Network application attack recovery

Meng Yu, Peng Liu, Wanyu Zang
Cyber Security Lab & Networking Research Center
Penn State University
http://ist.psu.edu/s2

How to defend?

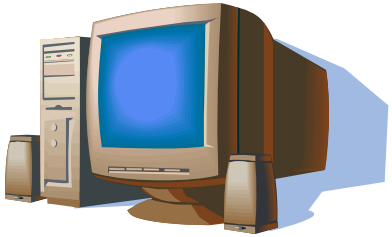
- Protection (access control, authentication, etc.)
- Detection (intrusion detection systems)
- Response (push back against DDoS attacks)
- Recovery (restore the system to its original integrity level)

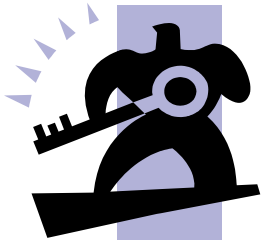
Why do we need recovery?

- No perfect defense.
- Attackers can always compromise your system.
- We need to recover the system under successful attacks.
- Improve the survivability.

How does damage spread?

Attacks: x := 2



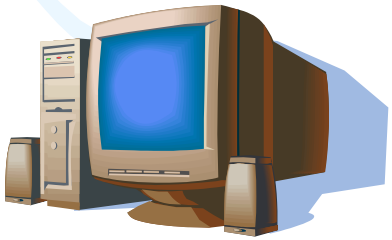


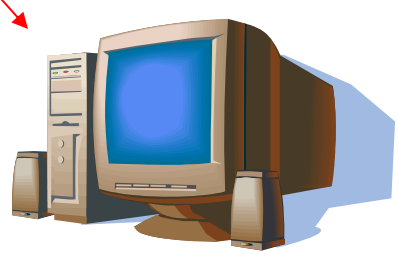
Through data dependences: generates wrong y

Through the control dependence: invoke wrong task

Infected: y := x + 1

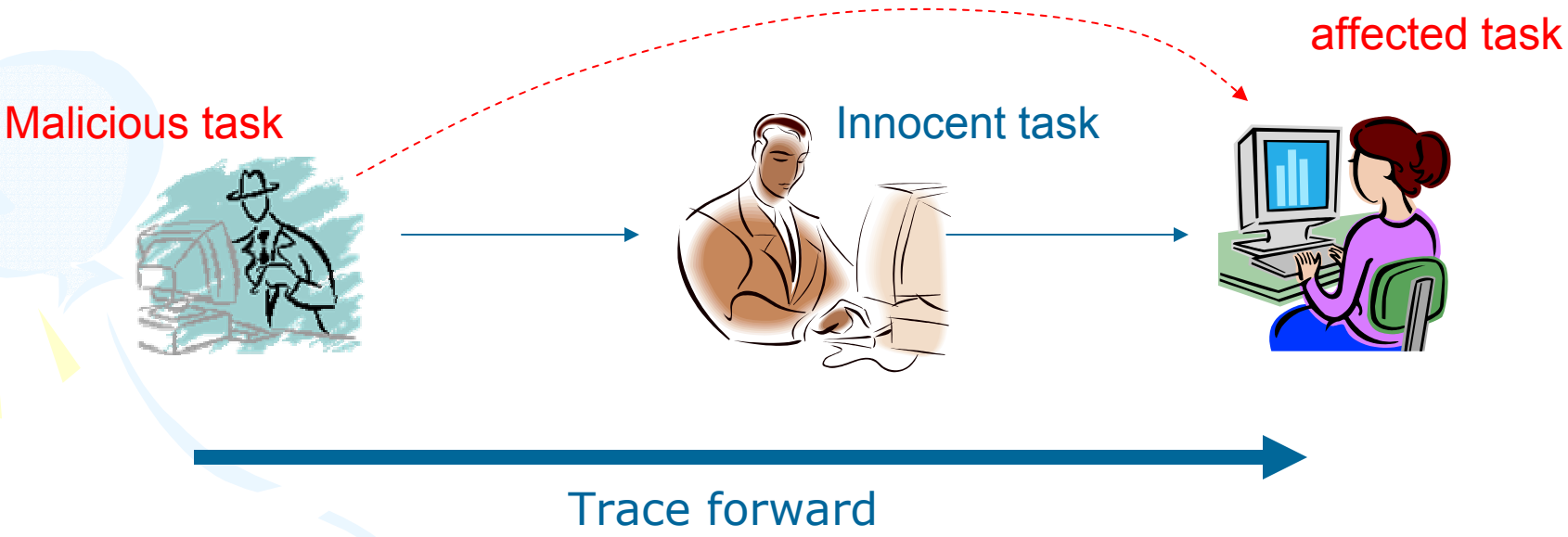
Infected: if (x<10) then y = 5





How to trace the damage?

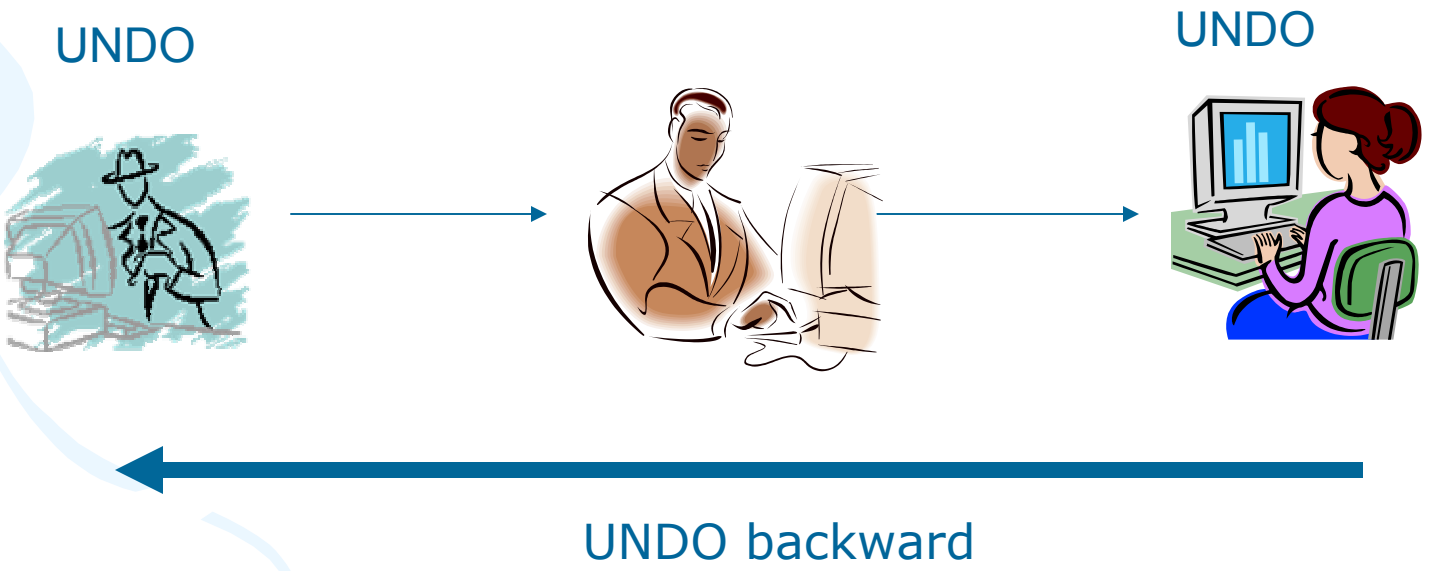
- Inspect dependence relations to trace damage spreading.



Check if a transaction is dependent on (affected by) known malicious transactions to determine if it is corrupted.

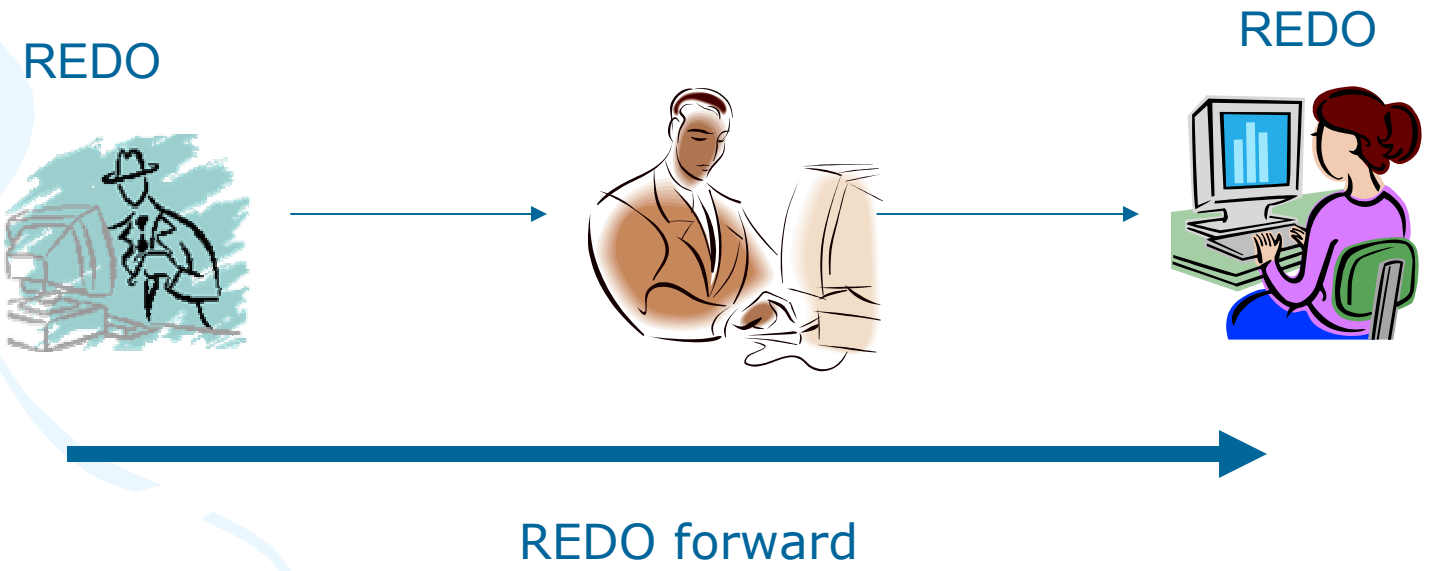
How to remove the effects of damage?

- UNDO affected transactions.



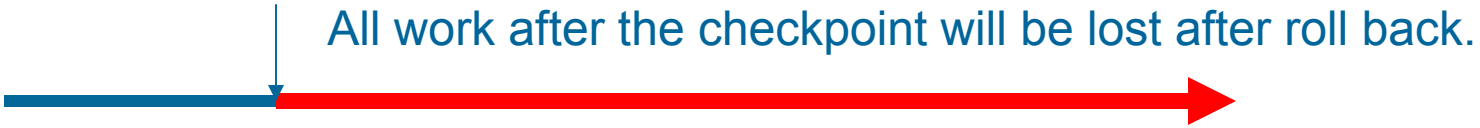
How to repair the damage?

- REDO affected transactions.

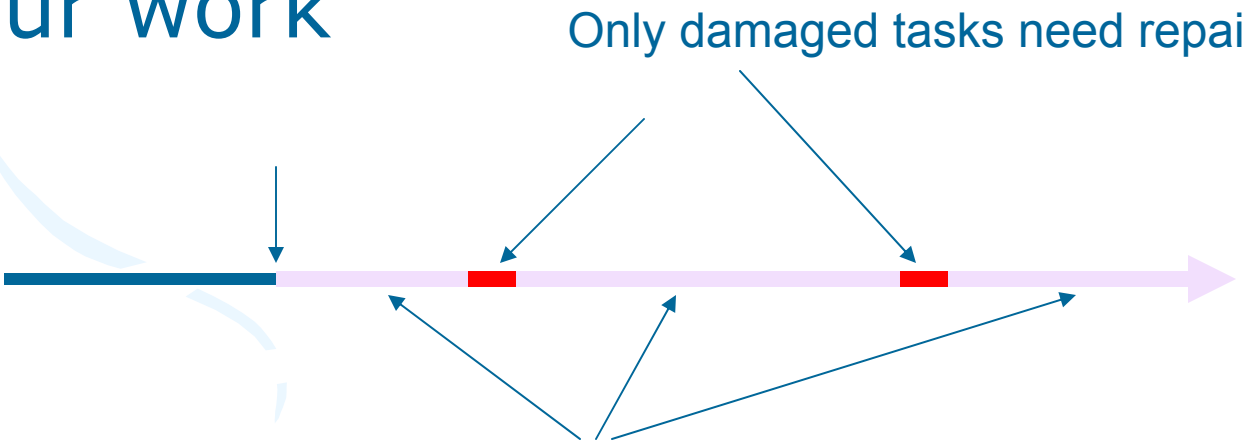


More efficient than checkpoints

- Checkpoints

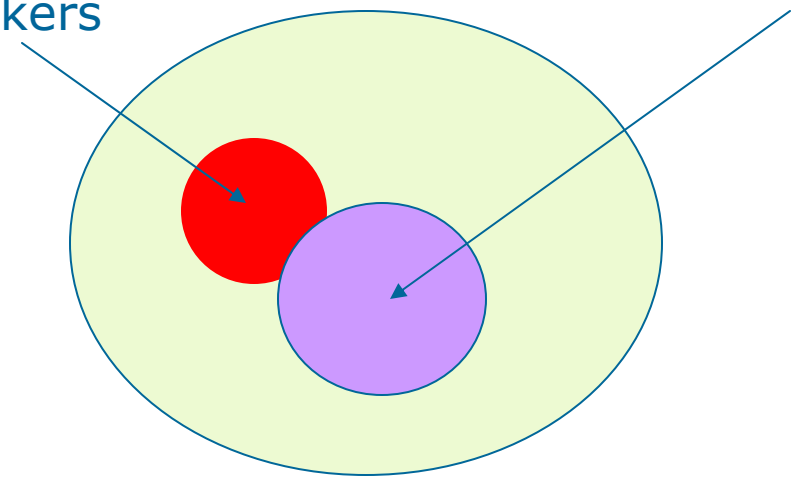


- Our work



Comparison with Intrusion Detection Systems

A: Damage caused directly by attackers

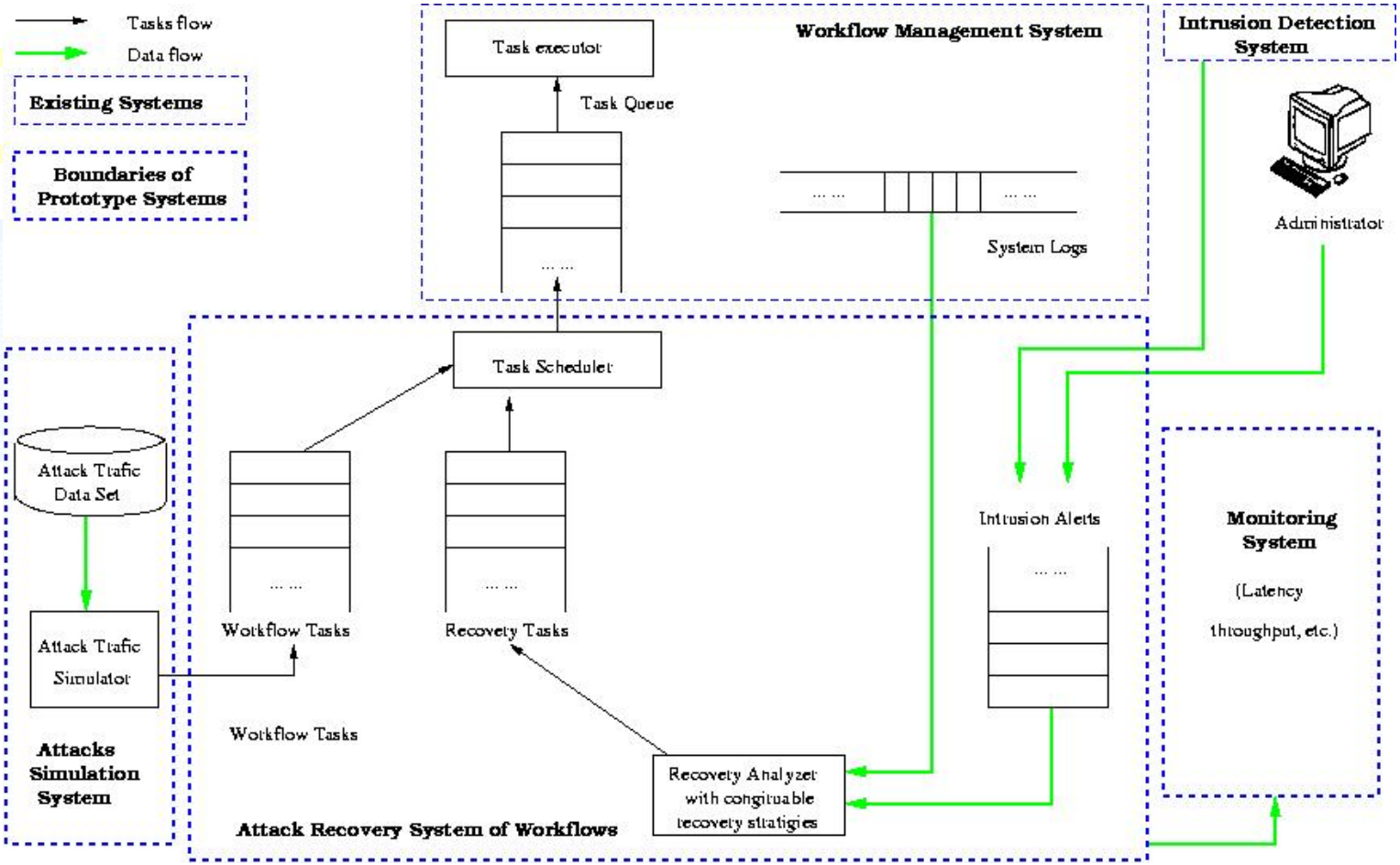


B: Damage caused by executing legitimate tasks which are dependent on damaged tasks.

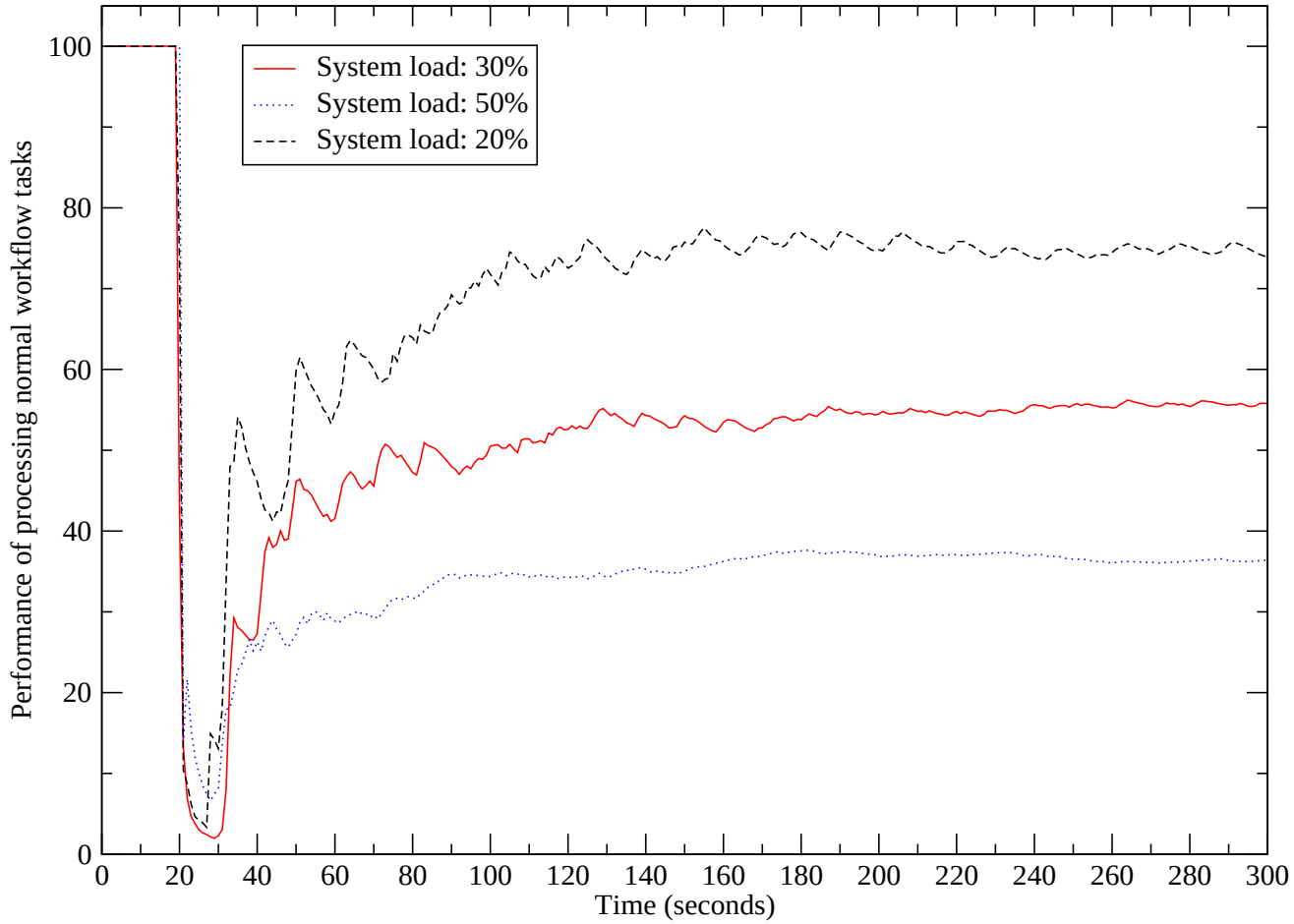
Intrusion Detection Systems: can find A; cannot find B.

Our system: based on A can find B

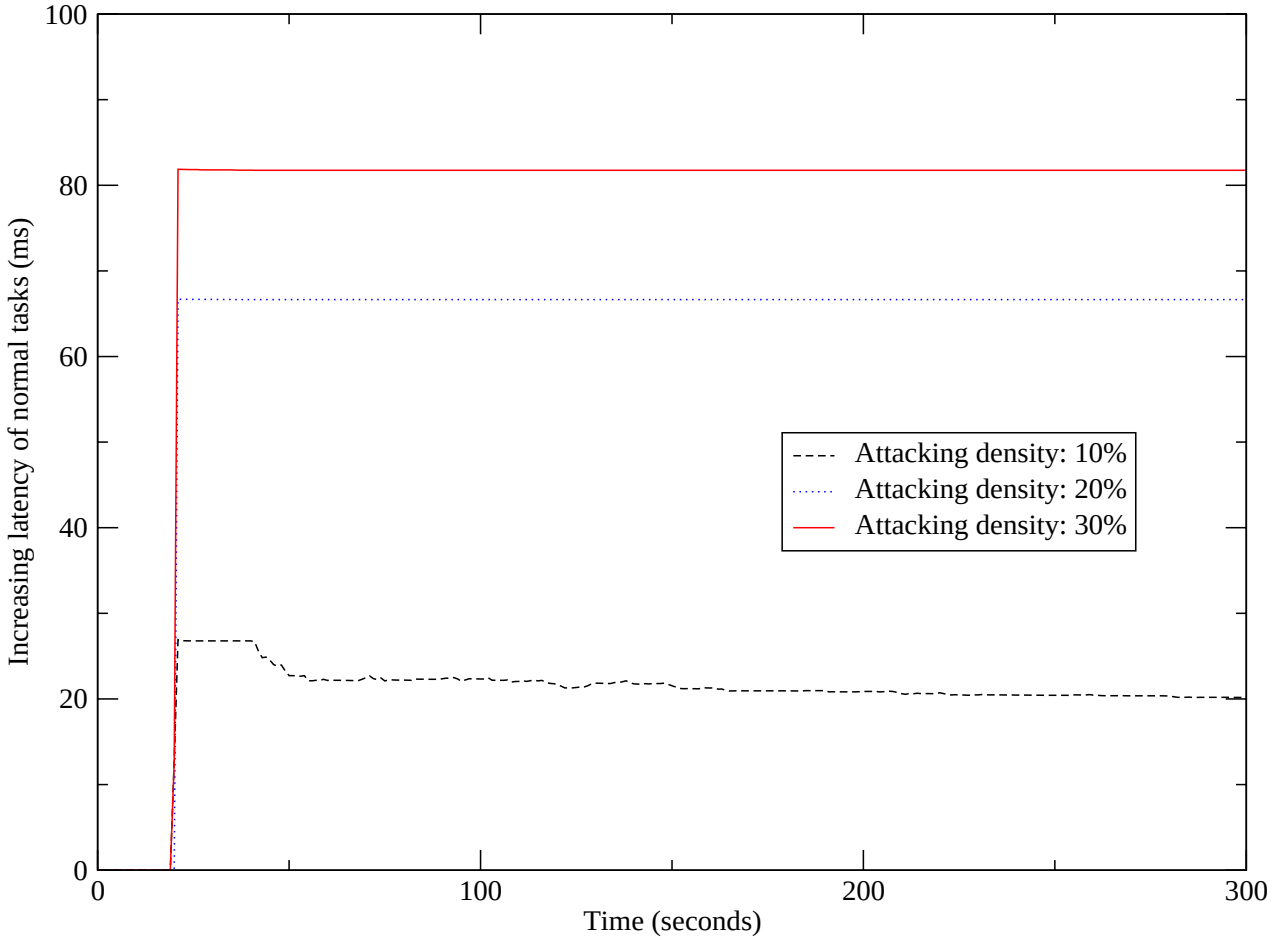
Our Prototype System



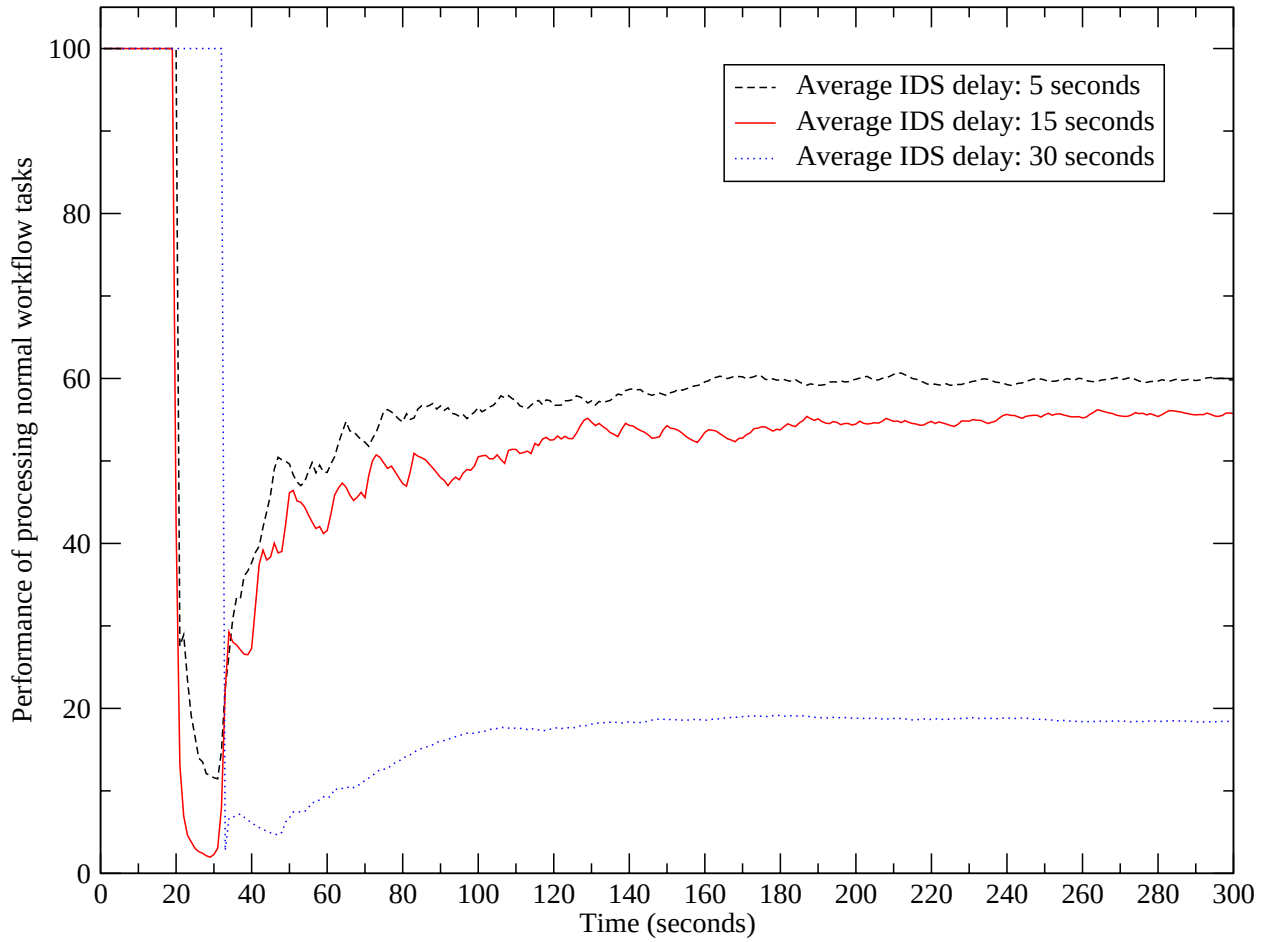
Impact of the system load



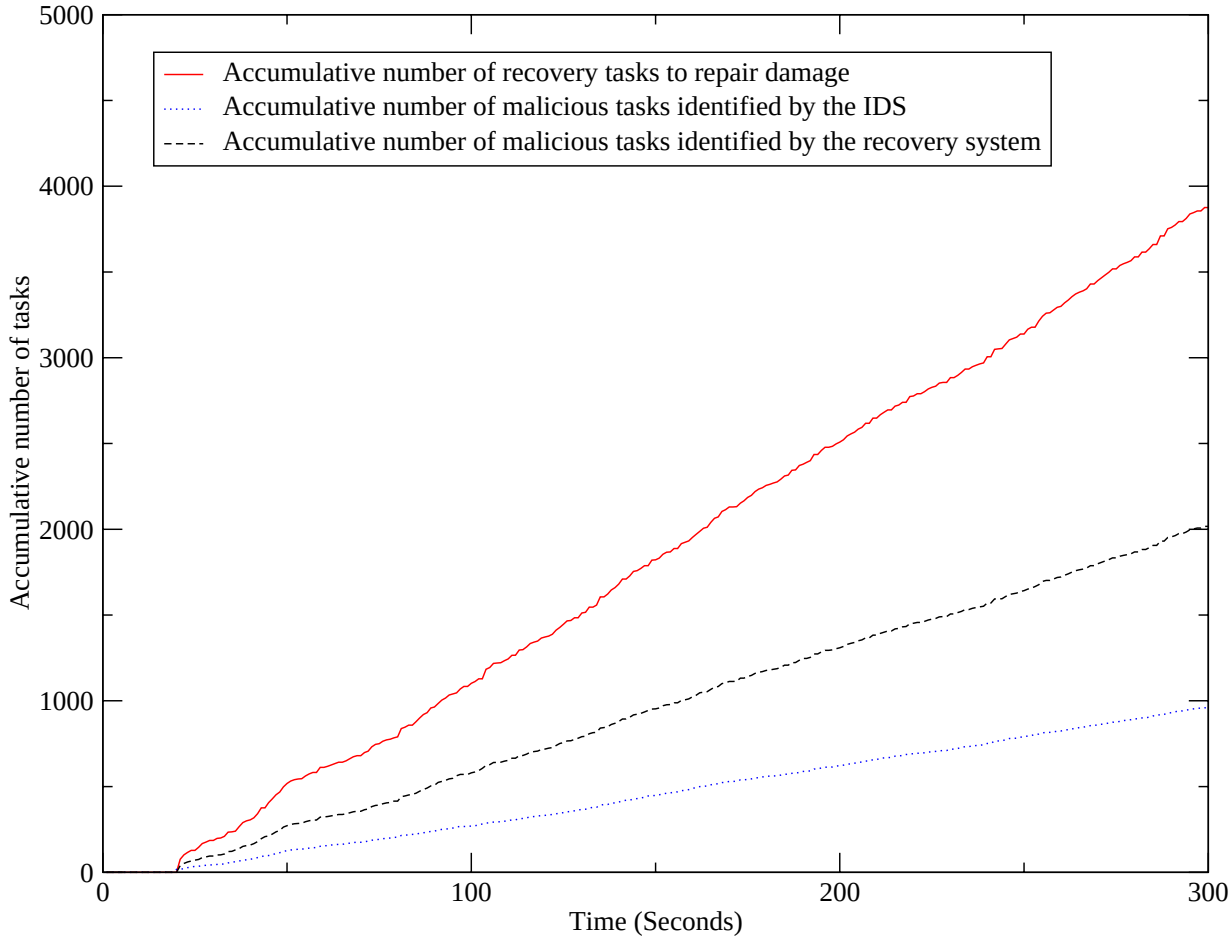
Impact of the attacking density



Impact of the IDS delay



Task numbers



Interesting?

- We proposed three different recovery strategies (conservative, optimistic, and aggressive).
- We proposed two mathematical models for performance evaluation (Continuous Time Markov Chain and queuing network)
- We built a prototype system and obtained exciting experimental results.
- Published in ICDCS'04, And more!

More work in the future

- Collaborative recovery in a distributed system.
- Effective and efficient recovery information exchanging.
- Configurable and adaptive recovery strategies.