Autonomic Security Management in Dynamic Networks

Jianguo DING

Jianguo.Ding@uni.lu
SnT, Univ. of Luxembourg

Oct. 18, 2010

Dynamic networks

- Dynamic structures (space change)
  - Mobile/wireless networks
    - Mobile devices
    - Mobile users
    - Mobile servers
    - Mobile transactions
  - Mobile Internet
  - Overlay (virtual) networks
- Dynamic applications
  - Dynamic transactions
  - Stochastic interoperation between peers
- Dynamic functions
  - communications/storage
  - Dynamic peer computing
- Network evolution (time change)
  - Unique evolution
  - Heterogeneous networks

Dynamic Networks Examples

- Wireless networks
- Mobile ad hoc networks
  - Wireless sensor networks
  - Vehicle networks
  - Body networks
  - …
- Overlay networks
  - VPN
  - P2P
  - Social networks

Technical advances in dynamic networks (Emerging computing models)

- Nomadic computing
  - Mobile terminals (devices)
  - Mobile services
  - Nomadic users
  - Dynamic communications

- Context-aware and autonomic computing
  - Mobile mechanism
  - Intelligent and adaptive services
  - Autonomic communication
    - human to human
    - human to machine
    - machine to machine
  - Autonomic decision

- Opportunistic computing
  - Dynamic situations
  - Plug-in and plug-out services
  - Reliable services in unreliable environments
- Cognitive computing
  - Self-learning and reasoning
  - Self-* (self-managing, self-optimizing, self-monitoring, self-repairing, self-protection, self-adaptation, self-healing, etc.)

Security challenges in dynamic networks (vs. traditional networks) (1)

- Vulnerable systems
  - Wireless medium
  - Lack of central coordination
  - Unprotected routing in multicasting and multi-hop communication
- Threatened networks
  - Less robust systems
  - Increased applications and attacks

Security challenges in dynamic networks (2)

- Uncertainty
  - Deficient observation
  - Uncertain dependency verification
  - Mis-interpretation
- Limited computing (energy resouces)
- Dynamic topologies
- Scalable networks
- Dynamic key management

Typical attacks for dynamic networks (1)

- External attack vs. internal attack
- Passive attacks
  - Eavesdropping
  - Traffic analysis & monitoring
- Active attack
  - MAC layer attack
    - Jamming attack
  - Network layer attack
    - Wormhole
    - Blackhole
    - Byzantine
    - information disclosure
    - Resource consumption
    - Routing
    - IP spoofing
    - Sybil
    - State pollution
    - Fabricate
    - Modification

Typical attacks for dynamic networks (2)

- Active attack (cont.)
  - **Transport layer attack**
    - Session hijacking
    - SYN flooding
  - **Application layer attack**
    - Repudiation
    - Data corruption
  - **Miscellaneous attack**
    - Denial of service
    - Impersonation or spoofing
    - Device tampering
    - Flooding
    - Gray hole
    - Colluding misrelay
    - Location disclosure
    - Link spoofing
    - Neighbour
    - Jellyfish

Autonomic security management

- Self-protection
  - Self-prevention
  - Self-detection
  - Self-reaction
- Context-aware
- Proactive
- Resilient
- Dynamic computing models
  - Autonomic computing
  - Cognitive computing
  - Opportunistic computing

Aim at establishing autonomic security management framework and self-protection system for dynamic networks

Objectives

- Investigate the principles of dynamic changes and uncertain factors in dynamic networks
- Quantitative dependency measurement mechanism between key security factors
- Setup optimized architecture/schemes for autonomic security management
- Research autonomic and resilient security strategies for dynamic networks
- Empirical research for autonomic security management

Available for Cooperation

- Hope to join new research areas
- Eager to be involved in related projects
- Look for opportunities to cooperate with intern & extern colleagues

Thank you!