Modelling Social Networks as Authorised Domains with Decay

Nicholas Paul Sheppard\textsuperscript{1} Reihaneh Safavi-Naini\textsuperscript{2}

\textsuperscript{1}School of Computer Science and Software Engineering
The University of Wollongong, Australia

\textsuperscript{2}Department of Computer Science
The University of Calgary, Canada

Introduction

Typical multimedia users have friends with whom they would like to share commercial multimedia.
Introduction

Typical multimedia users have friends with whom they would like to share commercial multimedia.

Small degrees of sharing aren’t necessarily detrimental to multimedia creators:
  - “network effect”
  - “sampling effect”
Introduction

Typical multimedia users have friends with whom they would like to share commercial multimedia.

Small degrees of sharing aren’t necessarily detrimental to multimedia creators:

• “network effect”
• “sampling effect”

Digital rights management systems impose strong restrictions on sharing to prevent wide-scale sharing. We propose to model small-scale sharing using *acquaintance domains*.
Authorised Domains

Authorised domains implement sharing in digital rights management

- e.g. OMA DRM, Marlin, others

A domain is a collection of devices.
Authorised Domains

*Authorised domains* implement sharing in digital rights management

- e.g. OMA DRM, Marlin, others

A domain is a collection of devices.

The right to access multimedia can be awarded to a domain. Every device in the domain inherits the rights of its domain.
Authorised Domains

Household Domains
Domains are typically targeted at households.
Authorised Domains

Household Domains
Domains are typically targeted at households.

- devices join the domain when they are purchased

Acquaintance Domains
We want domains in which devices are members if their owners are acquainted.
Authorised Domains

Household Domains
Domains are typically targeted at households.

- devices join the domain when they are purchased
- devices share access to the multimedia owned by the household
Authorised Domains

Household Domains
Domains are typically targeted at households.

- devices join the domain when they are purchased
- devices share access to the multimedia owned by the household
- devices leave a domain when they are discarded or sold
Authorised Domains

Household Domains
Domains are typically targeted at households.

- devices join the domain when they are purchased
- devices share access to the multimedia owned by the household
- devices leave a domain when they are discarded or sold

Acquaintance Domains
We want domains in which devices are members if their owners are acquainted.
Fuzzy Authorised Domains

Alice may be acquainted with Bob to varying degrees.
Fuzzy Authorised Domains

Alice may be acquainted with Bob to varying degrees.

We model “acquaintance” as membership of a fuzzy set.

- a member of a fuzzy set has a degree of membership between zero and one
- the degree of membership is computed using a membership function
Fuzzy Authorised Domains

We define a fuzzy authorised domain with membership analogous to membership of a fuzzy set.
Fuzzy Authorised Domains

We define a *fuzzy authorised domain* with membership analogous to membership of a fuzzy set.

The right of a domain to access multimedia is determined as normal.

- Device with membership 1: access the multimedia as normal
- Device with membership 0: reject access as normal
- Device with partial membership: access with sanctions
Fuzzy Authorised Domains

We define a fuzzy authorised domain with membership analogous to membership of a fuzzy set.

The right of a domain to access multimedia is determined as normal.

- Device with membership 1: access the multimedia as normal
Fuzzy Authorised Domains

We define a fuzzy *authorised domain* with membership analogous to membership of a fuzzy set.

The right of a domain to access multimedia is determined as normal.
- Device with membership 1: access the multimedia as normal
- Device with membership 0: reject access as normal
Fuzzy Authorised Domains

We define a fuzzy *authorised domain* with membership analogous to membership of a fuzzy set.

The right of a domain to access multimedia is determined as normal.

- Device with membership 1: access the multimedia as normal
- Device with membership 0: reject access as normal
- Device with partial membership: access with sanctions
Sanctions

- Warning
- Degradation
- Denial of premium content
- “Fade” (Macrovision)
- Watermarking
- Domain shrinkage
- Randomness

Acquaintance Domains

Assume every human user is associated with a fuzzy acquaintance domain.
Acquaintance Domains

Assume every human user is associated with a fuzzy acquaintance domain.

Permanent Members
Devices owned by the user are permanent members of the acquaintance domain.
Acquaintance Domains

Assume every human user is associated with a fuzzy *acquaintance domain*.

**Permanent Members**
Devices owned by the user are *permanent members* of the acquaintance domain.

**Temporary Members**
Others devices may become *temporary members* subject to a membership function.
Acquaintance Domains

Assume every human user is associated with a fuzzy acquaintance domain.

Permanent Members
Devices owned by the user are permanent members of the acquaintance domain.

Temporary Members
Others devices may become temporary members subject to a membership function.

Membership Functions
Membership functions may depend on physical proximity, frequency of contact, etc.
Examples

One-hop Domains

A user may nominate a fixed number of acquainted devices to belong to his or her acquaintance domain. Nomination expires after a month.
Examples

One-hop Domains
A user may nominate a fixed number of acquainted devices to belong to his or her acquaintance domain. Nomination expires after a month.

Proximity Domains
A device may become acquainted by coming within Bluetooth range of a permanent member. Membership decreases with time unless contact is renewed.
Implementation

Our implementation is based on the OMA DRM specification.

- OMA DRM is a simple digital rights management system for mobile devices
- chosen because we had an OMA DRM implementation available
- other domain-sharing systems can be treated similarly
OMA DRM Domains

OMA DRM v2 defines a simple domain-sharing system.
OMA DRM Domains

OMA DRM v2 defines a simple domain-sharing system.

- Domains are created by a *rights issuer*
OMA DRM v2 defines a simple domain-sharing system.

- Domains are created by a rights issuer
- *DRM agents* may join and leave domains by contacting the rights issuer
OMA DRM Domains

OMA DRM v2 defines a simple domain-sharing system.

- Domains are created by a rights issuer
- DRM agents may join and leave domains by contacting the rights issuer
- Rights objects may be issued to domains by rights issuers
OMA DRM Domains

OMA DRM v2 defines a simple domain-sharing system.

- Domains are created by a rights issuer
- DRM agents may join and leave domains by contacting the rights issuer
- Rights objects may be issued to domains by rights issuers
- Rights objects confer the right to access multimedia objects
OMA DRM Domains

OMA DRM v2 defines a simple domain-sharing system.

- Domains are created by a *rights issuer*
- *DRM agents* may join and leave domains by contacting the rights issuer
- *Rights objects* may be issued to domains by rights issuers
- Rights objects confer the right to access multimedia objects
- All DRM agents in the domain may use such rights objects
Fuzzifying OMA DRM Domains

We don’t need to modify the cryptographic architecture of the OMA DRM system.
Fuzzifying OMA DRM Domains

We don’t need to modify the cryptographic architecture of the OMA DRM system.

Join/Leave Domain

The OMA DRM domain protocols need to be extended to communicate a membership function to DRM agents as they join the domain.
Fuzzifying OMA DRM Domains

We don’t need to modify the cryptographic architecture of the OMA DRM system.

Join/Leave Domain

The OMA DRM domain protocols need to be extended to communicate a membership function to DRM agents as they join the domain.

DRM Agents

The OMA DRM agent needs to be extended to reduce the quality of an action if it is a partial member of a domain.
Fuzzifying OMA DRM Domains

- Multimedia
- Decryptor
- Rights Object
- Rights Object Interpreter
- Renderer
- CEK
- DK
- Domain Database
Fuzzifying OMA DRM Domains

Diagram:

- Multimedia
  - Decryptor
  - Filter
  - Renderer

- Rights Object
  - Rights Object Interpreter
  - Membership Function

- Domain Database
  - DK
  - CEK
  - age
  - half-life
  - degree
Acquaintance Domains in OMA DRM

Membership Function
Every domain has a half-life. For every half-life that has elapsed since a DRM agent last joined the domain, the agent’s degree of membership is halved.
Acquaintance Domains in OMA DRM

Membership Function
Every domain has a half-life. For every half-life that has elapsed since a DRM agent last joined the domain, the agent’s degree of membership is halved.

Join/Leave Domain
Our implementation does not impose a policy. Re-joining a domain resets the membership function.
Acquaintance Domains in OMA DRM

Membership Function
Every domain has a half-life. For every half-life that has elapsed since a DRM agent last joined the domain, the agent’s degree of membership is halved.

Join/Leave Domain
Our implementation does not impose a policy. Re-joining a domain resets the membership function.

Sanctions
We used down-sampling. An image is displayed at $1024 \times 768$ upon joining, at $512 \times 384$ after one half-life, and so on.
No Half-Lives Elapsed
One Half-Life Elapsed
Two Half-Lives Elapsed
Conclusion

- Fuzzy authorised domains can model the decay of acquaintance over time
  - frequent contact: strong acquaintances
  - rare contact: weak acquaintances
  - one-off contact: ephemeral acquaintances

Existing authorised domain schemes can be "fuzzified" without modifying the security architecture of the scheme.
Conclusion

- Fuzzy authorised domains can model the decay of acquaintance over time
  - frequent contact: strong acquaintances
  - rare contact: weak acquaintances
  - one-off contact: ephemeral acquaintances

- Existing authorised domain schemes can be “fuzzified” without modifying the security architecture of the scheme
Open Questions

• What kinds of membership functions might be useful?
Open Questions

• What kinds of membership functions might be useful?
• What kinds of sanctions might be useful?
Open Questions

- What kinds of membership functions might be useful?
- What kinds of sanctions might be useful?
- What other scenarios can be modelled as fuzzy domains?