Justin P. Rohrer
rohrej@ku.edu
EECS-800: Wireless Security
2006.12.12

SECURITY IN HETEROGENEOUS NETWORKS: GENERIC SECURITY PROTOCOL

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Introduction

- Looking at Heterogeneous networks in the context of the next-generation Internet
- Will certainly be more diverse than current Internet
- Needs a unified approach to security
- Security policy needs to be communicated beyond trust boundaries
- Work based on *proposed* architecture, details not yet defined

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Background

- This work is an extension of Postmodern Internetwork Architecture (PoMo),
- Funded by NSF under NeTS-FIND 10/2006
- Unconstrained by backward-compatibility issues
- Considers security to be a fundamental requirement for each network component

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Security Categories

- Authentication
  - Use existing methods
- Collaboration Incentives
  - Network access treated as privilege which can be lost due to misbehavior
  - Current mindset difficult to change
- Denial of Service Prevention
  - Can be malicious or accidental
  - Needs continued research

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Related Work

- Two categories of DOS avoidance research
  - Improved resource management
  - Attack prevention
- Each approach addresses a specific scenario
  - 3G cellular multicast
  - 3G cellular scheduling
  - Cellular SMS
  - (Cellular is a popular topic)

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Environmental Model

- PoMo consists of the basic elements *links*
- *Links* interconnect *nodes*
- *Nodes* may be single devices or entire sub-networks defined recursively
- These virtual nodes are referred to as *realms*
- *Realms* are separated from one-another by trust/policy boundaries
- Centralized administration with trusted resources
- Unforgeable return path for each packet

Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Design: Goals

- Generic Security Protocol (GSP) [1]
- Unify policy implementation
- Facilitate inter-domain policy communication
- Enhance performance, resilience, and survivability of the network as a whole

Design: Proposed Solution

- Protocol which operates within network stack
- Roughly layer 4.5
- Relies on PoMo Internetwork layer and below
- Required for all realms, but not every individual node
- Placement comparable to BGP

Design: Framework

- Security Agent (SA) run within each realm
- Security Client (SC) optionally run on end nodes
- Security Packets (SP) carry information between entities

Design: Security Agents

- Centralized or distributed within realm
- Run on devices associated with security
  - Gateways
  - Firewalls
  - Intrusion Prevention Systems
- Policy defined around links
- Policy distributed to all SA in realm
- Events trigger response based on policy

Design: Security Clients

- Receives relevant policy info from SA within own realm
- Communicates upwards with application and/or user
- Optional implementation on given end node

Design: Security Packets

- Packet format with fields needed by GSP
  - Authentication (Both source and message contents)
  - GSP code
  - Content field for user customizable data
- Encapsulated in PoMo packet which provides source, destination, and routing/forwarding info

Design: Security Domains

- Intra-Realm
  - Implement unified policy
  - Coordinate security measures (and appliances)
- Inter-Realm
  - Communicate policy to other realms on as-needed basis
  - SP's prioritized above other traffic to ensure delivery even in DOS scenario

Security of GSP

- GSP has potential to become liability if exploited
- Public key encryption used for authentication
- SP's examined at injection and every trust boundary
- Details left to future work, must be bulletproof prior to mass deployment

Overview

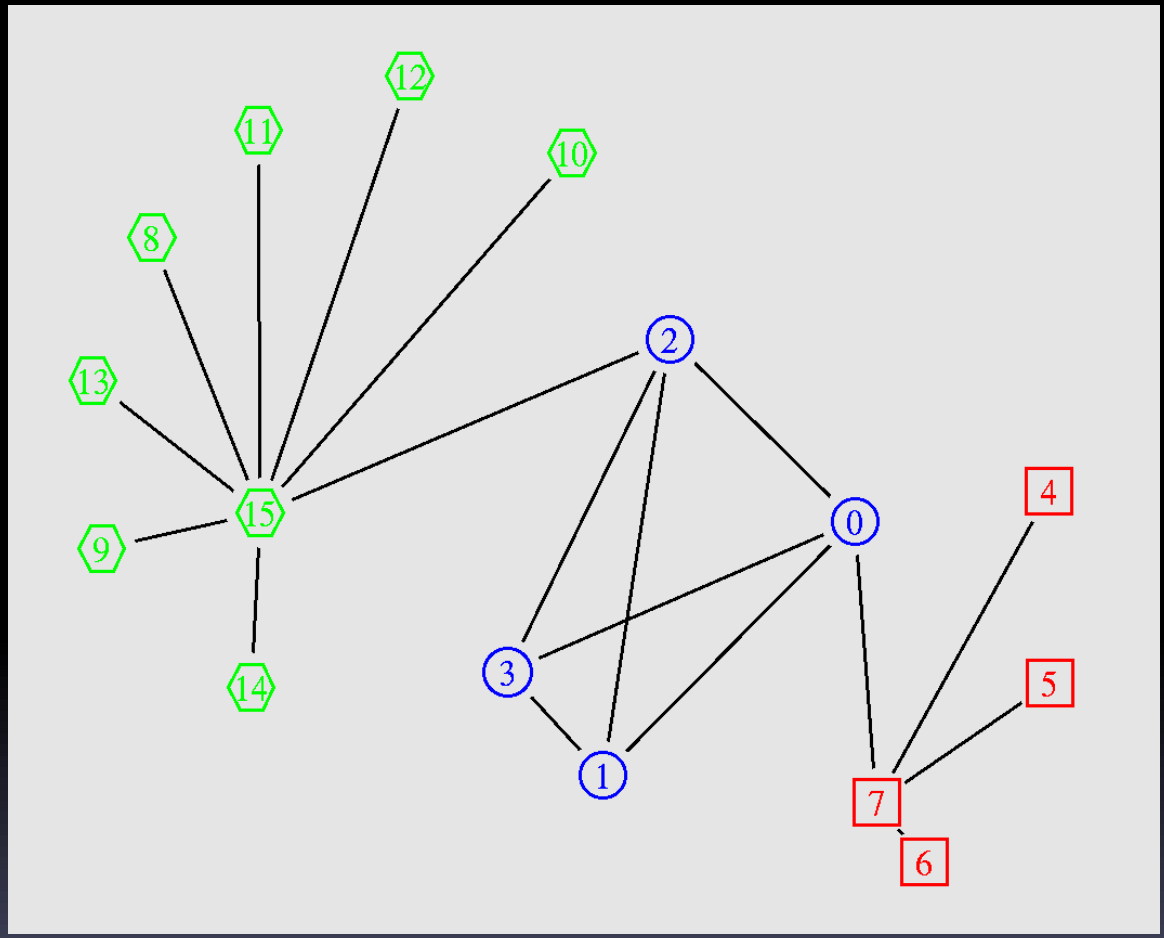
- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

Simulations

- ns-2, three realms with different bandwidth links
- duplex links with drop-tail queuing
- Legitimate traffic simulated with PackMime traffic generator
- Misbehaving traffic simulated using single CBR stream

Simulations

- Green nodes on low bandwidth network
- Blue nodes high-bandwidth core
- Red nodes server farm
- Well behaved HTTP 1.1 traffic generated at rate of 1 request per node per second

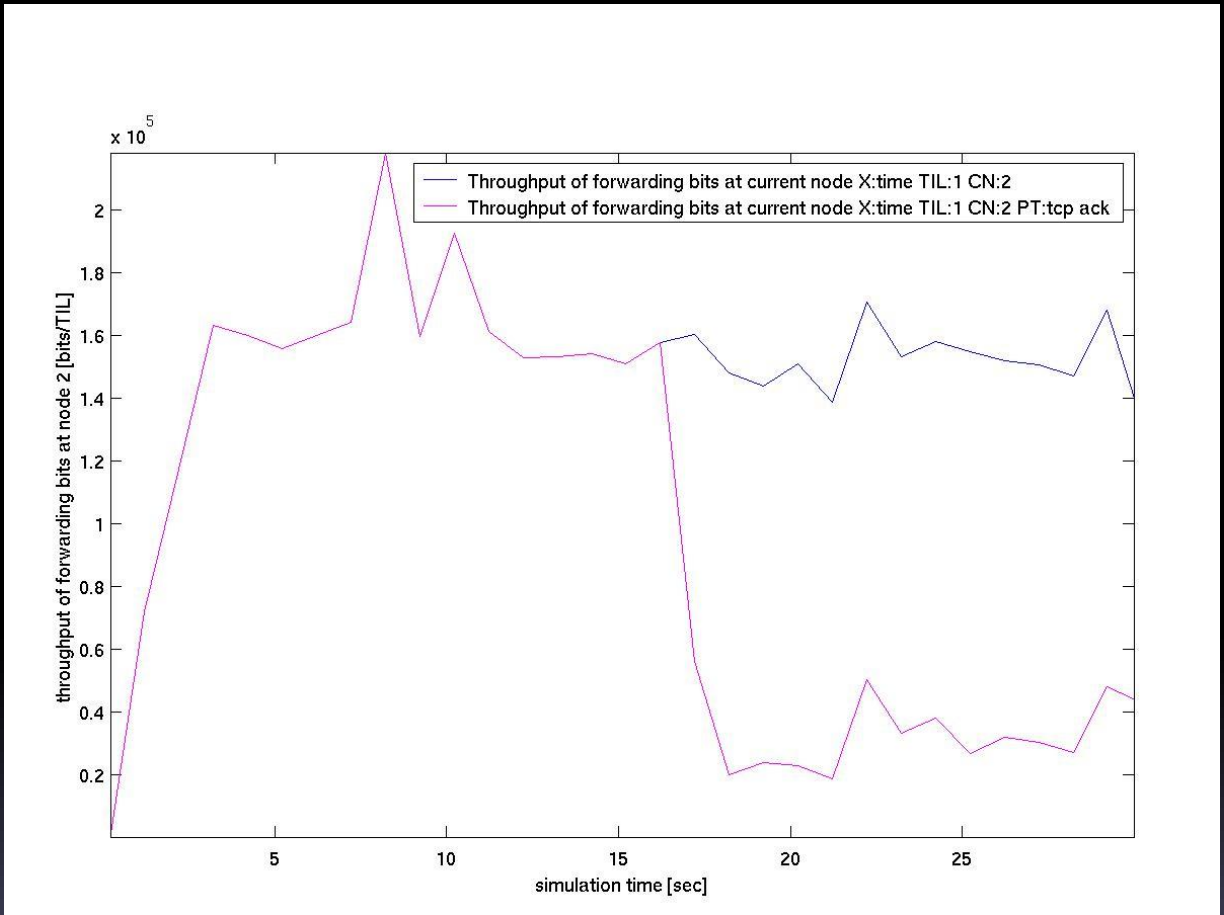


Overview

- Introduction
- Background
- Security Categories
- Related Work
- Environmental Model
- Design
- Simulations
- Results
- Conclusion

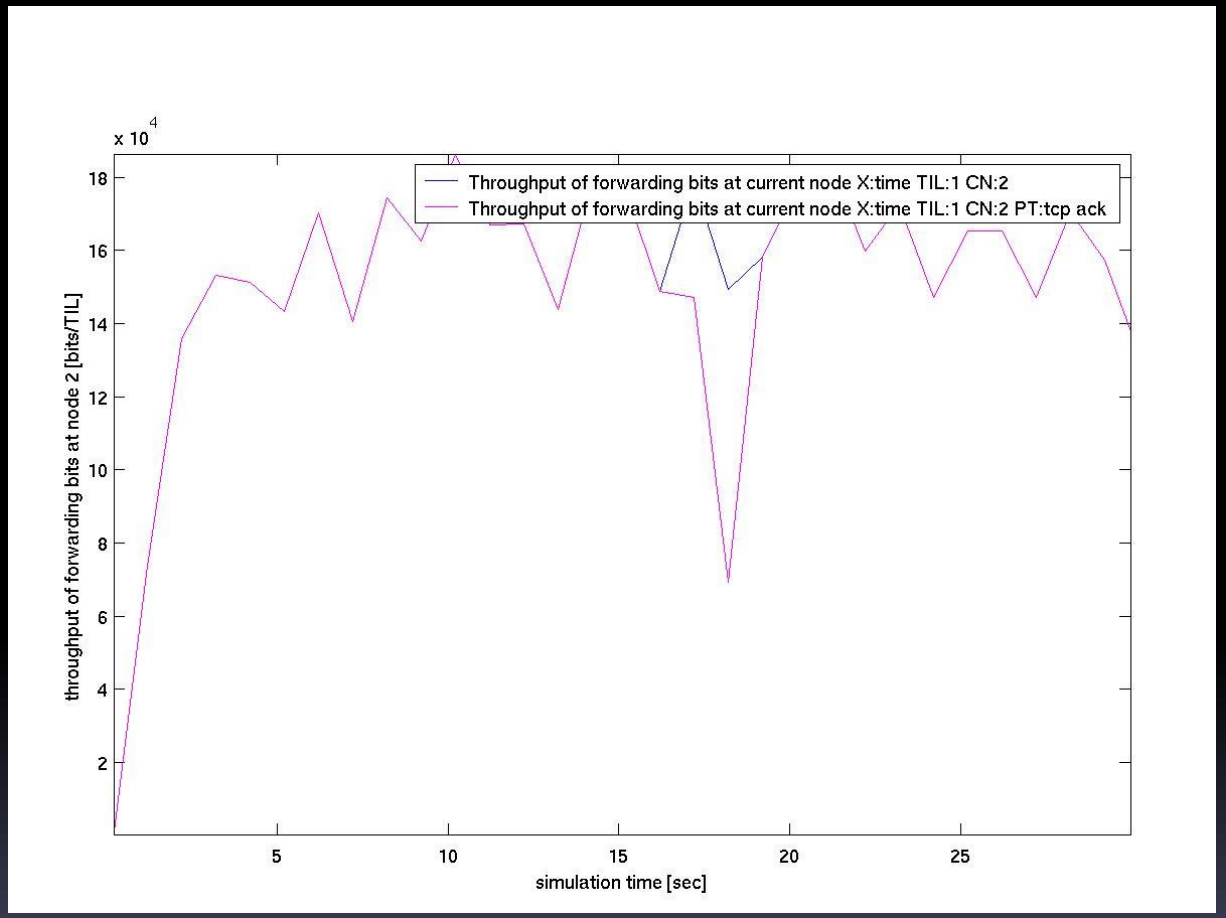
Results: Without GSP

- Node 15 acts as ordinary firewall
- Graph shows goodput on link 2-15
- CBR stream starts at about 16s
- Poor performance due to both DOS and TCP backoff



Results: With GSP

- Node 15 is a firewall with a SA
- Signals node 7 when CBR stream is detected
- Misbehaving traffic blocked at source
- Goodput returns to normal after brief downward spike



Conclusions

- Simulation limited in scope, intended to show power and flexibility of approach
- Could have been a spam flood or SSH brute force attack being block
- Many more scenarios to simulate, whole PoMo project in infancy
- Most difficult aspect will be ensuring that GSP cannot be exploited

Questions

References

- [1] Evans, J.B., Wang, W. and Ewy, B.J. (2006) 'Wireless networking security: open issues in trust, management, interoperation and measurement', *Int. J. Security and Networks*, Vol. 1, Nos. ½, pp. 84-94
- [2] Bhattacharjee, B., Calvert, K., Griffioen, J., Spring, N., and Sterbenz, J. (2006) 'NeTS-FIND: Postmodern Internetwork Architecture', *NSF Proposal*, Funded 10/2006

References Cont.

- [3] Durst, R.C., Miller, G.J., Travis, E.J., 'TCP Extensions for Space Communications', *Proceedings of the 2nd annual international conference on Mobile computing and Networking,* pp. 15 - 26, ACM Press, November 1996, ISBN:0-89791-872-X
- [4] Burleigh, S., Hooke, A., Torgerson, L., Fall, K., Cerf, V., Durst, B., Scott, K., Weiss, H., 'Delay-Tolerant Networking: An Approach to Interplanetary Internet', *Communications Magazine*, IEEE, Volume 41, Issue 6, June 2003 pp. 128 - 136

References Cont.

- [5] Bhargava, B., Wu, X., Lu, Y. and Wang, W. (2004) 'Integrating heterogeneous wireless technologies: a cellular-assisted mobile ad hoc networks', *Mobile Network and Applications*, Vol. 9, No. 4, pp.393-408
- [6] Wang, W., Liang, W. and Agarwal, A. (2005) 'Integration of authentication and mobility management in third generation and WLAN data networks', *Journal of Wireless Communications and Mobile Computing*, Vol. 5, No. 6, pp.665-678

References Cont.

- [7] Yang, H. and Lu, S. (2002) 'Self-organized network layer security in mobile ad hoc networks', *Proceedings of the First ACM Workshop on Wireless Security (WISE)*, pp.11-20
- [8] Lamparter, B., Paul, K. and Westhoff, D. (2003) 'Charging support for ad hoc stub networks', *Journal of Computer Communication, Vol. 26, No. 13, pp. 1504-1515*

References Cont.

- [9] Ben Salem, N., Buttyan, L., Hubaux, J-P. and Jakobsson, M. (2003) 'A charging and rewarding scheme for packet forwarding in multi-hop cellular networks', *Proceedings of Forth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc),* pp.13-24
- [10] Bhatia, R., Li, L.E., Luo, H. and Ramjee, R. (2006) 'ICAM: integrated cellular and ad-hoc multicast', *IEEE Transactions on Mobile Computing, Vol. 5, No. 8, pp. 1004-1015*

References Cont.

- [11] Soahant Bali All Hands Meeting Presentation at ITTC 2006.11.09
- [12] Traynor, P., Enck, W., McDaniel, P., and La Porta, T. (2006) 'Mitigating attacks on open functionality in SMS-capable cellular networks', *Proceedings of the 12th Annual international Conference on Mobile Computing and Networking (MobiCom)*, pp. 182-193

References Cont.

- [13] Enck, W., Traynor, P., McDaniel, P. and La Porta, T. (2005) 'Exploiting open functionality in SMS-capable cellular networks', *Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS)*, pp.393-404