



中国移动通信  
CHINA MOBILE

中国2010年上海世博会全球合作伙伴  
Global Partner of Expo 2010 Shanghai China

# Security Consideration on IMS P2P

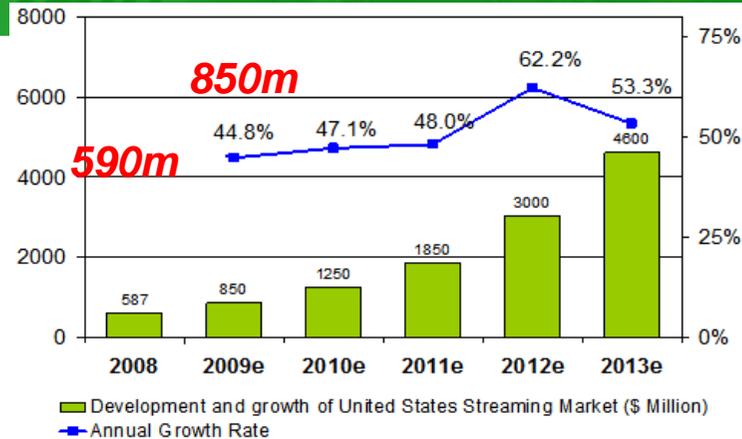
## China Mobile, ZTE



# Outline

- n Background
- n A general use case of IMS P2P
- n Security Analysis
- n Conclusion

# 1 Four Facts



**Internet streaming services have been showing good market potential.**

## 2

### Stronger Mobile UE

- Stronger processor performance (>400MHz)
- Expanded storage (GBytes)
- Larger runtime heap (>100 Mbytes)
- Improved electrical power (particularly netbooks)

**Nokia N97:**  
434 MHz  
32 GB Storage  
128 MB RAM



### High speed mobile broadband access

- LTE or beyond:
  - Peak: downlink > 100Mbps, uplink > 50Mbps

**Technically possible to support content services (even a P2P one) over mobile access**

## 3



### iPhone (2G&3G)

Over 6.4 million users till Apr, 2009

37% watch video on their phone (6x as likely as the typical subscriber), mostly through Youtube (not P2P)

**Mobile Streaming is already in our life and it's amazing!**

## 4

The following data is excerpted from a P2P VoD streaming system test via fixed broadband access on internet.

	C/S Streaming	P2P Streaming
Concurrent view	10,000	10,000
Stream data rate per view	500K ~ 1Mbps	500K ~ 1Mbps
Required Servers	50	5
Required bandwidth	Dedicated 5,000Mbps	Dedicated 500Mbps

**P2P makes over 90% server's throughput saving from service provider's perspective**

# What can P2P CDS bring to us?

## ***For Users***

- | Higher service availability due to lowered pressure on content server's throughput
- | Bundled new services with lowered cost (e.g. charged content plus free VoIP)
- | Chance to earn through contribution (computing capability, storage and bandwidth)

## ***For Operators***

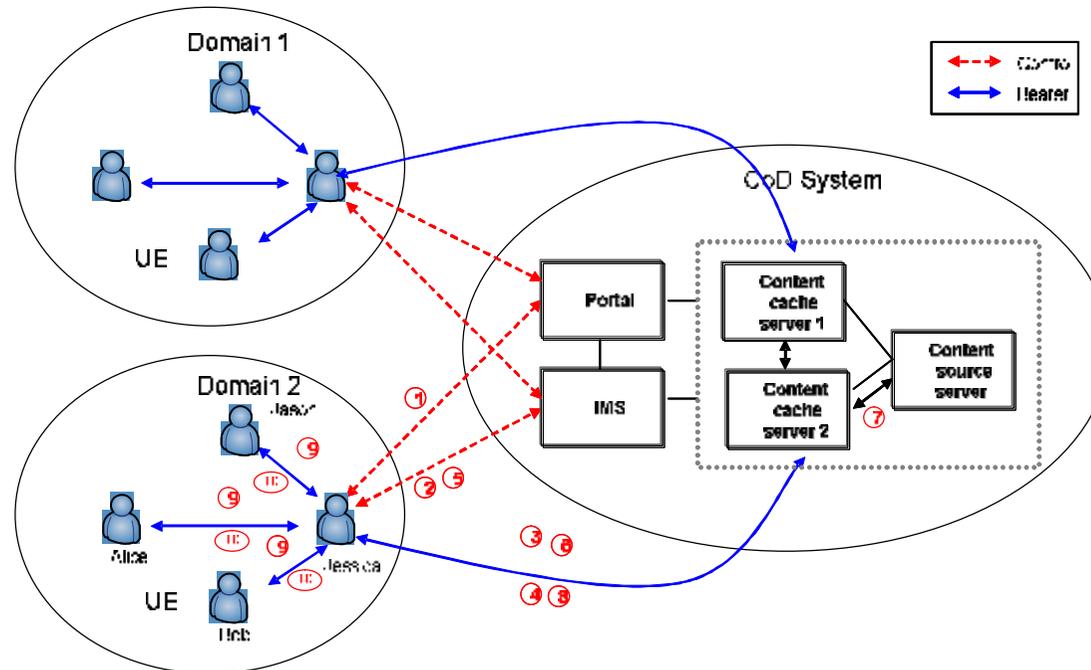
- | Good scalability of CDS, pressure on content's server's throughput lowered
- | Avoidance to provide "dumb pipe" by earning from content service and its ramification (advertising)
- | If based on IMS, it may become the "killer application" of IMS

## ***FOR Vendors***

- | New core network or service equipments or modules may be needed
- | Requirement from users to further upgrade UE step by step
- | Escalation of access network and bearer network if P2P CDS brings profit successfully to operators
- | Lowered cost for transformation from telecommunications vendor to Internet vendor

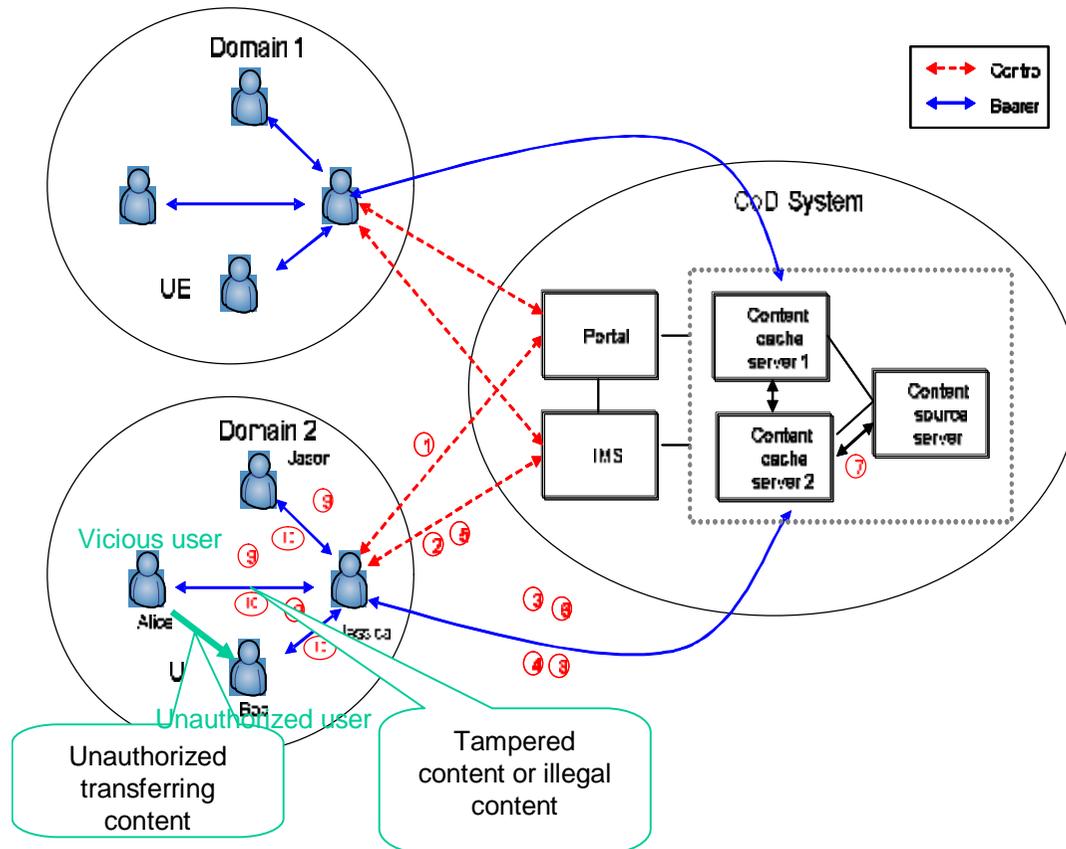
# A general use case of IMS P2P

## An example to make content of distribution



1. Jessica get the program information to from IMS P2P application (Portal) after registration. Jessica then selects a content to tell the P2P application
2. Portal searches and finds Content cache server(CS)2 is the best choice among those who have some segments and then reply to Jessica its address and content information.
- 3-5. Jessica establishes a connection with CS2 to get segment information, then download segments from CS2. CS2 will get other segments from Content source server(SS). Jessica's UE will updates the segments information to P2P application service and retrieves the latest information periodically.
- 6-8. More users in Domain2 want to download the same content but other segments from CS2. CS2 can get these segments from CS1 instead of SS if SS is too busy to work.
- 9-10 Jessica can get other segments from other UEs if the CS1 and CS2 are out of work.

# Security Analysis based on SA1 22.906



1. **Black hole attacking:** Alice may dishonestly report the information of their contributed resources (e.g. cached or stored content). It will result that many other users can't get the correct content from Alice, even that Alice can initiate further attacks to other user peers.
2. **Content tampering:** If Alice is a vicious user, Jessica can get tampered content or illegal content when she chooses to get a segment from Alice as CS1 and CS2 are out of work.
3. **Free riding:** If Alice is an authorized user and she has got the complete content of a film, she can transfer it to her good friend Bob who is an unauthorized user. This behavior may infringe the copyright of content author or issuer.
4. **Active attacking:** If Alice is a vicious user, she may distribute some illegal content to other users through p2p technology.

# Some more security analysis

## n Privacy:

- n When Alice can provide segments, it will be recorded by P2P application and be broadcasted to everyone who needs these segments. So its name will be known by everyone. It means that users' privacy are harmed by P2P technology

## n Eavesdropping

- n When Jessica is connected with Alice to download segments it needs, the security between Jessica and Alice may not as strong as the connect with network. So Bob is more likely to eavesdrop what segments transferred between Jessica and Alice.

