Networking Named Content

Xinghong Fang (xf214)
The Problems

● Networking abstraction
  ○ Host-to-host

● Availability
  ○ Pre-planned mechanism
  ○ Extra bandwidth cost

● Security
  ○ Untrustworthy location

● Location-dependence
  ○ Complicated mapping configuration
Related Works

- **DONA**
  - Name and content are not bond securely
  - Content must be published or registered
  - Resolution handler: large forwarding table
- **DHT-based System**
  - Require explicit content publishing
  - No guarantee to retrieve the closest copy
- **PSIRP**
  - Unsecure directory service
- **TRIAD**
  - Relies on trusted directory to authenticate
Key Idea of CCN

● New networking abstraction
  ○ "named host" -> "named data"
  ○ No notion of host
  ○ Address names content

● Plus TCP/IP design decision
  ○ makes it simple, robust and scalable
  ○ e.g. FIB, longest-prefix match
Main Contributions of CCN

- Decoupling location from
  - identity, security and access
- Scalability, security and performance
- Layer over anything
- Strategy
  - Take advantage of multiple connectivities
  - Operate under changing conditions
- Security
  - Secure content itself
CCN Node Model

- Two packet types
  - Interest and Data
- Basic pattern
  - Consumer broadcasting interest
  - Node with data respond on hearing interest
- ContentName
  - Hierarchical: prefix match
  - Allow dynamic generation
  - Can be context-dependent
CCN Node Model - Data Structures

- **Forward Information Base (FIB)**
  - Forward interest to potential data holders
  - Allow multiple interface, parallel query

- **ContentStore**
  - Remember data packet
  - Reducing upstream bandwidth demand
  - Minimising downstream delay

- **Pending Interest Table (PIT)**
  - Keep track of interest source
  - Timeout & re-express interest
Strength of the model

● Consumer driven
  ○ Screen unsolicited data

● ContentStore
  ○ Transparent caching
  ○ Sharing by multicasting

● Multipoint data retrieval
  ○ Maintain communication in highly dynamic environment
  ○ DTN: works in isolated location
Weakness of the model

- **Stateful vs Stateless**
  - Install states in every nodes
  - Complicated forwarding node implementation
- **ContentStore**
  - Require extra cache memory
  - Needs explicit version control
Transport

● On top of unreliable packet delivery service
  ○ Retransmission (strategy layer)
  ○ Discard duplicated packets
    ■ Packet network
    ■ Multipoint distribution

● Flow control
  ○ No need for congestion control over a path

● Rich connectivity
  ○ No bind between IP address to MAC address
  ○ Strategy layer
Routing

- Reuse routing schemes for IP
- Prefix announcement
  - IP: need spanning tree, traffics go through a single node
  - CCN: interests forwarded to all the nodes to announce the prefix
Security

- Content-based security
- Digital signature, encryption
  - publicly authenticatable
  - a set of algorithms: fit performance requirement
  - individually verifiable
- Content validated by receiver
  - IP: must retrieve from original source to trust it
- Authenticate binds
  - Names, contents and supporting data
- User/application-meaningful names
  - Instead of self-certifying name
  - No need for indirection infrastructure
Security (cont.)

- Trust depends on the purpose of use
  - more flexible and easier
- Allowing content to securely link to others
  - allow content to certify other content
- Tackling traditional key management problems
  - keys accessible via simple naming conventions
  - Trust relationship ("key + name" signed by key)
- Evidence-based security
  - delegation, secure reference
- No trusted server required
  - only authorised user can decrypt
Security - Attack Protection

- Hard to attack a specific target
  - no notion of host
- Hard to perform DDoS
  - Flow balance between Interests and Data
  - Consumer driven (rate controlled by consumer)
  - Multiple request to same data will be combined
    - Upstream bandwidth not affected
Strength of Security

- Flexibility in algorithm and packet authentication
- No need for secured connection
- Secure reference to other content
- Chain of trust
- Attack protection
Weakness of Security

- Encryption/Decryption overhead
- Consumer's discretion of trust
- Risk of root key leaks
- Unsecure referenced content
Issues in Evaluation

- **Bulk data transfer**
  - 6MB, is the size too small?
  - 5x pipelining than TCP (store-and-forward)

- **Content distribution**
  - strength: little increase of total download time when clients increases

- **VoIP**
  - Capability to use multiple connectivity
Conclusion

- Named data
- Inherited from TCP/IP design decision
- Consumer driven
- Attack protection
- Encryption overhead
- Issues of content reference
Questions?