S.R0141-0
Version 1.0
Date: 9 December 2010

3RD GENERATION PARTNERSHIP PROJECT 2 "3GPP2"

Study for

Machine-to-Machine (M2M) Communication

for cdma2000 Networks

Editor

Eileen McGrath, NEC Corporation, eileen.mcgrath@mac.com

Clifton Barber, KDDI, cbarber@cjbarberconsulting.com

Revision History

Revision	**Description of Changes**	**Date**
Rev0 v1.0	Initial Publication	9 December 2010

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

FOREWORD

This foreword is not part of this study.

3GPP2 Study for M2M Communication references material initially presented in the following publication:

- SC.R5003-0 v1.0: “3GPP2 Vision for 2009 and Beyond”

1 INTRODUCTION

1.1 Scope

The intent of this document is to evaluate the aspects of Machine-to-Machine (M2M) communications that are required to ensure that cdma2000®[1] network infrastructure is a viable communication network option for the M2M applications, including:

- Identify M2M service functionalities that capture the fundamentals of M2M communications and possible M2M applications.
- Identify applicable M2M communications use cases and characteristics to ensure that they are the basis for the evaluated network enhancements through out this study.
- Identify the list of potential requirements needed to enable machine type communications on cdma2000 networks based on the identified M2M service functionalities.
- Evaluate the impact of the anticipated large number of M2M devices and how to minimize this impact on the cdma2000 networks (e.g., a clear definition of M2M Group Based communications and its usage).
- Identify possible enhancements that would help in providing cdma2000 network operators with lower operational complexities when offering machine-type communication services.
- Optimize network operations to minimize the impact on device battery power usage.

This study of M2M Communication is targeting the enablement of machine-type data communication services and M2M applications on cdma2000 networks.

1.2 Document Conventions

"Shall" and "shall not" identify requirements to be followed strictly to conform to this document and from which no deviation is permitted. "Should" and "should not" indicate that one of several possibilities is recommended as particularly suitable, without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that (in the

---

[1]cdma2000® is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. When applied to goods and services, the cdma2000® mark certifies their compliance with cdma2000® standards. Geographically (and as of the date of publication), cdma2000® is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

negative form) a certain possibility or course of action is discouraged but not prohibited. “May” and “need not” indicate a course of action permissible within the limits of the document. “Can” and “cannot” are used for statements of possibility and capability, whether physical or causal.

1.3 References

All references are informative.

[1] ETSI TS 102 671 Release 9, “Smartcards; Machine To Machine UICC; Physical and logical characteristic”, April 2010.

[2] 3GPP2 C.S0024 cdma2000 High Rate Packet Data Air Interface Specification

2 Acronyms, Abbreviations, and Terminology

ACRONYM & ABBREVIATION	TERM	DEFINITION
API	Application Programming Interface	An interface implemented by a software program that enables interaction with other software by use of applications, libraries and operating systems.
ATI	Access Terminal Identifier	Link layer addressing identifier, typically assigned by the access network to a wireless terminal. (See C.S0024[2] for further details.)
CSIM	cdma2000 Subscriber Identity Module	cdma2000 Application residing on the UICC or M2M UICC.
DOS	Data Over Signaling	Method to support Access Channel utilization of segmentation and reassembly for small payloads.
M2M or MTC	Machine-to-Machine	A form of data communication that involves one or more entities that do not necessarily require human interaction. MTC is synonymous with “M2M Communication”.
M2M Characteristic	M2M Characteristic	A specific property of M2M communication that defines the device or system function.

ACRONYM & ABBREVIATION	TERM	DEFINITION
M2M UICC	M2M Universal IC Card	A UICC with specific properties for use in M2M environments, this includes existing form factors and the new M2M Form Factors MFF1 and MFF2 as defined in ETSI TS 102 671[1].
M2M Use Case	M2M Use Case	A description of how M2M device(s) and/or the M2M server utilize one or more of the M2M characteristics to accomplish a given task.

3 M2M Communication and Services Overview

3.1 Introduction

Machine-to-Machine (M2M) communication, also referred to as Machine Type Communication (MTC), is a form of data communication that involves one or more entities that do not necessarily require human interaction or intervention in the process of communication.

M2M communication can be used to enable different types of services that are valuable to the end user. Smart metering, healthcare monitoring, fleet management and tracking, remote security sensing, and on-demand business charging transactions are few examples of the M2M communication services.

Although all of the M2M communication services share a common set of characteristics, each M2M communication service has its own specific characteristics that may require a special handling or optimization by the wireless network. Because of the nature of M2M communication services, an optimal network for human-to-human communications may not be optimal for M2M communications.

cdma2000 networks may need to be optimized to accommodate the nature of M2M communication services taking into consideration the M2M communication services common characteristics first. Based on the value added by the M2M communication service, the network needs to address the selected specific characteristic(s). M2M communication services common characteristics involve:

- communication scenarios that do not require human control
- limited human interaction in the comunication process
- anticipation of a potentially huge number of communicating devices

- lower complexity and less effort compared to human communication
- the use of data communications (packet/circuit-switched)
- low volumes of traffic per device for a majority of M2M applications

3.2 Potential Impact of M2M Communication Services on Network Operational Complexities

Today, there is a wide range of M2M applications and new applications are being developed every day. While data usage for some M2M applications is similar to the existing data applications, others may have a very different behavior. Depending on the application, there could be potential impacts to the network operation in one or more of the following areas:

- Subscription Management: With the introduction of an M2M application, (e.g., Smart Grid application) to an existing service area, many new "subscribers" will be added rapidly. Since the behavior of these M2M devices can be drastically different from a human data communication user, there is a need to investigate an effective way to manage these kinds of new subscriptions.
- Network Resource: Typically, the current cdma2000 networks have been designed and optimized to support both voice and data services. With the deployment of the M2M devices, system capacity can be significantly impacted. Although some M2M devices may transmit intermittently, these devices may compete with one another and with other data users for network resources.
- Billing: The impact on the billing comes as a consequence of the impact on subscription and network resource management.

4 M2M Communication Services and Scenarios

4.1 Introduction

Each M2M communication service is developed to address one or more of the M2M communication characteristics. The M2M communication service is usually enabled using a specific M2M application. In addition, the M2M service or application is developed to address a specific M2M scenario.

The M2M characteristics that should be considered for further analysis and support by the cdma2000 network are listed in section 4.2. Additional M2M characteristics may be identified in the future, and if so, should be included in the analysis. After such analysis, it could become clear that in order for the cdma2000 network to support the enablement of such M2M services or applications, certain network optimization may become inevitable.

Each M2M communication application is developed with a specific M2M communication scenario in mind. In addition, these M2M applications need to consider the possibility of an M2M device communicating with one or more M2M communication server(s) or another device(s). Thus far, three communication scenarios for M2M have been identified:

- M2M device communicates with one or more M2M Communication Servers
- M2M devices communicate with one another
- M2M communication servers/concentrators communicate hierarchically with each other

Sections 4.3 through 4.4 provide further details on these M2M communication scenarios.

4.2 M2M Communication Characteristics

Table 1 describes M2M Characteristics supported by cdma2000 networks and is presented for consideration and analysis.

Table 1: List of M2M Characteristics

M2M CHARACTERISTIC	M2M CHARACTERISTIC DESCRIPTION
Delay Sensitive	M2M applications that require extremely fast access to the network and cannot tolerate much delay (e.g., smart grid recovery operations, and emergency automatic shutdown of a gas pipeline in case of earthquake or other calamity).
Group Based M2M Characteristics ▪ Group Based Policing ▪ Group Based Addressing	M2M devices which could share the same subscription and a common set of M2M characteristics can be handled by the network as a group rather than individually.
Location Specific Trigger	M2M devices that are known by the M2M Application to be in a particular area or location.
Low Mobility	M2M devices that have a limited scope of movement (e.g., fixed, infrequent movement, or move only within a specific region).
M2M Monitoring	This characteristic monitors M2M device-related events.
Mobile Originated Only	M2M devices that only support mobile originated communications.
Packet Switched (PS) Only	M2M devices that require packet-switched data services only.
Priority Access	M2M devices that are given preference for ingress and egress access over other devices competing for the same resources (e.g., communication in emergency situations and public safety).
Priority Alarm	M2M devices that issue a priority alarm when certain event occurs (e.g., theft, or other event that needs immediate attention).

M2M CHARACTERISTIC	M2M CHARACTERISTIC DESCRIPTION
Secure Connection	M2M applications that require secure communications between an M2M device and the M2M server.
Small Payload	M2M devices that send or receive small amounts of data in each distinct communication.
Time Controlled	M2M applications that can tolerate sending or receiving data during certain time intervals, thus reducing signaling load. Network operator may allow communication outside these time intervals but charge differently.
Time Tolerant	M2M applications that can postpone or tolerate delay of their data transmissions based on network conditions or other circumstances.
Uplink Data for Provided Network Destination	M2M applications that require all data from an M2M device to be sent to a specific network destination using the provisioned destination IP address.

4.3 M2M Device Communications with One or More M2M Server(s)

The M2M device communicates with a single M2M server or multiple M2M servers. The M2M device may use the same application to communicate simultaneously with different M2M servers for access to similar types of M2M services from multiple resources. In addition, the M2M device could communicate with different M2M servers using different applications to receive different M2M services.

In the case of such M2M communication scenarios, the following use cases have been identified (see Figure 1):

4.3.1 M2M server is located inside the cdma2000 network

- The network operator offers Application Programming Interface (API) on its M2M Servers(s)
- M2M User accesses M2M Server(s) of the operator's network via an API

4.3.2 M2M Server is located outside the cdma2000 network

- The network operator offers the network connectivity to the M2M Server(s) located outside of the operator's network
- The cdma2000 network works as a transmission medium for the M2M communication

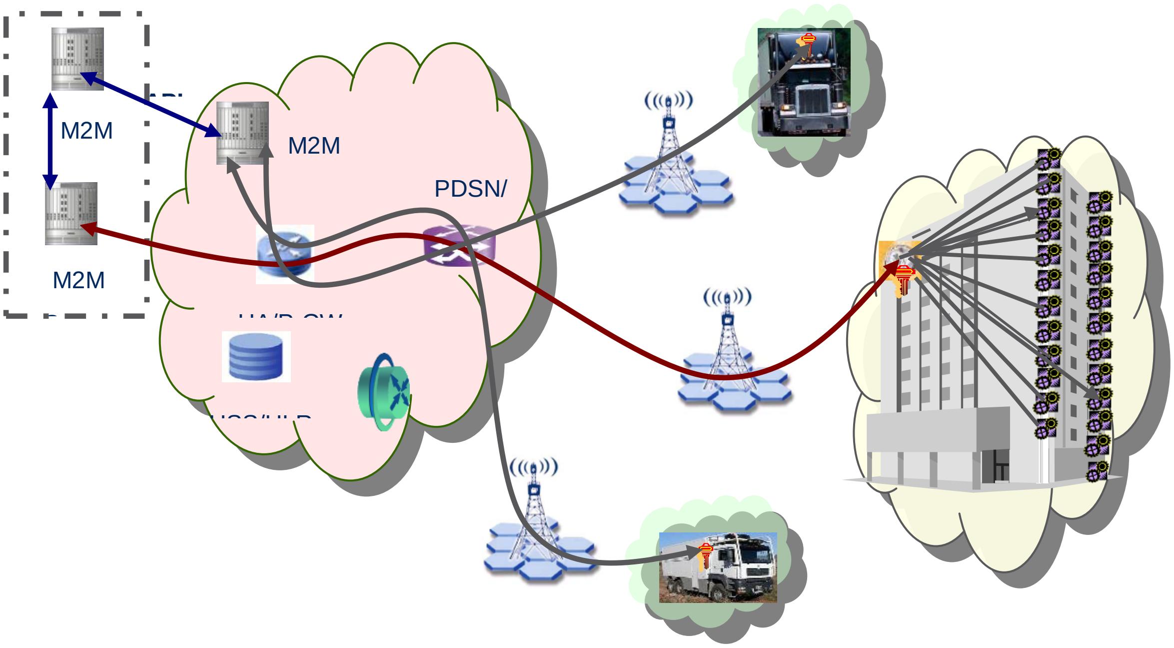

Figure 1: M2M Devices Communicating with M2M Server(s)

4.4 M2M Device Communications with M2M Device(s)

This is the communication scenario where the M2M devices communicate directly without an intermediate M2M server (see Figure 2).

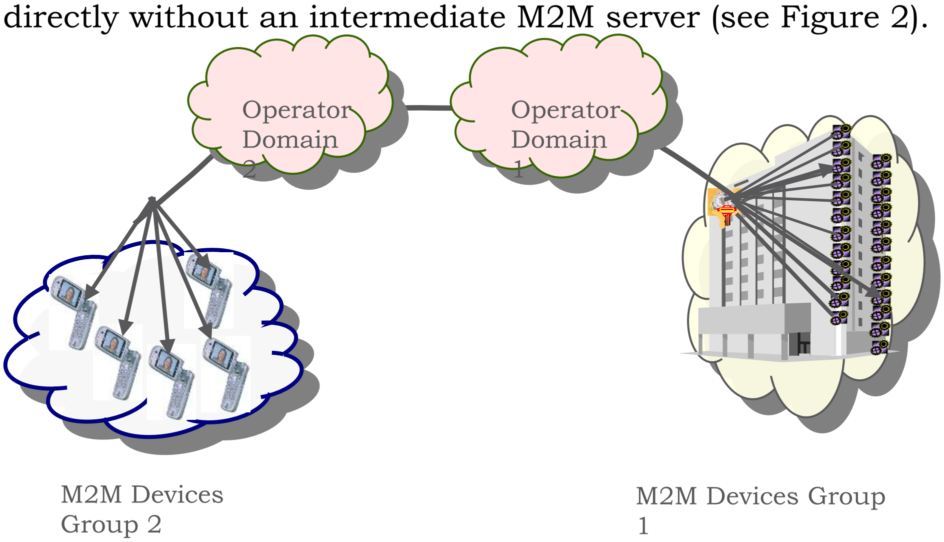

Figure 2: Inter-M2M Devices Communication

4.5 M2M Access Hierarchical Architecture

In order to avoid congestion to the cellular air interface, a M2M gateway acting as an aggregator node and/or a proxy on behalf of the network could be used. The M2M gateway connects the underlying M2M devices either through cdma2000 or via other means of communication. In addition, the gateway can perform several functions such as data forwarding, data aggregation, admission control, protocol translation, device monitoring, etc.

As show in figure 3 below, the M-G interface can be cdma2000 or other means of communication, the G-B interface is a cdma2000 air interface.

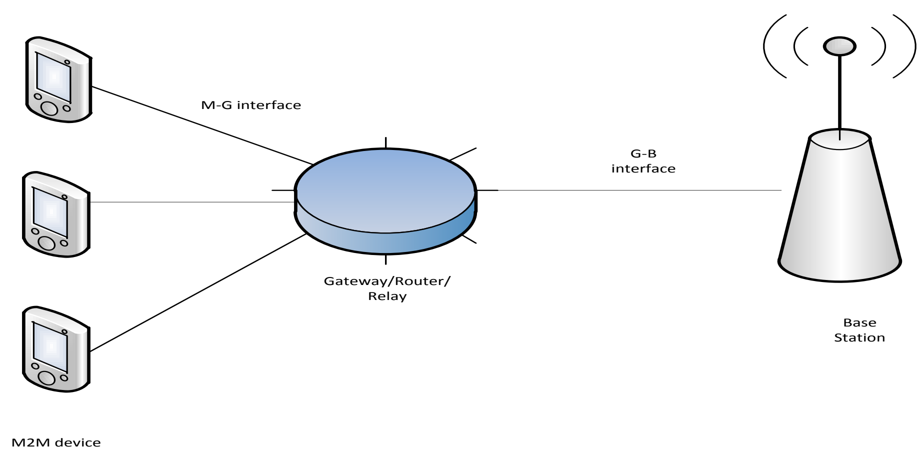

Figure 3: M2M Gateway Architecture

5 M2M ADDRESSING AND IDENTIFIERS

For the purpose of device and network management, any M2M device deployed in the cdma2000 systems should have a unique identity to provide information related to either subscription or the physical characteristic of the device. Furthermore, an M2M device deployed in a cdma2000 network should adopt a direct or indirect addressing means so that it can be independently addressed.

Depending on how an M2M device is attached in the network architecture of the various Communication Scenarios depicted in Section 4, the M2M device in a service network should communicate with the application server(s) or other device(s) through one of the following modes:

- Through direct addressing (e.g., the M2M device has an unique IP address);
- Through another subsystem's internal addressing mechanism (e.g., through a "Home Gateway", or a "Data Aggregator");
- Through a logical mapping of pre-registered information (e.g., use ATI to access an M2M device in a cell in an HRPD network).

Although it is straightforward to have each M2M device equipped with an IP address, it may not be practical due to the complexity limitation of some M2M devices, such as a simple motion sensor of a security monitoring system.

Addressing through another subsystem is a typical solution to accommodate the M2M devices with limited complexities or to shield certain M2M devices from being directly accessed from the external addressing mode (e.g., through direct IP access).

Each M2M device should be uniquely identified. Typically, an M2M device must have an identifier associated with the physical identity (e.g., a serial number) so that it can be uniquely tracked for device management purposes.

Those M2M devices that connect directly to the cdma2000 network need a subscription for a service, and hence, a subscription identity is required. The subscription identity, preferably, should be uniquely associated with the M2M device; however, there may be occasions the subscription identity indicates a “group service”, which is applicable to a group of M2M devices.

In order for an M2M device to transmit data or for the network to page an M2M device within a cell more efficiently, a physical identity (or a subscription identity) can be mapped to a logical identity with an access ID in a shorter format. For example, in cdma2000 network, the physical identity of an M2M device can be mapped into a logical identity such as an Access Terminal Identifier (ATI) after the M2M device has been registered with a valid subscription identity. The logical identity can then be used to identify the M2M device in the same way as the physical identity but in a more compact format for the transmission efficiency over the air link.

In order to support the class of M2M devices that require end-to-end IP communication capability, each M2M device directly connected to the cdma2000 network may need to have a unique IP address. M2M devices connected to the network via some type of M2M Gateway may or may not use IP addressing.

It is recommended that the device identity be separated from the subscription identity. Comprehensive recommendations on device numbering and addressing related to the M2M subscription identity and the device identity for the cdma2000 systems can be found in the SC report on this subject.

6 POTENTIAL M2M COMMUNICATION SERVICE REQUIREMENTS

6.1 Improved Management of M2M Communication Groups

M2M Service subscribers will be able to assign multiple devices that can be managed on an individual or group basis. For an operator supporting M2M devices on its network, it would be helpful if there is a broadcast message that can be sent from the network for the purpose of controlling or alerting a group of M2M devices. From the viewpoint of radio congestion, it is preferable to utilize aggregate control via broadcast messaging rather than individual simultaneous messaging addressed to each one of the multiple M2M subscribed devices.

M2M Services will be able to send a broadcast message to a large group of M2M devices affiliated with a single subscriber (e.g., to page the M2M devices).

6.2 Reduced Complexity

There is a need for a class of M2M devices with reduced design complexity (e.g., reduced radio interface design complexity due to low data transmission rate) for certain M2M applications such as vending machine, Supervisory Control And Data Acquisition (SCADA), electric meters, home security, etc. All of these devices generally send a small amount of data on a relatively low duty cycle and usually require no mobility.

6.3 Device Management

M2M devices such as vending machines, electric meters, SCADA, etc. may not have any direct human interaction. It is necessary to provide a way to provision, diagnose and even upgrade software over the air interface.

7 M2M Communication Use Cases

An M2M use case refers to a set of M2M devices that uses one or more M2M characteristics when connected via cdma2000 network. Table 2 presents a list of M2M use cases and their associated M2M characteristics. Each of these M2M use cases can be used for testing and evaluating the cdma2000 enhancements that address the respective M2M characteristics.

Table 2: List of M2M Use Cases

M2M USE CASE	M2M CHARACTERISTICS & NOTES	
Connected Home Appliances	o Fixed o Small Payload o Time Tolerant o Time Controlled o Group-based Policy o Group-based Billing	
Fleet Management Tracking	o Small Payload o Mobile Device o Group-based Policy o Group-based Billing	
Payment Machine	o Fixed or low mobility	Most vending machines are stationary. Some payment terminals (e.g., hand-held credit card machines used in restaurants) have low mobility. Exception cases include vending machines on high-mobility transportation (e.g., trains).
	o Small Payload	Payment transactions and credit card verifications typically require small amounts of transmitted or received data.
	o Asynchronous transmission	All data transmissions are asynchronous because the payment transactions typically are triggered by random user input and responses are sequential to that input.
	o Infrequent mobile termination	Most transactions are mobile-originated. Mobile-terminated transactions typically occur in response to operator queries.
	o Security	Financial transactions typically require enhanced security support.

M2M USE CASE	M2M CHARACTERISTICS & NOTES	
	o Group-based address & policy	The operator might want to address this type of device on a group basis.
Professional Health Care Monitoring	o Low Mobility o Small Payload o Delay Sensitive o High Priority o Priority Alarm	
Public Safety	o Priority Access o Small Payload o Group-based Policy	
Security and Surveillance	o Delay Sensitive o Priority Alarm o Uplink Data for Provided Network Destination o M2M Monitoring o Secure Connection o Small Payload (if real time audio and/or video monitoring is not required)	
Smart Grid Control	o Fixed to Low Mobility o Small Payload o Delay Sensitive o Group-based Billing o Group-based Addressing o Group-based Policy o Priority Alarm o Priority Access	
Smart Metering	o Fixed to Low Mobility o Small Payload o Time Controlled o Group-based Policy o Group-based Billing o Group-based Addressing	

8 System Enhancements for M2M Communications Services Support

M2M applications provide a mechanism to support the ever increasing use of automation in every day life. These applications or services are not new to us, and many M2M applications such as home automation, security, alarms systems, and meter reading are aleady deployed. However, most of these M2M applications are deployed independently or in isolation from other M2M applications. The goal of this study is to examine current cdma2000 technologies in order to best support various types of M2M applications.

Wireless networks are becoming ubiquitous, covering both congested urban and outlying rural communities around the world. It is clear that wireless networks provide a flexible communication platform for M2M applications. M2M applications can provide new potential markets and business opportunities for wireless communications. cdma2000 is optimized for spectral efficiency. cdma2000 was not initially created with M2M applications in mind, yet key enhancements will leverage the cdma2000 technologies, including the spectral efficiency, to successfully support M2M applications.

8.1 3GPP2 System Architecture Enhancements Overview

8.1.1 Communication Model

The M2M applications use the client-sever communication model for the M2M terminals to communicate with the M2M application servers on the network.

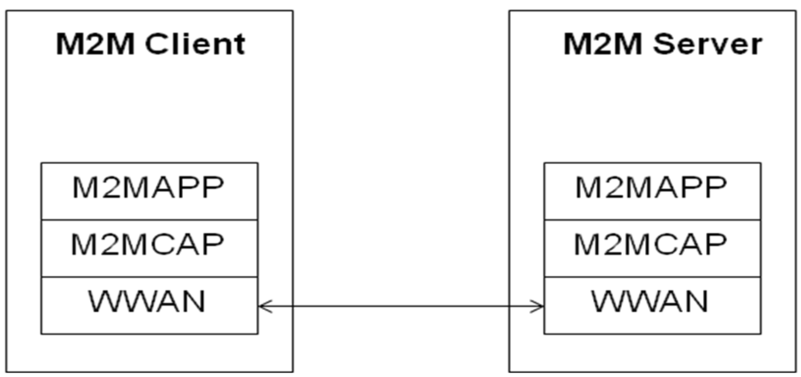

Figure 4: M2M Client Server Communication Model

A M2M Client resides in an M2M terminal, while the M2M Server is on the operator's core network or connected through it.

M2M Client contains three protocol suites:

- M2M Application Protocols (M2MAPP) define specifications for different M2M applications such as smart grid, meter reading, traffic control, etc. M2M applications could send data to the next layer protocol M2MCAP directly. In some other applications, M2MAPP could be a communication node of a short range wireless network such as Wireless Sensor Network (WSN). The Blue Tooth, ZigBee etc. capable devices could transmit data over Blue Tooth, or ZigBee network to the M2M Client as M2MAPP data.

- M2M Communication Adaptation Protocol. See the detail in next section.
- Wireless Wide Area Network (WWAN) protocol such as cdma2000 mobile station protocol provides the wireless communication to the M2M server over WWAN network.

M2M Server also contains three protocols suites matching with M2M Client's protocol suites. M2M Server shown here is a logic entity in the network. In real implementation, each protocol suite could reside in different physical node. For example, WWAN could be an existing cdma2000 network entity, while M2MCAP could reside in an independent network node to connect to many M2M application servers for different applications.

M2M Client-Server supports N to 1 communication model, which allows multple M2M clients to access the M2M server simultaneously.

8.1.2 M2M Communication Adaptation Protocol

The M2M applications might utilize different means of communication, such as fixed wired network, WiFi, etc, whenever they are available and when devices are capable. The cellular communication network is one such communication means to provide wide area coverage. In order to make M2M applications more independent from the communication networks and more adaptive to many environments, it would be necessary to define a communication adaption protocol (M2MCAP) layer between M2M applications and communication networks.

- M2MCAP provides an adaption to different communication networks, such as cdma2000 1x SMS, cdma2000 1x Circuit Data, HRPD Packet Data, WiFi, etc. and carries M2M application payloads over such networks.
- M2MCAP provides the capability for the M2M Server to monitor, diagnose, authenticate, and upgrade M2M devices over such networks.
- M2MCAP provides the re-transmission mechanism for reliable delivery of M2M application packets.
- M2MCAP could interface with M2M devices directly or via a communication node of the WSN on the client side.
- M2MCAP could interface to the M2M applications over IP network on the server side.

8.1.3 New M2M Terminal Class

Introducing new M2M terminal classes would help to separate M2M terminals from existing cdma2000 mobile stations. With those new M2M terminal classes, the optimization would be applicable to the particular M2M terminals without impact existing mobile stations. In addition, the new classes would also help to distinguish M2M applications.

8.2 cdma2000 Radio Enhancements

8.2.1 Transmission Efficiency of Communication Networks

8.2.1.1 Reverse Link Transmission Efficiency

The existing CDMA2000 network is evolved from voice centric network architecture in which human utilizes the network facilities for the forward and reverse link symmetric communications.

In packet data applications, the information is stored in the Internet. People use applications such as web browsing, video and music down loading, etc. on mobile stations to access the network to get information from the Internet. These types of applications create asymmetric traffic between forward and reverse links. It typically requires much larger radio access network capacity on the forward link than the reverse link.

In M2M applications, on the other hand, the information typically originates on the machine terminals and is required to be transmitted to the network over the wireless communication networks. Therefore, efficient reverse link transmission of the wireless network is important for M2M applications.

Most current applications such as voice and data, over cdma2000 networks require establishment of connections first. After a traffic channel is set up, a mobile station would be able to transmit the data over traffic channels. Due to characteristics of M2M applications, however, many M2M applications only need to send short bursty packets. Therefore using connection oriented transmission would generate many signaling exchanges between M2M terminals and the network, hence reducing transmission efficiency for M2M applications.

8.2.1.1.1 Access Mechanism Enhancement

In some of M2M applications, a large number of machine terminals might require access to the network at the same time, for example as follows:

- In Telematics applications, many vehicles could transmit a large amount data to the network when they are located or concentrated in specific locations, such as near traffic signals and ready to move into traffic.
- In instant delivery applications, some messages to a large number of smart phones located in a small area, such as stadium, may generate many pages to these terminals leading to unwieldy amounts of network access and attempts to establish network connections.

- If there is a network failure, a large number of M2M devices may fail in their attempts to establish connections. These devices may be driven by the application behavior to repeatedly attempt network access.

In these examples, application behavior may generate access congestion. The congestion may be aggravated if the M2M terminals try to repeat their access attempts and increase their access probes. As a result, some terminals may not achieve access successfully after several attempts. If not properly controlled, this could negatively impact system performance.

Adding M2M devices to a cdma2000 network should not degrade native cdma2000 services (e.g., voice, video, or data) assuming adequate capacity is provisioned to support M2M. M2M devices and networks should have access control mechanisms fully activated to mitigate access attempt overload. In addition, requirements should be developed that protect the cdma2000 network from M2M "storms" in forward and reverse links during times of system access and transmission of data.

Optimized mechanisms for access control should be considered, as follows:

- control access frequency of M2M terminals
- reduce collisions which cause re-transmission and access delay
- differentiate M2M terminals or some M2M applications from ordinary voice and data applications, thereby prioritizing M2M applications via special treatment in case of congestion or failure, as appropriate.

Another possibility is to consider the connectionless transmission over the access channel for M2M applications. The connectionless transmission is not new in cdma2000. When a mobile station is in idle state, the signaling transmission uses connectionless transmission mechanism over the access channel. Since the access channel is designed to carry signaling, it might need to be optimized for carrying a large amount of M2M application data.

8.2.1.1.2 Lower Minimum Transmission Rate

Existing radio network specifications have some limitation on the minimum transmission rate on the reverse link. In many M2M applications, the payload from M2M applications can be very short. Such limitation on the minimum transmission rate, may reduce efficiency of reverse link transmission. In addition, such transmission rate may require a relative good radio environment. Therefore reducing the minimum transmission rate and providing adaptation of different transmission rates to the radio environment, payload size and other traffic conditions could potentially improve the transmission efficiency for M2M applications.

When considering lowering the minimum transmission rate, overall system throughput may be affected.

8.2.1.1.3 Reduce Transmission Overhead

When an M2M terminal transmits data over a shared reverse link common channel, it needs some identification to distinguish itself from other M2M terminals. The overhead in such shared common channel might take a large portion of transmitted data over the air compared to the application payload. Reducing the overhead would help to improve the reverse link transmission efficiency over the common channel.

8.2.2 Improve Radio Link Reliability and Extend Coverage

M2M applications are very diverse and can have significant variance on the communication requirements. Thanks to the availability of wireless cellular network, quite a few M2M applications are using cellular network to provide wide area coverage of M2M communications to reduce the deployment effort. In some deployment situations, however, the radio signal on the wide area coverage might be very low or in deep fading. This would result in radio link reliability issue and coverage shrinkage.

8.2.2.1 Reduce the Minimum Transmission Rate

A indicated in the discussion on Reverse Link Transmission Efficiency (see section 8.2.1.1.2), reducing the minimum transmission rate could potentially improve the transmission efficiency for M2M applications. Since many M2M applications are only required to a send short data packet per each transmission, this optimization would also help improve the radio link reliability and extend radio coverage.

8.2.2.2 Improved Access Channel Performance

As numerous M2M devices with short bursty transmissions are deployed, Access Channel load is expected to increase. Therefore, it is prudent to look at opportunities to improve Access Channel performance.

Some of the following measures should be studied for opportunities to improve Access Channel performance in M2M environment:

- Increase in access channel capacity (e.g., access parameter settings);
- Reduce the rate of access probe collisions and retransmissions over the access channel;
- Implementation of sophisticated access persistence controls for various terminals access classes, commensurate with delay tolerance of M2M applications;
- Fine tuning of access parameter settings in terms of probe spacing and power increment;

- Studying the feasibility of separation by Access Channel receiver of multi-path signals belonging to a single device from signals belonging to different devices;
- Studying the possibility of soft combining Access Channel modulation symbols from multiple receivers, while ensuring that such method does not cause probe acknowledge delays;

The possibility of soft (selective) combining entails a technique that is available for the Traffic Channel which helps reduce reverse link transmit power and improve capacity, but is not currently common practice on Access Channel. When studying this technique for Access Channel, care should be taken that processing delays involved do not cause sluggish access probe acknowledgement, since that may cause the terminal to increase probe power and retransmit before acknowledgement is received. This means that soft combining may be viable in case of receivers in two or more sectors of the same BS/AN. For the case of two distinctly located BSs/ANs, a selective response to the access probe could be sent from the best reverse link of the BSs/ANs.

8.2.2.3 Improve FL and RL Balance

In existing cellular system, a M2M terminal can transmit an access probe over the reverse link on the same cell which it is monitoring on the forward link. Which cell an M2M terminal is monitoring depends on the pilot signal strength on forward link of the cell and its neighbor cells. In other word, the existing specification always assumes the best forward link serving cell is the best reverse link serving cell. However in a typical deployment scenario, the forward and reverse link serving cells are not balanced, i.e., the best forward link serving cell to an M2M terminal might not be its best reveres link serving cell. This imbalance of forward and reverse link serving cells might cause the M2M terminal to use extra transmit power or to re-transmit unnecessary access probes.

Solving this imbalance on forward and reverse link serving cells would reduce reverse link interference, curtail unnecessary probe retransmission, and extend battery life of battery operated M2M devices.

8.2.3 M2M Terminal Management

8.2.3.1 M2M Terminal ID Management

M2M applications require managing a huge number of M2M terminals in the field even as most of them are in the inactive state at any given time. The number of M2M terminals might be larger than the current number of cellular phones in the world.

An M2M terminal may use MEID to identify itself, similar to mobile stations. A 56-bit MEID can uniquely identify a mobile station globally. Unlike mobile stations which could roam to other places, many M2M terminals might be installed permanently at particular locations. This creates the question of necessity to use such long bits identity for the fixed M2M deployment, since ID transmission overhead will reduce transmission efficiency.

Using short form identity of M2M termnals for the fixed deployment would help to improve transmission efficiency. However, this strategy should be balanced with consideration of premature identifer exhaust for operators to manage M2M terminals in a scalable deployment.

8.2.3.2 M2M Terminal Security

M2M devices might use detachable devices such as M2M UICC [4] with CSIM application or R-UIM to store subscription information for M2M applications. Since many of M2M terminals might be installed outside and not be monitored in real time, the detachable device for storing subscription information would create security issue. It might be required to develop a mechanism to prevent theft, tampering with subscription credentials and mis-use of subscription information. In addition, it might be necessary to develop some special mechanism to authenticate M2M terminals.

8.2.4 Battery Life Improvement for Battery Operated M2M Devices

Battery life is very important for the battery operated M2M devices. It is critical for the success of M2M applications. Existing mobile devices are battery-operated in most cases. Since they are supposed to be used by humans, it should not be difficult to recharge when the battery runs out. Therefore current wireless technology does not put emphasis on the requirements for low or extremely low power consumption of battery operated M2M devices.

Unlike traditional mobile stations, many M2M devices might not need to wake up often to monitor the network. This provides an opportunity to save battery life by configuring M2M devices for different sleep duration and wakeup time.

Reducing unnecessary re-transmissions of M2M application packets might be another way to extend the battery life. Due to uncertainty of radio environment, wireless devices are typically required to re-transmit packets if the previous transmission fails. Those transmission failures might be caused by low signal quality, imbalanced forward and reverse link , or transmission collision over the shared channel. Reducing the possibility of failures decreases re-transmissions and improves battery life, accordingly.

M2M applications may have very different transmission latency requirements. Many M2M applications might not need real time (low latency) communication. They can allow more transmission delay and response delay. Therefore M2M applications may be divided into the following latency categories:

- Low latency
- Medium latency
- High latency

Based on the category of M2M application, the M2M client and server can provide an efficient way to schedule transmission of M2M data. For some high latency (delay tolerant) applications, the transmission might be scheduled at low traffic period so as to lower transmit power by M2M terminals and help reduce access storm effects on the network.

In principle, an M2M device can initiate communication with the network at any time. The network is always on and available to receive access attempts from an M2M device to support an application. In order to reduce power consumption levels, an M2M device may want to schedule periodic network-initiated messaging in support of an application so that the device itself can maintain a known sleep cycle for longer periods of time.

M2M services will be able to minimize power consumption in every situation. Operation at the lowest possible power consumption level needs to be supported to extend battery life, including establishing periodic network-initiated messaging to an M2M device.

8.3 cdma2000 Core Network Enhancements

8.3.1 Resource Management Mechanism Enhancement

In some existing M2M applications, the upper layer data session (such as PPP) terminates in a private network or at a server that resides outside the (not visible to) operator's core network. The application may cause M2M terminal to transmit a heartbeat message over the radio access network to keep the upper layer data session alive. This heartbeat message could be a "dummy" data packet from the application layer or a keep-alive message generated by the PPP protocol. As a result, the core network cannot release radio link and bearer resources even if there is no useful data being transmitted for a period of time. This causes waste of radio and other network resources in the operator's network. To address this issue, enhancements to network resource management mechanisms should be considered.

8.3.2 Paging Enhancement

In order to prevent a huge number of M2M devices tying up network resources, consideration should be given to release the PPP links of M2M devices in some applications after data transmission. However, in the scenario wherein the network pushed data to the M2M devices, there is a requirement for network to page the M2M devices during a null state.

8.3.3 Circuit Switch Core Networks Enhancements

No specific standards impact has been identified.

8.3.4 Packet Data Core Network Enhancements

No specific standards impact has been identified.

Annex A M2M Parking Lot

This annex is used to track some of the issues that need to be studied and considered while evaluating the system enhancements. They are listed here in order not to lose track of them.

Table A-1: List of NOT to Lose M2M Enhancements

M2M ENHANCEMENT	NOTES
Enhanced Registration	Associate a given M2M device with various subtypes and define a set of attributes associated with such a device to apply to registration procedures.
Access Channel	Define or modify registration procedures to allow system access to a high priority user (how does a high priority user obtain access to the system, if low priority users are on the system), M2M, Low priority, High Priority.
Supporting Access Channel over Data Over Signaling (DOS)	Utilization of segmentation and reassembly in support of small payloads.