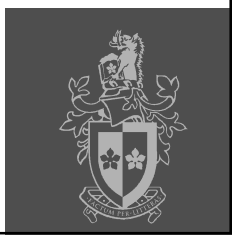
SWINBURNE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Controlling Excessive Resource Consumption In IP Network

Minh N. Tran



Talk outline

- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

Talk outline

- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

Spam and anti-spam

- "Mass unsolicited electronic mail"

  (RFC 2505, "Anti-Spam Recommendations for SMTP MTAs ", http://www.ietf.org/rfc/rfc2505.txt)
- Researchers attempt to characterise spam

  Motivation:

  - identifying signature of spam to be used in developing more effective spam controlling techniques [14]
  - proposing models of user behaviors [17,18]
  - evaluating techniques of detecting and controlling spam [19]
  - identifying factors that lead to that fact that some domains and users are more likely to receive spam [20]

Spam and anti-spam

- Spam signature:
- The authors [14] quantitatively and qualitatively characterize features that distinguish spam from non-spam traffic:
  - email arrival process: Exponential distribution
  - email size: Log-normal distribution/ Coefficient of Variation (CV)
  - email popularity
  - number of recipients per mailbox: Zipf-like distribution
- Social factors
- Clear daily/ weekly patterns for spam >< Insensitive to measurement period for non-spam

Spam and anti-spam

- Anti-spam techniques:
- Black-listing:
  - White >< black listing -> challenge-response
  - Local >< DNSBL (spam sources and open relay)
- Statistical content filtering
- Other anti-spam methods

Spam and anti-spam

- Evaluate DNSBL techniques:
  - The authors [21] evaluate relationship between inbound email traffic and DNS lookup in MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) based on packet traces taken in December 2000 and February 2004
  - Findings:
    - 80% spam sources are listed in some DNSBL
    - Distribution of incoming SMTP connection per spam sources is a Zipf-like in 2004, but not 2000 -> capability of DNSBL
    - Strong coherence between open relay DNSBLs
    - Week correlation between spam sources and open relay DNSBLs
    - Conditional probability matrix :
      - Determine probability of a remote host
      - Choose members of correlated lists which smallest false positive

Spam and anti-spam

- Statistical approach:
  - From text characterisation to machine learning algorithms
  - Machine learning:
    - Training stage
    - Classification stage
  - From vector-space models to feature-pruning
  - Performance measure: cost (λ) and TCR (total cost ratio)
- Statistical spam filtering:
  - Authors [16] evaluates five supervised learning methods in the context of statistical spam filtering: Baye naive, maximum entropy, memory-based, Support Vending machine, AdaBoost

    Findings:
    - SVM, maximum entropy, and AdaBoost are top performers on cost-sensitive
    - The choice of filtering classifiers outweighs the choice of feature selection methods
    - Importance of message header
    - Filtering techniques are language independent

Talk outline

- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

Denial-Of-Service (DOS) attack

- What is DOS?

  A Denial of Service (DoS) attack is an attack which attempts to prevent the victim from being able to use all or part of their network connection [22].

- Financial cost: power, bandwidth, memory, diskspace.

  One PC with modem connection can consume about 1Gbps bandwidth and can overload many servers in high speed network [1]

- Technical difficulty:
  - Push-back mechanism against DOS is expensive and hard to deploy.
  - Source address spoofing
  - Reflection attack.
  - Many zombie relaying machines cause DDOS.
  - Attack in combined with worms, virus.

Denial-Of-Service (DOS) attack

- Prevent against DOS attack:
  - DOS resistant architecture [1]:
    - Separate client and server address
    - Non-global client address
    - RPF (reversed path forwarding)
    - State setup bit
    - Middlewalls
    - Source-Specific-Multicast
  - Puzzle suggested by [2]
  - Author [3] suggests use sender capacity to determine the ability to send packets: Request-To-Send (RTS) servers and Verification Points (VPs)
  - Internet Indirection Infrastructure (i3) [4] suggest different change in Internet architecture by obfuscating the address of server and has many disposable immediate triggers.
- Issues and future research

Talk outline

- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

Consumption in Ad-hoc network

- Security issues:
  - Survivability in military network
  - Support Anonymity
  - DOS attack
- Adhoc network and price-based approach:
  - Motivation: problems of user stimulation of forwarding the packets due to power, bandwidth constrains
  - Malicious nodes
  - Different approaches have been proposed

Security requirement in Ad-hoc network

- Military and survivability:
  - The Three Rs: Resistance, Recognition, and Recovery [8]
  - Multimodal operation
  - Auto-configuration
- Support Anonymity:
  - Anonymous routing protocol [9]: based on onion routing concept used in wired networks
- DOS attack

DOS attack in Ad-hoc network

- **Damage of successful DOS:**
  - quantifying resilience in Ad-hoc network [5]
  - Simulation models:
    - Closed-loop attack: Jelly-fish
      - Packet misordering
      - Periodic dropping
      - Delay variance
    - Open-loop attack: Black-hole
  - Relationship of resource controlled by attacker and performance (goodput and systemwide fairness) impact on the network

Security requirement in Ad-hoc network

- Different types of DOS attack:
  - Black-hole attack and TCP compliance attacks
  - Rushing attack
  - Route-request-flooding attack
- Research on methods against DOS attack:
  - Passive ACK (PACK) [23], watch-dog mechanism [24], blacklisting [7]
  - Rushing Attack Prevention (RAP) [6]
  - Prevent against route-request-flooding attack [7]

Price-based approach in Ad-hoc network

- Problem:
  Motivate user's cooperation and eliminate malicious nodes
- Price-based approach
- Research works:
  - Virtual money [10]
  - Watchdog and pathrater [13]
  - CONFIDANT [12]: a neighborhood monitor, a trust manager, a reputation system, a path manager
- Future research

Talk outline

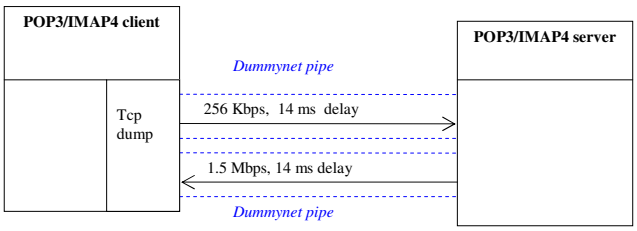
- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

Experiment on spam consumption

- Motivation:
  - To study the effect of different email retrieving methods on spam traffic consumption
  - To study the financial implication of spam
- Experimental Testbed:
  - Software/tools used:
    - Courier 0.45.4 PO3/IMAP4 server
    - Getmail 4.3.6 POP3/IMAP4 mail client
    - Ipfw/dummynet
    - Tcpdump 6.6.0
    - Tcptrace
    - Author's traffic plot sofware for tcpdump files
    - Matlab6.5

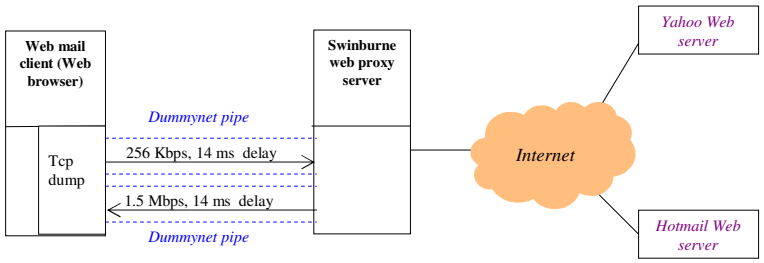
Experiment on spam consumption

- Testbed setup:

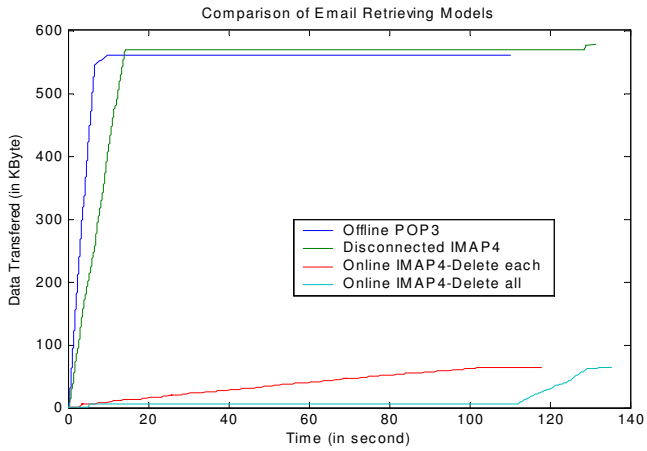


Experiment on spam consumption

- Testbed setup:

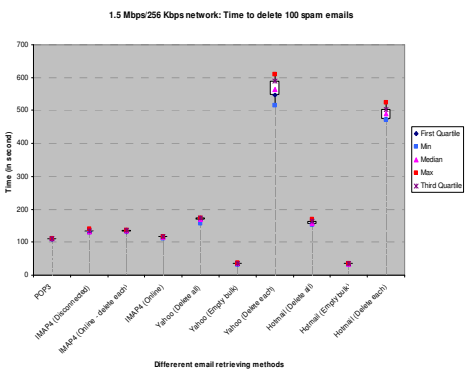


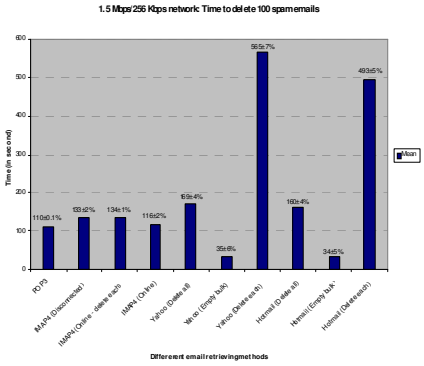
Experiment on spam consumption



Experiment on spam consumption

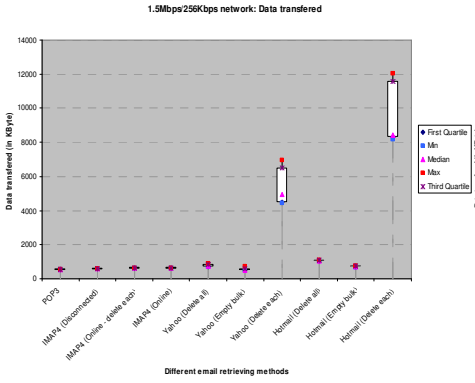
'Time to read and delete spam emails' Comparison

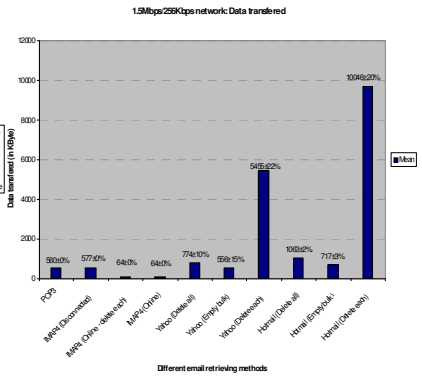




Experiment on spam consumption

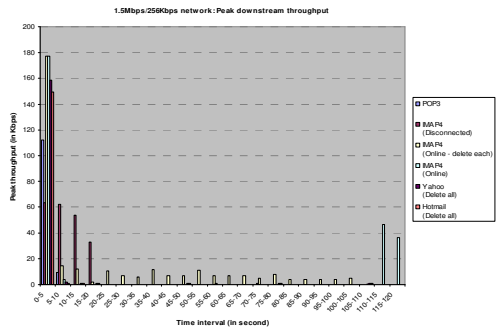
Data Transferred Comparison

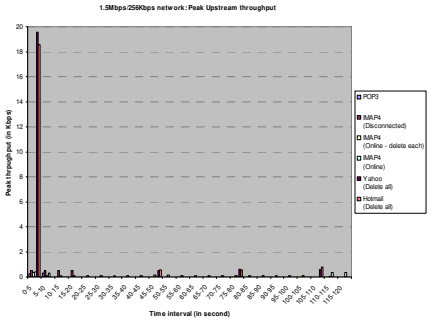




Experiment on spam consumption

Peak Downstream and Upstream Throughput Comparison

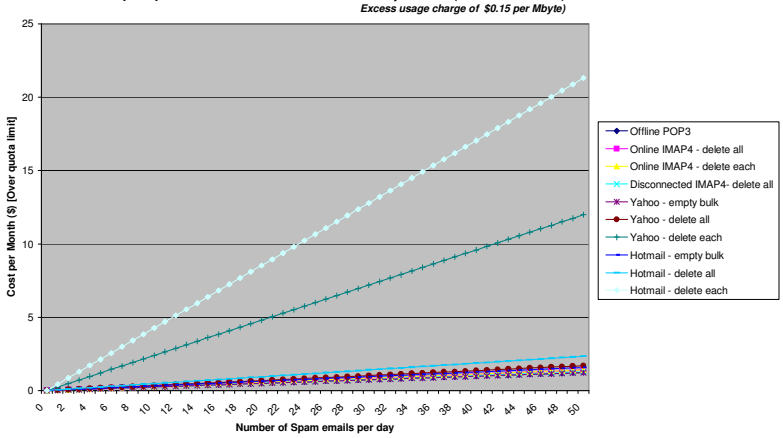




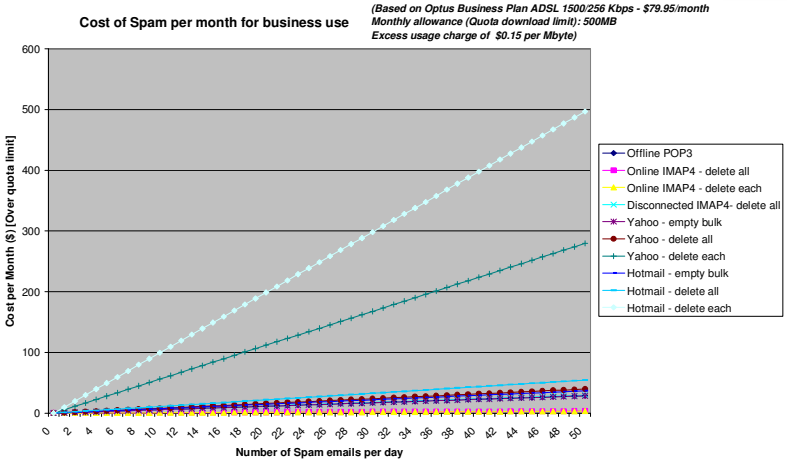
Experiment on spam consumption

Cost of Spam per month for residential use

(Based on Telstra BigPond Residential Plan ADSL 1500/256 Kbps - $79.95/month
Monthly allowance (Quota download limit): 500MB
Excess usage charge of $0.15 per Mbyte)



Experiment on spam consumption



Talk outline

- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

Conclusion

- Review the architecture challenges of IP network, which allows for a wide range of IP-based services' incontrollable consumption
- Protect excessive network consumption: cost-based and resilient protocols, algorithms, techniques
- Challenges of coupling between network resource consumption and the ability of controlling arbitrary hosts' access to the network

Talk outline

- Introduction
- Spam and anti-spam
- Denial-Of-Service attack
- Ad-hoc network security issue and price-based approach
- Experiment on spam consumption
- Conclusion
- References

References

1. M.Hanley and A.Greenhalgh, Steps Towards a DoS-resistant Internet Architecture, Sigcom 2004 Workshop
2. W. Feng. The case for TCP/IP puzzles, Proceedings of the ACM SIGCOMM workshop on Future directions in network architecture 2003
3. D. W. Tom Anderson, Timothy Roscoe. Preventing internet denial-of-service with capabilities, ACM SIGCOMM Computer Communication Review Volume 34 , Issue 1 (January 2004), Pages: 39 - 44
4. K. Lakshminarayanan, D. Adkins, A. Perrig, and I. Stoica. Taming IP packet flooding attacks, ACM SIGCOMM Computer Communication Review archive Volume 34 , Issue 1 (January 2004), Pages: 45 - 50
5. M. Hejmo, B. Mark, C. Zouridaki and R.K. Thomas, Denial of Service Resilience in Ad Hoc Networks, SASN 2004
6. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of WiSe 2003*, September 2003.
7. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks.
8. J. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R.Ramanathan, and J. Zao, Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions

References

9. A. Boukerche, K.El-Khatib, L.Xu, L. Korba, A Novel Solution for Achieving Anonymity in Wireless Ad hoc Networks, PE-WASUN 2004
10. L. Buttyan and J. Hubaux, Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, Mobile Networks and Applications 8, 579–592, 2003
11. Yih-Chun Hu, Adrian Perrig, and David B. Johnson. Efficient security mechanisms for routing protocols. In Network and Distributed System Security Symposium, NDSS '03, February 2003.
12. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes — Fairness In Dynamic Ad-hoc Networks, Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing
13. S. Marti, T.J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (Mobicom), Boston, MA (August 2000).
14. L. H. Gomes, C. Cazita, J. M. Almeida, V. Almeida, W.Meira, Characterizing a Spam Traffic, IMC 2004
15. Quantitative Assessment of IP Service Quality in 802.11b Networks Thuy T.T. Nguyen, Grenville J. Armitage, Proc. 3rd Workshop on the Internet, Telecommunications and Signal Processing, December 2004

References

16. An Evaluation of Statistical Spam Filtering Techniques, L.Zang, J.Zhu, T.Yaho, Natural Language Processing Laboratory, Institute of Computer Software & Theory Northeastern University, China
17. L. Bertolotti and M. C. Calzarossa, “Models of mail server workloads,” Performance Evaluation, vol. 46, no. 2-3, pp.65–76, September 2001
18. L. Bertolotti and M. C. Calzarossa, “Workload characterization of mail servers,” in *Proc. SPECTS 2000*, Vancouver, Canada, July 2000.
19. R. D. Twining, M. M. Willianson, M. Mowbray, and M. Rahmouni, “Email prioritization: Reducing delays on legitimate mail caused by junk mail,” in *Proc. Usenix Annual Technical Conference*, Boston, MA, June 2004
20. L. F. Cranor and B. A. LaMacchia, “Spam!,” *Comm. of the ACM*, vol. 41(8), pp. 74–83, August 1998.
21. J. Jung, E. Si, An Empirical Study of Spam Traffic and the Use of DNS Black Lists, IMC’04
22. http://www.tech-faq.com/dos-denial-of-service-attack.shtml

23. David B. Johnson and D. Maltz. The dynamic source routing protocol for mobile ad hoc networks (DSR), April 2003
24. Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker, Mitigating routing misbehavior in mobile ad hoc networks, Mobile Computing and Networking, pages 255–265, 2000.