

# Future Trends in Mobile Commerce: Service Offerings, Technological Advances and Security Challenges

Ali Grami and Bernadette H. Schell

Faculty of Business and Information Technology  
University of Ontario Institute of Technology  
ali.grami@uoit.ca and bernadette.schell@uoit.ca

**Abstract**—Driven by the ubiquitous deployment of mobile systems, the widespread use of the Internet, the rapid advances in wireless technologies, the insatiable demand for high-speed interactive multimedia services, and the growing need for secure wireless machine-to-machine communications, mobile commerce is rapidly approaching the business forefront. In this paper, future trends in major aspects of mobile commerce are discussed. In light of the fact that the highly-personalized, context-aware, location-sensitive, time-critical, pin-point information presentation forms the basis upon which promising applications can be built, mobile commerce services are presented. In order to provide a multitude of attractive applications and ensure their success in future, a plethora of enabling technologies is identified. Finally, privacy concerns, trust issues, and security challenges in wireless arena are discussed.

**Index Terms**—Mobile commerce, m-commerce services, privacy, security, trust, wireless technologies.

## I. INTRODUCTION

Mobile commerce—the conduct of business transactions over the Internet-enabled wireless devices—is slowly becoming a dominant force in business and society. The push for advancing technology and the pull of public demand for low-cost, high-speed communications and ubiquitous access to information anytime anywhere have revolutionized the telecommunications industry over the past two decades. This revolution has led Canada to have one of the lowest Internet access charges among G7 nations and to also have the lowest mobile communications of them all [1] and [2]. More recently, Internet access and high computing power in wireless devices began to pave the way for the introduction of broadband interactive multimedia applications. Nevertheless, the wireless Web market is still in its infancy, and mobile commerce (m-commerce) is expected to evolve significantly in the future, especially in view of the current implementation of 3G systems and the future deployment of 4G systems, inter-connecting a multitude of diverse wireless networks, such as WBAN, WPAN, WLAN, and WMAN.

As shown in Fig. 1, m-commerce is the product of interaction among business transactions, Internet

applications, and mobile communications. It is a highly evolved version of the 1980's t-commerce (commerce via telephony) and the 1990's e-commerce (commerce via the Internet). As highlighted in Fig. 2, there has been a revolutionary change in cellular mobile communications in every decade. The first generation (1G) systems, introduced in the early 1980s, provided analog voice-only communications and the second generation (2G) systems, introduced in the early 1990s, provided digital voice applications and circuit-switched low-speed data services [3]. The introduction of third-generation (3G) systems resumed in the 21<sup>st</sup> century, with the focus shifting to packet data instead of just voice [4]. The fourth-generation (4G) systems will likely provide broadband IP-based multimedia services around the 2010 time-frame [5] and [6].

As wireless evolves from a secondary means of communication to a principal means of communication, it leads to the graying of lines between personal interactions and business transactions [7]. Although the growth and pervasiveness of this continuing wireless revolution appears to be inevitable, the path and speed of growth of this technology are not so predictable. It is clear that different generations of mobile communication systems have evolved to satisfy the demands of high data rate, high mobility, wide area coverage, diverse applications, high spectral efficiency, high flexibility of mobile devices and networks, and low costs. In view of this backdrop, it is anticipated that m-commerce will become widely popular and ubiquitously available. In this paper, future trends in m-commerce services and technologies, as well as privacy concerns and security challenges will be highlighted.

## II. WIRELESS USER EQUIPMENT AND SYSTEMS

Today's communication-centric and computing-centric devices are becoming a single intelligent wireless device. The future user wireless devices, dubbed as universal wireless handheld devices, will have numerous functionalities, all aiming to establish communications, enhance education, furnish entertainment, provide information, and conduct transactions for mobile users. Few of the device features are

already available in handheld devices, but many of them, yet to be incorporated, will need to increase the device size, weight, complexity, power, memory, and processing requirements. To this end, engineering design trade-offs will be required to form the right balance between devices' capabilities and their constraints.

With low-power requirements and long-lasting batteries, the universal wireless handheld devices will be small, low-cost, light-weight, easy-to-use, and IC-card-reader equipped. They can be attached to desk-/lap-top computers and their peripherals, including keyboards, printers, scanners, loud speakers, and fax machines. They will have high-resolution color screens to present pin-point information, thus minimizing the burden on users' attention. They will also possess features such as simple icon-menu, touch-pad, and artificial-intelligence-based natural languages. The wireless devices and networks will employ intrusion detection systems to detect cracking attempts in real time and to take effective protective measures based on the information it has. These devices include anti-virus software to handle malicious code and to support for authenticating users, servers, and applications.

On a standalone basis, the devices will function as alarms, clocks, calculators, timers, flash lights, calendars, organizers, dictionaries, tape recorders, compasses, cameras, pocket PCs (with office applications), radios, TVs, biometric control devices, audio and video players. They will also be able to measure the temperature, pressure, humidity, and heartbeat. They will all have high-speed, always-on, packet-switched bandwidth-on-demand access capabilities to the Internet and other networks, as well as to other wireless devices and equipment, anytime anywhere. While connected, they will function as virtual keys, secure ID cards, digital cash, tag-readers, remote control devices, pagers, locating devices, and phones, and will also get e-books, e-newspapers, e-mails, voice-mails, and video-mails.

Although use of data, and, in general, multimedia continue to accelerate exponentially, voice will remain a dominant mode of communications while the user is on the move, for talking or listening provides hands- and eye-free operations and is also several times faster than typing or reading text messages. However, to convey the same information, typed texts require less bandwidth than spoken words; hence, the immense popularity of SMS. In view of the fact that voice, video, keypad, and pen can be all used as a means to input, and text, audio, and video can represent output formats, a number of I/O enabling technologies will have to be incorporated in the wireless devices. These technologies may include:

- speech recognition (converting spoken words to text to avoid the use of alpha-numeric key pads),
- speech synthesis (converting e-mails to intelligible speech so as to hear the received e-mails),

- voice activation (bringing voice-control to navigate the Web sites and to replace a long series of sequential inputs in an automated voice-menu-driven phone system), and
- optical character recognition (converting hand-written text to typed-written format with a high degree of accuracy and an inherent learning mechanism).

It is envisaged that a user's device will have a unique permanent calling number through which the mobile user can communicate with anyone, anytime, and anywhere, all facilitated by international roaming, global mobility, and seamless connectivity to heterogeneous networks. To achieve such, the user's device should be multi-band, multi-mode, multi-functional, and multi-standard to accommodate in a transparent fashion all types of wireless systems. These wireless systems may include analog cellular systems (1G: AMPS), digital cellular systems (2G: IS-54/-136, IS-95, GSM, DCS-1800, PDC; 2.5G: HSCSD, GPRS, CDMA2000-1X; 3G: EDGE, CDMA2000-1XV, WCDMA, TD-CDMA), digital cordless phones (DECT, HomeRF), wireless PBXs, wireless LANs (IEEE 802.11 family, European HiperLAN), WPANs (Bluetooth, Infrared, Ultra-Wideband), WMANs (WiMax, LMDS, MMDS, FSO), and mobile (L-/S-band) satellite and GPS systems [8] and [9]. Accordingly, diverse radio interfaces are required, which may be met by the implementation of radio-defined software technologies [10]. It is important to note that due to the cellular nature of mobile services with myriad wireless interface requirements, both horizontal and vertical hand-off processes are required so as to be able to achieve seamless mobile communications.

3G systems, which are now being deployed, need smaller cells, resulting in more base stations and higher systems costs. These characteristics are primarily due to their operating frequency, modulation and power management requirements. It may, therefore, not be very economical to install 3G systems in large rural areas. Thus, 2G systems and even 1G analog system will continue to exist, especially in remote and isolated regions. The primary contributions to 3G devices' higher costs are flash memory, RAM, miscellaneous communications-related functionalities, as well as radio-frequency and baseband chips. 3G systems promise transmission speeds of up to 2 Mbps in stationary applications, 384 Kbps for slow-moving users, and 128 Kbps for users in fast-moving vehicles. Unlike for 2G systems, for 3G systems, authentication is mutual (i.e., the wireless device also authenticates the network), and the encryption is mandatory—unless the device and network both agree on an unciphered connection [4] and [11].

In the future, 4G systems will focus on seamlessly integrating all wireless networks, and they will be the platform for mobile systems. This focus contrasts with 3G systems, which merely focus on developing new standards and hardware. 4G systems will be all IP-based multimedia

services in heterogeneous networks that allow users to use any system at anytime anywhere. The new challenge facing the mobile industry is to minimize the fragmentation of the market and to enable seamless interoperability so as to simulate the growth of mobile services. 4G devices should be multi-band, multi-functional, and multi-mode capable and be able to handle various contents. Also, 4G systems will provide the best connection to users [7] and [8]. It is believed that the interfaces for 4G systems will exploit the new frequency spectrum that is to be identified by WRC-2007; therefore, a speculative time scale for a mature 4G system is beyond 2010. 4G systems will be an evolved version of 3G systems and will also be based on a cellular system but will require very small cells [10] and [12]. 4G systems will warrant the realization of automatic switching functions for such flexible networks, mobility control, coordination functions between layers 2 and 3 to realize fast handover, rapid routing of packets, and so on. 4G systems will improve coverage in highly populated areas (i.e., hot spots) to carry more traffic by utilizing diverse access technologies to deliver the best possible services, while taking into account both cost and bandwidth efficiency [13]-[16].

The primary 4G systems objectives over 3G systems objectives—higher transmission rate (by two orders of magnitude), larger capacity (by one order of magnitude), higher frequency band (beyond 3 GHz), single-device (ubiquitous, multi-functional, multi-service, multi-band), increased coverage (global roaming), simple billing (one bill with reduced total access cost), high quality of service (accommodating varying transmission rates, channel characteristics, bandwidth allocation, fault-tolerance levels, and different hand-off support), and lower system costs (one order of magnitude)—will directly play pivotal roles in all aspects of the next generation of m-commerce.

### III. M-COMMERCE SERVICES, PAYMENT, AND VALUE CHAIN

There appears to be no m-commerce application that can be qualified as a “killer” application, per se. However, the key advantage of m-commerce is its ability to support a wide variety of attractive and innovative applications, and that will be the “killer” characteristic of m-commerce. It is worth highlighting that the highly-personalized, context-aware, location-sensitive, time-critical applications, conducted in a very secure environment are the most promising m-commerce applications. There are indications that the next-generation of wireless communications services based on 4G systems will not be limited to human (as it has been before) but rather to anything that very small wireless chips can be attached to (i.e., machine-to-machine communications) [17]-[20]. Table-1 highlights the m-commerce service categories encompassing sets of attractive applications.

Mobile communications services originated from voice telephony. However, the cellular phone market, when measured in terms of the number of wireless devices, is becoming saturated at a rather rapid pace. In short, there can be no significant increase in traffic merely through voice telephony. In view of this limitation, there appear to be two viable strategies to achieve growth in mobile communications: (i) implementation of new mobile services with an array of diverse multimedia applications, and (ii) the introduction of new wireless devices with enhanced features, including direct device-to-device communications capabilities. The mobile multimedia applications warrant high transmission rates and allow various modalities—such as voice, data, image, music, text, and video—to be transmitted simultaneously and in an integrated fashion. The ubiquitous wireless devices with various radio interfaces possess capabilities to connect to a multitude of heterogeneous networks, including the Internet, PSTN, ISDN, and WLAN. They can also allow communications directly with other wireless devices, such as tetherless machine-to-machine communications. Both of these developments can lead to a great increase in the volume of user traffic, thus increasing the average revenue per user, a key metric for measuring the profitability of mobile-based businesses.

Future mobile systems will introduce various quality-of-service (QoS) levels in order to provide various types of best-effort multimedia services corresponding to users’ demand. QoS may include priority, reliability, bit error rate, security, delay, jitter, and throughput measures. The conversational services, with their real-time voice/video, connection-oriented applications, are characterized by a low fixed delay of about 20 – 30 milliseconds, a modest bit error rate of about  $1E-03$  to  $1E-05$ , and a low-blocking probability for network access. On the other hand, transactional, retrieval, messaging, and distribution (e.g., multicasting) services, with their non-real-time connectionless applications, are characterized by a varying delay of 150 milliseconds or more, a low bit error rate of  $1E-05$  to  $1E-07$  to aim high data integrity, and a low-delay probability for network access [4]. It is worth noting that the effective user transmission rate (i.e., throughput) which can characterize, to a large extent, the set of m-commerce applications available to the user is a function of the cell size and the speed of the mobile user. For instance, a user in a stationary position in an urban area characterized by small cells can have a throughput 10 to 20 times higher than a user driving fast on a highway in a rural area consisting of large cells would have [21].

Every generation of mobile services (e.g., 2G, 3G, and 4G) brings about more efficient spectrum utilization; that is, more users per unit spectrum per unit area (bits per second per Hz per square kilometers). Spectral efficiency measures the ability of a wireless system to deliver information or billable services. There are many factors which can contribute to the

spectral efficiency of a system, including modulation format, channel coding technique, air interface overhead, multiple access method, and acceptable interference level, to name a few. The spectral efficiency for 2G systems is about 0.15 to 0.20, that for 3G systems is about 0.25 to 0.30, and that for 4G systems will likely be as high as 3 to 4 bits per second per Hz [22]. This efficiency will, in turn, reduce the overall service cost quite significantly.

There are many factors shaping mobile billing, in general, and m-commerce payment, in particular. A major determining factor for the success of m-commerce is service affordability—such as low access, subscription, and usage fees. What basically the customer will have to pay depends on the fact that North America’s called-party-pays strategy, or Europe’s calling-party-pays strategy, or a reasonable mix of both will be employed. The service charge will also have to be a function of the user’s location, the time of call, the service type, the call priority, the service duration (measured in call seconds and/or Mega bytes), the call frequencies (to accommodate frequent micro-payments), and the payment plans (pre-pay or on-credit) [8] and [23]. Also, mobile payments, which are virtual payments, can be divided into macro-payments—typically a payment of \$10 or more—and micro-payments—typically a payment of \$10 or less. For a macro-payment, authentication through a trusted financial institution is required, which must be carried out over the public wireless access and wired-line backbone networks, while invoking all possible security measures. On the other hand, a micro-payment may use the operator’s infrastructure or involve a cash card (in addition to the ID card which stores the confidential information, such as the user’s secret authentication key) and proximity payments through short distances by using Bluetooth, Infra-Red, RFID, and UWB technologies [24].

Fig. 3 presents a generic payment model for mobile commerce [23]-[25]. This model provides an abstract view of what information is passed between various parties to conclude a transaction and does not depict any particular ordering of the information flow. In the selection phase, the customer indicates what goods and services are desired, and he/she negotiates the price of the goods and services and the terms of conditions. The transaction details highlight the description of goods or services, the customer’s name, and other required details. The customer then responds with transaction credentials (which may contain the payment credentials), the transaction details, and some authentication of the customer. Upon authentication, the payment is approved, the funds are transferred, and the goods will be delivered, or services will be provided.

In mobile payment, although confidentiality (making sure information is not visible to eavesdroppers), integrity (finding out the content has not been tampered with), and non-repudiation (proving the transaction has taken place) are

primary concerns, authentication (ensuring communicating parties are certain of each other’s identity) is of paramount importance. As a result, public key cryptography, which is slower but more powerful than symmetric key cryptography, will be used for authentication and the exchange of symmetric session keys. In order to prevent a false (cracker’s) public key as a legitimate public key, a certificate authority issues a public key certificate that would contain the name, the public key, and the expiration date. In view of the fact that the emerging wireless devices will have more throughputs, processing power, and memory, more complex encryption techniques—such as longer keys and/or more sophisticated multi-level algorithms—will be employed to enhance mobile payment security [26]. Although encryption can be the most effective tool for both privacy and security, it is generally used only as a security measure when m-commerce transactions are conducted and not when essential data are generally stored in databases.

The development environment for m-commerce is significantly more complex than e-commerce, thus requiring a broader base of expertise. In m-commerce, it is virtually impossible to achieve all technical and business requirements simultaneously, for some are clearly in conflict with others. For instance, in the current state of technology, not all technical requirements (such as high-speed access and low-power devices) and business requirements (such as low-access fee and high-quality of service) can be completely fulfilled at the same time. Moreover, there are constraints associated with business and regulatory environments that can influence some of these requirements, such as service coverage, location determination, backward compatibility, and privacy concerns, to name a few.

The m-commerce applications can be successfully provided to mobile users only when a number of enterprises, called the m-commerce value chain, are complementarily involved in the creation and delivery of these services, with the goal of sharing revenue. In order to drive interoperability of mobile data services, the world’s mobile operators, device and network suppliers, information and communication technology companies, application developers and content providers have joined forces to ensure seamless mobile services for end-users anywhere. This outcome will be achieved by defining industry-wide requirements, architectural frameworks, and industry specifications for enabling technologies and end-to-end interoperability, all based on open specifications of standards, protocols, and interfaces [12], [23] and [25].

The federal government also plays a pivotal role, not only in terms of setting policies and ensuring that regulatory issues are fully respected, but in terms of auctioning spectrum (instead of comparative bidding and lottery as licensing methods) [27]. This role, in turn, can lead to huge investment requirements, which need to be met by some major players.

M-commerce services with compelling contents are provided by tight business and strategic partnership arrangements and by involving a large number of companies, with each influencing other parties in the value chain. While no two value chains are the same, a company can assume multiple roles in the value chain for m-commerce, or a single role for a multiplicity of services, such as m-commerce, e-commerce and, iTV. Table-2 identifies the main categories of players in the m-commerce value chain.

#### IV. M-COMMERCE ENABLING TECHNOLOGIES

Providing mobile users with wireless communications functions for their communications, information, education, entertainment, and business needs, as well as giving wireless communications functions to stationary places for access and security and to moving objects for asset and logistic purposes form the cornerstones of mobile commerce. To achieve these goals, significant technological advances in a number of enabling technologies are anticipated.

*Radio frequency identification (RFID)* is a generic term for technologies that use radio waves to automatically identify individual items or some of their attributes. RFID possesses several benefits over bar codes. First, it does not need to meet line-of-sight requirements as long as the RFID tags are within the range of a reader. Second, quite many number of RFID tags can be read simultaneously. Third, every unique item can have its own RFID tags. The mobile consumer will use RFID readers in their mobile phones to scan RFID tags, say in the packaging of products on store shelves, to pay for tolls and access fees, to purchase at vending machines and points of sales, to access secure rooms, buildings, and other partitioned areas, and to control home and office appliances. With RFID, a scanner can read the encoded information even when the tag is concealed. For example, it may be embedded in a product's casing, or sewn into an item of clothing, or sandwiched between a banknote's layered paper. The stealthy nature of RFID technology has raised concerns among privacy advocates that RFID tags could be tracked beyond their intended use. For example, security agencies might use them to covertly monitor individuals or their belongings. Lower frequencies (LF and MF) usually are cheaper, use less power, are better able to penetrate non-metallic substances, and are ideal for scanning objects with high-water content. On the other hand, higher frequencies (HF and UHF) typically offer a better range and can transfer data faster; they tend to be more directed and, thus, require a clearer path. Active tags can have a farther read range than passive tags, but passive tags are less expensive and require no maintenance. RFID will play a critical role in emerging wireless access and monitoring applications [6], [17], [28] and [29], especially in today's security-aware era.

*Location determination* is seen to be an indispensable feature for mobile commerce. Network-based positioning is carried out by terrestrial systems through various techniques, such as cell of origin, time of arrival, angle of arrival, and enhanced observed time difference. The device-based positioning is carried out by satellite systems typically using three or four MEO satellites, also known as GPS. However, a hybrid approach delivering the accuracy of device-centric option, while avoiding a line-of-sight requirement as well as increased cost, size, and power consumption, is also used. Though FCC does not require the mobile network operators to use a specific technology, it has indicated specific performance metrics for location-enabled technology. For network-based technology, location information accuracy is required to be within 100 meters 67% of the time and within 300 meters 95% of the time [27]. But for the device-centric technology, these distances must be halved. In view of possible launches of LEO satellites and the significant increase in the processing capabilities of the wireless devices, as well as the fact that the cell sizes are shrinking from macro to micro to pico, the location-based technologies are expected to become more accurate and less costly in the future [30].

*Software defined radio (SDR)* enables reconfigurable system architectures for wireless networks and user devices. To provide users with m-commerce services under an array of heterogeneous networks, certain design problems (such as limitations in device size, cost, power consumption, and backward compatibilities to systems) must all be overcome. The most viable way of implementing these types of wireless devices is to adopt a software radio approach. The received analog signal is processed by a reprogrammable baseband digital signal processor in accordance with the wireless environment. However, certain problems then need to be addressed—such as an analog radio interface with multiple antennas and amplifiers and very fast high-speed analog-to-digital conversions and DSP functions—which can all, in turn, add to the circuit complexity and high-power consumption and dissipation. SDR can provide the user with a single piece of scalable hardware that is at once compatible at a global scale [15] and [31].

*Adaptive modulation and coding (AMC)* is one of the most viable and effective means to dynamically combat wireless channel degradation and meet performance requirements. In AMC, for the same symbol rate (i.e., occupied bandwidth), the signal power, the modulation technique, the information rate, and the channel-coding rate, can all be adjusted in accordance with instantaneous variations in channel conditions (such as multi-path and proximity to the base station) and quality of service requirements. Forward-error-correcting (FEC) codes (whose rates may range from 1/2 to 5/6) and digital modulation techniques (ranging from QPSK to 64 QAM) will be dynamically adapted for every single

individual, giving rise to up to a six-fold spectral efficiency (bits per second per Hz) [15] and [32].

*Digital signal compression*, also known as source coding, is employed to reduce the bit rate requirements (bandwidth demands). It is widely applied to all sources of modality. Both proprietary and standard techniques are widely available and are constantly being improved upon. Texts, software, and faxes generally employ lossless compression techniques, such as the Lempel-Ziv and Huffman codes. On the other hand, MPEG video, JPEG image, and MP3 audio coding standards employ lossy compression, where known limitations of the human visual and audio systems are exploited to introduce losses but in a controlled manner. With advances in compression, a wider array of feature-rich m-commerce applications and/or lower service costs can be provided [20] and [26].

*Biometrics* as an essential security measure will play an imperative role in the next-generation m-commerce services. Traditionally, most security systems authenticate the user based on something that he/she knows, such as a password. However, where security really matters, it makes sense to add a second layer, which could be something that he/she has (e.g., a smartcard). Also, as a third option, and probably the most authentic method, could be something that he/she is, something that, at least theoretically, would be virtually impossible to forge. Biometric control measuring physical characteristics and behavioral patterns will be widely employed to allow the user to access his/her own wireless device, to enable the user to access certain places, and to allow the user to monitor assets. Of course, depending on their effectiveness, cost, intrusiveness, and accuracy, more than one biometric controls may be simultaneously employed. Biometric control may include finger imaging, palm print, hand geometry, iris and retina vascular pattern, facial recognition and thermography, signature and handwriting, key stroke dynamics, and voice recognition and speech patterns [33].

*WAP* (Wireless Application Protocols) appears to be the key to future IP-based m-commerce applications. WAP, an industry-initiated world standard, has emerged as a common communications technology and uniform interface standard for presenting and delivering wireless services on wireless devices [34]. WAP specifications include a micro-browser, access functions, and layered communication specifications for sessions, transport, and security. The WAP gateway is used to translate the WAP protocols (protocols that have been optimized for low bandwidth, low power consumption, limited screen size, and low storage) into the traditional Internet protocols (TCP/IP). These specifications enable bearer-independent and interoperable applications. In short, future trends clearly indicate that the device manufacturers, as well as service and infrastructure providers, will keep adopting the WAP standard [25].

*IPv6*, the Internet Protocol version 6, is a permanent solution to the address shortage and uses a 128-bit address, split into 16 bytes, vis-à-vis IPv4's 32-bit address [35]. With IPv6, there will always be enough IP addresses for all mobile devices and moving tags. IPv6 is a feature-rich standard, including built-in-security by supporting IPSec to promote interoperability between different IPv6 implementations. IPv6 also allows for better support for quality of service through traffic identification. Mobile IPv6 is a standardized IP-based mobility protocol for IPv6 wireless systems. In this design, each device has an IPv6 home address. Whenever the device moves outside the local network, the home address becomes invalid; therefore, the device obtains a new IPv6 address (called a care-of-address) in the visited network. This hand-off process causes an increase in the system load, a high handover latency, and packet losses. Because 3G systems works with IPv6, it is anticipated that 4G systems will work with IPv6 as well [36].

*Mobile ad hoc networks*, vis-à-vis fixed topology wireless networks, may be characterized by wireless nodes, the lack of fixed infrastructure support, dynamic topologies, bandwidth-constrained variable-capacity links, energy-constrained operations, and limited physical security. In such peer-to-peer networks, end-user wireless handsets also act as secure wireless routers that are part of the overall network infrastructure. Upstream and downstream transmissions hop through subscriber handsets and fixed wireless routers to reach the destination. Routing for the best path is defined for the least power. Mobile ad hoc networks will help a community of subscribers to increase dramatically spectrum reuse and reduce overall power consumption. Mobile ad hoc networks bring about a host of challenges and opportunities, but due to emerging wireless device-to-device connectivity requirements, mobile ad hoc networks will prove to be an ever-essential component [37].

*MIMO*, multiple-input multiple-output, can significantly increase system capacity, range, and reliability [22] and [32]. The wireless broadband channel is a non-line-of-sight channel and includes impairments, such as time-selective and frequency-selective fading. To circumvent these problems, MIMO exploits propagation environment characteristics by employing multiple antennas at the transmitter and receiver to create spatial channels, for it is not very likely that all the channels will fade simultaneously. The space diversity, enabled by smart antennas using phased array and digital beam forming techniques, combines multiple antenna elements with digital signal processing to optimize their radiation/reception pattern. It is anticipated that MIMO, in combination with other advanced techniques such as OFDM and CDMA will be heavily utilized for 4G systems to enhance the system capacity and performance.

*OFDM*, orthogonal frequency division multiplexing, is selected over a single-carrier solution due to lower

complexity of equalizers for high data rates. Multiple narrowband carriers (tones), which are orthogonal to one another, are more robust to multipath. With proper coding and interleaving across frequencies, multipath turns into an OFDM system advantage by yielding frequency diversity. In addition to MIMO's space diversity and OFDM's frequency diversity, site diversity for base stations and time diversity for non-time-sensitive applications will also be employed to improve the system capacity and performance [38].

*CDMA*, code division multiple access, is the access scheme for 3G systems, and it will almost certainly be for future 4G systems, for it can significantly enhance capacity through effective use of orthogonal codes. The primary advantage of CDMA is its ability to reject interference whether it be the unintentional interference by another user simultaneously attempting to transmit through the channel or the intentional interference by a hostile transmitter attempting to jam the transmission. CDMA, as opposed to FDMA and TDMA, can allow an increase in system capacity at the expense of a modest and gradual degradation in performance. It is worth noting that combining multi-carrier OFDM transmissions with CDMA gives rise to exploiting the wideband channel's inherent frequency diversity by spreading each symbol across multiple subcarriers [38].

*Turbo codes*—demonstrated experimentally and by simulation but not yet proven theoretically—are capable of approaching the Shannon theoretical limit of channel capacity in a computationally feasible manner. This capability is in contrast to the traditional FEC codes where to significantly improve the FEC performance, its code-word length of a linear block code or the constraint length of a convolutional code must be increased significantly, which in turn, causes the computational complexity of a maximum likelihood decoder to increase exponentially. The error performance of the Turbo code decoder significantly improves with the number of iterations of the soft-input-soft-output decoding algorithm, but at the expense of additional computational complexity and decoding delay. Turbo codes' performances can be impacted by interleaving type and length, number of iterations, code rate, type (block or convolutional) and structure (series or parallel) [21]. Even a small reduction in the link threshold can improve the system capacity and/or enhance the link performance significantly.

*Data encryption* is the best approach to handle security in the wireless and m-commerce arena. The primary goals are to provide an easy and inexpensive means of encryption to all authorized users possessing the appropriate key and to ensure the cracker's task of producing an estimate of the plaintext without the benefit of the key is made difficult and expensive. Depending on the wireless devices' constraints (such as limited processing power, memory and power) and m-commerce applications' requirements in terms of delay and burstiness, secret key cryptography (symmetric key) based on

multi-layer algorithms, or public (asymmetric) key cryptography based on elliptic curve techniques, or a hybrid of both will have to be employed [39]. In the absence of effective encryption, there can be no m-commerce applications.

## V. PRIVACY, SECURITY, AND TRUST IN M-COMMERCE

The growth of the Internet and e-commerce has dramatically increased the amount of personal information that can be potentially collected about individuals by corporations and governments. Such data collections, along with usage tracking (clickstream data) and the sharing of information with third parties are always invoking issues of privacy, especially in view of the fact that they can be easily done through high-speed links and high-capacity storage devices in a very accurate fashion, and most often without the consumer's or citizen's expressed knowledge or consent [40]-[42]. This valuable information, often collected by hidden tools such as cookies and Web bugs can be shared with third parties for marketing purposes and surveillance operations, and its perceived value has been occasionally behind the stock-market valuations of some companies. In fact, this detailed information can be combined with other off-line data such as demographic and psychographic data to predict a user's interests, needs, and possible future purchases. To deal with the problem of profiling, trust seals and government regulations appear to be two forces pushing for more and better privacy disclosures on the Web. The former tend to promote privacy in the form of self-regulation, where they may eventually become more of a privacy advocate for corporations rather than for consumers. The latter can advance privacy through legislation but can also potentially create privacy worries for citizens by monitoring their telecommunications traffic. For instance, the FBI's powerful DCS1000 Carnivore program is a computer-automated snooping tool that is capable of intercepting and sorting out millions of text messages, such as telephone conversations and e-mails passing through ISPs by monitoring incoming and outgoing messages to specific IP addresses [41]. It is clear that governments' regulations and legislation can be as likely to thwart privacy as to enforce it.

Even though wireless communications possess numerous merits, privacy is not one of them. M-commerce possesses, in addition to all privacy issues related to e-commerce, another major privacy threat: the sharing of knowledge about a user's location with others. There are basically three solutions to this positioning problem: i) the network-based solution, where the calculations are carried out by the cellular network and the positioning information may then be passed to the user; ii) the device-based solution, where the wireless device computes its own position; and iii) a hybrid solution. The pitfall associated with the network-based positioning is that

the information about the user's whereabouts can be collected but not necessarily passed to the user. Instead, the information may be exploited by other entities, all without the user's knowledge, let alone his/her consent. Also, there are some privacy implications about the requirement that wireless devices need to be embedded with a location-tracking technology to provide location-based services, such as targeted advertising and finding the nearest "X." For instance, if location records were kept over time, an in-depth profile could be compiled for other, perhaps unwarranted, purposes.

Many countries, such as Canada and those in the European Union, strictly regulate the collection and use of personal data by business corporations and government agencies. They have opted for regulated self-regulation. For instance, the privacy provisions of Canada's PIPEDA set out rules for the protection of personal information collected, used, or disclosed in all sectors of the economy, so as to strike a pragmatic balance between privacy and economy [42]. For instance, PIPEDA warrants all mobile service providers in Canada to take steps to ensure that i) they are responsible for personal information under their control, ii) they obtain expressed consent before using or disclosing customers' location information, iii) they limit to the purpose identified for the collection of information, and iv) they protect with the necessary security to safeguard the personal information.

In contrast, the United States has chosen self-regulation as their basic strategy, based on the model of the well-informed, the rational and the self-protecting consumer [43]. In this model, privacy may be considered to be a barrier for m-commerce, and accordingly a minimum level of protection is to be desired. A case in point is that in 2002, the FCC turned down the wireless industry's request to adopt location information privacy rules [41] and [44]. The rules mainly reflected the privacy principles of notice, consent, security, and integrity of consumer data. Due to the FCC's reluctance to regulate location-based wireless services, the users may now need those mobile services where they themselves can turn off location-tracking features (with the exception of E-911) and reception of targeted ads be subjected to a user's affirmative response. Currently, the "opting-out" options are available to the m-commerce consumers. It is anticipated that privacy advocates will continue to push for "opting-in" options instead, through which consumers would, by default, be opted in and would have to take action to let companies use their information. In any event, even if there were a method to absolutely ensure privacy, service providers and customers may not embrace the technology quite as readily, because it may be inexpensive in practice and offer a lower quality of service. Since every cellular telephone is a physical-locating device even when the user is not in a call, and there is no known way to avoid revealing the caller's

location when a cell phone is in use, privacy about the mobile user's location can always be potentially compromised.

With the apparent omnipresent availability of wireless devices, m-commerce services have a very promising prospect. However, the success of m-commerce depends much on the security of the underlying mobile technologies. Wireless technology, by its nature, violates fundamental security principles. In short, wireless communications rely on open and public transmission media (i.e., over the air) that raise further security vulnerabilities, in addition to the security threats generally found in wired networks. For instance, the chargeback rate for credit card transactions on the Internet (that is for e-commerce) is about fifteen times more than that for point-of-sale credit card transactions [45]; this, in turn, points to the fact that security will always be an indispensable factor in the success of m-commerce. The m-commerce security challenges relate to the user's mobile device, the wireless access network, the wired-line backbone network, and m-commerce applications. Security threats in m-commerce may be passive (such as information monitoring and release for fraudulent purposes) or active (such as the modification of information through denial-of-service and unauthorized access). Unlike the wire-line networks, the unique characteristics of wireless networks pose a number of non-trivial challenges to security design, such as vulnerability of the air interface, an open peer-to-peer network architecture (in mobile ad hoc networks), a shared wireless medium, the limited computing power of mobile devices, a highly dynamic network topology, and the low data rates and frequent "disconnects" of wireless communications. There are basically two approaches to the challenges to wireless security: being proactive and being reactive. The proactive approach attempts *a priori* to prevent a cracker from launching attacks in the first place, typically through various cryptographic techniques. In contrast, the reactive approach seeks to detect security threats *a posteriori* and to react accordingly. Due to the absence of a clear line of defense, a complete security solution should integrate both approaches. Because security is a chain, it is only as secure as the weakest link. A failed link may significantly degrade the strength of the overall security solutions. Enhanced security features require additional overhead (increased bandwidth), increased complexity (additional cost), and processing delay (degraded performance), which, in turn, can adversely impact network performance.

Mobile services are prone to two types of fraud risks: subscription fraud and device theft. Subscription fraud (also known as identity theft) is the same problem that issuers of credit cards have when someone pretends to be another subscriber [44] and [45]. As with other forms of credit-related identity theft, the imposter fails to pay the bills and the service is eventually cut off. Although the customer will not be responsible for paying the imposter's bills, as he/she may

have to take steps to clear his/her credit report. Device theft has become more attractive to thieves as the wireless devices become smaller and more powerful. The charges incurred by the thief appear on the legitimate consumer's monthly bill, and it's not certain that the service provider will remove these charges from the customer's account. Almost as soon as the stolen device is reported, the location technology can be employed to help track down the thief. Also, to combat theft, in addition to the usage of password, a device could be tailored to its owner, using effective, yet inexpensive, biometric control technologies. But it appears that most of the device manufacturers are not very keen to include these biometric technologies, for a more palatable option is to have their products stolen so their customers will have to replace them frequently.

Calls made on digital cellular networks are clearer, more secure, and more feature-rich than calls made on analog cellular networks, and virtually the entire population in North America is covered by digital network. Significant portions of the land area do not have access to digital services, and will almost always be covered by analog systems. Standard radio scanners can monitor analog signals, but cannot decipher digital ones, unless law enforcement-grade scanners are employed. The cloning (also known as service theft) of a cellular phone occurs when the electronic serial number (ESN) and the mobile identification number (MIN) of a cellular phone are stolen by radio scanners sniffing the cellular frequency bands and reprogrammed into another cellular phone without the knowledge of the carrier or subscriber through the use of electronic scanning devices [46]. After this process is completed, both phones (the legitimate and the cloned) are billed to the original, legitimate account. That problem has been reduced by almost two orders of magnitude through the application of digital technology, including advanced access schemes and compression techniques. Means to detect cloned phones on the analog systems are as follows: i) duplicate detection (the network sees the same phone being used in two places at the same time and reacts by shutting them both off), ii) velocity trap (the network notices that the phone seems to be moving at impossible or most unlikely speeds), iii) radio-frequency fingerprinting (the network spots the clones with the same identity but different RF fingerprints), iv) usage profiling (customers' phone usage patterns are kept, and when discrepancies are noticed, the customer is contacted), v) call counting (both the phone and the network keep track of calls made with the phone, and should they differ, service is denied), and vi) PIN codes (a user enters a PIN code to unlock and lock a cell phone).

There are wireless threats that are significantly more likely to occur in WLANs than in cellular networks, such as interception (passive eavesdropping), man-in-the-middle attack (active eavesdropping), and denial-of-service

(jamming). Interception occurs when the signal is transmitted over a radio path (which is an open, uncontrolled medium) and compatible receivers, equipped with mobile scanners, can listen to the message. The sender and the intended receiver of the message may not even be aware of the intrusion. Interception is used to gather information on the network under attack, such as who uses the network, what is accessible, and what the coverage area is. A man-in-the-middle attack aims to subvert the confidentiality and integrity of the session. Here, attacker impersonates a network resource to sniff the traffic of another wireless client by sending unsolicited signals to target stations. The target stations will send all traffic to the attacker instead of the intended destination, and the attacker is now in a position to modify communications. In the default mode, WLANs do not provide any security [47]. In order to provide a certain level of security, the IEEE-defined Wired Equivalent Privacy (WEP) was designed to provide security. However, it is now clear that WEP authentication is completely insecure [45]; an attacker can intercept an authentication exchange without knowing the secret keys. In fact, if many frames are intercepted, the WEP keys can be recovered using statistical analysis. There is another limitation. Due to the fact that all participants must have the same key, public portals (e.g., hotels, airport) provide no security. In response to the deficiencies in WEP standards, the emerging IEEE 802.11i standards have been introduced to improve the WLAN security problems and to turn wireless networking into a trusted medium for all wireless users [48]. Denial-of-services is caused when the entire network is jammed. The jamming attack could be against the client's wireless device or against the network's access point. The jamming may be difficult to prevent or stop. Most wireless local area networking technologies use unlicensed frequencies and are subject to interference from a variety of sources. To prevent unintentional jamming, site surveys are recommended, and to stop intentional denial-of-service, jamming equipment must be identified and removed [8], [49], and [50].

The essence of a business transaction is based on trust, and trust must be mutual. Trust in a business context may be expressed in laws, contracts, regulations, and policies, as well as in personal reputations and long-term relationships, but these measures are not easily transferable to an online environment. The people online are generally rather too trusting when involved in personal interactions, such as downloading software or engaging in chat rooms with strangers, but they are rather distrustful when involved in business transactions. A major barrier to the success of online businesses has been the fundamental lack of faith between most businesses and consumers. This lack of trust is mainly due to the fact that consumers must provide detailed personal and confidential information upon request. For instance, the seller is not sure if the credit card number is genuine and

belongs to the buyer, nor is the buyer sure that the seller would not misuse the credit card number for purposes other than the one allowed. It takes a very long time for the parties in click-and-mortar businesses (i.e., e-commerce) to establish the same level of trust which has existed for so long between the parties in brick-and-mortar businesses, and it will take an even longer time for push-and-mortar businesses (i.e., m-commerce) to achieve the same level of trust.

The reliability and security of the technology is an essential trust-related characteristic of online interaction, where certain vulnerabilities are unknown, even to the most knowledgeable consumers. It is obvious that wireless communications, in general, cannot be as reliable as wired communications. Thus, the occurrence of a technical or technological failure is more likely for m-commerce than for e-commerce, and that can, in turn, further diminish the level of trust. For instance, dropped calls (a carrier fails to hand off a call in progress), busy signals (too many customers in a cell call at the same time), and dead spots (an area where the signal between the handset and the cell tower is blocked) can all impact the wireless service performance, thus potentially adversely impacting on the level of trust in m-commerce [21]. The emerging advances in m-commerce—whether they be through telecommunications technologies to help realize higher rates, wider coverage, and higher quality of service, or through business frameworks to cultivate measures such as informed consent, minimum-risk insurance, Website quality, information clarity, company competence and integrity, and public and private policies—will all help build trust in m-commerce [51] and [52]. The mass adoption of m-commerce will be realized after wireless users (potential customers) trust mobile services.

In wireless arenas, higher transmission rates, better quality of service, and more spectral efficiency (i.e., more end users and thus lower service costs) generally warrant higher power transmissions and, thus, more radiation. The level of energy emitted by WLAN and WPAN devices is much less than the electromagnetic energy emitted by mobile phones. The scientific consensus is that the radiation from mobile phones is harmful, but the dosage is so low at any given time that most people will suffer no apparent medical problems. However, the impact of their use for very many years is not known at the present time, and their long-term effects could remain unknown for a generation. The limit for public exposure from cellular telephones is set by a government; thus, any cell phone at or below these levels is considered to be a “safe” phone [27]. In m-commerce, as opposed to mere wireless voice communications, the device is generally in front of the user (i.e., the device is not next to the user’s ear). Noting that the signal power is attenuated by the square of distance, health hazard for m-commerce applications, where they are generally more visually-based than audio-based, will be even less serious than mobile phone calls. In fact, for

mobile phone calls, well-designed hands-free headsets could prove to be quite safe, especially if a very low-power wireless technology, such as Bluetooth, is employed to provide a link between the device and headset [8].

The issue of health and safety in wireless devices, either as legally imposed by the governments’ regulations or as apparently complied by the manufacturers raises the issue of trust. In principle, the strong majority of people accept the safety guidelines, health recommendations, and regulatory standards issued by governments and what the manufacturers claim to respect. But, on the other hand, some of the health and safety guidelines in the past did not protect citizens’ safety and consumers’ health. The guidelines and advisories for nuclear tests and smoking during the fifties are two cases in point.

## VI. CONCLUSION

The major limitations of m-commerce, as viewed today, are small screens on wireless devices, limited processing power, modest memory, restricted power consumption, poor voice quality, low-speed data transmission, non-ubiquitous coverage, unproven security, scarce bandwidth, and possible health hazards. In view of the fact that mobile computing is accelerating at a rate faster than Moore’s law, and according to Edholm’s law of bandwidth [53], wireless transmission rates also follow Moore’s law, many of these limitations are expected to diminish, if not being eliminated, over time.

In light of the fact that m-commerce is just at its inception, the real potential has yet to be visualized, let alone tapped. Noting that the highly-personalized, context-aware, location-sensitive, time-critical applications are the most promising applications in m-commerce, there are many m-commerce applications envisaged to become very widely popular. They include: i) digital cash (to enable mobile users to settle transactions requiring micro-payments), ii) human-to-machine communications (to facilitate mobile users to communicate to stationary locations for access and security and to moving objects for asset and logistic purposes using RFID technologies), iii) telemetry (to activate remote recording devices for sensing and measurement information), and iv) broadband-interactive multimedia communications and messaging anytime, anywhere.

4G systems with more security, higher speeds, higher capacity, lower costs, and more intelligent infrastructures and devices will help realize m-commerce applications. With improved wireless security and privacy through data encryption and user education, on the one hand, and with the wide deployment of 4G systems, on the other hand, it is anticipated that m-commerce will, inescapably, become the most dominant method of conducting business transactions.

## REFERENCES

- [1] ITU, *World Telecommunications Development Report*, 2003
- [2] Merrill Lynch, *Wireless Matrix*, 3Q03.
- [3] A. Mehrotra, *Cellular Radio: Analog and Digital Systems*, Artech House, 1994.
- [4] www.umts-forum.org
- [5] www.docomo.com
- [6] K. Tachikawa, "A perspective on the evolution of mobile communications," *IEEE Communications Magazine*, pp. 66-73, October 2003.
- [7] Y. Kim *et al.*, "Beyond 3G: vision, requirements, and enabling technologies," *IEEE Communications Magazine*, pp. 120-124, March 2003.
- [8] A. Dorman, *The Essential Guide to Wireless Communications Applications*, Prentice-Hall, 2001.
- [9] N. J. Muller, *Wireless A to Z*, McGraw-Hill, 2003.
- [10] U. Varshney and R. Jain, "Issues in emerging 4G wireless networks," *IEEE Computer Magazine*, pp. 94-96, June 2001.
- [11] L. Garber, "Will 3G really be the next big wireless technology?" *IEEE Computer Magazine*, pp. 26-32, January 2002.
- [12] Y. Yuan and J. J. Zhang, "Toward an appropriate business model for m-commerce," *International Journal of Mobile Communications*, pp. 35-56, January 2003.
- [13] B. G. Evans and K. Baughan, "Visions of 4G," *Electronics and Communication Engineering Journal*, pp. 293-303, December 2000.
- [14] J. Z. Sun, J. Sauvola, and D. Howie "Features in future: 4G visions from a technical perspective," *Proceedings of IEEE GlobeCom Conference*, pp. 3533-3537, November 2001.
- [15] T. Zahariadis, "Trends in the path to 4G," *Communications Engineer*, pp. 12-15, February 2003.
- [16] S. K. Hui and K. H. Yeung, "Challenges in the migration to 4G mobile systems," *IEEE Communications Magazine*, pp. 54-59, December 2003.
- [17] J. A. Senn, "The emergence of m-commerce," *IEEE Computer Magazine*, pp. 148-150, December 2000.
- [18] E. Turban, D. King, J. Lee, and D. Viehland, *Electronic Commerce 2004: a Managerial Perspective*, Pearson, 2004.
- [19] K. Siau and Z. Shen, "Mobile communications and mobile services," *International Journal of Mobile Communications*, pp. 3-14, January 2003.
- [20] K. Raina and A. Harsh, *M-Commerce Security*, McGraw-Hill, 2000.
- [21] S. G. Glisic, *Advanced Wireless Communications: 4G Technologies*, John Wiley & Sons, 2004.
- [22] W. W. Lu, "4G mobile research in Asia," *IEEE Communications Magazine*, pp. 104-106, March 2003.
- [23] N. Sadeh, *M-commerce Technologies, Services, and Business Models*, John Wiley & Sons, 2002.
- [24] www.mobilepaymentforum.org.
- [25] www.openmobilealliance.org.
- [26] B. Sklar, *Digital Communication*, Prentice-Hall, 2001.
- [27] www.fcc.gov.
- [28] I.D. Robertson and I. Jalaly, "RF ID tagging explained", *IEEE Communications Engineer*, pp. 20-24, February 2003.
- [29] K. Finkenzerler, *RFID Handbook*, John Wiley & Sons, 2003.
- [30] R. Unni and R. Harmon, "Location-based services: models for strategy development in m-commerce," *Proceedings of IEEE International Conference on Management of Engineering Technology*, pp. 416-424, July 2003.
- [31] E. Buracchini, "The software radio concept", *IEEE Communications Magazine*, pp. 138-143, September 2000.
- [32] H. Sampath, S. Talwar, J. Tellado, V. Erceg, and A. Paulraj, "A fourth-generation MIMO-OFDM broadband wireless system: design, performance, and field trial results," *IEEE Communications Magazine*, pp. 143-148, September 2002.
- [33] P. Reid, *Biometrics for Network Security*, Prentice-Hall, 2004.
- [34] U. Varshney and R. Vetter, "Mobile commerce: framework, applications and networking support," *Kluwer Mobile Networks and Applications*, pp. 185-198, 2002.
- [35] www.microsoft.com
- [36] S. H. Hui and K. H. Yeung, "Challenges in the migration to 4G mobile systems," *IEEE Communications Magazine*, pp. 54-59, December 2003.
- [37] U. Varshney, "Multicast support in mobile commerce applications," *IEEE Computer Magazine*, February 2002.
- [38] L. Hanzo, M. Munster, B.J., Choi, and T. Keller, *OFDM and MC-CDMA for Broadband Multi-User Communications, WLANs, and Broadcasting*, IEEE Press, 2004.
- [39] K. Lauter, "The advantages of elliptic curve cryptography for wireless security", *IEEE Wireless Communications*, pp. 62-67, February 2004.
- [40] C. V. Slyke and F. Belanger, *E-Business Technologies*, John Wiley & Sons, 2003.
- [41] www.privacyrights.org
- [42] www.privcom.gc.ca
- [43] D. van Harten, "Debating privacy and ICT, before and after September 11th," *Proceedings of International*



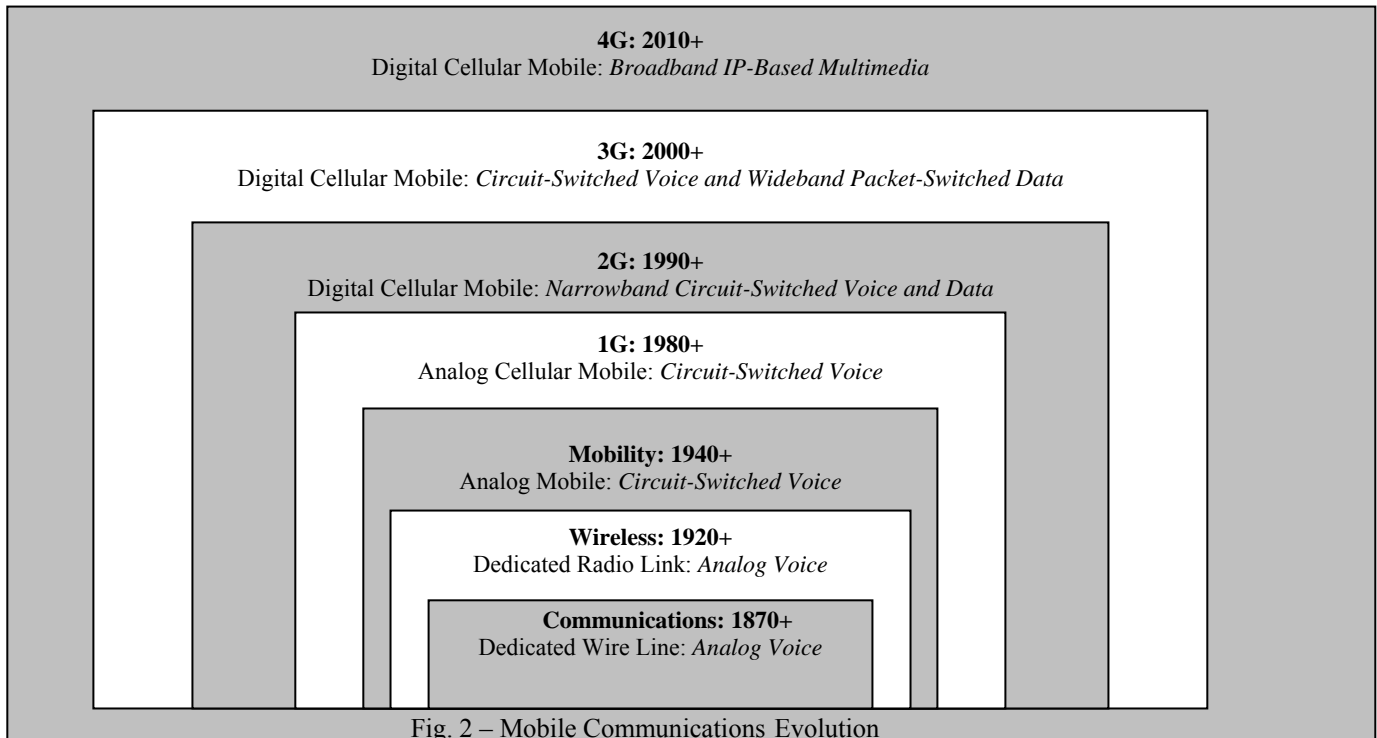


Table 1 – M-Commerce Value Chain

<b>Players</b>	<b>Roles</b>
Telecom Infrastructure Providers	provide the communications networks.
Infrastructure Equipment Vendors	manufacture the mobile base stations and switching systems.
Mobile Network Operators	provide wireless access to mobile users.
Mobile Device Manufacturers	manufacture wireless devices (e.g., phones, pagers, PDAs).
Mobile ISPs	provide mobile users with anytime, anywhere access to the Internet.
Mobile Content Providers	develop new content to deliver information and services.
Mobile Portal Providers	provide mobile users with access to all Internet needs.
Content Aggregators	focus on value creation by assembling content from multiple sources.
Mobile Location Brokers	supply info about user's position to everyone across the value chain.
Software Vendors	supply operating systems, databases, and micro-browsers.
Third-Party Billing Providers	make it possible for users to make payments.
Server Wallet Providers	store both payment information and other valuable personal data.
Security Providers	ensure secure payments through digital signatures and biometrics.
Push/Pull Advertisers	furnish users with messages to influence them.
Voice Portals	provides users with audio interfaces
Mobile Technology	provide technologies to introduce new applications.
Online Retailers	sell product and services to mobile users over the Internet.
Financial Organizations	allow all users to pay using debits/credit cards.
Wireless Applications Providers	develop, maintain, and/or host applications.

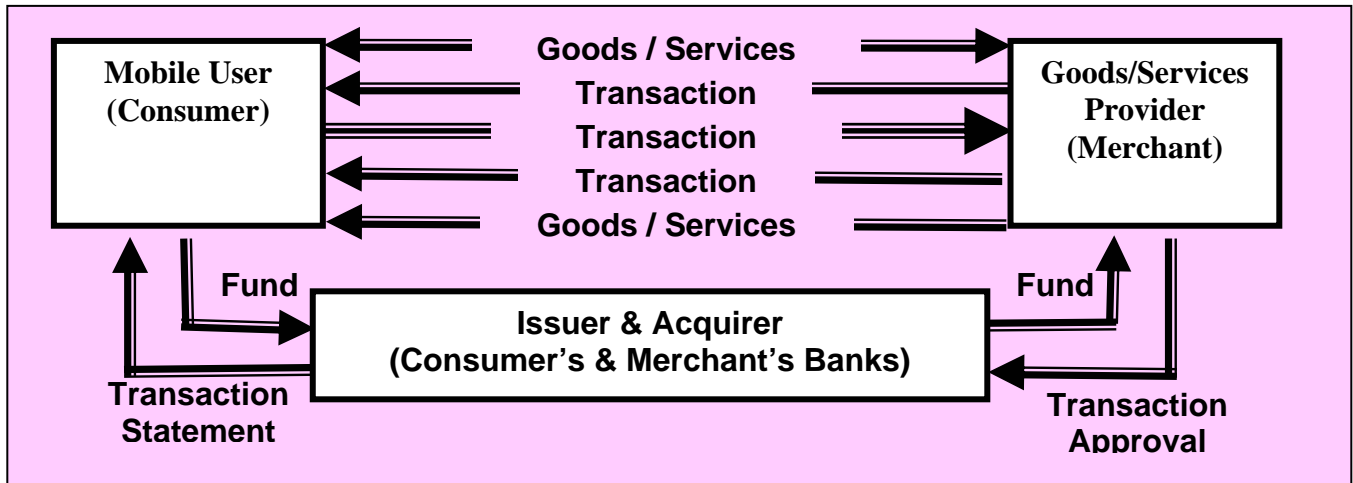


Fig. 3 – Mobile Commerce Payment Model

Table 2 – M-Commerce Services and Applications

<b>Service Categories</b>	<b>Applications Types</b>
<i>Portal Services:</i>	SMS, E-mail/voice-mail/video-mail, interactive voice, instant messaging, soft fax, Web browsing, synching with PC, video-conferencing, file transfers, MMS
<i>Entertainment Services:</i>	Interactive games, downloading music (MP3 files) and comics (jokes/cartoons/horoscope), uploading photos, streaming music/video on-demand, gambling
<i>Financial Services:</i>	Banking, stock trading, paying fees, bills, tolls, and e-cash
<i>E-Tailing Services:</i>	Shopping, booking, ticketing, advertising (user-specific/time-dependant/location-sensitive)
<i>Directory Services:</i>	Finding the nearest "X" (on-the-move yellow pages) and shortest route (driving directions)
<i>Information Services:</i>	News (e.g., sports, business, weather, traffic), crisis alert
<i>Distribution Services:</i>	Fleet tracking/dispatching of goods/people, broadcasting/multicasting, audio/video streaming
<i>Monitoring Services:</i>	Metering, trouble shooting, inventory control & management, tracing & tracking moveable/wearable objects, telemetry services, tracking assets, tracking stolen/lost cars/pets
<i>Social Services:</i>	Medical query/consultation, distance learning
<i>Security Services:</i>	Security and surveillance of people, locations, and things
<i>Emergency Services:</i>	911 & enhanced 911, taxi, roadside
<i>Micropayment Services:</i>	Wireless access to vending machines, parking meters, gas pumps
<i>Access Services:</i>	Wireless access to doors and toll booths