



ForNet: A Distributed Forensic Network

Kulesh Shanmugasundaram, Nasir Memon
{kulesh,memon}@isis.poly.edu

Polytechnic
UNIVERSITY



Outline

- Motivation
- Overview of Proposed System
- System Architecture
- An Illustrative Example
- Research Challenges



Current Security Infrastructure

- **Passive Security & Networks:**
 - Security is usually an overlay on network infrastructures
 - Network components are unaware of security needs
- **Vendors are beginning to realize the gap**
 - Cisco SAFE Initiative
 - Other NP-based solutions for IDS, Firewalls, VPNs etc.
- **Need for better network forensics:**
 - Lack of attack attribution on networks
 - Every year numerous cyber crimes go unsolved. Why?
 - Lack of a good response model
 - Increasing interest in prosecutions
 - Steady increase in financial losses due to cyber crimes



Current Response Model

- Typical Response to Breaches:
 1. Adversary breaks in & do his/her work
 2. Security personal identifies the breach
 3. Find out where the adversary came from (log files if still there)
 4. Pick-up the phone & call the ISP, FBI
 5. ISP/FBI notifies the other end
 6. Go To Step 2
- Average response time is in days/weeks
- Involves several human interventions
- Requires coordination among several administrative domains



Challenges Facing Network Forensics

- Lack of infrastructure for forensic data collection, storage, and dissemination
 - Packet logs are usually kept at network edges which do not witness many events inside a network
- Growth of network traffic outpaces Moore's law making prolonged storage, processing, and sharing of raw network data infeasible
- Most of the process is manual and spans multiple administrative domains making response times undesirably long (e.g. digital evidence disappears quickly)
- Inability of current logging mechanisms to help forensic analysts explore networks incrementally
- Unreliable logging mechanisms on hosts
- Growing support for mobility makes it difficult to maintain prudent logging policies on hosts



A Solution

- Let the network securely collect, store, disseminate, and process *synopsis* of network traffic
- Give networks ability to remember network events so that they can answer questions like:
 - Where did a worm appear first in a domain?
 - Who sent this (possibly spoofed) packet?
 - Where else was this packet observed on the network?
- Goal: development of tools, techniques, and infrastructure to aid rapid investigation and identification of cyber crimes

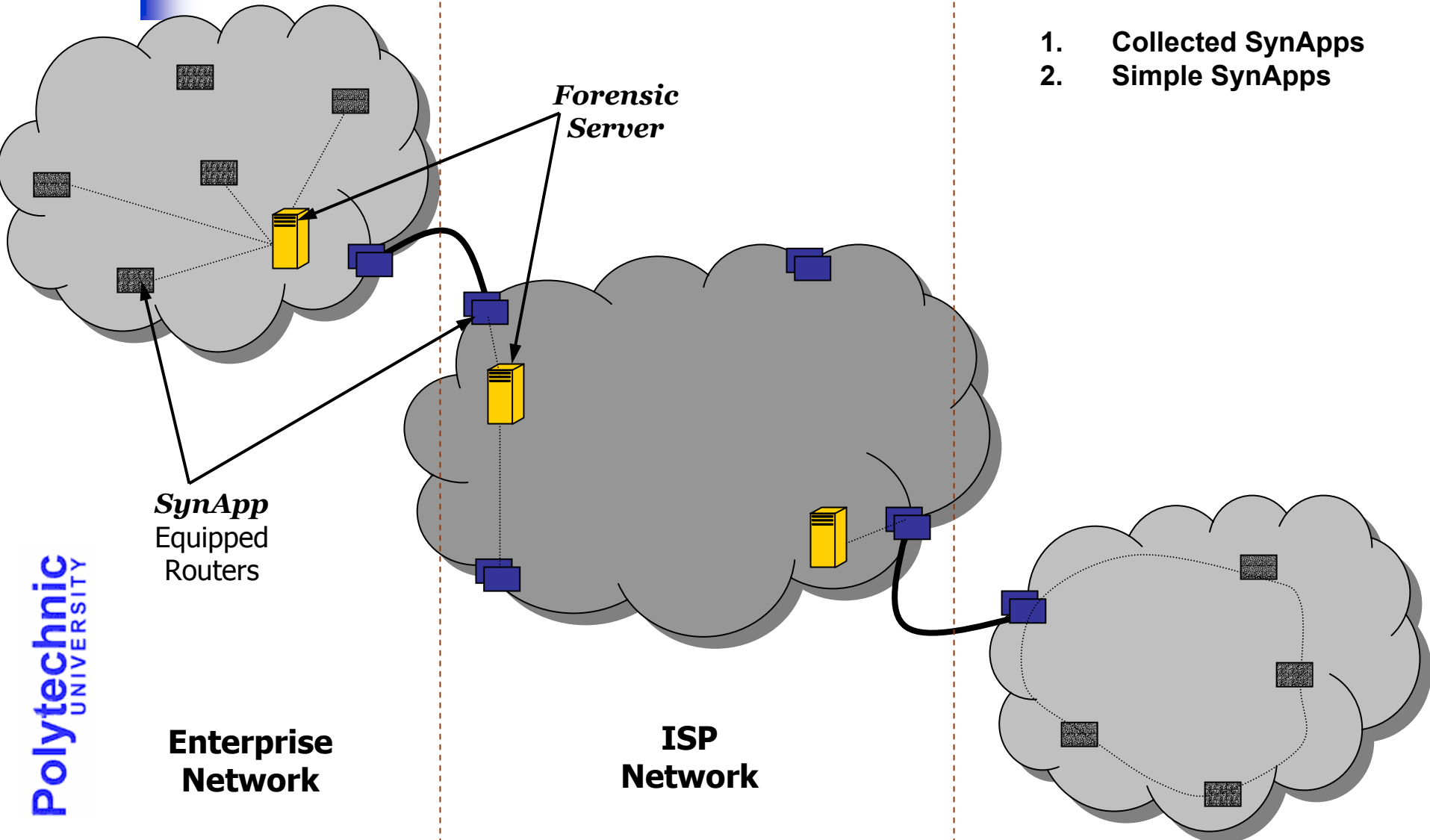


What is a Synopsis?

- Properties:
 - Contains information to answer certain classes of queries
 - Contains information to compute confidence interval
 - Have small memory footprint
 - Easy to update
- Examples of synopsis techniques:
 - Connection Records, Bloom Filters, Sampling, Histograms, Decision Trees/Clusters, Wavelets
- Advantages of using synopses:
 - Without synopses it is difficult to store network traffic
 - Succinct representation of base data makes it possible to transfer network data to disk/storage
 - Query processing would be expensive with raw data
 - Sharing/transferring raw data over network is impossible
 - Easily adaptable to various resource requirements



ForNet Blueprint



1. Collected SynApps
2. Simple SynApps

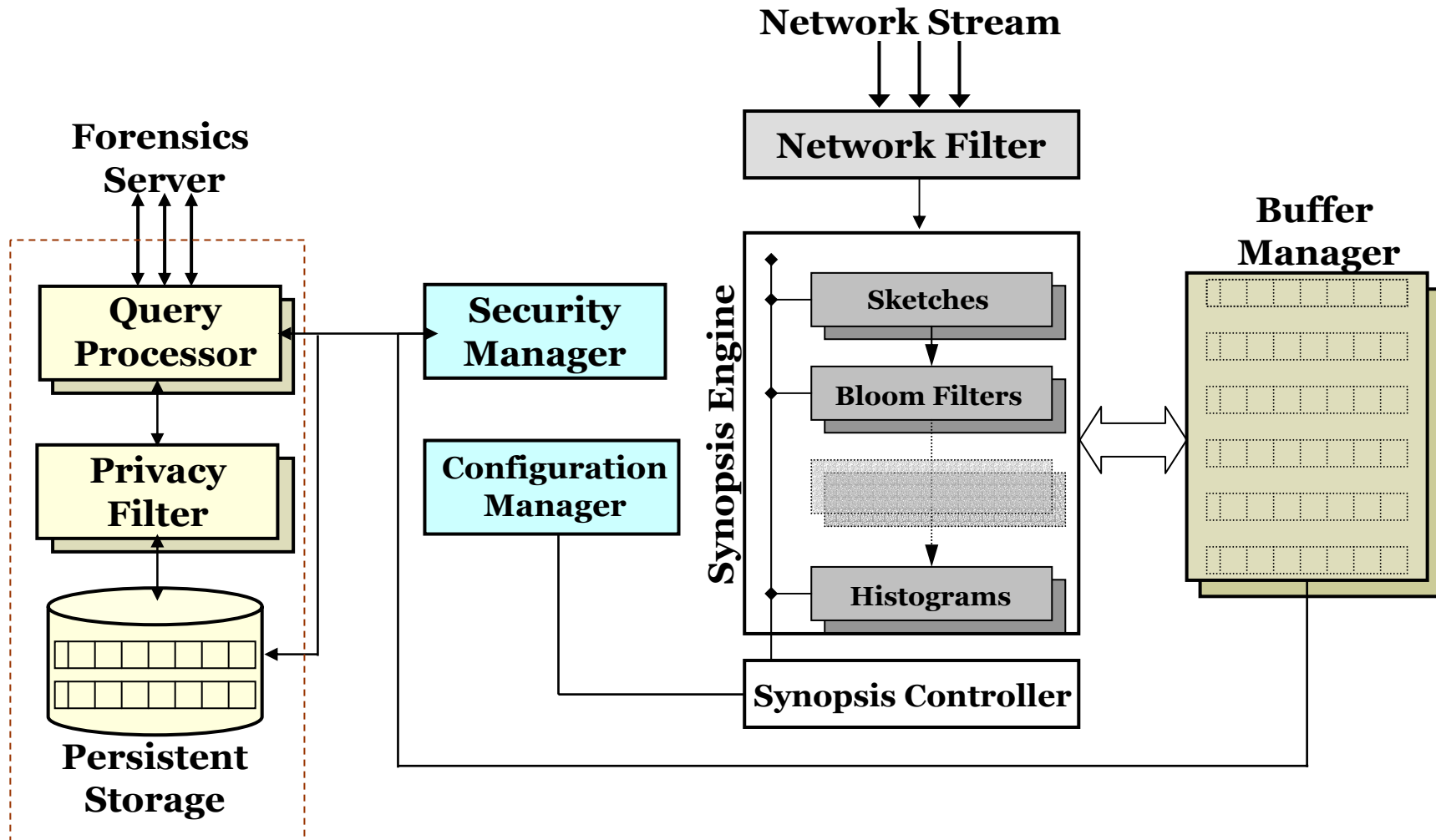
SynApp
Equipped
Routers

**Enterprise
Network**

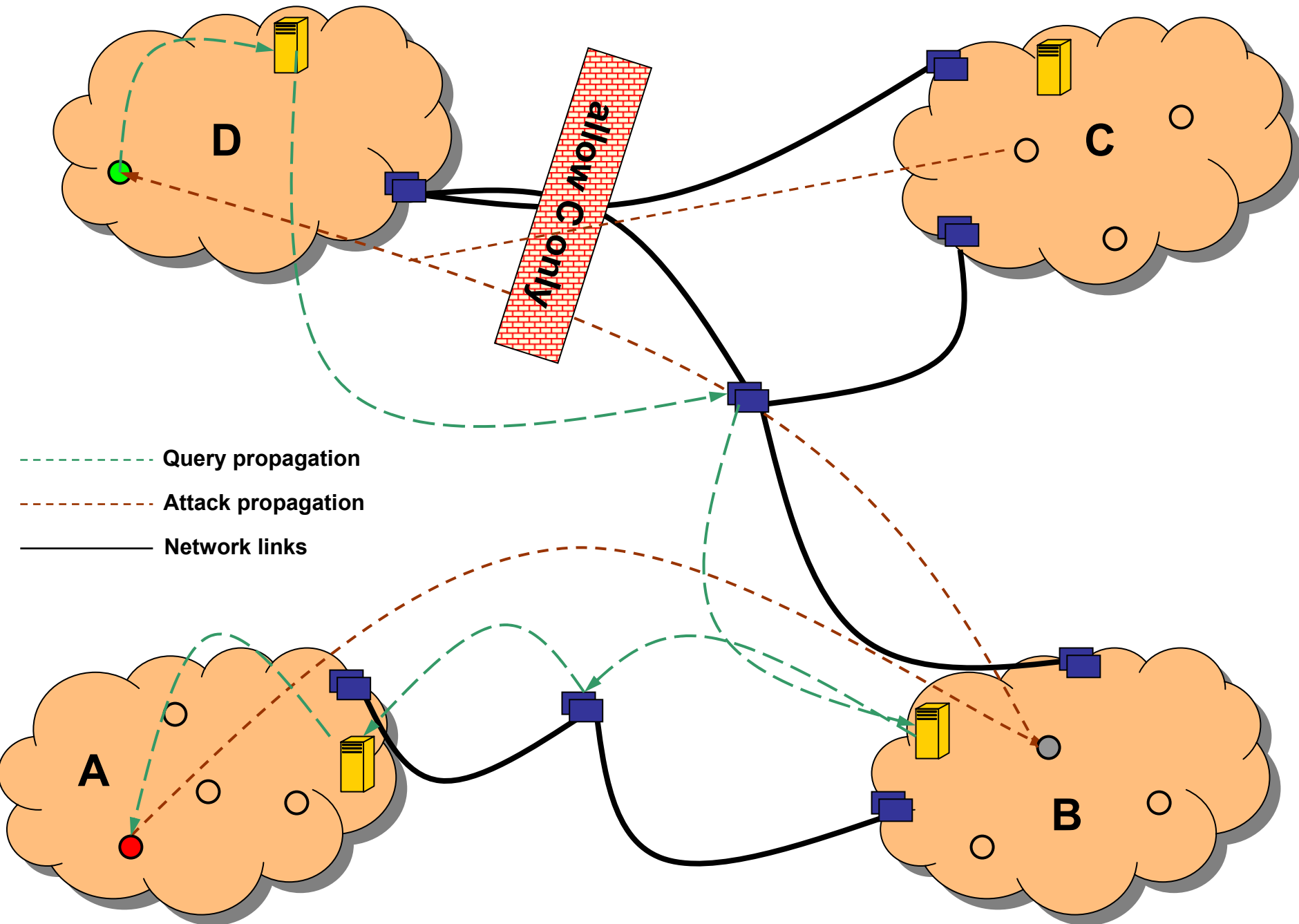
**ISP
Network**



Architecture of SynApp



An Illustrative Example



Research Challenges



Research Challenges

- Identification of useful network events
 - Network is the virtual crime scene that holds evidence in the form of network events
- Identification of various query types
 - Selection queries
 - Neighbor queries
 - Temporal queries
 - Similarity queries
 - Aggregate queries
 - Spatio-temporal joins
- Developing efficient synopses
 - Handling connection oriented & connectionless traffic
 - Cascading synopsis techniques to achieve various tradeoffs



Research Challenges

- Integration of information from synopses across networks
 - Real power of ForNet is realized when information from SynApps is fused to answer queries
 - Development of a protocol for secure communication of various ForNet components
- Storage and query processing of synopses
 - Various storage and garbage collection strategies for collected-SynApps
 - Storage and query processing infrastructure for Forensics Servers
 - A query language transparent of various underlying synopsis techniques
 - Optimization of query processing and storage



Questions...