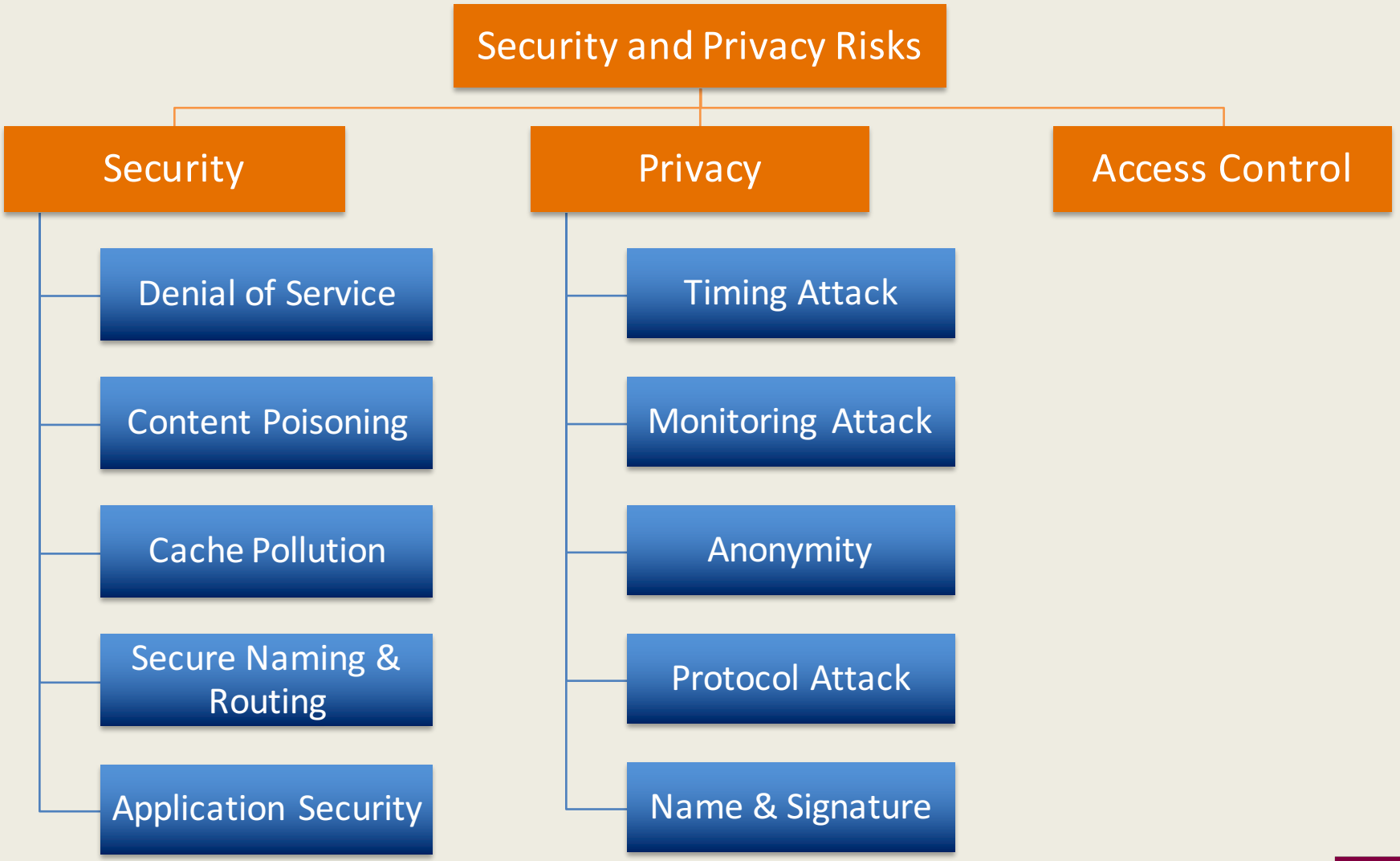
Security, Privacy, and Access Control in Information-Centric Networking: A Survey

Satyajayant (Jay) Misra

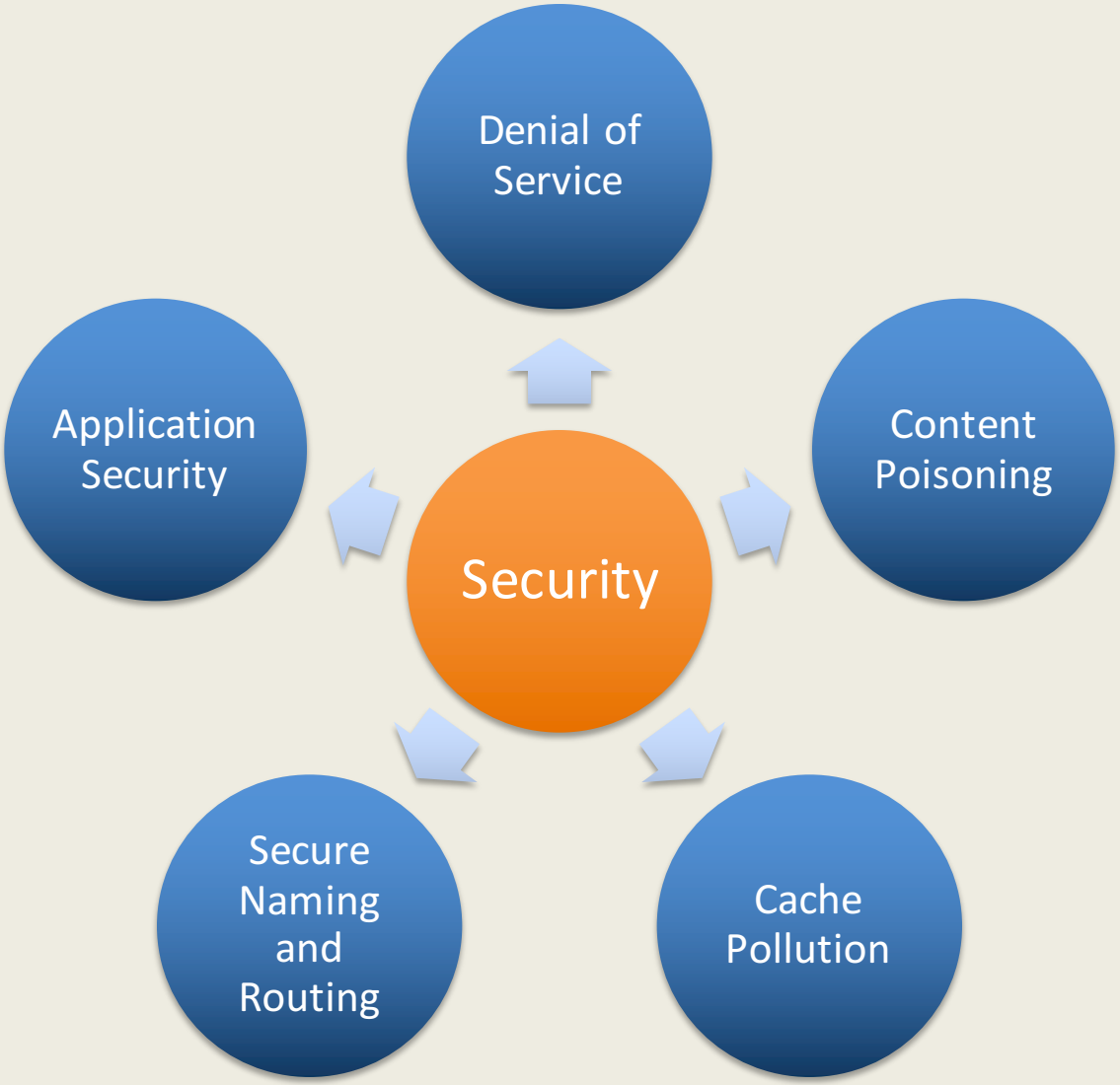
Computer Science Department

New Mexico State University

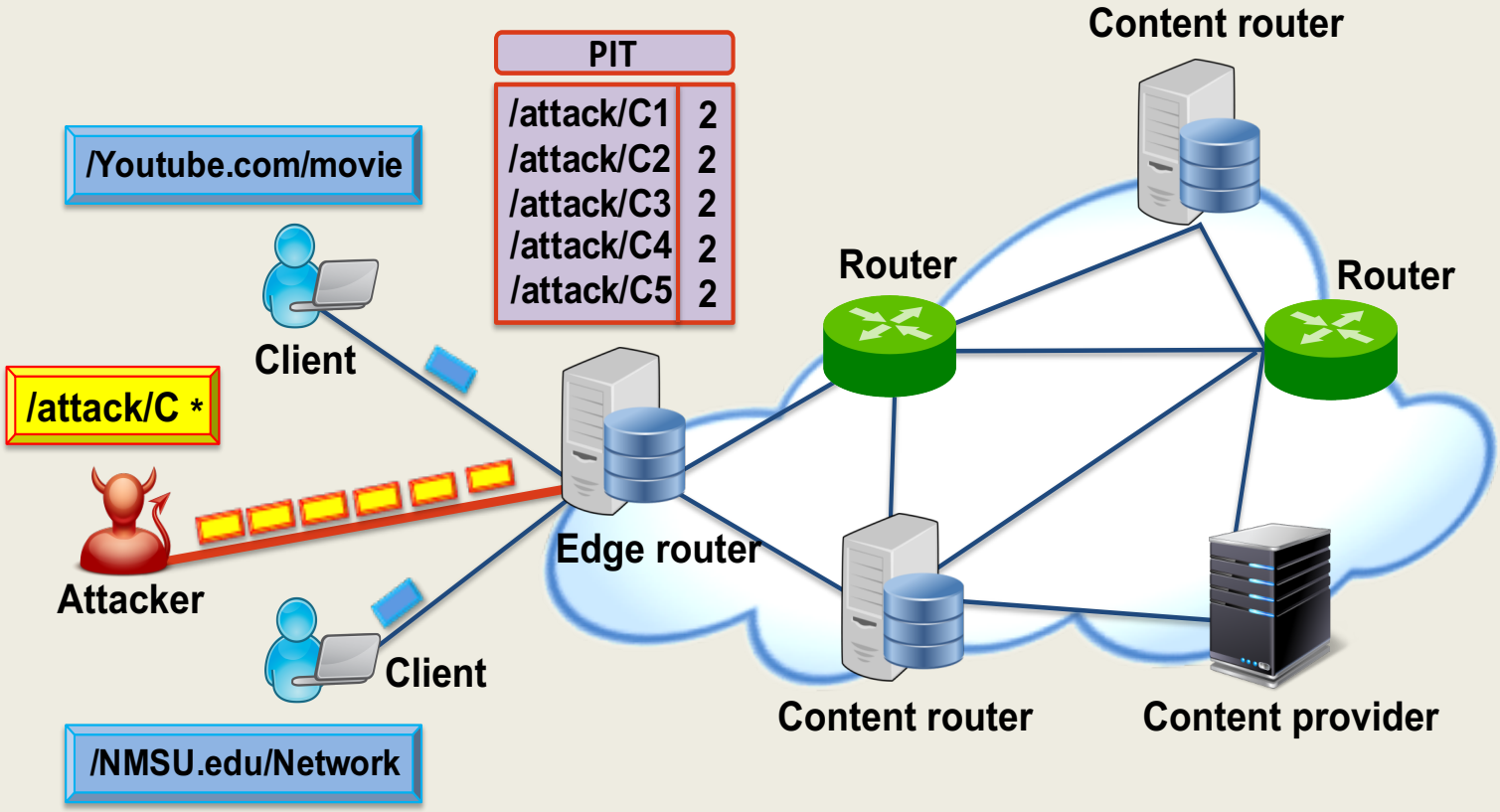
ICN's Security Challenge Categorization



Security in ICN



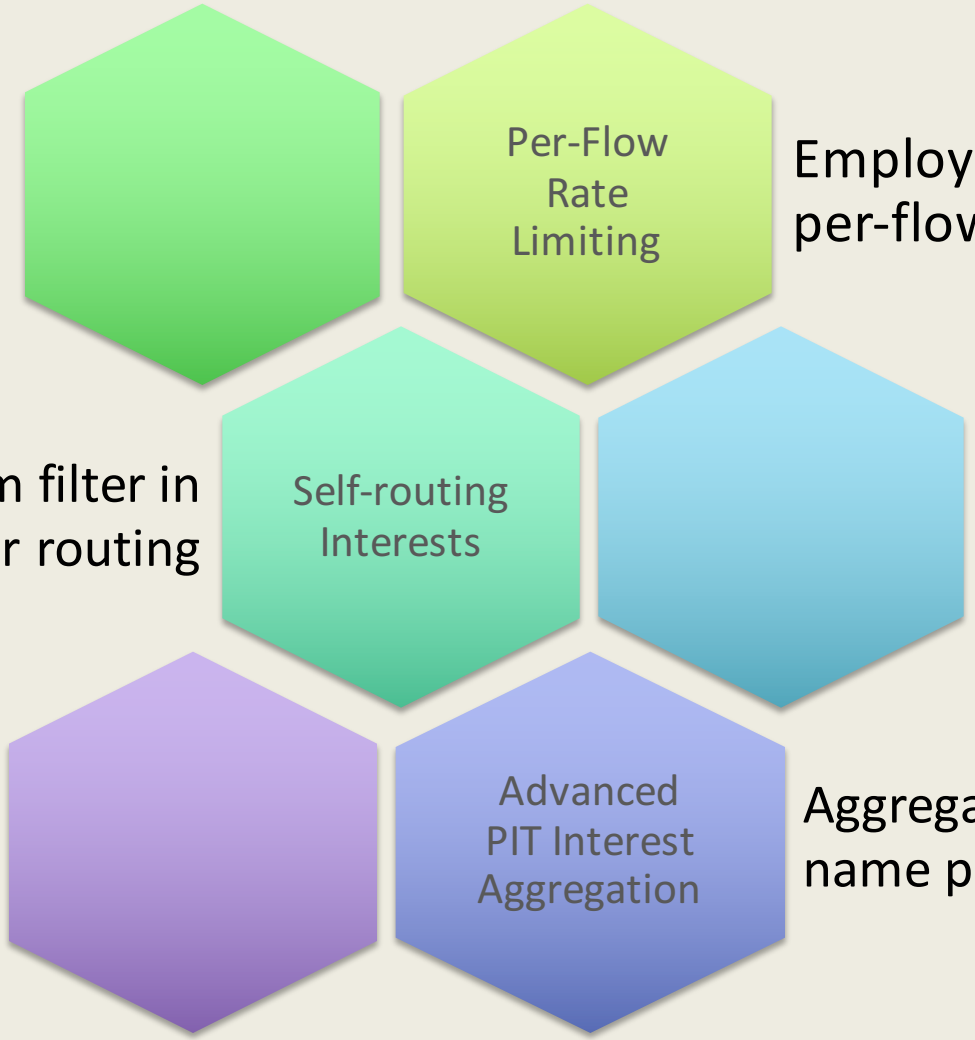
DoS: An attacker Floods the Network with Interests.



DoS: An attacker Floods the Network with Interests.

Authors	Target	Content Type	Approach	Router's Functionality	Collaboration Scope
Afanasayev et al.	Router	Non-Existent	Rate limiting & Per-face fairness; Per-face statistic & Priority	PIT extension & Storing statistics	Individual & Collaborative
Compagno et al.	Router	Non-Existent	Rate limiting & Per-face Statistics	Storing statistics	Collaborative
Dai et al.	Router	Non-Existent	Rate limiting & PIT size monitoring	Not Applicable	Collaborative
Gasti et al.	Router/Provider	All	Rate limiting & Per-face statistics	Storing statistics	Individual
Wang et al.	Provider	Existing	Caching period increase	Not Applicable	Individual
Li et al.	Provider	Dynamic	Client's Proof-of-Work per interest	Not Applicable	Not Applicable
Nguyen et al.	Router	Non-Existent	Statistical hypotheses testing theory	Storing statistics	Individual
Wang et al.	Router	Non-Existent	Decoupling malicious interest from PIT	Additional queue	Individual
Wang et al.	Router	Non-Existent	Fuzzy logic-based detection	Storing statistics	Collaborative

What can be done to mitigate DoS attack?

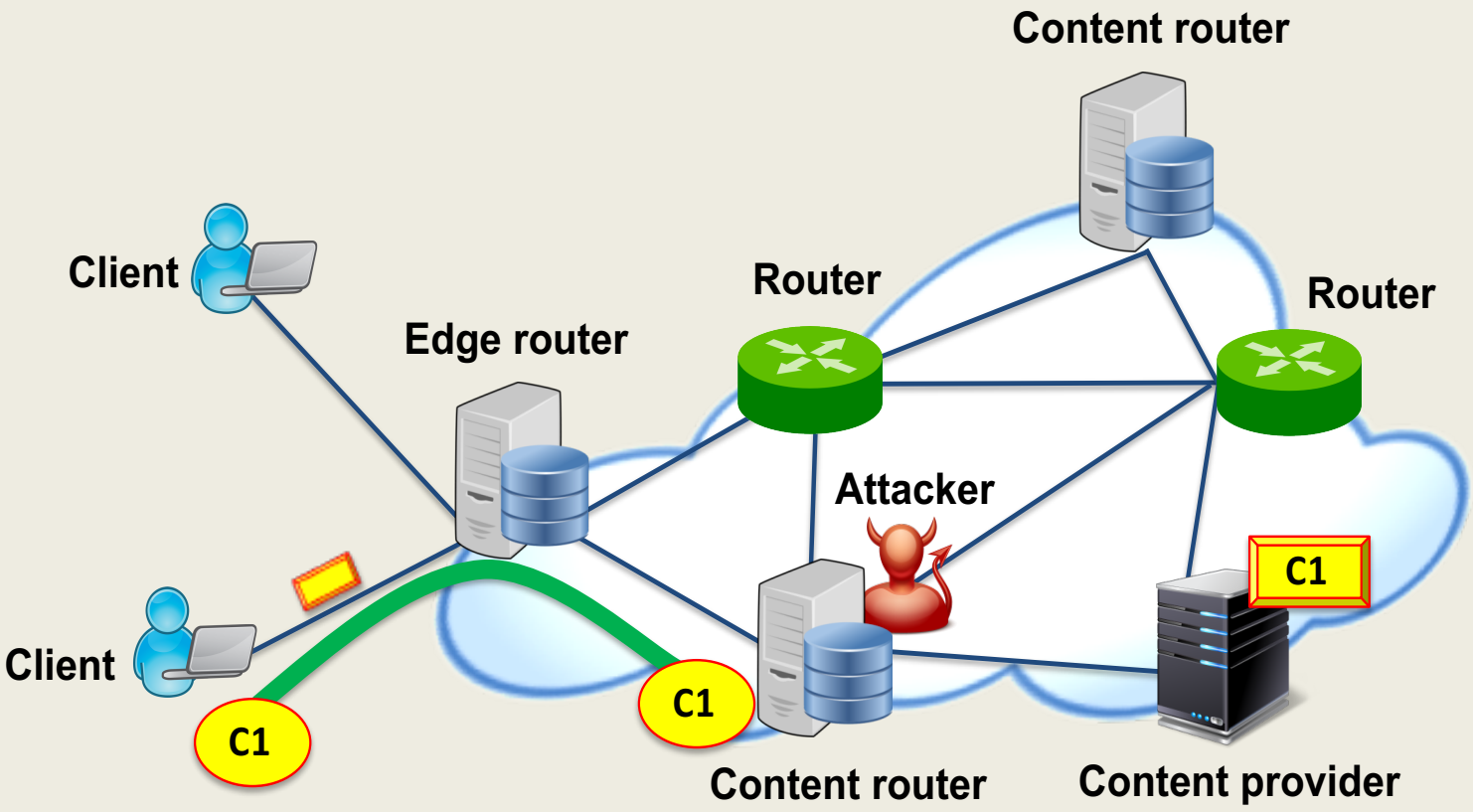


Employing SDN to per-flow operation

Using Bloom filter in interests for routing

Aggregate suspicious name prefixes in PIT

Content Poisoning: An attacker (a malicious router or provider) injects fake data into the network.



Content Poisoning: An attacker (a malicious router or provider) injects fake data to the network.

Authors	Mitigation Approach	Overhead
Gasti et al.	Self-certifying interest & Collaborative signature verification	Hash value comparison & Random signature verification
Ghali et al.	Client feedback & Content ranking	Content ranking calculation
Ghali et al.	Interest-Key binding & Adding provider's public key to content	PPKD comparison & Signature verification
Kim et al.	Collaborative signature verification of serving content	Signature verification on cache-hit

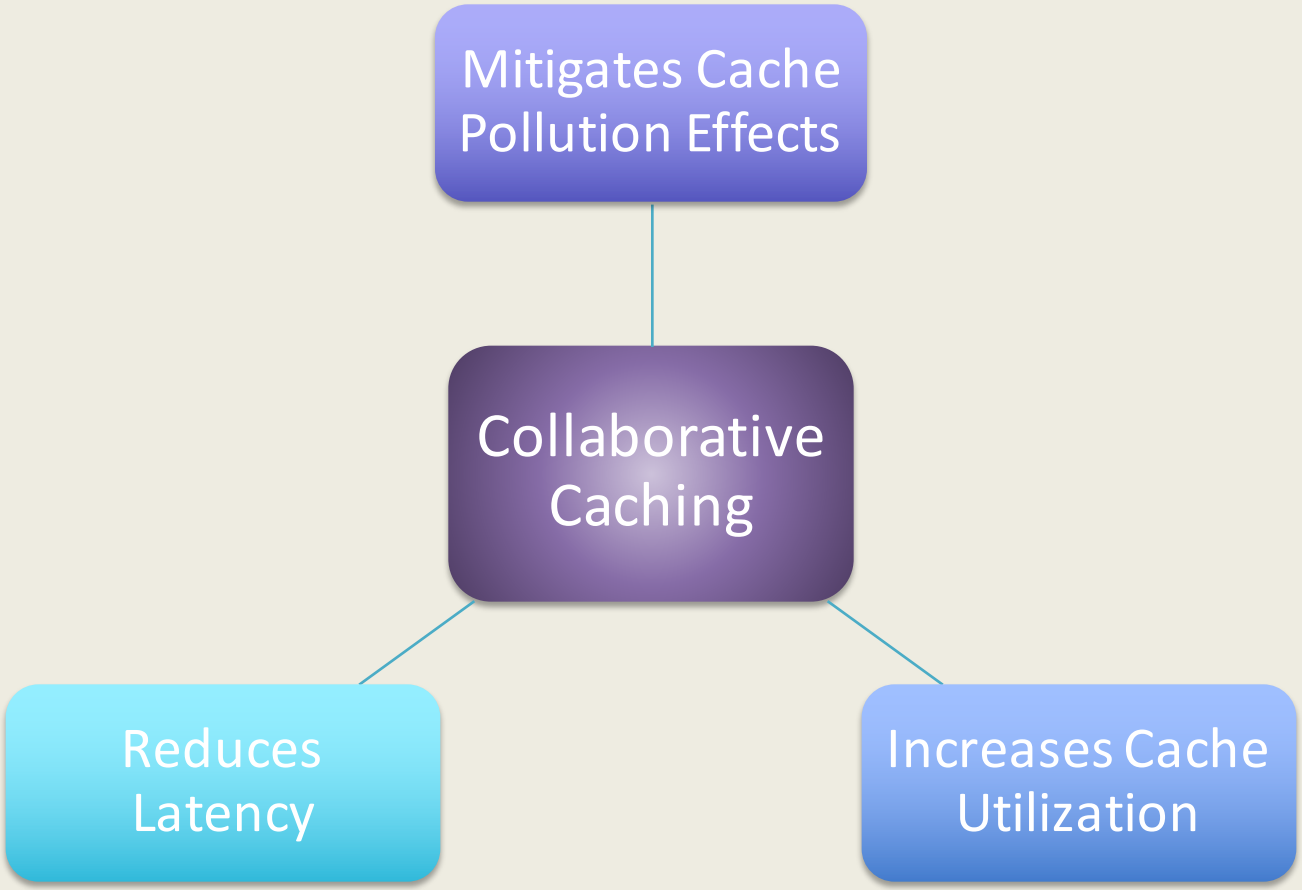
Future directions to mitigate content poisoning attacks.

- Attack origin identification and cache prevention
- Content digest comparison between interest-content

Cache Pollution: Malicious clients disrupt cached content popularity by requesting unpopular content.

Authors	Detection & Mitigation	Attack Type	Storage Overhead	Computation Overhead
Conti et al.	Random content sampling for attack threshold detection	Locality Disruption	Low	Moderate
Karami et al.	Adaptive neuro-fuzzy inference system replacement policy	Locality Disruption False Locality	Moderate	High
Mauri et al.	Honeypot installation & Hidden monitoring	False Locality (by Provider)	Moderate	Low
Park et al.	Cached content matrix ranking	Low-rate Locality Disruption	Low	High
Xie et al.	Probabilistic caching of popular content	Locality Disruption	Moderate	High

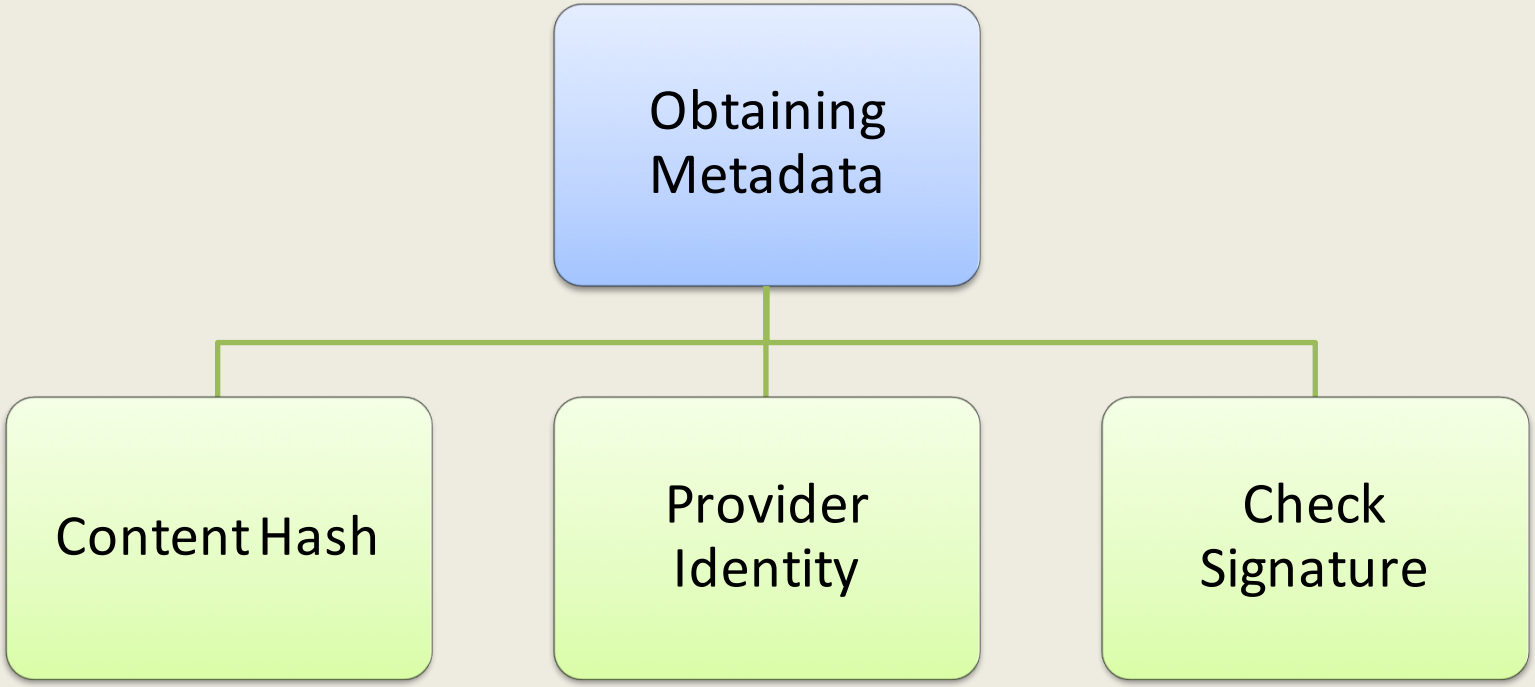
How to Mitigate Cache Pollution?



Cryptographic Secure Naming

Authors	Crypto Model	Provenance	Drawback
Dannewitz et al.	RSA	Public key digest	Lack of evaluation & Scalability issue
Hamdane et al.	HIBC	IBC signature	Signature verification overhead
Wong et al.	RSA	Public key digest	PKG requirement for private key generation
Zhang et al.	IBC	IBC signature	Scalability issue & Public key length

For secure naming, a client need to obtain the content manifest that contains chunks' names.



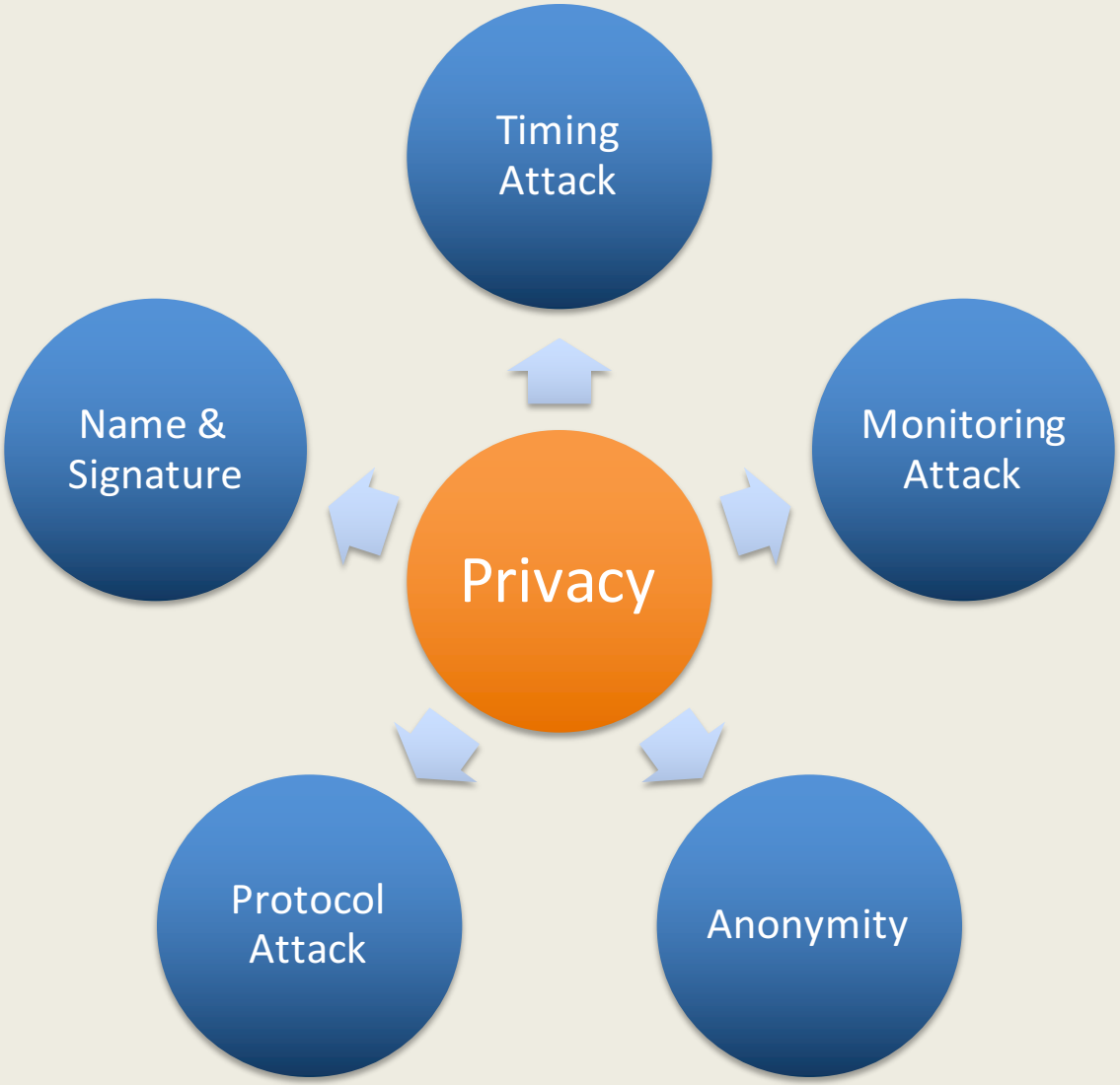
Secure Routing in ICN

Authors	Architecture	Mechanism
Afanasayev et al.	CCN/NDN	Namespace mapping for unknown prefix forwarding
Rambraz et l.	NetInf	Secure communication between public and private domains employing name resolvers
Alzahrani et al.	Publish/Subscribe	DoS resistant self-routing mechanism using dynamic link identifiers and temporal z-Filter
Yi et al.	NDN	Augmenting NDN forwarding plane by introducing NACK for unsatisfied interests

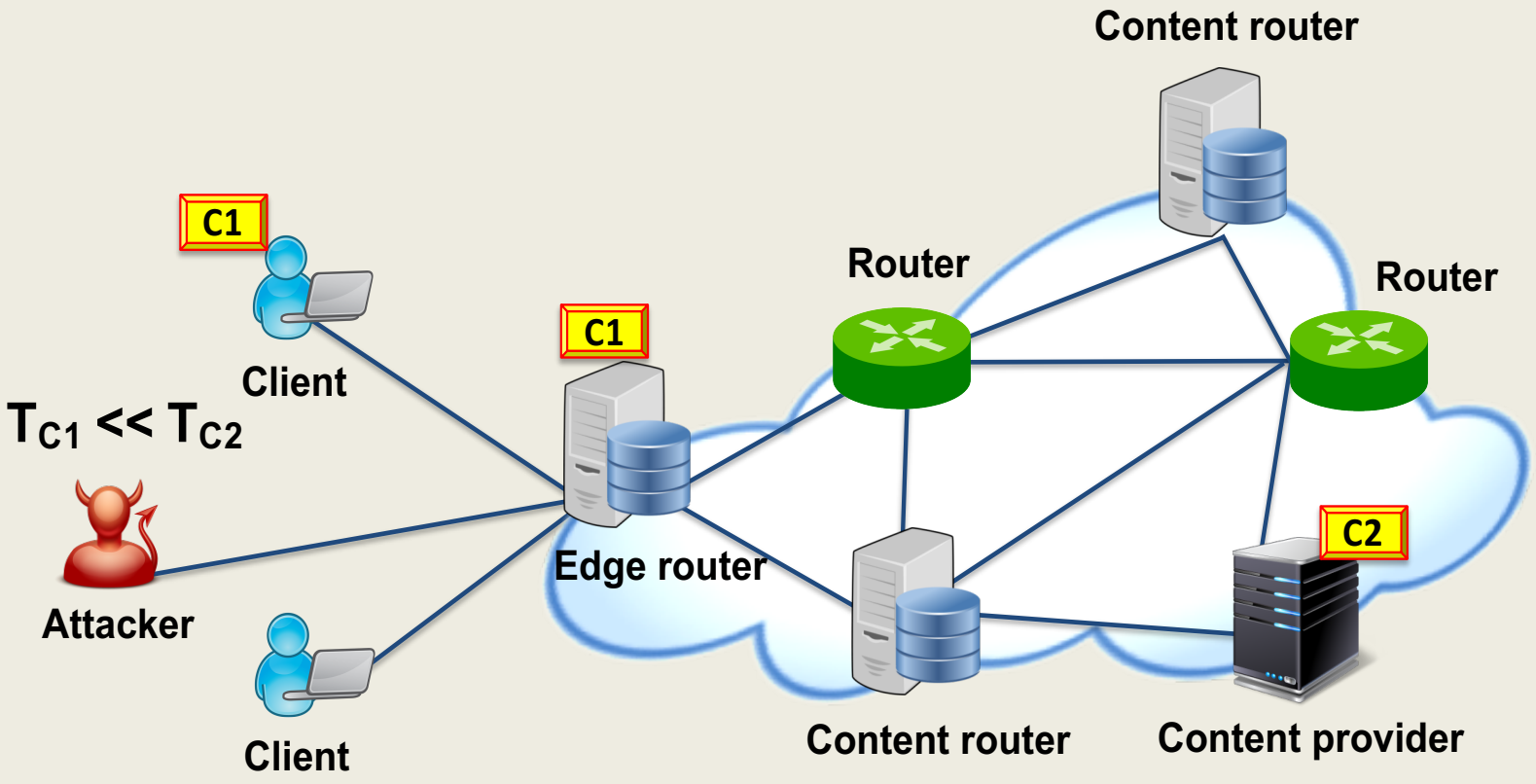
Application Level Security

Authors	Application	Approach
Ambrosin et al.	Ephemeral covert channel	Time difference analysis between cache-hit and cache-miss
Asami et al.	Moderator-controlled information sharing	Publisher signature followed by moderator signature for message publication
Burke et al.	Lighting control system	Submitting commands as signed interest or signed content
Burke et al.	Secure sensing in IoT	Assigning a sensor an ACL for content publishing
Fotiou et al.	Anti-spam mechanism	Information ranking based on publishers and subscribers votes
Goergen et al.	Traffic anomaly detection at routers	Statistical data analyses and SVM classification
Goergen et al.	Semantic firewall	Filtering by content name, provider's public key, and anomaly detection
Karami et al.	Anomaly detection	Fuzzy detection algorithm and traffic clustering
Saleem et al.	Secure email service	Asymmetric crypto with emails as independent objects
Vieira et al.	Security suite for Smart Grid	Content-based cryptography and access level distribution via security server
Wong et al.	Content integrity by security plane	Content signature and publisher authentication to security plane by challenge-response
Yu et al.	Trusted data publication/consumption	Schematized chain-of-trust
Seedorf et al.	Self-certifying names and RWI binding	Employing a Web-of-Trust

Privacy in ICN

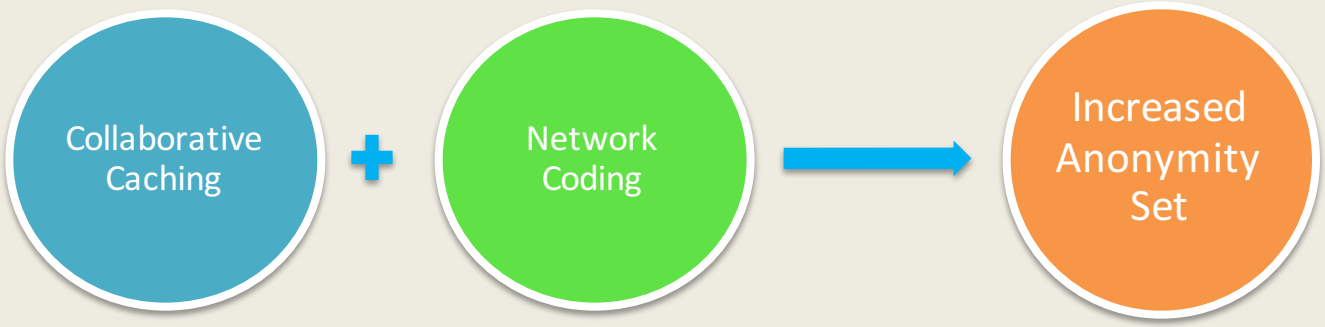


Timing Attack: An attacker probes the cached content by timing analysis between cache hit/miss.



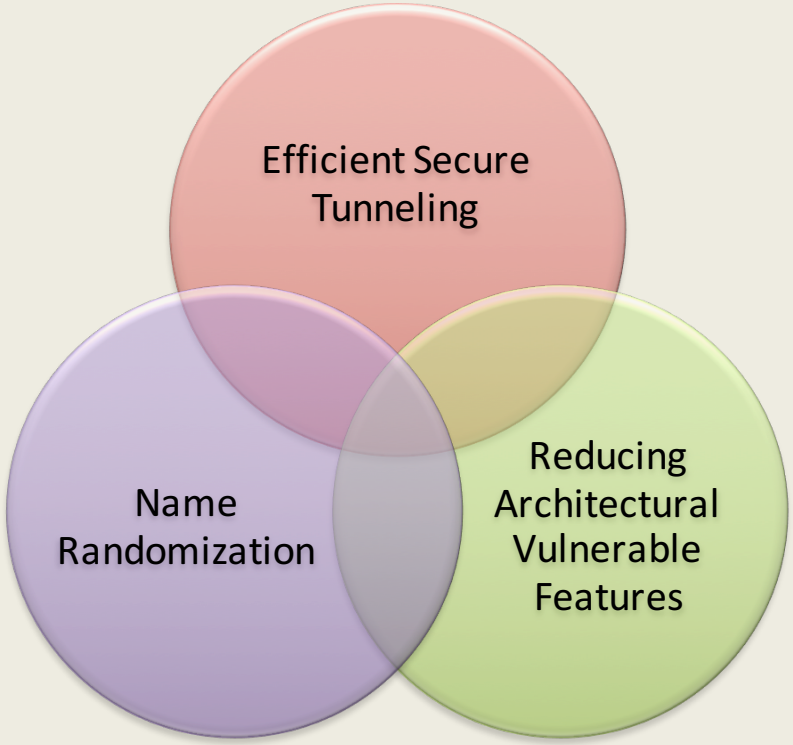
Timing Attack: An attacker probes the cached content by timing analysis between cache hit/miss.

Authors	Approach	Mitigation Entity
Ace et al.	Delay for the first K interests	Edge routers
Chaabane et al.	Delay for the first K interests	Edge routers
Mohaisen et al.	Delay for the first interest from each client	Edge routers & Access Points

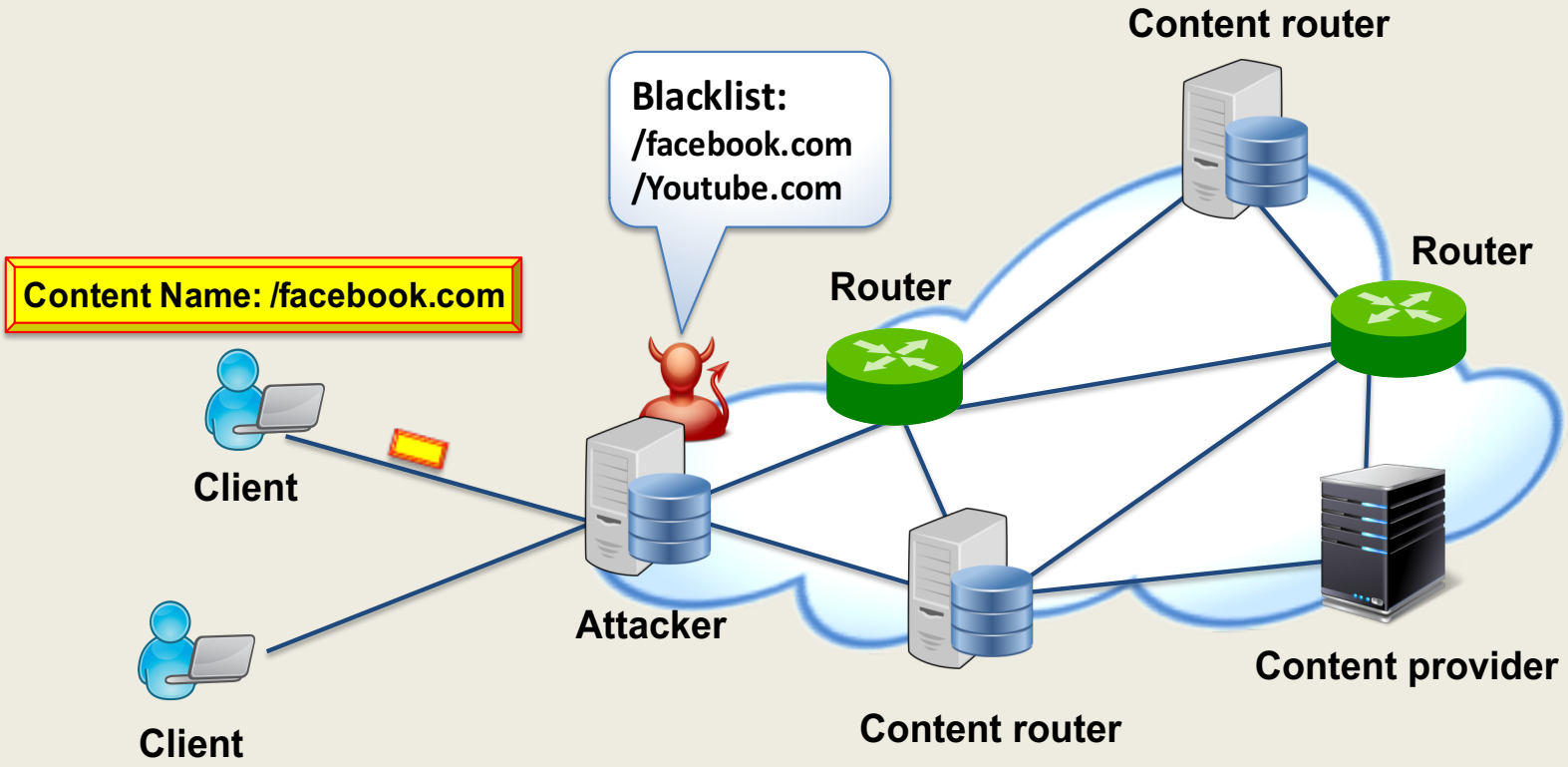


Communication Monitoring Attack

Authors	Approach	Drawback
Chaabane et al.	Secure tunneling (similar to SSL and TLS) & Broadcast encryption and proxy re-encryption	Undermines Caching Computation overhead
Lauinger et al.	Selective caching, secure tunneling, marking privacy sensitive communication to avoid caching	Undermines caching Computation overhead ISP trustworthiness



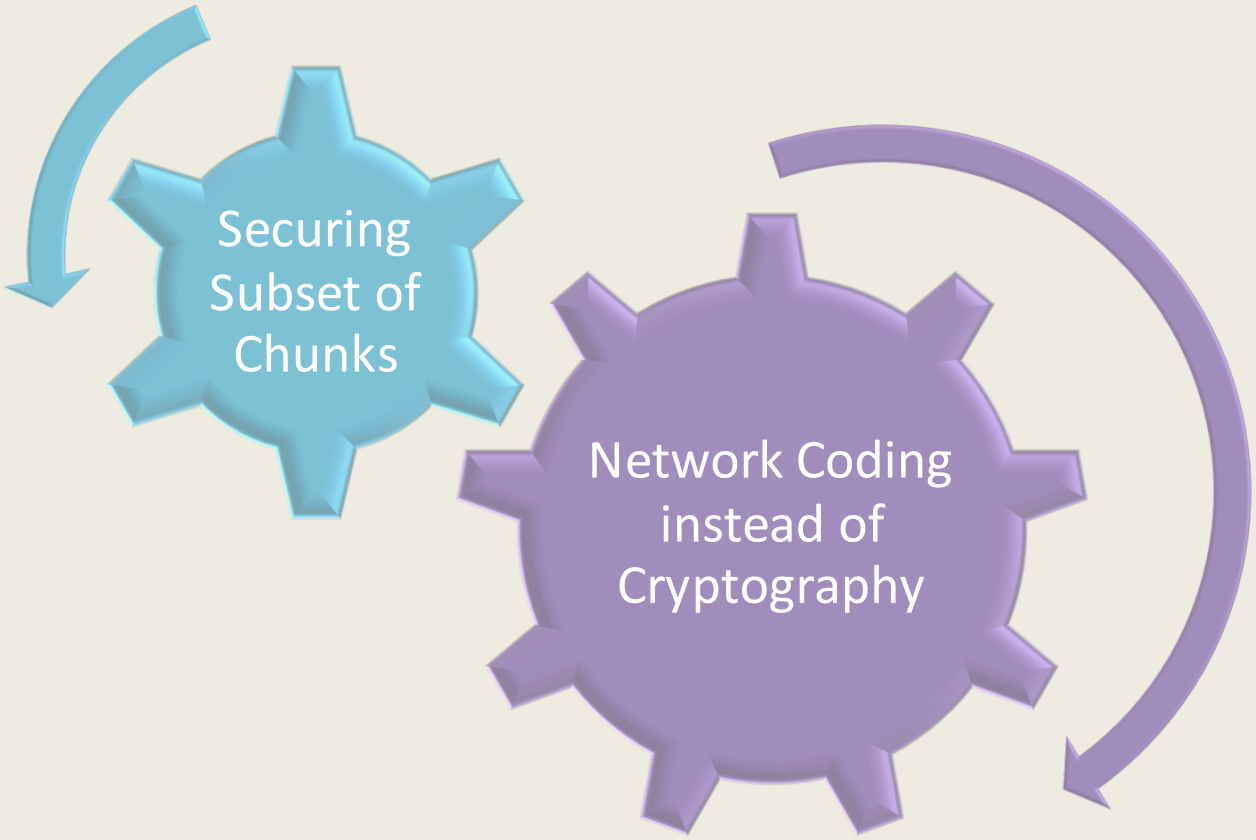
Censoring client's requests using content names in the interests undermines client privacy.



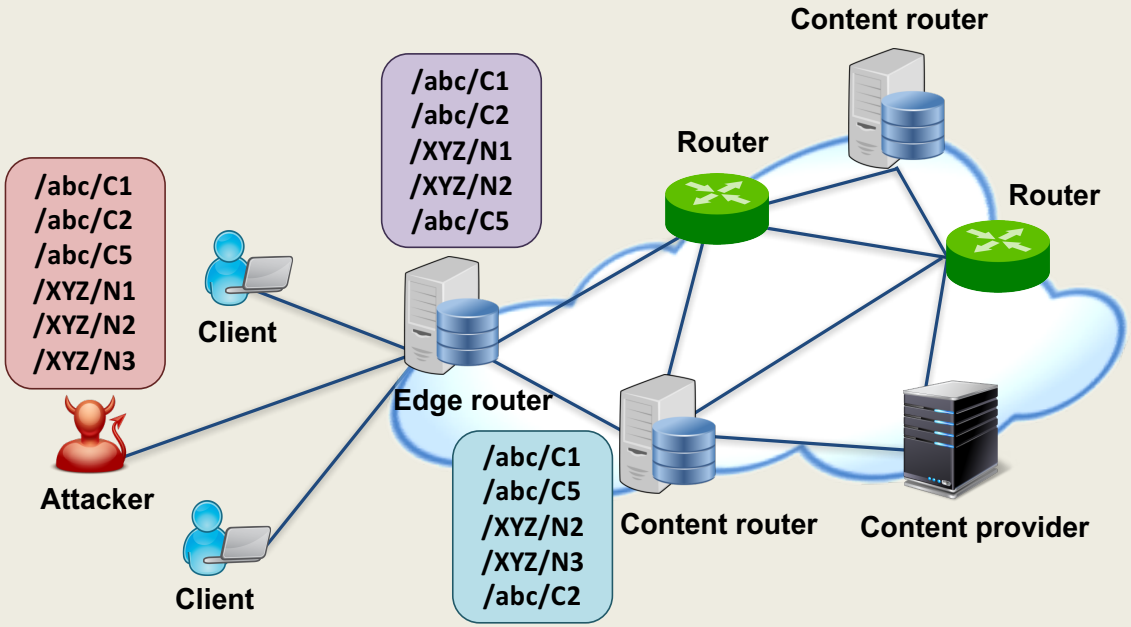
Censoring client's requests using content names in the interests undermines client privacy.

Authors	Approach	Infrastructure	Computation Complexity
Arianfar et al.	Encoding interest by mixing content and cover file	Not Applicable	High (cover & exclusive-or)
Chung et al.	TOR based model – 2 layers of encryption	Two Proxies	Moderate (symmetric key)
DiBenedetto et al.	TOR based model – 2 layers of encryption	Two Proxies	Moderate (symmetric key)
Elabidi et al.	Ephemeral identities for users	Requires three new entities	High (several interactions)
Fotiou et al.	Hierarchical DNS based brokering model	Brokering Network	High (Homomorphic cryptography)
Tao et al.	Random linear network encoded interest	One Proxy	Moderate (RLNC + PKI)
Tourani et al.	Huffman-based encoded interest	One Proxy-anonymizer	Low

Anti-censorship mechanisms need to be fast and efficient with low complexity.



Discovery and Protocol Attack



Leveraging protocols vulnerabilities such as prefix-based matching, scope field, and exclusion feature to probe caches of nearby routers and discover cached content.

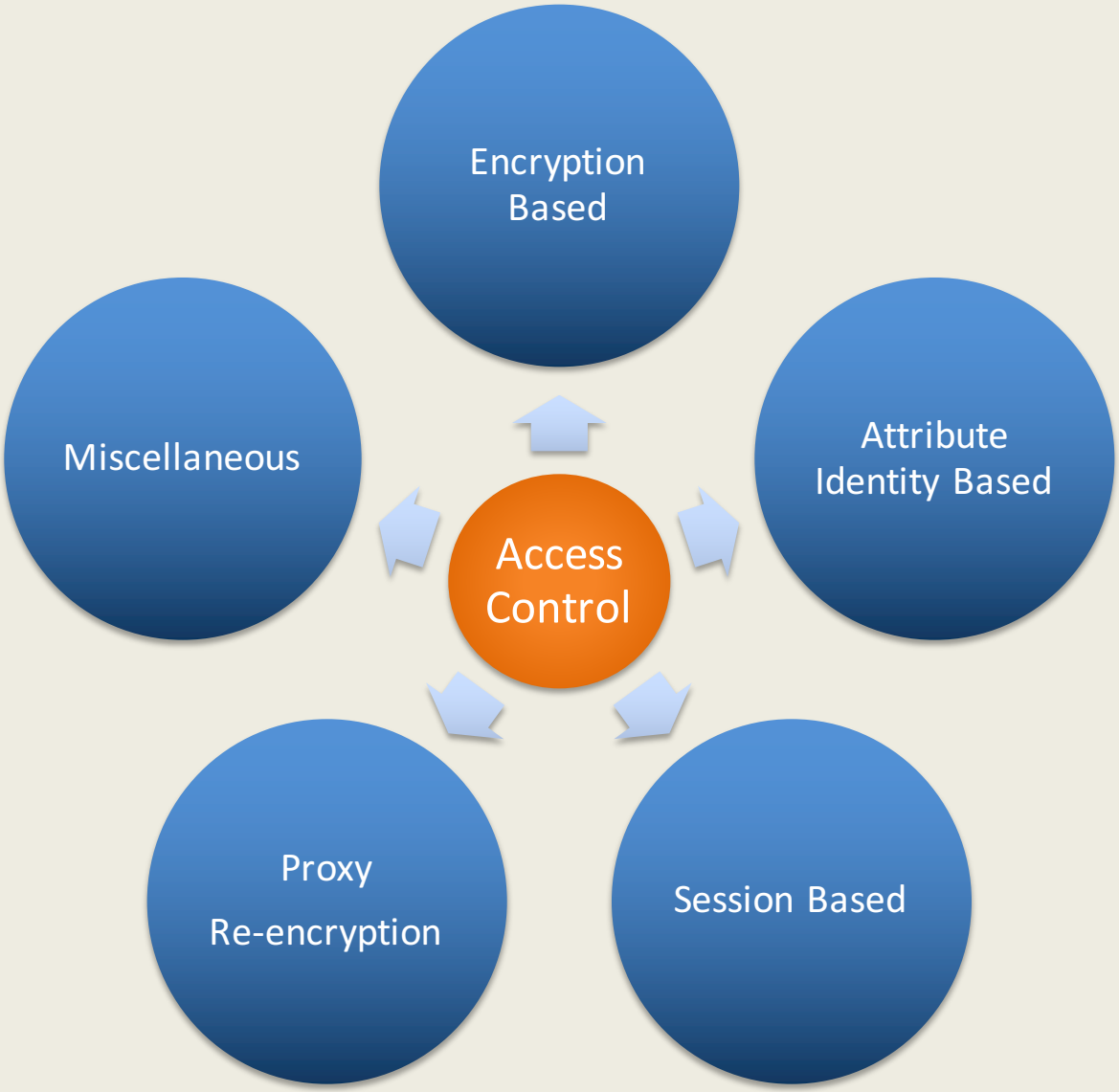
Authors	Approach	Architecture
Lauinger et al.	Object discovery attack using NDN prefix matching and exclusion feature	NDN
Chaabane et al.	Prefix-based matching and scoping attacks	NDN

Preserving Names and Signatures Privacy

Authors	Approach	Drawback
Baugher et al.	Cryptographic hash-based naming from a catalog (maps hashed name to human readable names)	Obtaining names Useful for read-only content
Martinez et al.	Overlay network and digital identities with domain	Requires infrastructure for connection establishment
Chaabane et al.	Bloom filter to represent content names	Bloom filter false-positive and its increasing size
Chaabane et al.	Confirmer signature, group signature, ring signature, and ephemeral identity	No elaboration
Katsaros et al.	Ephemeral content names	Undermines caching

Increasing publishers anonymity set by leveraging several certificates, which map to several identities, and group-based signature.

Access Control in ICN



Encryption-based and Attribute-based access control models.

Authors	Communication Overhead	Computation Burden	Client Revocation	Cache Utilization	Enforcement Entity
Misra et al.	Yes	Client	Threshold-Based	Yes	Client
Kurihara et al.	Yes	Network	Lazy Revocation	Yes	Provider
Chen et al.	Yes	Provider & Network & Client	Daily Re-encryption	Limited	Provider & Network
Aiash et al.	Yes	Non	Not Considered	No	Provider
Da Silva et al.	Yes	Network	Key Update per Revocation	Yes	Network
Hamdane et al.	Yes	Client	Not Considered	Yes	Network
Hamdane et al.	Yes	Non	System Re-key	Yes	Provider
Ion et al.	Yes	Non	Not Considered	Yes	Client
Li et al.	Yes	Provider & Client	Not Considered	Yes	Client
Raykova et al.	No	Provider & Client	Not Considered	No	Client

Session-based, Proxy Re-encryption, and other access control models.

Authors	Communication Overhead	Computation Burden	Client Revocation	Cache Utilization	Enforcement Entity
Renault et al.	Yes	Non	Not Considered	No	Network
Wang et al.	Yes	Provider	Not Considered	No	Provider
Mangili et al.	Yes	Provider & Client	Partial Re-encryption	Yes	Client
Wood et al.	Yes	Provider	Not Considered	Yes	Provider
Zheng et al.	Yes	Provider & Network	Not Considered	Yes	Network
Fotiou et al.	Yes	Network	Not Considered	Yes	Network
Ghali et al.	No	Provider & Network & Client	Not Considered	Limited	Provider & Network
Li et al.	Yes	Provider & Network	Not Considered	Yes	Provider
Singh et al.	Yes	Network	Not Considered	Yes	Network
Tan et al.	Yes	Provider	Considered	Yes	Provider

Thank you!

Email:misra@cs.nmsu.edu

Research funded by the US National Science Foundation and the US Dept. of Defense.