Exploiting the Short Message Service as a Control Channel in Challenged Network Environments

Earl Oliver

PhD Candidate
Tetherless Computing Lab, School of Computer Science
University of Waterloo

September 15, 2008

Outline

1. Introduction
   - Motivation
   - Objectives
2. Understanding SMS
   - Characteristics
   - Sample message flows
3. Design
   - Protocol
   - Architecture
   - Implementation
4. Summary

Outline

1. Introduction
   - Motivation
   - Objectives
2. Understanding SMS
   - Characteristics
   - Sample message flows
3. Design
   - Protocol
   - Architecture
   - Implementation
4. Summary

Outline

1. Introduction
   - Motivation
   - Objectives
2. Understanding SMS
   - Characteristics
   - Sample message flows
3. Design
   - Protocol
   - Architecture
   - Implementation
4. Summary

Outline

1. Introduction
   - Motivation
   - Objectives
2. Understanding SMS
   - Characteristics
   - Sample message flows
3. Design
   - Protocol
   - Architecture
   - Implementation
4. Summary

Take home points

- Cellular network is highly erratic under bursty workloads.
- Characterized properties of the SMS network using bursty workloads using a variety of commondity hardware.
- Designed and built a robust data channel on top of SMS.

Take home points

- Cellular network is highly erratic under bursty workloads.
- Characterized properties of the SMS network using bursty workloads using a variety of commondity hardware.
- Designed and built a robust data channel on top of SMS.

Take home points

- Cellular network is highly erratic under bursty workloads.
- Characterized properties of the SMS network using bursty workloads using a variety of commondity hardware.
- Designed and built a robust data channel on top of SMS.

Motivation

Growth of SMS

- Cellular networks are ubiquitous.
  - Over 1 trillion SMS message sent in 2005.
  - Projected to be 3.7 trillion SMS messages per year by 2012.
- Competition between carriers, growth of MMS, and data services are driving down prices*.
  - (India) smsjunction.com : Rs. 0.09 ($0.002 USD) / message
  - (India) znisms.com : Rs. 0.28 ($0.006 USD) / message
  - (US) AT&T : unlimited SMS messages for $5 USD / month

* Except in Canada: no unlimited plans and charges for incoming messages.

Motivation

Growth of SMS

- Cellular networks are ubiquitous.
  - Over 1 trillion SMS message sent in 2005.
  - Projected to be 3.7 trillion SMS messages per year by 2012.
- Competition between carriers, growth of MMS, and data services are driving down prices*.
  - (India) smsjunction.com : Rs. 0.09 ($0.002 USD) / message
  - (India) znisms.com : Rs. 0.28 ($0.006 USD) / message
  - (US) AT&T : unlimited SMS messages for $5 USD / month

* Except in Canada: no unlimited plans and charges for incoming messages.

Motivation

Growth of SMS

- Cellular networks are ubiquitous.
  - Over 1 trillion SMS message sent in 2005.
  - Projected to be 3.7 trillion SMS messages per year by 2012.
- Competition between carriers, growth of MMS, and data services are driving down prices*.
  - (India) smsjunction.com : Rs. 0.09 ($0.002 USD) / message
  - (India) znisms.com : Rs. 0.28 ($0.006 USD) / message
  - (US) AT&T : unlimited SMS messages for $5 USD / month

* Except in Canada: no unlimited plans and charges for incoming messages.

Motivation

Growth of SMS

- Cellular networks are ubiquitous.
  - Over 1 trillion SMS message sent in 2005.
  - Projected to be 3.7 trillion SMS messages per year by 2012.
- Competition between carriers, growth of MMS, and data services are driving down prices*.
  - (India) smsjunction.com : Rs. 0.09 ($0.002 USD) / message
  - (India) znisms.com : Rs. 0.28 ($0.006 USD) / message
  - (US) AT&T : unlimited SMS messages for $5 USD / month

* Except in Canada: no unlimited plans and charges for incoming messages.

Applications of SMS

Existing applications

- Messaging, e-voting/surveys, Internet search, e-commerce, system monitoring, notifications, etc.
  - Nearly always constrained to a single SMS message.

Can SMS be used to transport much larger quantities of data?

Applications of SMS

Existing applications

- Messaging, e-voting/surveys, Internet search, e-commerce, system monitoring, notifications, etc.
  - Nearly always constrained to a single SMS message.

Can SMS be used to transport much larger quantities of data?

Applications of SMS

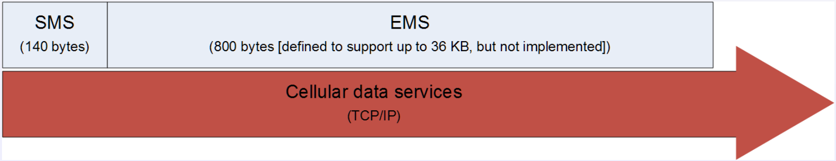
Existing applications

- Messaging, e-voting/surveys, Internet search, e-commerce, system monitoring, notifications, etc.
  - Nearly always constrained to a single SMS message.

Can SMS be used to transport much larger quantities of data?

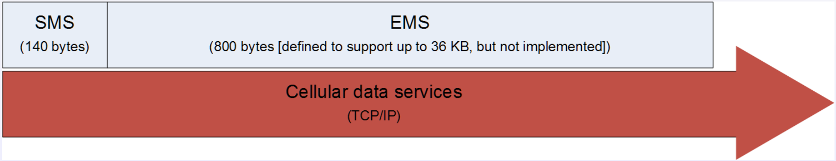
Existing solutions

- Enhanced Message Service (EMS)
  - Application layer extension to SMS.
  - Device support is poor.
- Cellular data services (GPRS/EDGE, EVDO)
  - Greatly superior as a data service.
  - Often two orders of magnitude cheaper.
  - Sparsely deployed in developing regions.
  - Mobile end-points often not reachable.


SMS
(140 bytes)
EMS
(800 bytes [defined to support up to 36 KB, but not implemented])
Cellular data services
(TCP/IP)

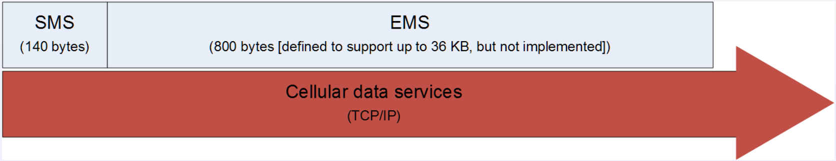
Existing solutions

- Enhanced Message Service (EMS)
  - Application layer extension to SMS.
  - Device support is poor.
- Cellular data services (GPRS/EDGE, EVDO)
  - Greatly superior as a data service.
  - Often two orders of magnitude cheaper.
  - Sparsely deployed in developing regions.
  - Mobile end-points often not reachable.


SMS
(140 bytes)
EMS
(800 bytes [defined to support up to 36 KB, but not implemented])
Cellular data services
(TCP/IP)

Existing solutions

- Enhanced Message Service (EMS)
  - Application layer extension to SMS.
  - Device support is poor.
- Cellular data services (GPRS/EDGE, EVDO)
  - Greatly superior as a data service.
  - Often two orders of magnitude cheaper.
  - Sparsely deployed in developing regions.
  - Mobile end-points often not reachable.



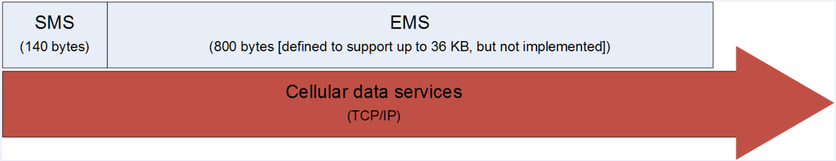
SMS
(140 bytes)

EMS
(800 bytes [defined to support up to 36 KB, but not implemented])

Cellular data services
(TCP/IP)

Existing solutions

- Enhanced Message Service (EMS)
  - Application layer extension to SMS.
  - Device support is poor.
- Cellular data services (GPRS/EDGE, EVDO)
  - Greatly superior as a data service.
  - Often two orders of magnitude cheaper.
  - Sparsely deployed in developing regions.
  - Mobile end-points often not reachable.



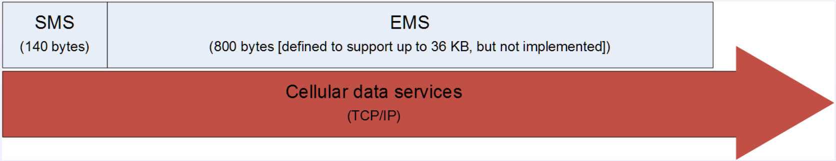
SMS
(140 bytes)

EMS
(800 bytes [defined to support up to 36 KB, but not implemented])

Cellular data services
(TCP/IP)

Existing solutions

- Enhanced Message Service (EMS)
  - Application layer extension to SMS.
  - Device support is poor.
- Cellular data services (GPRS/EDGE, EVDO)
  - Greatly superior as a data service.
  - Often two orders of magnitude cheaper.
  - Sparsely deployed in developing regions.
  - Mobile end-points often not reachable.



SMS
(140 bytes)

EMS
(800 bytes [defined to support up to 36 KB, but not implemented])

Cellular data services
(TCP/IP)

Claim: there are many practical applications for SMS.

Such as:

- Exchanging cryptographic keys.
- DTN routing table updates.
- Synchronous user creation at rural kiosks.
- And many more ...

Claim: there are many practical applications for SMS.

Such as:

- Exchanging cryptographic keys.
- DTN routing table updates.
- Synchronous user creation at rural kiosks.
- And many more ...

Claim: there are many practical applications for SMS.

Such as:

- Exchanging cryptographic keys.
- DTN routing table updates.
- Synchronous user creation at rural kiosks.
- And many more ...

Claim: there are many practical applications for SMS.

Such as:

- Exchanging cryptographic keys.
- DTN routing table updates.
- Synchronous user creation at rural kiosks.
- And many more ...

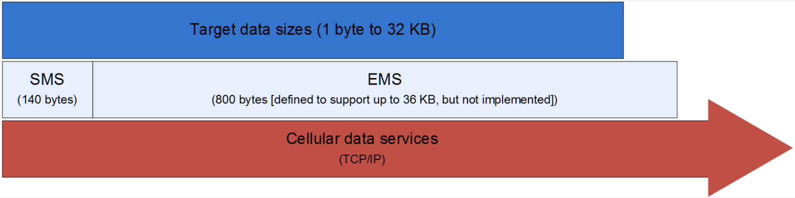
Claim: there are many practical applications for SMS.

Such as:

- Exchanging cryptographic keys.
- DTN routing table updates.
- Synchronous user creation at rural kiosks.
- And many more ...

Goal

To build a general purposed data channel on top of SMS.


Target data sizes (1 byte to 32 KB)
SMS
(140 bytes)
EMS
(800 bytes [defined to support up to 36 KB, but not implemented])
Cellular data services
(TCP/IP)

Objectives

- Fully utilize the capacity of the SMS network.
- Minimize monetary cost by reducing redundant messages.
- Reliable and robust to errors in hardware and the network.
- Must run on (or interact with) a wide range of devices.
  - From current smartphones to previous generation/recycled cell phones.
- Compact and integrate seamlessly with existing mobile systems.

Objectives

- Fully utilize the capacity of the SMS network.
- Minimize monetary cost by reducing redundant messages.
- Reliable and robust to errors in hardware and the network.
- Must run on (or interact with) a wide range of devices.
  - From current smartphones to previous generation/recycled cell phones.
- Compact and integrate seamlessly with existing mobile systems.

Objectives

- Fully utilize the capacity of the SMS network.
- Minimize monetary cost by reducing redundant messages.
- Reliable and robust to errors in hardware and the network.
- Must run on (or interact with) a wide range of devices.
    - From current smartphones to previous generation/recycled cell phones.
- Compact and integrate seamlessly with existing mobile systems.

Objectives

- Fully utilize the capacity of the SMS network.
- Minimize monetary cost by reducing redundant messages.
- Reliable and robust to errors in hardware and the network.
- Must run on (or interact with) a wide range of devices.
  - From current smartphones to previous generation/recycled cell phones.
- Compact and integrate seamlessly with existing mobile systems.

Objectives

- Fully utilize the capacity of the SMS network.
- Minimize monetary cost by reducing redundant messages.
- Reliable and robust to errors in hardware and the network.
- Must run on (or interact with) a wide range of devices.
    - From current smartphones to previous generation/recycled cell phones.
- Compact and integrate seamlessly with existing mobile systems.

How does the SMS network behave?

Previous work

- Traced based analysis of India's cellular network.
- Does not examine mass message senders as an isolated group.

In this work

- Focus on traffic patterns that differ significantly from normal human generated traffic.
  - Transmission rate
  - Delay
  - Loss rate
  - Other properties: transmission failure rate and reordering

How does the SMS network behave?

Previous work

- Traced based analysis of India's cellular network.
- Does not examine mass message senders as an isolated group.

In this work

- Focus on traffic patterns that differ significantly from normal human generated traffic.
  - Transmission rate
  - Delay
  - Loss rate
  - Other properties: transmission failure rate and reordering

How does the SMS network behave?

Previous work

- Traced based analysis of India's cellular network.
- Does not examine mass message senders as an isolated group.

In this work

- Focus on traffic patterns that differ significantly from normal human generated traffic.
    - Transmission rate
    - Delay
    - Loss rate
    - Other properties: transmission failure rate and reordering

How does the SMS network behave?

Previous work

- Traced based analysis of India's cellular network.
- Does not examine mass message senders as an isolated group.

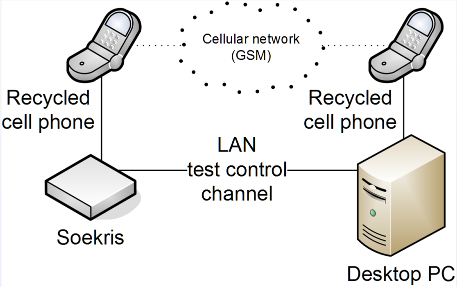
In this work

- Focus on traffic patterns that differ significantly from normal human generated traffic.
  - Transmission rate
  - Delay
  - Loss rate
  - Other properties: transmission failure rate and reordering

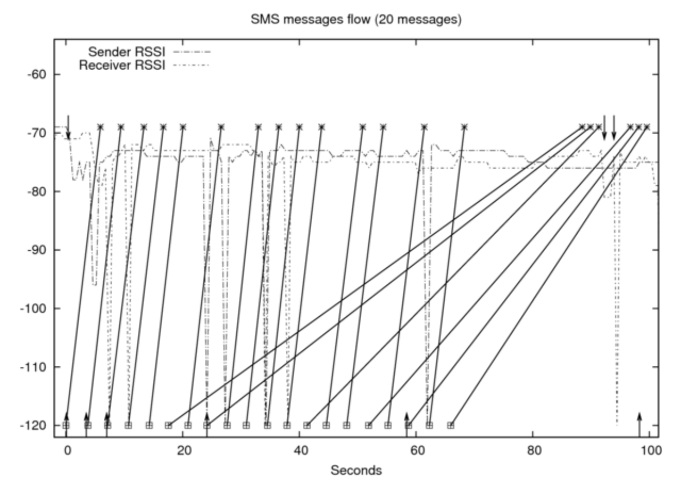
Characterizing SMS

Testbed

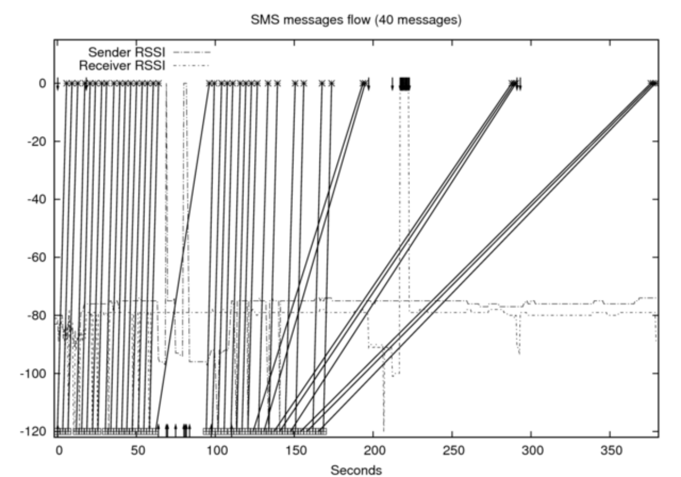
- Two testbed configurations that represent common usage scenarios:
  - Messages exchanged between cell phones tethered to commodity PCs.
  - Messages exchanged between smartphones.



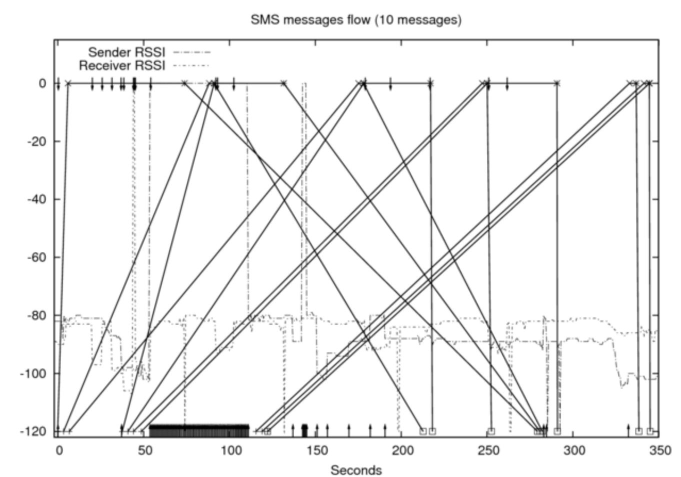
Unidirectional flow (20 messages)



Unidirectional flow (40 messages)



Bidirectional flow (10 messages)



Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Design

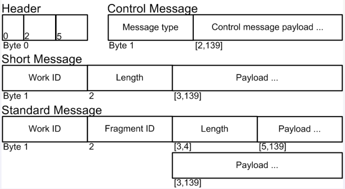
Key points derived from the SMS characterization

- NIC dependency - the choice of hardware impacts the behaviour of SMS.
- Significant message reordering (2.53% to 41.95%)
- Bidirectional traffic significantly increases transmission time, delay, and reordering.
- Messages are rarely lost (4%).
- Messages are duplicated (3.1%).
- Variable delay/inter-message arrival times.
- Burst size has no effect - we can send as fast as possible.
- Messages remain intact.

Protocol

Message format

- Message headers range from 2 - 3 bytes in length.
  - Maximize the fixed 140 byte message payload.
- Base 64 mode to support
  - Reduces effective payload to 120 bytes.
  - Supports communication with a wide range of devices (that only accept printable ASCII characters).
- Details are in the paper.



Header

0 | 2 | 5

Byte 0

Control Message

Message type | Control message payload ...

Byte 1 | [2,139]

Short Message

Work ID | Length | Payload ...

Byte 1 | 2 | [3,139]

Standard Message

Work ID | Fragment ID | Length | Payload ...

Byte 1 | 2 | [3,4] | [5,139]

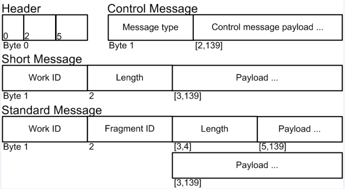
Payload ...

[3,139]

Protocol

Message format

- Message headers range from 2 - 3 bytes in length.
  - Maximize the fixed 140 byte message payload.
- Base 64 mode to support
  - Reduces effective payload to 120 bytes.
  - Supports communication with a wide range of devices (that only accept printable ASCII characters).
- Details are in the paper.



Header

0 2 5

Byte 0

Control Message

Message type | Control message payload ...

Byte 1 [2,139]

Short Message

Work ID | Length | Payload ...

Byte 1 2 [3,139]

Standard Message

Work ID | Fragment ID | Length | Payload ...

Byte 1 2 [3,4] [5,139]

Payload ...

[3,139]

Protocol (continued)

Flow control and error control

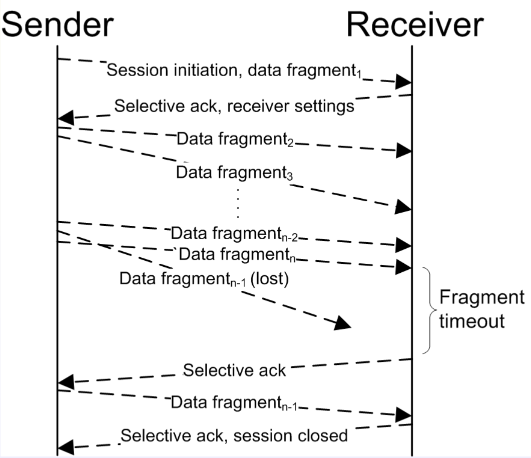
- Experimented with SMART and sliding window techniques.
- NETBLT

Protocol (continued)

Flow control and error control

- Experimented with SMART and sliding window techniques.
- NETBLT

NETBLT example



Advantages of NETBLT

- Sender may transmit a continuous series of messages since burst size has no effect on transmission rate, delay, or loss.
- Bidirectional traffic is minimized through the use of a cumulative ack.
- Cumulative selective ack is tolerant to message reordering, random losses, and variable inter-arrival times.
- Low SMS loss rate requires few acks to be sent.

Advantages of NETBLT

- Sender may transmit a continuous series of messages since burst size has no effect on transmission rate, delay, or loss.
- Bidirectional traffic is minimized through the use of a cumulative ack.
- Cumulative selective ack is tolerant to message reordering, random losses, and variable inter-arrival times.
- Low SMS loss rate requires few acks to be sent.

Advantages of NETBLT

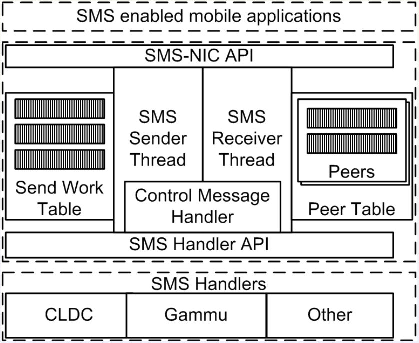
- Sender may transmit a continuous series of messages since burst size has no effect on transmission rate, delay, or loss.
- Bidirectional traffic is minimized through the use of a cumulative ack.
- Cumulative selective ack is tolerant to message reordering, random losses, and variable inter-arrival times.
- Low SMS loss rate requires few acks to be sent.

Advantages of NETBLT

- Sender may transmit a continuous series of messages since burst size has no effect on transmission rate, delay, or loss.
- Bidirectional traffic is minimized through the use of a cumulative ack.
- Cumulative selective ack is tolerant to message reordering, random losses, and variable inter-arrival times.
- Low SMS loss rate requires few acks to be sent.

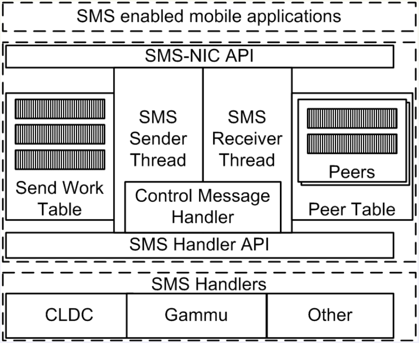
Architecture

- Extensible architecture that allows for integration into existing mobile systems.
- Device *plug-ins* supported provided through *SMS Handler* API.
- Detailed architectural description in the paper.



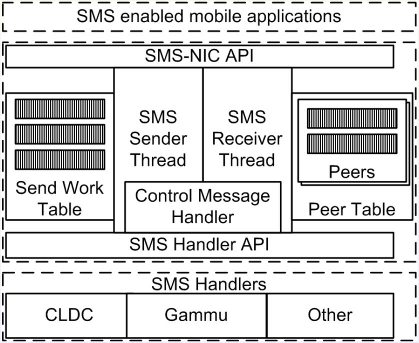
Architecture

- Extensible architecture that allows for integration into existing mobile systems.
- Device *plug-ins* supported provided through *SMS Handler* API.
- Detailed architectural description in the paper.



Architecture

- Extensible architecture that allows for integration into existing mobile systems.
- Device *plug-ins* supported provided through *SMS Handler* API.
- Detailed architectural description in the paper.



Implementation and evaluation

Summary

- The *SMS-NIC* is implemented in Java Micro Edition.
- CLDC compliant.
- Runs on WIDE range of existing mobile cell phones and smartphones.

Sample workloads

	GPS position (1 msg)	2 KB RSA key (16 msgs)	4 KB BLOB (31 msgs)
SMS-NIC	37.32 sec	97.23 sec	212.11 sec

Implementation details and evaluation are in the paper.

Implementation and evaluation

Summary

- The *SMS-NIC* is implemented in Java Micro Edition.
- CLDC compliant.
- Runs on WIDE range of existing mobile cell phones and smartphones.

Sample workloads

	GPS position (1 msg)	2 KB RSA key (16 msgs)	4 KB BLOB (31 msgs)
SMS-NIC	37.32 sec	97.23 sec	212.11 sec

Implementation details and evaluation are in the paper.

Implementation and evaluation

Summary

- The *SMS-NIC* is implemented in Java Micro Edition.
- CLDC compliant.
- Runs on WIDE range of existing mobile cell phones and smartphones.

Sample workloads

	GPS position (1 msg)	**2 KB RSA key (16 msgs)**	**4 KB BLOB (31 msgs)**
SMS-NIC	37.32 sec	97.23 sec	212.11 sec

Implementation details and evaluation are in the paper.

Implementation and evaluation

Summary

- The *SMS-NIC* is implemented in Java Micro Edition.
- CLDC compliant.
- Runs on WIDE range of existing mobile cell phones and smartphones.

Sample workloads

	GPS position (1 msg)	2 KB RSA key (16 msgs)	4 KB BLOB (31 msgs)
SMS-NIC	37.32 sec	97.23 sec	212.11 sec

Implementation details and evaluation are in the paper.

Summary of work

- Characterized the behaviour of SMS under continuous, bursty workloads.
- Designed and implemented a reliable and robust data channel built on top of SMS.
- Through an extensible architecture the SMS-NIC runs on or works with a wide range of mobile devices.

Using the SMS-NIC

Available for download

- SMS-NIC source code is available at: *http://blizzard.cs.uwaterloo.ca/eaoliver/sms/*
- Includes plug-ins for CLDC enabled devices and Gammu.
- Apache open source license.

Current user

- KioskNet *http://blizzard.cs.uwaterloo.ca/kiosknet/*
- Nearby Friend *http://crysp.uwaterloo.ca/software/nearbyfriend/*
- PaperSpeckle *http://cater.cs.nyu.edu/wiki/index.php/PaperSpeckle*

Using the SMS-NIC

Available for download

- SMS-NIC source code is available at: *http://blizzard.cs.uwaterloo.ca/eaoliver/sms/*
- Includes plug-ins for CLDC enabled devices and Gammu.
- Apache open source license.

Current user

- KioskNet *http://blizzard.cs.uwaterloo.ca/kiosknet/*
- Nearby Friend *http://crysp.uwaterloo.ca/software/nearbyfriend/*
- PaperSpeckle *http://cater.cs.nyu.edu/wiki/index.php/PaperSpeckle*

Using the SMS-NIC

Available for download

- SMS-NIC source code is available at: *http://blizzard.cs.uwaterloo.ca/eaoliver/sms/*
- Includes plug-ins for CLDC enabled devices and Gammu.
- Apache open source license.

Current user

- KioskNet *http://blizzard.cs.uwaterloo.ca/kiosknet/*
- Nearby Friend *http://crysp.uwaterloo.ca/software/nearbyfriend/*
- PaperSpeckle *http://cater.cs.nyu.edu/wiki/index.php/PaperSpeckle*

Using the SMS-NIC

Available for download

- SMS-NIC source code is available at: *http://blizzard.cs.uwaterloo.ca/eaoliver/sms/*
- Includes plug-ins for CLDC enabled devices and Gammu.
- Apache open source license.

Current user

- KioskNet *http://blizzard.cs.uwaterloo.ca/kiosknet/*
- Nearby Friend *http://crysp.uwaterloo.ca/software/nearbyfriend/*
- PaperSpeckle *http://cater.cs.nyu.edu/wiki/index.php/PaperSpeckle*

Questions?

Questions?