# A Review of M-Commerce Concepts

Jack F. Freund III

Nova Southeastern University, Ft. Lauderdale, FL

# A Review of M-Commerce Concepts

Since the invention of the wireless phone, there has been the understanding of its substantial potential. It has perhaps the most potential in the area of electronic commerce, where a mobile device can aid in the purchasing of goods and services from anywhere in the world while anywhere in the world. This field is m-commerce and provides us with several interesting areas for research and study. A subset of e-commerce, m-commerce is e-commerce conducted on wireless infrastructures. Several primary elements enable mobile commerce. First, there is a mobile device. This device travels with the user in most places. It is differentiated from other devices by being smaller and having lower power consumption requirements. It communicates via radio frequencies to a cell tower, also called a base station. The radio frequency is itself a big piece of m-commerce. It has an incredibly high cost, as it must be licensed from the government in the area of operation. The base stations act as receivers and transmitters for the radio frequency. The towers are connected via various infrastructure elements to the public switched telephone network (PSTN), and from there to the Internet. The website that is chosen to visit is important because it needs to be capable of handling the mobile device's communications. In order to facilitate this, many protocols have been developed that aid in this. By using a common platform, the websites can help increase their appeal. Much of the design for mobile clients is to shrink the data presented as much as possible. This typically means text in lieu of complex graphics and scripting. WAP is the default specification for browsing the web via a mobile device, and for designing websites for mobile devices. There are many other elements to mobile commerce besides those physically tangible ones. It is important to have a legal and financial infrastructure that also supports mobile technologies. Regrettably, it is only recently that we see major financial institutions embracing web transactions and indemnifying their clients in

instances of fraud. A major deterrent to Internet commerce appears as a deterrent in mobile commerce as well. Security and privacy concerns are a major problem for mobile subscribers and mobile operators. These topics and issues provide us with interesting research problems. This treatment explores three topics in m-commerce that are of major importance to its developing sciences. Supporting these topics are papers by authors with distinct perspectives on each of these areas.

## Concepts

The three concepts that will be reviewed here are integral to the further understanding of m-commerce. The first reviewed concept is the ability for applications and services to perform based on the mobile device's location. One version of this is referred to as location-based advertising (LBA); it promises to be a juggernaut in the advertising industry. The basic premise is that the mobile device is able to ascertain its location (most likely through a GPS system), and the advertisers access this information to make specific advertising attempts. Second, we pursue a review of m-commerce security. The largest obstacle to global m-commerce acceptance is the inability to provide a completely secure computing environment. However, constructing a secure system is difficult when the entire set of factors specific to mobility are included. Thus, a general review of security and the security inhibitors to larger m-commerce adoption is presented. Lastly, we will present an overview of m-commerce infrastructure elements. This review will center on WAP, its features and its limitations. A treatment of the generic wireless elements will also be presented.

## Research

### *Location Aware Services*

We have selected four articles to aid in our review of the location-aware concepts. Cousins and Varshney (2001, 43-47) review the technologies that enable business-to-consumer (B2C) and business-to-business (B2B) location-aware applications. They begin by breaking down those types of applications that are driven by governments and those that are business-driven. These types of services are all dependent upon location-aware systems. This review establishes the applications that will require location-aware services. E911 is one such application. It is an overlay to the existing 911 emergency systems in the United States. Under existing structures, the 911 operators can only tell the cell in which the user is calling, and the best can approximate the caller's location within several city blocks. Under E911, the expectation is to pinpoint the caller to within 15 feet. Thus, a reliable location determination system is essential. Other applications include mobile supply chain operations, fleet management, job dispatch, and mobile sales forces. In each way, the mobile applications provide services that are heretofore unknown. They enable the operators to perform in a more nimble fashion and empower many of the lower levels of employees.

This gives us several options for how the mobile network operator can enable location aware services in their product offerings. The two groups of services are handset based, and network based. The only handset based technology, and the most popular, is Global Positioning Systems (GPS). The mobile device communicates with satellites in order to pinpoint its exact location. GPS handsets are more expensive than non-GPS enabled handsets. Thus, the network based technologies emerged. These systems make use of the phenomenon of radio waves and

their behavior in a cellular network. The handset reports its location indirectly to the cell towers through the physics of the radio waves.

The main theory Cousins (2001) gives is the establishment of a framework that helps to certify the mobile aware applications. The major enabling element in that framework is the repositories, which keep the application-level data accessible to the mobile elements and help to ease the network load associated with certain types of business activities. For example, in an application that allows for mobile supply chain management, there is the need for trucks to keep a digital inventory of everything on board. This information would then be transmitted back to the company's central location for incorporation in to the repository. A customer with an emergency order could search the repository for the quickest delivery time. This technology would then inform the truck to deviate from course to aid the customer in his emergency need.

The technologies that help support the repository are mobile standards. First is the Wireless Application Protocol (WAP). WAP acts as the go-between for the mobile handset's data transmission and the wired Internet's transmissions. It includes specifications for transmission of secure data, data-link, and network transmission layers. XML, and its derivatives are essential to this solution. By allowing for ad-hoc queries and custom labeling of data, the repositories can build meta-data indices to accelerate the mobile queries.

In another article by Varshney (2001, 1-6), he argues the requirements of a location management system. The theory he presents here is that different location-aware applications have different requirements for location infrastructure. He divides the application's needs into

four areas: precision, performance, coverage, and number of entities. For example, each application does not have the same requirements for location precision. E911 has a very high requirement, while mobile banking may only need precision to within a few-hundred feet. The same is true with each of the other elements. The response time for location-based advertising is a few minutes, while auctioning systems require very fast response times. Coverage needs are essential to supply chain applications; others only require local coverage. The bigger theory that emerges here is that the current wireless infrastructures may not be sufficient to support these types of applications. Thus, he proposed the overlay of GPS on the current infrastructure to support those levels of service that cannot be serviced by current devices (triangulation, and handset-protocols, among others). In addition to GPS, several databases would be added: Location databases, user preference databases, and application specific databases (product pricing, availability, etc.).

The next papers introduce us to user-centric issues in location services. First, O'Hara and Perry speak to the issues regarding consumer purchases. Their aim was to identify those issues that deterred people from making mobile purchases. They began by equipping people with disposable cameras to take a picture of what they wanted to buy, and then asked them to detail those reasons why they did not. This type of information is essential to the purchasing decisions made by potential m-commerce customers. What they had hoped to find was that there were substantial technological elements that were impeding these purchases. Indeed, some of these were because of that—no available retail location from which to purchase immediately nearby. Instead, they found there were primarily "soft" issues. Some of these include being able to discuss the purchase with peers to ensure a good buy, others wanted to be able to compare prices

with other locations and online portals. Lastly, there was the situation were certain people were satisfied with coming close to a purchase; akin to "flirting" with the idea of a purchase. They explained that doing this gave them sufficient pleasure, which negated the need to actually buy the item. Big-ticket items are usually involved here. Thus, the authors create the environment where a substantial location-aware application could facilitate these purchases. From a retailer standpoint, reducing the amount of issues that impede purchases is the goal.

Our last location-aware articles deal with the actual mobile device. The purpose of this study was to examine the ways in which people uses information tools during their day in an attempt to design a far more useful mobile device (PDA) (Marcus, Chen, 2002, 34-44). The study expounds at great length how the subjects used current information devices. The also detail how their proposed designs will meet those needs better than current devices. For our discussion on location-aware services, however, the article gives us insights into what the users feel should be possible. At its core, the users look for boundless services. They want to be able to communicate with others during flights, while in the car and while walking around the corporate or collegiate campus. In many ways, this can be accomplished with or without location-aware applications. However, Sadeh, Chan, Van, Kwon, and Takizawa (2003, 268-269) illustrate how useful location-based applications become interesting and almost imperative. At the Carnegie Mellon University, they have installed an 802.11x wireless infrastructure and applications that utilize the users' locations. Specifically, their location on the campus is available to their "buddy lists." They also support contextual reminders and appointments, such as being reminded to visit the Dean's office when you are in the administration building.

*Security*

The Cousins (2001) article mentioned above gives us a very acute insight into some of the problems of m-commerce. They refer to "chips which contain all personal information such as social security number, medical background, and passport information [being] embedded in mobile device[s]" (44). The temptation for the undesirable Internet element to misuse this kind of all-access pass must be overwhelming. This leads us to our second concept: m-commerce security. We have three articles in this area to highlight the security concepts relevant to m-commerce.

Any discussion of security in m-commerce cannot avoid WAP and WML. The Wireless Application Protocol (WAP) is the specification for a set of communication protocols that enable mobile data communication. It is composed of four layers: 1) Wireless Application Environment (WAE), 2) Wireless Session Layer (WSL), 3) Wireless Transport Layer Security (WTLS), and 4) Wireless Transport Layer (WTP). Most are familiar with the wired Internet secure transmission protocol, SSL. In order for wireless devices to communicate with a SSL encrypted website, they use the WTLS layer of WAP. The keystone in the WAP design is the WAP gateway, which translates the WAP packets into TCP/IP packets—in this case, it is converted from WTLS to SSL. Several authors point out the deficiencies in the WAP standard that allow for compromise. Jøsang and Sanderud (2003, ¶ 22) have this to say about the WAP gateway: "In addition to making authentication meaningless, this solution also creates and unavoidable plain text gap in the WAP gateway." Indeed, it appears that the actual encryption protocol utilized at both ends is indeed above scrutiny. However, the existence of the WAP gateway is what provides a target for attack. During the conversion process, the actual encrypted data will be available as plain text,

right before it is SSL encrypted. This means that with a timely script in the right place it will be able to recover the data (Ghosh, Swaminatha, 2001, 53). As in any security breech, the weakest point will be the major target.

WML is the Wireless Markup Language and its wired Internet counterpart would be HTML/XML. The ability to execute scripts is ubiquitous on the Internet, and accessing it through a mobile device will be no exception. Java is also pervasive in the wired and now the wireless world. However, the physical limitations of the mobile devices themselves have forced certain limitations in the implementation of these scripting languages. Most notably missing is any security measures such as sandboxing. Normally the mobile device has only limited control over scripting, and is limited to "allow all" or "deny all." They will likely ship with the "allow all" setting enabled. However, even if they do not, there is little use for a scripting language if it cannot be used.

What these two articles give us by way of theory is quite interesting. Ghosh surmises that because wireless devices are difficult to trace, and have no fixed location, or geographical zone, they will become the ideal location for launching attacks against fixed networks. By compromising enough wireless devices, a virtual army of virus-spreaders could be amassed with no real certainty of where they are physically located. This potential rises proportionally with the increasing power of the mobile device.

Jøsang (2003), show us security from an economical viewpoint. He comments on the relative lack of security in today's devices. He gives the reasons for this thusly:

> A typical characteristic of security is that it provides no additional functionality to an application other than security itself, i.e. it does not provide the functionality in which users are primarily interested…the current insecurity of commercial systems on the Internet is thus perfectly rational from the economists' viewpoint, however undesirable to the users' (Jøsang).

This very succinctly identifies the pull between functionality and security in modern computers systems, and indeed mobile ones. Without users explicitly paying for security features, we will find that they will conversely be paying to not have them.

Our last article specifically deals with a Distributed Denial of Service (DDoS) Attack. Geng, Huang and Whinston (2002, 213-223), discuss the importance of the timeliness in m-commerce. They contend it is not a simple matter of duplicating e-commerce in a wireless environment. Instead, there may be a negative adoption rate if users try to use mobile services without success. This, they argue, is where a DDoS attack could be the most dangerous. It would be even more difficult to track down a wireless DDoS culprit because of the inherent anonymity of using a wireless device, such as having no fixed geographic location, or the potential for different carries when roaming.

### *Infrastructure*

The last m-commerce concept for discussion is mobile commerce infrastructure. We have two articles here that touch on this concept. Varshney and Vetter (2002, 185-198) discuss architectures that can aid in the adoption of m-commerce. The basic premise is that if a mobile

commerce framework used open standards for these platforms, the networks could be built in an ad hoc fashion with mix and match pieces from multiple vendors. There is also a hint that users in the networks will be more inclined to participate if they are to receive one bill rather than individual bills from different participants in the network. This type of billing is also referred to as bundled services. In order to support this, the open standards will need to be employed to enable the different participants (Service Provider, Content Provider, and Application Developer) the opportunity to participate in an unabated way. Thus, the theory goes, the ability to easily enter into the market will allow a phenomenal growth of m-commerce. This idea is supported on its face; however, through further application of probable business scenarios, we can encounter areas where the theory no longer holds.

The authors themselves uncover one such scenario later in their article. They discuss that in creating more hardware independent mobile applications, they will increase the lines of code required to enable these applications. The reason, they surmise, is that by not being able to leverage the inherit advantages of proprietary hardware systems they will need additional lines of code to replicate the same functionality. Indeed, this problem is constantly being debated in other computing realms such as the argument over RISC and CISC processors provide faster services (i.e. whether a proprietary HP server should be employed, or a more generic Intel based solution is better). The research here is mixed, but the authors have indeed pointed out a major problem in overcoming proprietary hardware. Another issue is the premise that service providers wish to receive their hardware from a multitude of different vendors (thus necessitating the need for open standards). In fact, the majority of service providers prefer single-vendor solutions. The last dissonant premise is that service providers are unlikely to act as content or application providers. Such a scenario has yet to be played out, but with the merger of AOL-Time Warner,

we can see how access companies are being aggregated with content providers, thus further reducing the need for a framework that gives each participant transparent access to one another.

In another paper, (Malloy, Varshney, Snow, 2002, 225-234), the argument is made for two mobile architectures that will increase the availability and dependence of the networks. First, they surmise that by increasing the reliability of the composite components, the reliability of the entire network increases. This is a precise observation and accurate in its message. However, it transfers reliability issues from the service providers and wireless manufacturers to the wireless manufacturers' contract manufacturer. Their next suggestion provides the service provider the means to control the reliability of their own networks. Nevertheless, there are serious costs associated with this. Their more elaborate example shows the same geographical areas covered by multiple base stations. The basic premise being that by involving more base stations to cover the same area, it only follows that reliability would increase as well. Naturally, this is true, but ignores the more esoteric financial performance measurements used by the service providers, such as revenue per square foot. This is a measurement of the average amount of revenue generated per square foot of equipment in the mobile switching centers and base stations. This inclusion of entire fail-over systems would irreparably damage these performance measures.

## Future Research Directions

Clearly, the cornerstone for all growth in m-commerce is dependent upon wireless security. Without a proper framework for the development of all wireless applications, consumer response will be lukewarm. Clearly, the WAP specification is not as strong a foundation as is required for future growth. The WAP forum has made updates to the WAP

specification that essentially amounts to tunneling SSL through the WTLS layers. This is a suitable answer to the WAP gateway issues, however the overhead associated with tunneling will quickly become unacceptable and a bottleneck. Therefore, this area can use some significant research to develop a framework that is supportive enough to encourage application development, yet secure enough to dissuade most malicious intents.

Location based services have the potential to become a significant source of income for service providers. Research here can be done in areas that aid in the stability of non-GPS systems, and ways in which they can compete effectively with GPS systems. GPS costs are still a large enough barrier to discourage widespread adoption. Without a widely installed cell phone base with GPS receivers, the system is not functional. Therefore, an economic model needs to be developed that will allow for more cost effective GPS receiver distribution.

Lastly, an overall wireless data infrastructure that is more fault-tolerant, reliable, and dependable is paramount. Any work in this area should be greatly encouraged. There is some parallel work that can be done in other disciplines (such as chip and PCB manufacturing) involving component mean-time-between-failure (MTBF), however, a suitable IS solution should be worked as well.

## Conclusions

The concepts reviewed in this treatise are essential to the development of m-commerce research. Essentially, m-commerce research can be approached with a building-blocks metaphor. An apposite framework for m-commerce is paramount. In many cases the m-commerce infrastructure will require more than what is being deployed for voice-grade mobile

networks. In designing these systems, it is paramount that attention be paid to areas of security. The mobile cell phone will have access to two highly important systems for commerce in the US: the public telephone system and the Internet. Never before, have such devices existed in such numbers. Therefore, it is important to keep security in the forefront of design. The need for user acceptance is also high to support the high costs of wireless operations. Users, although conscious of security needs, will spend the most money on new features and services. All of these sometimes highly divergent, sometimes highly homogenous forces together will shape the future of m-commerce.

# References

References marked with an asterisk indicates studies included in the meta-analysis

*Batni, R. P., Lee, C. C., & Varney, D. W. (2000). *Enhanced Services in WAP-Enabled Networks*. Bell Labs Technical Journal, 5(3), 145-152.

*Bui, T., & Ondrus, J., (2002). *M-Computing for Real Time Negotiation Support*. *Proceedings of the 34th Hawaii International Conference on System Sciences*, (pp. 1-9). New York: IEEE.

Cousins, K. & Varshney, U. (2001). A Product Location Framework for Mobile Commerce Environment. *Proceedings of the First International Workshop on Mobile Commerce*, Rome, Italy (pp. 43-47). New York: ACM Press.

Geng, X., Huang, Y., & Whinston, A. B. (2002). *Defending Wireless Infrastructure Against the Challenges of DDoS Attacks*. Mobile Networks and Applications, 7(3), 213-223.

Ghosh, A. K., & Swaminatha, T. M. (Feb 2001). *Software Security and Privacy Risks in Mobile E-Commerce*. Communications of the ACM, 31(2), 51-57.

Jøsang, A. & Sanderud, G. (2003). Security in Mobile Communications: Challenges and Opportunities. *Proceedings of the Australasian Information Security Workshop Conference* (pp. 43-48). Darlinghurst, Australia, Australia: Australian Computer Society, Inc.

Malloy, A. D., Varshney, U., & Snow, A. P. (2002). *Supporting Mobile Commerce Applications Using Dependable Wireless Networks*. Mobile Networks and Applications, 7(3), 225-234.

*Mandry, T., Pernul, G., & Röhm, A. W., (2000). *Mobile Agents in Electronic Markets: Opportunities, Risks, Agent Protection*. International Journal of Electronic Commerce, 5(2), 47-60.

Marcus, A., & Chen, E. (2002). *Designing the PDA of the Future*. Interactions, 9(1), 34-44.

*Nohria, N. & Leestma, M., (2001). *A Moving Target: The Mobile-Commerce Customer*. MIT Sloan Management Review, 42(3), 104.

*O'Hara, K., & Perry, M., (2001). Shopping Anytime Anywhere. *Conference on Human Factors and Computing Systems*, Seattle, Washington, USA (pp. 345-346). New York: ACM Press.

*Patel, S., Ramzan, Z., & Sundaram, G. S., (2002). *Security for Wireless Internet Access*. Bell Labs Technical Journal, 6(2), 74-83.

*Ratsimor, O., Korolev, V., Joshi, A., & Finin, T., (2001). Agents2Go: An Infrastructure for Location-Dependent Service Discovery in the Mobile Electronic Commerce Environment. *Proceedings of the First International Workshop on Mobile Commerce*, Rome, Italy (pp. 31-37). New York: ACM Press.

Sadeh, N. M., Chan, T., Van, L., Kwon, O., & Takizawa, K. (2003). A Semantic Web Environment for Context-Aware M-Commerce. *Proceedings of the Conference on Electronic Commerce*, San Diego, CA, USA (pp. 268-269). New York: ACM Press.

*Shih, G., & Shim, S. S. Y., (Jun 2002). *A Service Management Framework for M-Commerce Applications*. Mobile Networks and Applications, 7(3), 199-212.

*Siau, K., & Zixing, S., (2003). *Building Customer Trust in Mobile Commerce*. Communications of the ACM, 46(4), 91-94.

Varshney, U. (2001). Location Management Support for Mobile Commerce. *Proceedings of the First International Workshop on Mobile Commerce*, Rome, Italy (pp. 1-6). New York: ACM Press.

Varshney, U. & Vetter, R. (2002). *Mobile Commerce: Framework, Applications and Networking Support*. Mobile Networks and Applications, 7(3), 185-198.

*Varshney, U., & Vetter, R., (2001). A Framework for the Emerging Mobile Commerce Applications. *Proceedings of the 34th Hawaii International Conference on System Sciences*, (pp 1-10). New York: IEEE.