47	1446
Core i3-4005U	1.7 GHz	15 W		1.250	0.0086	116.05	1393
Core i3-4010U	1.7 GHz	15 W		1.250	0.0086	116.05	1393
Core i7-4650U	1.70 GHz	15 W		1.250	0.0086	116.05	1393
Core i3-4010Y	1.3 GHz	11.5 W		0.958	0.0086	115.76	1389
Core i7-3517U	1.90 GHz	17 W		1.417	0.0087	114.45	1373
Pentium III-M ULV 800	800 MHz	7 W		0.583	0.0088	114.29	1371
Celeron M 800	800 MHz	7 W		0.583	0.0088	114.29	1371
Core Duo L2400	1.66 GHz	15 W		1.250	0.0088	113.32	1360
Core 2 Duo SL9400	1.86 GHz	17 W		1.417	0.0089	112.04	1344
PowerPC MGT560	56 MHz	0.5 W	2.7 V	0.042	0.0089	112.00	1344
Pentium M LV 718	1.3 GHz	12 W		1.000	0.0090	110.93	1331
Core i5-4200U	1.60 GHz	15 W		1.250	0.0092	109.23	1311
Core 2 Duo P8800	2.66 GHz	25 W		2.083	0.0092	108.95	1307
Core 2 Duo P9600	2.66 GHz	25 W		2.083	0.0092	108.95	1307
Core 2 Duo U7500	1.06 GHz	10 W		0.833	0.0092	108.54	1303
Core 2 Duo LV7700	1.8 GHz	17 W		1.417	0.0092	108.42	1301
Core 2 Duo SL9380	1.8 GHz	17 W		1.417	0.0092	108.42	1301
Core i3-3217U	1.8 GHz	17 W		1.417	0.0092	108.42	1301
Core i5-3427UM	1.80 GHz	17 W		1.417	0.0092	108.42	1301
Pentium III-M ULV 750	750 MHz	7 W		0.583	0.0093	107.14	1286
Pentium III-M ULV 733	733 MHz	7 W		0.583	0.0095	104.71	1257
Core 2 Duo P8700	2.53 GHz	25 W		2.083	0.0096	103.63	1244
Core 2 Duo P9500	2.53 GHz	25 W		2.083	0.0096	103.63	1244
Core 2 Duo SP9600	2.53 GHz	25 W		2.083	0.0096	103.63	1244

Pentium M LV 1.2	1.2 GHz	12 W		1.000	0.0098	102.40	1229
Core Duo L2300	1.5 GHz	15 W		1.250	0.0098	102.40	1229
Core i7-4550U	1.50 GHz	15 W		1.250	0.0098	102.40	1229
Core i5-3317UM	1.70 GHz	17 W		1.417	0.0098	102.40	1229
Pentium M 765	2.1 GHz	21 W		1.750	0.0098	102.40	1229
Core 2 Duo P9700	2.8 GHz	28 W		2.333	0.0098	102.40	1229
Core i7-4558U	2.80 GHz	28 W		2.333	0.0098	102.40	1229
PowerPC 750CXe	600 MHz	6 W	1.8 V	0.500	0.0100	100.00	1200
Pentium III-M ULV 700	700 MHz	7 W		0.583	0.0100	100.00	1200
Core 2 Duo P8600	2.4 GHz	25 W		2.083	0.0102	98.30	1180
Core 2 Duo SP9400	2.4 GHz	25 W		2.083	0.0102	98.30	1180
Pentium M 755	2 GHz	21 W		1.750	0.0103	97.52	1170
Core 2 Duo LV7500	1.6 GHz	17 W		1.417	0.0104	96.38	1157
Core 2 Duo SL9300	1.6 GHz	17 W		1.417	0.0104	96.38	1157
Core i5-4350U	1.40 GHz	15 W		1.250	0.0105	95.57	1147
Core i5-4288U	2.60 GHz	28 W		2.333	0.0105	95.09	1141
Pentium M LV 1.1	1.1 GHz	12 W		1.000	0.0107	93.87	1126
Pentium III-M LV 1000	1 GHz	11 W		0.917	0.0107	93.09	1117
Core 2 Duo P7550	2.26 GHz	25 W		2.083	0.0108	92.57	1111
Core 2 Duo P8400	2.26 GHz	25 W		2.083	0.0108	92.57	1111
Core 2 Duo SP9300	2.26 GHz	25 W		2.083	0.0108	92.57	1111
Core i7-660LM	2.26 GHz	25 W		2.083	0.0108	92.57	1111
Core 2 Duo LV7400	1.5 GHz	17 W		1.417	0.0111	90.35	1084
Core 2 Duo T9900	3.06 GHz	35 W		2.917	0.0112	89.53	1074
Pentium III-M LV 933	933 MHz	10.5 W		0.875	0.0113	88.86	1066
Core i5-4250U	1.30 GHz	15 W		1.250	0.0113	88.75	1065
Pentium M 745	1.8 GHz	21 W		1.750	0.0114	87.77	1053
Pentium M 745A	1.8 GHz	21 W		1.750	0.0114	87.77	1053

Core i5-4258U	2.40 GHz	28 W		2.333	0.0114	87.77	1053
Core 2 Duo P7450	2.13 GHz	25 W		2.083	0.0115	87.24	1047
Core i7-640LM	2.13 GHz	25 W		2.083	0.0115	87.24	1047
Pentium III-M LV 800	800 MHz	9.25 W		0.771	0.0116	86.49	1038
Pentium III-M LV 866	866 MHz	10.1 W		0.842	0.0117	85.74	1029
Core 2 Duo T9800	2.93 GHz	35 W		2.917	0.0117	85.72	1029
Celeron M 600	600 MHz	7 W		0.583	0.0117	85.71	1029
Pentium M 780	2.26 GHz	27 W		2.250	0.0117	85.71	1029
Pentium III-M LV 850	850 MHz	10 W		0.833	0.0118	85.00	1020
Core 2 Duo LV7300	1.4 GHz	17 W		1.417	0.0119	84.33	1012
Core i3-2367M	1.4 GHz	17 W		1.417	0.0119	84.33	1012
Core i7-680UM	1.46 GHz	18 W		1.500	0.0120	83.06	997
Pentium M 735	1.7 GHz	21 W		1.750	0.0121	82.90	995
Pentium M 735A	1.7 GHz	21 W		1.750	0.0121	82.90	995
Core Solo T1600	2.16 GHz	27 W		2.250	0.0122	81.92	983
Core 2 Duo P7350	2 GHz	25 W		2.083	0.0122	81.92	983
Core 2 Duo P7370	2 GHz	25 W		2.083	0.0122	81.92	983
Core i7-620LM	2.00 GHz	25 W		2.083	0.0122	81.92	983
Core i7-620LE	2.00 GHz	25 W		2.083	0.0122	81.92	983
Dual-core PowerPC MPC8641D	2 GHz	15-25 W	1.2 V	2.083	0.0122	81.92	983
Core 2 Duo T9600	2.8 GHz	35 W		2.917	0.0122	81.92	983
Core i5-3360M	2.80 GHz	35 W		2.917	0.0122	81.92	983
Core i7-640M	2.80 GHz	35 W		2.917	0.0122	81.92	983
Pentium M 770	2.13 GHz	27 W		2.250	0.0124	80.78	969
Core i7-4600M	2.90 GHz	37 W		3.083	0.0125	80.26	963
Core 2 Duo LV7200	1.33 GHz	17 W		1.417	0.0125	80.11	961
Pentium III-M LV 750	750 MHz	9.4 W		0.783	0.0125	79.79	957

Pentium III-M LV 733	733 MHz	9.3 W		0.775	0.0127	78.82	946
Core i3-2357M	1.3 GHz	17 W		1.417	0.0128	78.31	940
Pentium M 725	1.6 GHz	21 W		1.750	0.0128	78.02	936
Pentium M 725A	1.6 GHz	21 W		1.750	0.0128	78.02	936
Celeron M 380	1.6 GHz	21 W		1.750	0.0128	78.02	936
Core 2 Duo T9550	2.66 GHz	35 W		2.917	0.0128	77.82	934
Core i5-560M	2.66 GHz	35 W		2.917	0.0128	77.82	934
Core i5-580M	2.66 GHz	35 W		2.917	0.0128	77.82	934
Core i7-620M	2.66 GHz	35 W		2.917	0.0128	77.82	934
Core i5-4330M	2.80 GHz	37 W		3.083	0.0129	77.49	930
Core Duo T2700	2.33 GHz	31 W		2.583	0.0130	76.97	924
Pentium 4-M 2.6	2.6 GHz	35 W		2.917	0.0131	76.07	913
Core 2 Duo T7800	2.6 GHz	35 W		2.917	0.0131	76.07	913
Core 2 Duo T9500	2.6 GHz	35 W		2.917	0.0131	76.07	913
Core i5-3230M	2.60 GHz	35 W		2.917	0.0131	76.07	913
Pentium M 760	2 GHz	27 W		2.250	0.0132	75.85	910
Core Solo T1500	2 GHz	27 W		2.250	0.0132	75.85	910
Core i3-380UM	1.33 GHz	18 W		1.500	0.0132	75.66	908
Core i5-470UM	1.33 GHz	18 W		1.500	0.0132	75.66	908
Core i5-560UM	1.33 GHz	18 W		1.500	0.0132	75.66	908
Core i7-660UM	1.33 GHz	18 W		1.500	0.0132	75.66	908
Core i7-660UE	1.33 GHz	18 W		1.500	0.0132	75.66	908
Core 2 Duo T9400	2.53 GHz	35 W		2.917	0.0135	74.02	888
Core i3-380M	2.53 GHz	35 W		2.917	0.0135	74.02	888
Core i5-460M	2.53 GHz	35 W		2.917	0.0135	74.02	888
Core i5-540M	2.53 GHz	35 W		2.917	0.0135	74.02	888
Core i7-610E	2.53 GHz	35 W		2.917	0.0135	74.02	888
Pentium 4-M 2.5	2.5 GHz	35 W		2.917	0.0137	73.14	878

Core 2 Duo T9300	2.5 GHz	35 W		2.917	0.0137	73.14	878
Core i5-2450M	2.50 GHz	35 W		2.917	0.0137	73.14	878
Pentium M 715	1.5 GHz	21 W		1.750	0.0137	73.14	878
Pentium M 715A	1.5 GHz	21 W		1.750	0.0137	73.14	878
Celeron M 370	1.5 GHz	21 W		1.750	0.0137	73.14	878
Core i3-4158U	2.0 GHz	28 W		2.333	0.0137	73.14	878
Core i5-4300M	2.60 GHz	37 W		3.083	0.0139	71.96	863
Core Duo T2600	2.16 GHz	31 W		2.583	0.0140	71.35	856
Core 2 Extreme X9100	3.06 GHz	44 W		3.667	0.0140	71.21	855
Pentium M 1.7	1.7 GHz	24.5 W		2.042	0.0141	71.05	853
Pentium M 750	1.86 GHz	27 W		2.250	0.0142	70.54	847
Pentium 4-M 2.4	2.4 GHz	35 W		2.917	0.0142	70.22	843
Core 2 Duo T7700	2.4 GHz	35 W		2.917	0.0142	70.22	843
Core 2 Duo T8300	2.4 GHz	35 W		2.917	0.0142	70.22	843
Core i3-370M	2.40 GHz	35 W		2.917	0.0142	70.22	843
Core i3-2370M	2.4 GHz	35 W		2.917	0.0142	70.22	843
Core i3-3110M	2.4 GHz	35 W		2.917	0.0142	70.22	843
Core i5-450M	2.40 GHz	35 W		2.917	0.0142	70.22	843
Core i5-520M	2.40 GHz	35 W		2.917	0.0142	70.22	843
Core i5-520E	2.40 GHz	35 W		2.917	0.0142	70.22	843
Core 2 Duo T7600	2.33 GHz	34 W		2.833	0.0143	70.17	842
Core Solo T1400	1.83 GHz	27 W		2.250	0.0144	69.40	833
Core i3-4100M	2.5 GHz	37 W		3.083	0.0145	69.19	830
Core i5-4200M	2.50 GHz	37 W		3.083	0.0145	69.19	830
Core i3-330UM	1.20 GHz	18 W		1.500	0.0146	68.27	819
Core i5-430UM	1.20 GHz	18 W		1.500	0.0146	68.27	819
Core i5-540UM	1.20 GHz	18 W		1.500	0.0146	68.27	819
Core i7-640UM	1.20 GHz	18 W		1.500	0.0146	68.27	819

Pentium M 710	1.4 GHz	21 W		1.750	0.0146	68.27	819
Celeron M 360	1.4 GHz	21 W		1.750	0.0146	68.27	819
Celeron M 360J	1.4 GHz	21 W		1.750	0.0146	68.27	819
Core i3-2350M	2.3 GHz	35 W		2.917	0.0149	67.29	807
Pentium M 1.6	1.6 GHz	24.5 W		2.042	0.0150	66.87	802
Core i3-4000M	2.4 GHz	37 W		3.083	0.0151	66.42	797
Core i3-350M	2.26 GHz	35 W		2.917	0.0151	66.12	793
Core i5-430M	2.26 GHz	35 W		2.917	0.0151	66.12	793
Core Duo T2450	2 GHz	31 W		2.583	0.0151	66.06	793
Core Duo T2500	2 GHz	31 W		2.583	0.0151	66.06	793
Pentium M 740	1.73 GHz	27 W		2.250	0.0152	65.61	787
Pentium III-M 1400	1.40 GHz	22 W		1.833	0.0153	65.16	782
Pentium M 1.4	1.4 GHz	22 W		1.833	0.0153	65.16	782
Core 2 Extreme X7900	2.8 GHz	44 W		3.667	0.0153	65.16	782
Core 2 Extreme X9000	2.8 GHz	44 W		3.667	0.0153	65.16	782
Core 2 Duo T7400	2.16 GHz	34 W		2.833	0.0154	65.05	781
Celeron 220	1.2 GHz	19 W		1.583	0.0155	64.67	776
Celeron M 390	1.7 GHz	27 W		2.250	0.0155	64.47	774
Celeron 450	2.2 GHz	35 W		2.917	0.0155	64.37	772
Pentium 4-M 2.2	2.2 GHz	35 W		2.917	0.0155	64.37	772
Core 2 Duo T5900	2.2 GHz	35 W		2.917	0.0155	64.37	772
Core 2 Duo T7500	2.2 GHz	35 W		2.917	0.0155	64.37	772
Core 2 Duo T6600	2.2 GHz	35 W		2.917	0.0155	64.37	772
Core 2 Duo T6670	2.2 GHz	35 W		2.917	0.0155	64.37	772
Core i3-2330M	2.2 GHz	35 W		2.917	0.0155	64.37	772
Pentium 4-M 2.0	2 GHz	32 W		2.667	0.0156	64.00	768
Celeron M 350	1.3 GHz	21 W		1.750	0.0158	63.39	761
Celeron M 350J	1.3 GHz	21 W		1.750	0.0158	63.39	761

Core 2 Duo T5850	2.16 GHz	35 W		2.917	0.0158	63.20	758
Pentium Dual-Core T3400	2.16 GHz	35 W		2.917	0.0158	63.20	758
Core Solo T1300	1.66 GHz	27 W		2.250	0.0159	62.96	755
Pentium M 1.5	1.5 GHz	24.5 W		2.042	0.0160	62.69	752
Celeron M 340	1.5 GHz	24.5 W		2.042	0.0160	62.69	752
Core i3-330M	2.13 GHz	35 W		2.917	0.0160	62.32	748
Core i3-330E	2.13 GHz	35 W		2.917	0.0160	62.32	748
Pentium III-M 1333	1.33 GHz	22 W		1.833	0.0162	61.91	743
Core 2 Duo T6500	2.1 GHz	35 W		2.917	0.0163	61.44	737
Core 2 Duo T6570	2.1 GHz	35 W		2.917	0.0163	61.44	737
Core 2 Duo T8100	2.1 GHz	35 W		2.917	0.0163	61.44	737
Core i3-2310M	2.1 GHz	35 W		2.917	0.0163	61.44	737
Celeron Dual-Core T3500	2.1 GHz	35 W		2.917	0.0163	61.44	737
Pentium T4300	2.1 GHz	35 W		2.917	0.0163	61.44	737
Pentium 4-M 1.8	1.8 GHz	30 W		2.500	0.0163	61.44	737
Core Solo T1350	1.86 GHz	31 W		2.583	0.0163	61.44	737
Core Duo T2350	1.86 GHz	31 W		2.583	0.0163	61.44	737
Pentium Dual-Core T2130	1.86 GHz	31 W		2.583	0.0163	61.44	737
Pentium Dual-Core T2350	1.86 GHz	31 W		2.583	0.0163	61.44	737
Core i5-4200H	2.80 GHz	47 W		3.917	0.0164	61.00	732
Core i7-4900MQ	2.80 GHz	47 W		3.917	0.0164	61.00	732
Core i7-4702HQ	2.20 GHz	37 W		3.083	0.0164	60.89	731
Core i7-4702MQ	2.20 GHz	37 W		3.083	0.0164	60.89	731
Pentium 4-M 1.9	1.9 GHz	32 W		2.667	0.0164	60.80	730

Pentium M 730	1.6 GHz	27 W		2.250	0.0165	60.68	728
Pentium M 1.3	1.3 GHz	22 W		1.833	0.0165	60.51	726
Core 2 Extreme X7800	2.6 GHz	44 W		3.667	0.0165	60.51	726
Core Duo T2400	1.83 GHz	31 W		2.583	0.0165	60.45	725
Core i5-520UM	1.06 GHz	18 W		1.500	0.0166	60.30	724
Core i7-620UM	1.06 GHz	18 W		1.500	0.0166	60.30	724
Core i7-620UE	1.06 GHz	18 W		1.500	0.0166	60.30	724
Core 2 Duo T7200	2 GHz	34 W		2.833	0.0166	60.24	723
Core i7-4800MQ	2.70 GHz	47 W		3.917	0.0170	58.83	706
Pentium III-M 1266	1.26 GHz	22 W		1.833	0.0171	58.65	704
Celeron M 205	1.2 GHz	21 W		1.750	0.0171	58.51	702
Celeron M 330	1.4 GHz	24.5 W		2.042	0.0171	58.51	702
Celeron 440	2 GHz	35 W		2.917	0.0171	58.51	702
Core 2 Duo T5750	2 GHz	35 W		2.917	0.0171	58.51	702
Core 2 Duo T5800	2 GHz	35 W		2.917	0.0171	58.51	702
Core 2 Duo T5870	2 GHz	35 W		2.917	0.0171	58.51	702
Core 2 Duo T7250	2 GHz	35 W		2.917	0.0171	58.51	702
Core 2 Duo T7300	2 GHz	35 W		2.917	0.0171	58.51	702
Core 2 Duo T6400	2 GHz	35 W		2.917	0.0171	58.51	702
Celeron Dual-Core T3300	2.0 GHz	35 W		2.917	0.0171	58.51	702
Pentium Dual-Core T2410	2 GHz	35 W		2.917	0.0171	58.51	702
Pentium Dual-Core T3200	2 GHz	35 W		2.917	0.0171	58.51	702
Pentium T4200	2 GHz	35 W		2.917	0.0171	58.51	702
Celeron M 215	1.53 GHz	27 W		2.250	0.0172	58.03	696
Pentium 4-M 1.7	1.7 GHz	30 W		2.500	0.0172	58.03	696

Core 2 Extreme QX9300	2.53 GHz	45 W		3.750	0.0174	57.57	691
Core Duo T2250	1.73 GHz	31 W		2.583	0.0175	57.15	686
Pentium Dual-Core T2080	1.73 GHz	31 W		2.583	0.0175	57.15	686
Windsor F2 Athlon 64 X2	2000 MHz	35 W	1.025 - 1.075 V	2.917	0.0175	57.14	686
Pentium 4-M 1.5	1.5 GHz	26.9 W		2.242	0.0175	57.10	685
Core Solo T1200	1.5 GHz	27 W		2.250	0.0176	56.89	683
Core i7-3770T	2.5 GHz	45 W		3.750	0.0176	56.89	683
Celeron D 365	3.6 GHz	65 W		5.417	0.0176	56.71	681
Pentium III-M 1200	1.2 GHz	22 W		1.833	0.0179	55.85	670
Celeron Dual-Core T3100	1.9 GHz	35 W		2.917	0.0180	55.59	667
Pentium 4-M 1.4	1.4 GHz	25.8 W		2.150	0.0180	55.57	667
Brisbane G2 Athlon 64 X2	2500 MHz	45 W	1.15/1.20/1.25 V	3.750	0.0180	55.56	667
Core 2 Duo T5600	1.83 GHz	34 W		2.833	0.0181	55.12	661
Core Duo T2300	1.66 GHz	31 W		2.583	0.0182	54.83	658
Core Duo T2300E	1.66 GHz	31 W		2.583	0.0182	54.83	658
Pentium 4-M 1.6	1.6 GHz	30 W		2.500	0.0183	54.61	655
Celeron D 360	3.46 GHz	65 W		5.417	0.0183	54.51	654
Celeron Dual-Core T1500	1.86 GHz	35 W		2.917	0.0184	54.42	653
Pentium Dual-Core T2390	1.86 GHz	35 W		2.917	0.0184	54.42	653
Celeron M 320	1.3 GHz	24.5 W		2.042	0.0184	54.33	652
Core i7-4930MX	3.00 GHz	57 W		4.750	0.0186	53.89	647
Core 2 Duo T5550	1.83 GHz	35 W		2.917	0.0187	53.54	642

Celeron Dual-Core T1700	1.83 GHz	35 W		2.917	0.0187	53.54	642
Pentium III-M 1133	1.13 GHz	21.8 W		1.817	0.0188	53.08	637
Core Duo T2050	1.6 GHz	31 W		2.583	0.0189	52.85	634
Pentium Dual-Core T2060	1.6 GHz	31 W		2.583	0.0189	52.85	634
Celeron 430	1.8 GHz	35 W		2.917	0.0190	52.66	632
Core 2 Duo T5670	1.8 GHz	35 W		2.917	0.0190	52.66	632
Core 2 Duo T7100	1.8 GHz	35 W		2.917	0.0190	52.66	632
Core 2 Duo E8600	3.33 GHz	65 W		5.417	0.0191	52.46	630
Core i7-4700HQ	2.40 GHz	47 W		3.917	0.0191	52.29	627
Core i7-4700MQ	2.40 GHz	47 W		3.917	0.0191	52.29	627
Core 2 Duo T5300	1.73 GHz	34 W		2.833	0.0192	52.10	625
Pentium III-M 1066	1.06 GHz	21 W		1.750	0.0193	51.69	620
Core 2 Quad Q9100	2.26 GHz	45 W		3.750	0.0194	51.43	617
Brisbane G2 Athlon 64 X2	2300 MHz	45 W	1.15/1.20/1.25 V	3.750	0.0196	51.11	613
Brisbane G2 Athlon X2	2300 MHz	45 W	1.25V	3.750	0.0196	51.11	613
Celeron Dual-Core T1400	1.73 GHz	35 W		2.917	0.0198	50.61	607
Pentium Dual-Core T2370	1.73 GHz	35 W		2.917	0.0198	50.61	607
Core i5-680	3.6 GHz	73 W		6.083	0.0198	50.50	606
Celeron M 310	1.2 GHz	24.5 W		2.042	0.0199	50.16	602
Core 2 Duo T5450	1.66 GHz	34 W		2.833	0.0200	50.00	600
Core 2 Duo T5500	1.66 GHz	34 W		2.833	0.0200	50.00	600
Pentium III-M 1000	1 GHz	20.5 W		1.708	0.0200	49.95	599
Core 2 Duo E8500	3.16 GHz	65 W		5.417	0.0201	49.78	597

Core i7-3770S	3.1 GHz	65 W		5.417	0.0205	48.84	586
Core i7-4770S	3.1 GHz	65 W		5.417	0.0205	48.84	586
Celeron Dual-Core T1600	1.66 GHz	35 W		2.917	0.0206	48.57	583
Core i5-670	3.46 GHz	73 W		6.083	0.0206	48.53	582
Core 2 Duo E7600	3.06 GHz	65 W		5.417	0.0207	48.21	578
Pentium E6600	3.06 GHz	65 W		5.417	0.0207	48.21	578
Core 2 Duo T5200	1.6 GHz	34 W		2.833	0.0208	48.19	578
Core 2 Duo T5470	1.6 GHz	34 W		2.833	0.0208	48.19	578
Celeron 600	600 MHz	12.6 W		1.050	0.0210	47.62	571
Celeron 533A	533 MHz	11.2 W		0.933	0.0210	47.59	571
Celeron 566	566 MHz	11.9 W		0.992	0.0210	47.56	571
Core 2 Duo E6850	3 GHz	65 W		5.417	0.0212	47.26	567
Core 2 Duo E8400	3 GHz	65 W		5.417	0.0212	47.26	567
Celeron 420	1.6 GHz	35 W		2.917	0.0214	46.81	562
Pentium Dual-Core T2330	1.6 GHz	35 W		2.917	0.0214	46.81	562
Core i3-560	3.33 GHz	73 W		6.083	0.0214	46.71	561
Core i5-660	3.33 GHz	73 W		6.083	0.0214	46.71	561
Brisbane G2 Athlon X2	2100 MHz	45 W	1.15/1.20/1.25 V	3.750	0.0214	46.67	560
Brisbane G1 Athlon X2	2100 MHz	45 W	1.25V	3.750	0.0214	46.67	560
Core i7-4790K	4.0 GHz	88 W		7.333	0.0215	46.55	559
Core i7-3770K	3.5 GHz	77 W		6.417	0.0215	46.55	559
Pentium III-M 933	933 MHz	20.1 W		1.675	0.0215	46.42	557
Core 2 Duo E7500	2.93 GHz	65 W		5.417	0.0217	46.16	554
Pentium E6500	2.93 GHz	65 W		5.417	0.0217	46.16	554
Pentium E6500K	2.93 GHz	65 W		5.417	0.0217	46.16	554

Pentium III 1400	1.4 GHz	31.2 W		2.600	0.0218	45.95	551
Core 2 Quad Q9000	2 GHz	45 W		3.750	0.0220	45.51	546
Core i7-3770	3.4 GHz	77 W		6.417	0.0221	45.22	543
Core i3-550	3.2 GHz	73 W		6.083	0.0223	44.89	539
Core i5-650	3.2 GHz	73 W		6.083	0.0223	44.89	539
Core i5-655K	3.2 GHz	73 W		6.083	0.0223	44.89	539
Celeron D 350	3.2 GHz	73 W		6.083	0.0223	44.89	539
Mobile Pentium 4 3.06	3.06 GHz	70 W		5.833	0.0223	44.76	537
Mobile Pentium 4 HT 2.66	2.66 GHz	61 W		5.083	0.0224	44.65	536
Brisbane G2 Athlon 64 X2	2900 MHz	65 W	1.30-1.35 V	5.417	0.0224	44.62	535
Core 2 Duo E8300	2.83 GHz	65 W		5.417	0.0224	44.58	535
Core 2 Quad Q9505S	2.83 GHz	65 W		5.417	0.0224	44.58	535
Core 2 Quad Q9550S	2.83 GHz	65 W		5.417	0.0224	44.58	535
Pentium III 1400S	1.4 GHz	32.2 W or 31.2 W		2.683	0.0225	44.52	534
Pentium III-M 866	866 MHz	19.5 W		1.625	0.0225	44.41	533
Core i7-2600S	2.8 GHz	65 W		5.417	0.0227	44.11	529
Core 2 Duo E7400	2.8 GHz	65 W		5.417	0.0227	44.11	529
Pentium Dual-Core E5500	2.8 GHz	65 W		5.417	0.0227	44.11	529
Pentium E6300	2.8 GHz	65 W		5.417	0.0227	44.11	529
Core 2 Duo T5250	1.5 GHz	35 W		2.917	0.0228	43.89	527
PowerPC 970	1.8 GHz	42 W	1.3 V	3.500	0.0228	43.89	527
Mobile Pentium 4 HT 3.06	3.06GHz	70 W		5.833	0.0228	43.89	527

Celeron 1400	1.4 GHz	33.2 W		2.767	0.0232	43.18	518
Mobile Pentium 4 HT 3.2	3.2 GHz	76 W		6.333	0.0232	43.12	517
Brisbane G2 Athlon 64 X2	2800 MHz	65 W	1.325V - 1.375 V	5.417	0.0232	43.08	517
Core i3-540	3.06 GHz	73 W		6.083	0.0233	42.92	515
Celeron D 345	3.06 GHz	73 W		6.083	0.0233	42.92	515
Pentium 4 HT 661	3.6 GHz	86 W or 65 W		7.167	0.0233	42.87	514
Pentium Dual-Core T2310	1.46 GHz	35 W		2.917	0.0234	42.72	513
Core i7-4770K	3.5 GHz	84 W		7.000	0.0234	42.67	512
Pentium Dual-Core E5400	2.7 GHz	65 W		5.417	0.0235	42.54	510
Pentium 4 2.6	2.6 GHz	62.6 W		5.217	0.0235	42.53	510
Celeron 2.6	2.6 GHz	62.6 W		5.217	0.0235	42.53	510
Pentium III 1266S	1.26 GHz	30.4 W or 29.5 W		2.533	0.0236	42.44	509
Core i7-840QM	1.86 GHz	45 W		3.750	0.0236	42.33	508
Brisbane G1 Athlon 64 X2	1900 MHz	45 W	1.25V	3.750	0.0237	42.22	507
Pentium 4 2.53	2.53 GHz	61.5 W		5.125	0.0237	42.13	506
Pentium 4 2.5	2.5 GHz	61 W		5.083	0.0238	41.97	504
Celeron 2.5	2.5 GHz	61 W		5.083	0.0238	41.97	504
Pentium 4 2.8	2.8 GHz	68.4 W		5.700	0.0239	41.92	503
Pentium 4 2.8B	2.8 GHz	68.4 W		5.700	0.0239	41.92	503
Celeron 2.8	2.8 GHz	68.4 W		5.700	0.0239	41.92	503
Mobile Pentium 4 2.8	2.8 GHz	68.4 W		5.700	0.0239	41.92	503

Mobile Pentium 4 HT 2.8	2.8 GHz	68.4 W		5.700	0.0239	41.92	503
Core 2 Duo E6700	2.66 GHz	65 W		5.417	0.0239	41.91	503
Core 2 Duo E6750	2.66 GHz	65 W		5.417	0.0239	41.91	503
Core 2 Duo E7300	2.66 GHz	65 W		5.417	0.0239	41.91	503
Core 2 Duo E8190	2.66 GHz	65 W		5.417	0.0239	41.91	503
Core 2 Duo E8200	2.66 GHz	65 W		5.417	0.0239	41.91	503
Core 2 Quad Q8400S	2.66 GHz	65 W		5.417	0.0239	41.91	503
Core 2 Quad Q9400S	2.66 GHz	65 W		5.417	0.0239	41.91	503
Celeron 1200	1.2 GHz	29.5 W		2.458	0.0240	41.65	500
Celeron 1300	1.3 GHz	32 W		2.667	0.0240	41.60	499
Brisbane G2 Athlon 64 X2	2700 MHz	65 W	1.325/1.35/1.375 V	5.417	0.0241	41.54	498
Pentium 4 HT 650	3.4 GHz	84 W		7.000	0.0241	41.45	497
Celeron 2.7	2.7 GHz	66.8 W		5.567	0.0242	41.39	497
Pentium 4 2.26	2.26 GHz	56.0 W		4.667	0.0242	41.33	496
Pentium 4 2.66	2.66 GHz	66.1 W		5.508	0.0243	41.21	494
Mobile Pentium 4 2.66	2.66 GHz	66.1 W		5.508	0.0243	41.21	494
Pentium 4 HT 2.8C	2.8 GHz	69.7 W		5.808	0.0243	41.14	494
Core i3-530	2.93 GHz	73 W		6.083	0.0243	41.10	493
Celeron D 340	2.93 GHz	73 W		6.083	0.0243	41.10	493
Pentium III 1200	1.2 GHz	29.9 W		2.492	0.0243	41.10	493
Pentium 4 2.4	2.4 GHz	59.8 W		4.983	0.0243	41.10	493
Pentium 4 2.4B	2.4 GHz	59.8 W		4.983	0.0243	41.10	493
Celeron 2.4	2.4 GHz	59.8 W		4.983	0.0243	41.10	493
Mobile Pentium 4 2.4	2.4 GHz	59.8 W		4.983	0.0243	41.10	493
Core 2 Duo T5270	1.4 GHz	35 W		2.917	0.0244	40.96	492
Core 2 Duo E4700	2.6 GHz	65 W		5.417	0.0244	40.96	492

Pentium Dual-Core E5300	2.6 GHz	65 W		5.417	0.0244	40.96	492
Pentium 4 2.2	2.2 GHz	55.18 W		4.598	0.0245	40.83	490
Celeron D 355	3.33 GHz	84 W		7.000	0.0246	40.59	487
Pentium 4 HT 651	3.4 GHz	86 W or 65 W		7.167	0.0247	40.48	486
Celeron 2.3	2.3 GHz	58.3 W		4.858	0.0248	40.40	485
Mobile Pentium 4 HT 552	3.46 GHz	88 W		7.333	0.0248	40.26	483
Pentium III 1333	1.33 GHz	33.9 W		2.825	0.0249	40.17	482
Pentium III 1133S	1.13 GHz	28.9 W or 27.9 W		2.408	0.0250	40.04	480
Core 2 Extreme X6800	2.93 GHz	75 W		6.250	0.0250	40.00	480
Windsor Athlon 64 X2	2600 MHz	65 W	1.20 - 1.25 V	5.417	0.0250	40.00	480
Windsor Athlon 64 X2	2600 MHz	65 W	1.20 - 1.25 V	5.417	0.0250	40.00	480
Brisbane Athlon 64 X2	2600 MHz	65 W	1.25 - 1.35 V	5.417	0.0250	40.00	480
Brisbane Athlon 64 X2	2600 MHz	65 W	1.25 - 1.35 V	5.417	0.0250	40.00	480
Pentium 4 HT 3.2	3.2 GHz	82 W		6.833	0.0250	39.96	480
Core 2 Duo E7200	2.53 GHz	65 W		5.417	0.0251	39.86	478
Pentium III 1133	1.13 GHz	29.1 W		2.425	0.0251	39.76	477
Pentium III 1133	1.13 GHz	29.1 W		2.425	0.0251	39.76	477
Core i7-940XM	2.13 GHz	55 W		4.583	0.0252	39.66	476
Celeron D 356	3.33 GHz	86 or 65		7.167	0.0252	39.65	476

		W					
Celeron 2.2	2.2 GHz	57.1 W		4.758	0.0253	39.45	473
Celeron Dual-Core E3300	2.5 GHz	65 W		5.417	0.0254	39.38	473
Pentium Dual-Core E5200	2.5 GHz	65 W		5.417	0.0254	39.38	473
Core i7-740QM	1.73 GHz	45 W		3.750	0.0254	39.37	472
Core i7-820QM	1.73 GHz	45 W		3.750	0.0254	39.37	472
Celeron D 335	2.8 GHz	73 W		6.083	0.0255	39.28	471
Pentium G6950	2.8 GHz	73 W		6.083	0.0255	39.28	471
Core i5-661	3.33 GHz	87 W		7.250	0.0255	39.19	470
Pentium 4 HT 3.4	3.4 GHz	89 W		7.417	0.0256	39.12	469
Pentium 4 HT 3.4E	3.4 GHz	89 W		7.417	0.0256	39.12	469
Pentium 4 2.0A	2.0 GHz	52.4 W		4.367	0.0256	39.08	469
Pentium 4 HT 540	3.2 GHz	84 W		7.000	0.0256	39.01	468
Pentium 4 HT 540J	3.2 GHz	84 W		7.000	0.0256	39.01	468
Pentium 4 HT 541	3.2 GHz	84 W		7.000	0.0256	39.01	468
Pentium 4 HT 640	3.2 GHz	84 W		7.000	0.0256	39.01	468
Celeron D 351	3.2 GHz	84 W		7.000	0.0256	39.01	468
Celeron 2.0	2 GHz	52.8 W		4.400	0.0258	38.79	465
Mobile Pentium 4 HT 548	3.33 GHz	88 W		7.333	0.0258	38.75	465
Celeron 2.1	2.1 GHz	55.5 W		4.625	0.0258	38.75	465
Pentium 4 HT 2.6	2.6 GHz	69 W		5.750	0.0259	38.59	463
UltraSPARC IIe Hummingbird	500 MHz	13 W		1.083	0.0260	38.46	462
Brisbane G1 Athlon 64 X2	2500 MHz	65 W	1.25V - 1.35 V	5.417	0.0260	38.46	462

Brisbane G2 Athlon 64 X2	2500 MHz	65 W	1.325 - 1.375V	5.417	0.0260	38.46	462
Pentium 4 3.06	3.06 GHz	81.8 W		6.817	0.0261	38.31	460
Celeron 1100A	1.1 GHz	29.5 W		2.458	0.0262	38.18	458
Pentium 4 HT 641	3.2 GHz	86 W or 65 W		7.167	0.0262	38.10	457
Celeron D 352	3.2 GHz	86 or 65 W		7.167	0.0262	38.10	457
Core 2 Duo E4600	2.4 GHz	65 W		5.417	0.0264	37.81	454
Core 2 Duo E6600	2.4 GHz	65 W		5.417	0.0264	37.81	454
Celeron Dual-Core E1600	2.4 GHz	65 W		5.417	0.0264	37.81	454
Celeron Dual-Core E3200	2.4 GHz	65 W		5.417	0.0264	37.81	454
Pentium Dual-Core E2220	2.4 GHz	65 W		5.417	0.0264	37.81	454
Core i7-2700K	3.5 GHz	95 W		7.917	0.0265	37.73	453
Pentium 4 HT 3.0	3 GHz	81.9 W		6.825	0.0267	37.51	450
Celeron D 330	2.66 GHz	73 W		6.083	0.0268	37.31	448
Pentium 4 519	3.06 GHz	84 W		7.000	0.0268	37.30	448
Pentium 4 519J	3.06 GHz	84 W		7.000	0.0268	37.30	448
Pentium 4 519K	3.06 GHz	84 W		7.000	0.0268	37.30	448
Pentium 4 HT 524	3.06 GHz	84 W		7.000	0.0268	37.30	448
Celeron D 345J	3.06 GHz	84 W		7.000	0.0268	37.30	448
Celeron D 346	3.06 GHz	84 W		7.000	0.0268	37.30	448
Core i7-920XM	2 GHz	55 W		4.583	0.0269	37.24	447
Mobile Pentium 4 HT 538	3.2 GHz	88 W		7.333	0.0269	37.24	447

Pentium 4 1.8A	1.8 GHz	49.6 W		4.133	0.0269	37.16	446
Pentium 4 HT 2.4C	2.4 GHz	66.2 W		5.517	0.0269	37.12	445
Pentium III 1000	1 GHz	27.6 W		2.300	0.0270	37.10	445
UltraSPARC IIi Phantom	650 MHz	17.6 W		1.467	0.0271	36.93	443
Windsor Athlon 64 X2	2400 MHz	65 W	1.20 - 1.25 V	5.417	0.0271	36.92	443
Windsor F2 Athlon 64 X2	2400 MHz	65 W	1.20 - 1.25 V	5.417	0.0271	36.92	443
Brisbane G2 Athlon 64 X2	2400 MHz	65 W	1.325/1.35/1.375 V	5.417	0.0271	36.92	443
Pentium 4 HT 3.2E	3.2 GHz	89 W		7.417	0.0272	36.82	442
Core 2 Duo E6540	2.33 GHz	65 W		5.417	0.0272	36.71	440
Core 2 Duo E6550	2.33 GHz	65 W		5.417	0.0272	36.71	440
Core 2 Quad Q8200S	2.33 GHz	65 W		5.417	0.0272	36.71	440
Core i7-2600	3.4 GHz	95 W		7.917	0.0273	36.65	440
Core i7-2600K	3.4 GHz	95 W		7.917	0.0273	36.65	440
Pentium D 945	3.4 GHz	95 W		7.917	0.0273	36.65	440
Pentium 4 HT 530	3 GHz	84 W		7.000	0.0273	36.57	439
Pentium 4 HT 530J	3 GHz	84 W		7.000	0.0273	36.57	439
Pentium 4 HT 531	3 GHz	84 W		7.000	0.0273	36.57	439
Pentium 4 HT 630	3 GHz	84 W		7.000	0.0273	36.57	439
Celeron D 347	3.06 GHz	86 or 65 W		7.167	0.0274	36.44	437
Core i7-720QM	1.6 GHz	45 W		3.750	0.0275	36.41	437
Pentium 4 HT 631	3 GHz	86 W or 65 W (D0 Stepping)		7.167	0.0280	35.72	429

Pentium 4 515	2.93 GHz	84 W		7.000	0.0280	35.72	429
Pentium 4 515J	2.93 GHz	84 W		7.000	0.0280	35.72	429
Pentium 4 516	2.93 GHz	84 W		7.000	0.0280	35.72	429
Pentium 4 HT 517	2.93 GHz	84 W		7.000	0.0280	35.72	429
Celeron D 340J	2.93 GHz	84 W		7.000	0.0280	35.72	429
Celeron D 341	2.93 GHz	84 W		7.000	0.0280	35.72	429
Mobile Pentium 4 HT 532	3.06 GHz	88 W		7.333	0.0281	35.61	427
Pentium 4 HT Extreme Edition 3.2	3.2 GHz	92.1 W		7.675	0.0281	35.58	427
Celeron D 325	2.53 GHz	73 W		6.083	0.0282	35.49	426
Brisbane G1 Athlon 64 X2	2300 MHz	65 W	1.25/1.35 V	5.417	0.0283	35.38	425
Brisbane G2 Athlon 64 X2	2300 MHz	65 W	1.325/1.35/1.375 V	5.417	0.0283	35.38	425
Celeron 1000	1 GHz	29 W		2.417	0.0283	35.31	424
Pentium 4 1.6A	1.6 GHz	46.8 W		3.900	0.0286	35.01	420
Brisbane G2 Athlon 64 X2	3100 MHz	89 W	1.30 - 1.35 V	7.417	0.0287	34.83	418
Celeron 1000A	1 GHz	29.5 W		2.458	0.0288	34.71	417
Pentium Dual-Core E2200	2.2 GHz	65 W		5.417	0.0289	34.66	416
Core 2 Duo E4500	2.2 GHz	65 W		5.417	0.0289	34.66	416
Celeron Dual-Core E1500	2.2 GHz	65 W		5.417	0.0289	34.66	416
Pentium Dual-Core E2200	2.2 GHz	65 W		5.417	0.0289	34.66	416

Pentium Dual-Core E2210	2.2 GHz	65 W		5.417	0.0289	34.66	416
Pentium 4 HT 3.0E	3 GHz	89 W		7.417	0.0290	34.52	414
Pentium D 935	3.2 GHz	95 W		7.917	0.0290	34.49	414
Pentium III 933	933 MHz	27.3 W		2.275	0.0293	34.18	410
PowerPC 7400e	1.0 GHz	30 W	1.6 V	2.500	0.0293	34.13	410
Celeron 1100	1.1 GHz	33 W		2.750	0.0293	34.13	410
Pentium 4 510	2.8 GHz	84 W		7.000	0.0293	34.13	410
Pentium 4 510J	2.8 GHz	84 W		7.000	0.0293	34.13	410
Pentium 4 511	2.8 GHz	84 W		7.000	0.0293	34.13	410
Pentium 4 HT 520	2.8 GHz	84 W		7.000	0.0293	34.13	410
Pentium 4 HT 520J	2.8 GHz	84 W		7.000	0.0293	34.13	410
Pentium 4 HT 521	2.8 GHz	84 W		7.000	0.0293	34.13	410
Pentium 4 HT 620	2.8 GHz	84 W		7.000	0.0293	34.13	410
Celeron D 335J	2.8 GHz	84 W		7.000	0.0293	34.13	410
Celeron D 336	2.8 GHz	84 W		7.000	0.0293	34.13	410
Celeron 950	950 MHz	28 W		2.333	0.0295	33.93	407
Windsor Athlon 64 X2	2200 MHz	65 W	1.20 - 1.25 V	5.417	0.0295	33.85	406
Windsor F2 Athlon 64 X2	2200 MHz	65 W	1.20V/1.25 V	5.417	0.0295	33.85	406
Brisbane G1 Athlon 64 X2	2200 MHz	65 W	1.25/1.30/1.325 V	5.417	0.0295	33.85	406
Pentium 4 HT 570	3.8 GHz	115 W		9.583	0.0296	33.84	406
Pentium 4 HT 570J	3.8 GHz	115 W		9.583	0.0296	33.84	406
Pentium 4 HT 571	3.8 GHz	115 W		9.583	0.0296	33.84	406
Pentium 4 HT 670	3.8 GHz	115 W		9.583	0.0296	33.84	406
Pentium 4 HT 672	3.8 GHz	115 W		9.583	0.0296	33.84	406

Celeron 900	900 MHz	26.7 W		2.225	0.0297	33.71	404
Celeron D 320	2.4 GHz	73 W		6.083	0.0297	33.67	404
Core 2 Duo E6400	2.13 GHz	65 W		5.417	0.0298	33.56	403
Core 2 Duo E6305	2.13 GHz	65 W		5.417	0.0298	33.56	403
Core 2 Duo E6320	2.13 GHz	65 W		5.417	0.0298	33.56	403
Pentium 4 HT Extreme Edition 3.73	3.73 GHz	115 W		9.583	0.0301	33.21	399
Celeron 850	850 MHz	25.7 W		2.142	0.0302	33.07	397
Core i7-880	3.067 GHz	95 W		7.917	0.0302	33.06	397
Celeron 800	800 MHz	24.5 W		2.042	0.0306	32.65	392
Mobile Pentium 4 HT 518	2.8 GHz	88 W		7.333	0.0307	32.58	391
Celeron 766	766 MHz	23.6 W		1.967	0.0308	32.46	389
Pentium 4 505	2.66 GHz	84 W		7.000	0.0308	32.43	389
Pentium 4 505J	2.66 GHz	84 W		7.000	0.0308	32.43	389
Pentium 4 506	2.66 GHz	84 W		7.000	0.0308	32.43	389
Celeron D 330J	2.66 GHz	84 W		7.000	0.0308	32.43	389
Celeron D 331	2.66 GHz	84 W		7.000	0.0308	32.43	389
Athlon XP 2700+	2.16 GHz	68.3 W		5.692	0.0309	32.38	389
Pentium D 925	3 GHz	95 W		7.917	0.0309	32.34	388
Pentium D 930	3 GHz	95 W		7.917	0.0309	32.34	388
Core 2 Quad Q9650	3 GHz	95 W		7.917	0.0309	32.34	388
Brisbane G1 Athlon 64 X2	2100 MHz	65 W	1.25 - 1.35 V	5.417	0.0310	32.31	388
Pentium 4 2.8A	2.8 GHz	89 W		7.417	0.0310	32.22	387
Pentium 4 HT 2.8E	2.8 GHz	89 W		7.417	0.0310	32.22	387
Celeron 733	733 MHz	22.8 W		1.900	0.0311	32.15	386

Pentium 4 HT 662	3.6 GHz	115 W or 84 W		9.583	0.0312	32.06	385
Pentium 4 HT 560	3.6 GHz	115 W		9.583	0.0312	32.06	385
Pentium 4 HT 560J	3.6 GHz	115 W		9.583	0.0312	32.06	385
Pentium 4 HT 561	3.6 GHz	115 W		9.583	0.0312	32.06	385
Pentium 4 HT 660	3.6 GHz	115 W		9.583	0.0312	32.06	385
Pentium 4 HT Extreme Edition 3.46	3.46 GHz	110.7 W		9.225	0.0312	32.01	384
Celeron 700	700 MHz	21.9 W		1.825	0.0313	31.96	384
Athlon XP 2600+	2.13 GHz	68.3 W		5.692	0.0313	31.93	383
Pentium 4 HT Extreme Edition 3.4	3.4 GHz	109.6 W or 102.9 W		9.133	0.0315	31.77	381
Celeron D 315	2.26 GHz	73 W		6.083	0.0315	31.70	380
Core i7-860S	2.533 GHz	82 W		6.833	0.0316	31.63	380
Core i7-870	2.933 GHz	95 W		7.917	0.0316	31.61	379
Celeron 667	667 MHz	21.1 W		1.758	0.0316	31.61	379
Core i7-875K	2.93 GHz	95 W		7.917	0.0317	31.58	379
Pentium Dual-Core E2180	2 GHz	65 W		5.417	0.0317	31.51	378
Core 2 Duo E4400	2 GHz	65 W		5.417	0.0317	31.51	378
Celeron Dual-Core E1400	2 GHz	65 W		5.417	0.0317	31.51	378
Pentium Dual-Core E2180	2 GHz	65 W		5.417	0.0317	31.51	378
Windsor F3 Athlon 64 X2	2800 MHz	89 W	1.30 - 1.35 V	7.417	0.0318	31.46	378

UltraSPARC IIIi Jalapeño	1.593 GHz	52 W		4.333	0.0319	31.37	376
Celeron 633	633 MHz	20.2 W		1.683	0.0319	31.34	376
Pentium III 500E	500 MHz	16 W		1.333	0.0320	31.25	375
Athlon XP 1900+	1.6 GHz	52.5 W		4.375	0.0320	31.21	374
Celeron 1.8	1.8 GHz	59.1 W		4.925	0.0321	31.19	374
Athlon XP 2600+	2.08 GHz	68.3 W		5.692	0.0321	31.18	374
Pentium III 1000B	1 GHz	32.98 W		2.748	0.0322	31.05	373
Celeron D 325J	2.53 GHz	84 W		7.000	0.0324	30.84	370
Celeron D 326	2.53 GHz	84 W		7.000	0.0324	30.84	370
Windsor F2 Athlon 64 X2	2000 MHz	65 W	1.20 - 1.25 V	5.417	0.0325	30.77	369
Windsor F2 Athlon 64 X2	2000 MHz	65 W	1.20 - 1.25 V	5.417	0.0325	30.77	369
Athlon 64 X2 3800+	2000 MHz	65 W	1.20-1.25 V	5.417	0.0325	30.77	369
Athlon XP 1800+	1.53 GHz	51 W		4.250	0.0326	30.72	369
Pentium III 866	800 MHz	26.1 W		2.175	0.0326	30.65	368
Pentium 4 2.66A	2.66 GHz	89 W		7.417	0.0327	30.60	367
Core 2 Quad Q9505	2.83 GHz	95 W		7.917	0.0328	30.50	366
Core 2 Quad Q9550	2.83 GHz	95 W		7.917	0.0328	30.50	366
Pentium 4 HT 550	3.4 GHz	115 W or 84 W		9.583	0.0330	30.27	363
Pentium 4 HT 550J	3.4 GHz	115 W or 84 W		9.583	0.0330	30.27	363
Pentium 4 HT 551	3.4 GHz	115 W or 84 W		9.583	0.0330	30.27	363
Athlon XP 1700+	1.46 GHz	49.4 W		4.117	0.0330	30.26	363

Pentium D 820	2.8 GHz	95 W		7.917	0.0331	30.18	362
Pentium D 915	2.8 GHz	95 W		7.917	0.0331	30.18	362
Pentium D 920	2.8 GHz	95 W		7.917	0.0331	30.18	362
Core i5-760	2.8 GHz	95 W		7.917	0.0331	30.18	362
Core i7-860	2.8 GHz	95 W		7.917	0.0331	30.18	362
Pentium III 667	667 MHz	22.61 W or 21.95 W		1.842	0.0331	30.18	362
Athlon XP 2400+	2.0 GHz	68.3 W		5.692	0.0333	29.99	360
Athlon XP 2700+	2 GHz	68.3 W		5.692	0.0333	29.99	360
Core i5-750S	2.4 GHz	82 W		6.833	0.0334	29.97	360
Celeron D 310	2.13 GHz	73 W		6.083	0.0335	29.88	359
Athlon XP 3000+	2.16 GHz	74.3 W		6.192	0.0336	29.77	357
Pentium III 533EB	533 MHz	18.02 W or 17.49 W		1.502	0.0338	29.58	355
Athlon XP 1600+	1.4 GHz	48.5 W		4.042	0.0338	29.56	355
Pentium III 550E	550 MHz	18.7 W or 18.15 W		1.558	0.0340	29.41	353
Pentium III 650	650 MHz	22.1 W or 21.45 W		1.842	0.0340	29.41	353
Pentium III 800	800 MHz	27.2 W or 26.4 W		2.267	0.0340	29.41	353
Pentium Extreme Edition 965	3.73 GHz	130 W		10.833	0.0340	29.38	353
Athlon XP 2200+	1.8 GHz	62.8 W		5.233	0.0341	29.35	352
Athlon XP 3200+	2.2 GHz	76.8 W		6.400	0.0341	29.33	352

Core 2 Duo E6300	1.86 GHz	65 W		5.417	0.0341	29.30	352
Core 2 Duo E6305	1.86 GHz	65 W		5.417	0.0341	29.30	352
Core 2 Duo E6320	1.86 GHz	65 W		5.417	0.0341	29.30	352
Pentium III 1133	1.13 GHz	39.55 W		3.296	0.0342	29.26	351
Athlon 64 X2 3600+	1900 MHz	65 W	1.25V-1.35 V	5.417	0.0342	29.23	351
Windsor Athlon 64 X2 5000+	2600 MHz	89 W	1.30 - 1.35 V	7.417	0.0342	29.21	351
Windsor F2 Athlon 64 X2 5000+	2600 MHz	89 W	1.30 - 1.35 V	7.417	0.0342	29.21	351
Core i7-4820K	3.7 GHz	130 W		10.833	0.0343	29.14	350
Pentium III 1000	1 GHz	35.35 W or 32.98 W		2.946	0.0345	28.97	348
Pentium D 805	2.66 GHz	95 W		7.917	0.0349	28.67	344
Core 2 Quad Q6700	2.66 GHz	95 W		7.917	0.0349	28.67	344
Core 2 Quad Q8400	2.66 GHz	95 W		7.917	0.0349	28.67	344
Core 2 Quad Q9400	2.66 GHz	95 W		7.917	0.0349	28.67	344
Core 2 Quad Q9450	2.66 GHz	95 W		7.917	0.0349	28.67	344
Core i5-750	2.66 GHz	95 W		7.917	0.0349	28.67	344
Athlon XP 2600+	1.91 GHz	68.3 W		5.692	0.0349	28.64	344
Athlon XP 2100+	1.73 GHz	62.1 W		5.175	0.0351	28.53	342
Pentium 4 2.0 (Socket 423)	2 GHz	71.8 W		5.983	0.0351	28.52	342
Pentium III 1100	1.1 GHz	39.55 W		3.296	0.0351	28.48	342
Pentium III 933	933 MHz	32.9 W or 30.09 W		2.742	0.0353	28.36	340

Core 2 Duo E4300	1.8 GHz	65 W		5.417	0.0353	28.36	340
Pentium Dual-Core E2160	1.8 GHz	65 W		5.417	0.0353	28.36	340
Pentium D 960	3.6 GHz	130 W or 95 W		10.833	0.0353	28.36	340
Core i7-4960X Extreme Edition	3.6 GHz	130 W		10.833	0.0353	28.36	340
Athlon XP 2000+	1.66 GHz	60.3 W		5.025	0.0355	28.19	338
Athlon XP 2000+	1.66 GHz	60.3 W		5.025	0.0355	28.19	338
Pentium III 866	866 MHz	30.8 W, 27.71 W or 26.9 W		2.567	0.0356	28.12	337
Pentium 4 1.9 (Socket 423)	1.9 GHz	69.2 W		5.767	0.0356	28.12	337
Pentium III 850	850 MHz	30.28 W, 27.54 W or 26.73 W		2.523	0.0356	28.07	337
Pentium III 900	900 MHz	32.2 W or 28.9 W		2.683	0.0358	27.95	335
Pentium 4 1.8 (Socket 478)	1.8 GHz	66.1 W		5.508	0.0359	27.89	335
Celeron 1.8	1.8 GHz	66.1 W		5.508	0.0359	27.89	335
Pentium 4 1.8 (Socket 423)	1.8 GHz	66.7 W		5.558	0.0362	27.63	332
Pentium 4 2.4A	2.4 GHz	89 W		7.417	0.0362	27.61	331

Pentium III 800EB	800 MHz	29.05 W, 27.2 W or 26.4 W		2.421	0.0363	27.54	330
Athlon XP 2500+	1.83 GHz	68.3 W		5.692	0.0364	27.44	329
Pentium 4 1.7 (Socket 478)	1.7 GHz	63.5 W		5.292	0.0365	27.41	329
Celeron 1.7	1.7 GHz	63.5 W		5.292	0.0365	27.41	329
Pentium III 750	750 MHz	27.48 W, 25.5 W or 24.75 W		2.290	0.0366	27.29	328
Pentium Extreme Edition 955	3.46 GHz	130 W		10.833	0.0367	27.25	327
Pentium III 600	600 MHz	22.05 W or 20.4 W		1.838	0.0368	27.21	327
Pentium 4 1.7 (Socket 423)	1.7 GHz	64 W		5.333	0.0368	27.20	326
Pentium III 733	733 MHz	26.95 W, 24.82 W or 24.09 W		2.246	0.0368	27.20	326
Pentium 4 2.0 (Socket 478)	2 GHz	75.3 W		6.275	0.0368	27.20	326
Pentium III 600EB	600 MHz	22.1 W, 21.45 W or 20.4 W		1.842	0.0368	27.15	326

Pentium III 600E	600 MHz	22.1 W or 21.45 W		1.842	0.0368	27.15	326
Athlon XP 2200+	1.8 GHz	67.9 W or 62.8 W		5.658	0.0368	27.15	326
Pentium III 700	700 MHz	25.9 W, 23.8 W or 23.1 W		2.158	0.0370	27.03	324
Windsor Athlon 64 X2 4600+	2400 MHz	89 W	1.30 - 1.35 V	7.417	0.0371	26.97	324
Windsor F2 Athlon 64 X2 4800+	2400 MHz	89 W	1.30 - 1.35 V	7.417	0.0371	26.97	324
Pentium 4 1.6 (Socket 478)	1.6 GHz	60.8 W		5.067	0.0371	26.95	323
Core 2 Quad Q8300	2.5 GHz	95 W		7.917	0.0371	26.95	323
Core 2 Quad Q9300	2.5 GHz	95 W		7.917	0.0371	26.95	323
Pentium 4 1.6 (Socket 423)	1.6 GHz	61 W		5.083	0.0372	26.86	322
Pentium D 950	3.4 GHz	130 W or 95 W		10.833	0.0373	26.78	321
Core i7-4930K	3.4 GHz	130 W		10.833	0.0373	26.78	321
Pentium III 1000	800 MHz	29.9 W		2.492	0.0374	26.76	321
Pentium 4 1.9 (Socket 478)	1.9 GHz	72.8 W		6.067	0.0374	26.73	321
Pentium 4 1.5 (Socket 423)	1.5 GHz	57.8 W		4.817	0.0376	26.57	319

Pentium 4 1.5 (Socket 478)	1.5 GHz	57.9 W		4.825	0.0377	26.53	318
Core i7-980X Extreme Edition	3.333 GHz	130 W		10.833	0.0381	26.25	315
Core i7-975 Extreme Edition	3.333 GHz	130 W		10.833	0.0381	26.25	315
Mobile Pentium II 333	333 MHz	12.7 W		1.058	0.0381	26.22	315
Pentium 4 1.4 (Socket 423)	1.4 GHz	54.7 W		4.558	0.0382	26.21	315
Core i7 3960X Extreme Edition	3.3 GHz	130 W		10.833	0.0385	25.99	312
Mobile Pentium II 366	366 MHz	14.1 W		1.175	0.0385	25.96	311
Pentium 4 1.4 (Socket 478)	1.4 GHz	55.3 W		4.608	0.0386	25.92	311
Mobile Pentium II 233	233 MHz	9 W		0.750	0.0386	25.89	311
Mobile Pentium II 300	300 MHz	11.6 W		0.967	0.0387	25.86	310
Mobile Pentium II 266	266 MHz	10.3 W		0.858	0.0387	25.83	310
Pentium 4 1.3	1.3 GHz	51.6 W		4.300	0.0388	25.80	310
Windsor F3 Athlon 64 X2 6400+ Black Edition	3200 MHz	125 W	1.35 - 1.40 V	10.417	0.0391	25.60	307
Core i7-5930K	3.5 GHz	140 W		11.667	0.0391	25.60	307
Core 2 Duo E4200	1.6 GHz	65 W		5.417	0.0397	25.21	302
Celeron Dual-Core E1200	1.6 GHz	65 W		5.417	0.0397	25.21	302
Pentium Dual-Core E2140	1.6 GHz	65 W		5.417	0.0397	25.21	302
Pentium D 940	3.2 GHz	130 W or 95 W		10.833	0.0397	25.21	302

Core i7-3930K	3.2 GHz	130 W		10.833	0.0397	25.21	302
Pentium D 840	3.2 GHz	130 W		10.833	0.0397	25.21	302
Pentium Extreme Edition 840	3.2 GHz	130 W		10.833	0.0397	25.21	302
Core i7-960	3.2 GHz	130 W		10.833	0.0397	25.21	302
Core i7-965 Extreme Edition	3.2 GHz	130 W		10.833	0.0397	25.21	302
Core i7-970	3.2 GHz	130 W		10.833	0.0397	25.21	302
Core 2 Quad Q8200	2.33 GHz	95 W		7.917	0.0398	25.11	301
Mobile Pentium II 266PE	266 MHz	10.6 W		0.883	0.0398	25.09	301
Mobile Pentium II 300PE	300 MHz	12 W		1.000	0.0400	25.00	300
Windsor Athlon 64 X2 4200+	2200 MHz	89 W	1.30 - 1.35 V	7.417	0.0405	24.72	297
Athlon 64 X2 4200+	2200 MHz	89 W	1.30-1.40 V	7.417	0.0405	24.72	297
Windsor F2 Athlon 64 X2 4400+	2200 MHz	89 W	1.30V/1.35 V	7.417	0.0405	24.72	297
Athlon XP 2100+	1.73 GHz	72 W		6.000	0.0406	24.60	295
Athlon XP 2000+	1.66 GHz	70 W		5.833	0.0412	24.28	291
Core i7-950	3.067 GHz	130 W		10.833	0.0414	24.16	290
Core i7-5820K	3.3 GHz	140 W		11.667	0.0414	24.14	290
Athlon XP 1900+	1.6 GHz	68 W		5.667	0.0415	24.09	289
Core 2 Extreme QX9770	3.2 GHz	136 W		11.333	0.0415	24.09	289
Windsor F3 Athlon 64 X2 6000+	3000 MHz	125 W	1.35 - 1.40 V	10.417	0.0417	24.00	288
Core i7 3970X Extreme Edition	3.5 GHz	150 W		12.500	0.0419	23.89	287
Athlon XP 1800+	1.53 GHz	66 W		5.500	0.0421	23.74	285

Pentium D 830	3 GHz	130 W		10.833	0.0423	23.63	284
Core 2 Extreme QX6850	3 GHz	130 W		10.833	0.0423	23.63	284
Core 2 Extreme QX9650	3 GHz	130 W		10.833	0.0423	23.63	284
Core 2 Quad Q6600	2.4 GHz	105 W or 95 W		8.750	0.0427	23.41	281
Athlon XP 1700+	1.46 GHz	64 W		5.333	0.0428	23.36	280
Core i7-940	2.933 GHz	130 W		10.833	0.0433	23.10	277
Core 2 Extreme QX6800	2.93 GHz	130 W		10.833	0.0433	23.08	277
Athlon XP 1600+	1.4 GHz	62.8 W		5.233	0.0438	22.83	274
Athlon XP 1500+	1.33 GHz	60 W		5.000	0.0441	22.70	272
Athlon 1000B	1.2 GHz	54.3 W		4.525	0.0442	22.63	272
Athlon 64 X2 3800+	2000 MHz	89 W/89 W	1.30-1.40 V	7.417	0.0445	22.47	270
Windsor F2 Athlon 64 X2 3800+	2000 MHz	89 W	1.30 - 1.35 V	7.417	0.0445	22.47	270
Core i7-930	2.8 GHz	130 W		10.833	0.0453	22.06	265
Core i7-5960X Extreme Edition	3 GHz	140 W		11.667	0.0456	21.94	263
Core 2 Extreme QX9775	3.2 GHz	150 W		12.500	0.0458	21.85	262
Athlon 64 X2 4800+	2400 MHz	110 W	1.30-1.40 V	9.167	0.0458	21.82	262
Athlon 64 X2 4600+	2400 MHz	110 W	1.30-1.40 V	9.167	0.0458	21.82	262
Core i7-920	2.667 GHz	130 W		10.833	0.0476	21.01	252
Core 2 Extreme QX6700	2.66 GHz	130 W		10.833	0.0477	20.95	251
Pentium III 800	800 MHz	38.2 W		3.183	0.0478	20.94	251
UltraSPARC IV+ Panther	1.8 GHz	90 W		7.500	0.0488	20.48	246

Athlon 64 X2 4400+	2200 MHz	89 W/110 W	1.30-1.40 V	9.167	0.0500	20.00	240
UltraSPARC T1 Niagara	1.4 GHz	72 W		6.000	0.0502	19.91	239
Athlon 1400B	1.4 GHz	72.1 W		6.008	0.0503	19.88	239
Athlon 1400C	1.4 GHz	72.1 W		6.008	0.0503	19.88	239
Athlon 1333C	1.33 GHz	69.8 W		5.817	0.0513	19.51	234
Athlon 1300B	1.3 GHz	68.3 W		5.692	0.0513	19.49	234
Athlon 1266C	1.26 GHz	66.9 W		5.575	0.0519	19.29	231
Athlon 850 (Slot A)	850 MHz	44.8 W		3.733	0.0527	18.97	228
Athlon 850 (Socket A)	850 MHz	44.8 W		3.733	0.0527	18.97	228
Athlon 1000 (Socket A)	1 GHz	54 W		4.500	0.0527	18.96	228
Athlon 1000 (Slot A)	1 GHz	54.3 W		4.525	0.0530	18.86	226
Celeron 533	533 MHz	28.3 W		2.358	0.0531	18.83	226
Athlon 800 (Slot A)	800 MHz	42.6 W		3.550	0.0533	18.78	225
Athlon 800 (Socket A)	800 MHz	42.6 W		3.550	0.0533	18.78	225
Athlon 750	750 MHz	40 W		3.333	0.0533	18.75	225
Athlon 1200B	1.2 GHz	65.7 W		5.475	0.0535	18.70	224
Athlon 1200C	1.2 GHz	65.7 W		5.475	0.0535	18.70	224
Athlon 1100B	1.1 GHz	60.3 W		5.025	0.0535	18.68	224
Athlon 1133C	1.13 GHz	62.1 W		5.175	0.0537	18.63	224
Athlon 1000C	1 GHz	55.1 W		4.592	0.0538	18.58	223
Athlon 750 (Slot A)	750 MHz	40.4 W		3.367	0.0539	18.56	223
Athlon 750 (Socket A)	750 MHz	40.4 W		3.367	0.0539	18.56	223
Celeron 500	500 MHz	27.2 W		2.267	0.0544	18.38	221
Athlon 700 (Slot A)	700 MHz	38.3 W		3.192	0.0547	18.28	219
Athlon 700 (Socket A)	700 MHz	38.3 W		3.192	0.0547	18.28	219
Athlon 950 (Slot A)	950 MHz	52 W		4.333	0.0547	18.27	219

Athlon 950 (Socket A)	950 MHz	52 W		4.333	0.0547	18.27	219
Celeron 466	466 MHz	25.7 W		2.142	0.0552	18.13	218
Athlon 900 (Slot A)	900 MHz	49.7 W		4.142	0.0552	18.11	217
Athlon 900 (Socket A)	900 MHz	49.7 W		4.142	0.0552	18.11	217
Athlon 650	650 MHz	36 W		3.000	0.0554	18.06	217
Athlon 650 (Slot A)	650 MHz	36.1 W		3.008	0.0555	18.01	216
Athlon 650 (Socket A)	650 MHz	36.1 W		3.008	0.0555	18.01	216
Celeron 433	433 MHz	24.1 W		2.008	0.0557	17.97	216
Athlon 700	700 MHz	39 W		3.250	0.0557	17.95	215
Athlon 550	550 MHz	31 W		2.583	0.0564	17.74	213
Athlon 600	600 MHz	34 W		2.833	0.0567	17.65	212
Celeron 433	433 MHz	24.6 W		2.050	0.0568	17.60	211
UltraSPARC T2 Niagara 2	1.6 GHz	95 W		7.917	0.0580	17.25	207
Athlon 850	850 MHz	50 W		4.167	0.0588	17.00	204
Celeron 400	400 MHz	23.7 W		1.975	0.0593	16.88	203
Celeron 400	400 MHz	23.7 W		1.975	0.0593	16.88	203
Celeron 366	366 MHz	21.7 W		1.808	0.0593	16.87	202
Celeron 366	366 MHz	21.7 W		1.808	0.0593	16.87	202
Athlon 800	800 MHz	48 W		4.000	0.0600	16.67	200
Pentium II 450	450 MHz	27.1 W		2.258	0.0602	16.61	199
Athlon 1000	1 GHz	62 W		5.167	0.0605	16.52	198
Pentium II 400	400 MHz	24.3 W		2.025	0.0608	16.46	198
Celeron 300	300 MHz	18.4 W		1.533	0.0613	16.30	196
Pentium II 350	350 MHz	21.5 W		1.792	0.0614	16.28	195
Pentium II 333	333 MHz	20.6 W		1.717	0.0619	16.17	194
Pentium II 300	300 MHz	18.6 W		1.550	0.0620	16.13	194
Celeron 266	266 MHz	16.6 W		1.383	0.0624	16.02	192

Celeron 333	333 MHz	20.9 W		1.742	0.0628	15.93	191
Celeron 333	333 MHz	20.9 W		1.742	0.0628	15.93	191
Pentium II 266	266 MHz	16.8 W		1.400	0.0632	15.83	190
Celeron 300A	300 MHz	19 W		1.583	0.0633	15.79	189
Athlon 950	950 MHz	62 W		5.167	0.0653	15.32	184
Athlon 900	900 MHz	60 W		5.000	0.0667	15.00	180
Athlon 900	900 MHz	60 W		5.000	0.0667	15.00	180
Celeron 300A	300 MHz	20.9 W		1.742	0.0697	14.35	172
Pentium III 600	600 MHz	42.76 W		3.563	0.0713	14.03	168
Pentium III 600B	600 MHz	42.76 W		3.563	0.0713	14.03	168
Athlon 700	700 MHz	50 W		4.167	0.0714	14.00	168
Pentium III 550	550 MHz	39.8 W		3.317	0.0724	13.82	166
Pentium III 533B	533 MHz	39.04 W		3.253	0.0732	13.65	164
Pentium III 450	450 MHz	33.76 W		2.813	0.0750	13.33	160
Pentium III 500	500 MHz	37.52 W		3.127	0.0750	13.33	160
Pentium MMX	233 MHz	17.9 W		1.492	0.0768	13.02	156
UltraSPARC III Cu Cheetah+	1.015 GHz	80 W		6.667	0.0770	12.99	156
Pentium	150 MHz	11.6 W		0.967	0.0773	12.93	155
Pentium	200 MHz	15.5 W		1.292	0.0775	12.90	155
UltraSPARC IV Jaguar	1.35 GHz	108 W		9.000	0.0781	12.80	154
SPARC T4 Yosemite Falls	3.0 GHz	240 W		20.000	0.0781	12.80	154
Pentium MMX	200 MHz	15.7 W		1.308	0.0785	12.74	153
Pentium MMX	166 MHz	13.1 W		1.092	0.0789	12.67	152
SPARC T3 Rainbow Falls	1.65 GHz	139 W		11.583	0.0823	12.16	146
Athlon 650	650 MHz	54 W		4.500	0.0831	12.04	144

Athlon 600	600 MHz	50 W		4.167	0.0833	12.00	144
Athlon 600	600 MHz	50 W		4.167	0.0833	12.00	144
Athlon 550	550 MHz	46 W		3.833	0.0836	11.96	143
Athlon 550	550 MHz	46 W		3.833	0.0836	11.96	143
Athlon 500	500 MHz	42 W		3.500	0.0840	11.90	143
Pentium	133 MHz	11.2 W		0.933	0.0842	11.88	143
Pentium	166 MHz	14.5 W		1.208	0.0873	11.45	137
UltraSPARC III Cheetah	600 MHz	53 W		4.417	0.0883	11.32	136
Pentium	120 MHz	11.9 W		0.992	0.0992	10.08	121
Pentium	90 MHz	9.0 W		0.750	0.1000	10.00	120
Pentium	100 MHz	10.1 W		0.842	0.1010	9.90	119
Pentium	75 MHz	8.1 W		0.675	0.1080	9.26	111
K5 PR120	90 MHz	12.6 W		1.050	0.1400	7.14	86
K5 PR133	100 MHz	14 W		1.167	0.1400	7.14	86
K5 PR166	116.7 MHz	16.4 W		1.367	0.1405	7.12	85
Pentium II 300	300 MHz	43 W		3.583	0.1433	6.98	84
Pentium II 266	266 MHz	38.2 W		3.183	0.1436	6.96	84
Pentium II 233	233 MHz	34.8 W		2.900	0.1494	6.70	80
K5 PR75	75 MHz	11.8 W		0.983	0.1573	6.36	76
K5 PR100	100 MHz	15.8 W		1.317	0.1580	6.33	76
K5 PR90	90 MHz	14.3 W		1.192	0.1589	6.29	76
Pentium Pro 200 (256 KB L2 Cache)	200 MHz	35 W		2.917	0.1750	5.71	69
Pentium Pro 200 (256 KB L2 Cache)	200 MHz	35 W		2.917	0.1750	5.71	69
Pentium Pro 180	180 MHz	31.7 W		2.642	0.1761	5.68	68
Pentium Pro 180	180 MHz	31.7 W		2.642	0.1761	5.68	68

Pentium Pro 200 (512 KB L2 Cache)	200 MHz	37.9 W		3.158	0.1895	5.28	63
Pentium Pro 200 (512 KB L2 Cache)	200 MHz	37.9 W		3.158	0.1895	5.28	63
Pentium Pro 150	150 MHz	29.2 W		2.433	0.1947	5.14	62
Pentium Pro 150	150 MHz	29.2 W		2.433	0.1947	5.14	62
Pentium Pro 166	166 MHz	35 W		2.917	0.2108	4.74	57
Pentium Pro 166	166 MHz	35 W		2.917	0.2108	4.74	57
Pentium Pro 200 (1 MB L2 Cache)	200 MHz	47 W		3.917	0.2350	4.26	51

APPENDIX E – Car starter ratings

A selection of 44 car starters was reviewed using data from an auto parts supplier ("CAR PARTS from Mister Auto - Your Parts at discount prices," 2015). The data is presented in Table 9.

Brand	Model	Voltage (V)	Rated Power (kW)	Vehicle brands
CEVAM	3844	12	0.9	Ford
BOSCH	96017060	12	1.1	Ford
CEVAM	3124	12	2.2	Ford
CEVAM	9762	12	2.2	Daihatsu, Toyota
CEVAM	3611	12	1	Mitsubishi
CEVAM	3467	12	2.3	
VALEO	726044	12	2	Audi, VW
BOSCH	986021810	12	2	Citroen, Ford, Rover, Fiat
BOSCH	15540	12	2.2	Fiat, Mercedes, Seat
CEVAM	9504	12	0.9	Mitsubishi
BOSCH	12301	12	0.9	Mitsubishi
VALEO	438105	12	0.7	Mitsubishi
VALEO	455963	12	0.9	Mitsubishi
VALEO	455562	12	0.7	Mitsubishi
VALEO	438097	12	0.9	Mitsubishi
HERTH+BUSS	J5215005	12	0.9	Mitsubishi
BOLK	B051033	12	2	Mercedes
CEVAM	3869	12	2	Mercedes
BOSCH	21360	12	1.7	Mercedes
BOSCH	18270	12	2.3	Mercedes
BOSCH	17260	12	2	Mercedes
VALEO	726008	12	2	Mercedes
VALEO	432644	12	2.2	Mercedes
CEVAM	3034	12	2	Seat
CEVAM	3849	12	2	Seat
CEVAM	3636	12	1.7	Seat
BOSCH	17460	12	2	Seat

BOSCH	16980	12	1.8	Seat
VALEO	726029	12	1.9	Seat
VALEO	726019	12	1.8	Seat
VALEO	726034	12	1.8	Seat
VALEO	438075	12	2	Seat
VALEO	433268	12	1.7	Seat
VALEO	455675	12	1.8	Seat
VALEO	436050	12	1.7	Seat
VALEO	438076	12	2	Seat
CEVAM	3141	12	1.1	Opel
BOSCH	21240	12	1.1	Opel
BOSCH	22730	12	1.8	Opel
VALEO	726039	12	1.3	Opel
VALEO	458375	12	1.2	Opel
VALEO	438168	12	1.3	Opel
VALEO	458178	12	2.4	Opel
VALEO	458351	12	1.8	Opel

Table 9 - Selected specifications for a sampling of car starters
source: http://www.mister-auto.ie/en/