End-to-End Secure Delivery of Scalable Video Streams

Mohamed Hefeeda

(Joint work with Kianoosh Mokhtarian)

5 June 2009
NOSSDAV 2009
Motivations

- Increasing demand for multimedia services
- Content often transported over open and insecure networks (Internet)
- Many applications require secure delivery of content
  - Videos for: surveillance, documentary, political debates, …
- Secure delivery = Ensuring authenticity of content
- Detect any malicious tampering
  - Removing, inserting, or modifying and portions of content
- Allow legitimate adaptation
  - Different frame rates, resolutions, quality levels
Our Work

- **New authentication scheme for scalable video streams**
  - End-to-end: transparent to proxies/CDN servers ➔ No need to trust third-parties or distribute keys
  - Ensures authenticity of any substream

- **Focus on most flexible, recent, scalable streams**
  - 3-d scalability (at the same time)
  - e.g., H.264/SVC

- **svcAuth**: Open-source authentication library (Java)
  - for H.264/SVC
Outline

- Brief background
  - Scalable streams (old and recent)
  - Previous authentication works

- Overview of the proposed authentication scheme

- Performance evaluation

- Conclusion
Background: Scalable Streams

- **Scalable coding:** encode once, decode in many ways
  - Spatial, temporal, and quality scalability
  - Heterogeneous receivers
  - Varying network conditions
  - Coding efficiency penalty

- **Traditional scalable (layered) video streams**
  - 1 Base layer, 0+ enhancement layers
  - 1-d scalability
  - Cumulative layers
Recent Scalable Streams (H.264/SVC)

- Higher flexibility, yet with higher coding efficiency

- 3-d scalability
  - three types at same time

- Very flexible adaptation and truncation

- more challenging to authenticate
Recent Scalable Streams (H.264/SVC)

- Non-cumulative
- Video packet-level truncation inside quality layers
Previous Work

- Only for traditional 1-d scalable streams

- Two main approaches:
  - Based on hash chaining [Skraparlis 03, Yu 04]
  - Based on Merkle hash trees [Kaced 06, Gentry 06, Wu 06]

- Can not support flexibility of recent 3-d scalable streams
Previous Work: Hash Chaining

- Assumes cumulative and complete layers
Previous Work: Merkle Hash Trees

- Requires trust/cooperation of proxies/CDN serves → not end-to-end
- Assumes complete layers
H.264/SVC: Spatial and Quality Scalability

- **Spatial scalability**
  - Dependency between layers is a DAG; not simple chain

- **Quality scalability**
  - Coarse-Grained Scalability (CGS)
    - Layer-level granularity
  - Medium-Grained Scalability (MGS)
    - Packet-level granularity
H.264/SVC: Temporal Scalability

- Hierarchical B-pictures in Group-of-Pictures (GoP)
H.264/SVC: Stream Structure

- **Stream**: sequence of GoPs
- **GoP**: set of video frames
- **Video frame**: multiple spatial layers
- **Spatial layer**: multiple CGS quality layers
- **CGS quality layer**: multiple MGS quality layers
- **MGS quality layer**: multiple video packets
Proposed Scheme: Overview

- **Content provider**
  - Generate auth info bottom up (packets, MGS, CGS, …, GoP)
  - Auth info is embedded into video stream
  - Transparent to third-party proxies

- **Receivers**
  - Verify **substreams** if their corresponding auth info received
  - Digests are re-computed and compared
Proposed Scheme: Overview

- Authenticating MGS quality layers

Mohamed Hefeeda
Proposed Scheme: Overview

- Authenticating MGS layers of a CGS/spatial layer
Proposed Scheme: Overview

- Authenticating video frame
Proposed Scheme: Overview

- Authenticating temporal layers

Temporal layer 4

Temporal layer 3

Temporal layer 2

Temporal layer 1

Temporal layer 0

GoP

GoP digest

FEC
Proposed Scheme: Overview

- **Authenticating a sequence of GoPs**
  - GoP blocks (individually signed)
  - Auth info of any GoP suffices for the block
Analysis and Evaluation

- **Security analysis**
  - Theorem: Proposed scheme ensures authenticity of any valid substream

- **Simulation Setup**
  - Simulate streaming 1-Mbps video over lossy network channel
  - Video: 4 temporal, 1 spatial, 2 CGS (each has 3 MGS) layers
    CIF, 30 fps, 40 dB (Y-PSNR)

- **Performance metrics**
  - Computation cost
  - Delay and buffering requirements
  - Robustness against packet losses
  - Communication overhead
Evaluation: Computation Cost

- \( n \) adjusts computation cost \( \sim \) delay
Performance Evaluation: Delay/Buffer

- **Server-side delay**
  - Generating a block of n GoPs

- **Receiver-side delay**
  - Typically zero; few GoPs if high loss rate

- **Total delay**
  - n GoPs for live streaming
  - Negligible for on-demand

- **Buffer required**
  - Few GoPs if high loss rate
Performance Evaluation: Delay/Buffer

- Delay for live-streaming
Performance Evaluation: Delay/Buffer

- **Delay ~ computation cost**
- **Buffer required: n GoPs worst case (< 1 MB)**
Evaluation: Communication Overhead

- Communication overhead impact: ~ 1 dB at most (< 8%)
Performance Evaluation: Loss Resilience

- Quality reduced by communication overhead: ~ 1 dB
- Quality reduced by increase in loss impact: Marginal
Conclusion and Future Work

- New scalable video streams offer high flexibility
  - 3-d scalability (temporal, spatial, quality)

- Current authentications schemes do not support such flexibility

- Proposed new authentication scheme
  - Supports full flexibility (H.264/SVC)
  - End-to-end authentication
  - Low overheads (delay, buffering, computation, …)

- Future work
  - Further reduce communication overhead
  - Release svcAuth library
Thank You!

Questions??

- More info at:

  http://nsl.cs.sfu.ca/