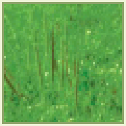
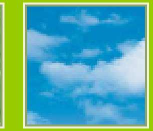



Network Security:
Making the Network Intelligent

BCS SGAI Symposium on Intelligence in Security and Forensic Computing

Edinburgh, 3rd April 2006

Dr. Bob Askwith

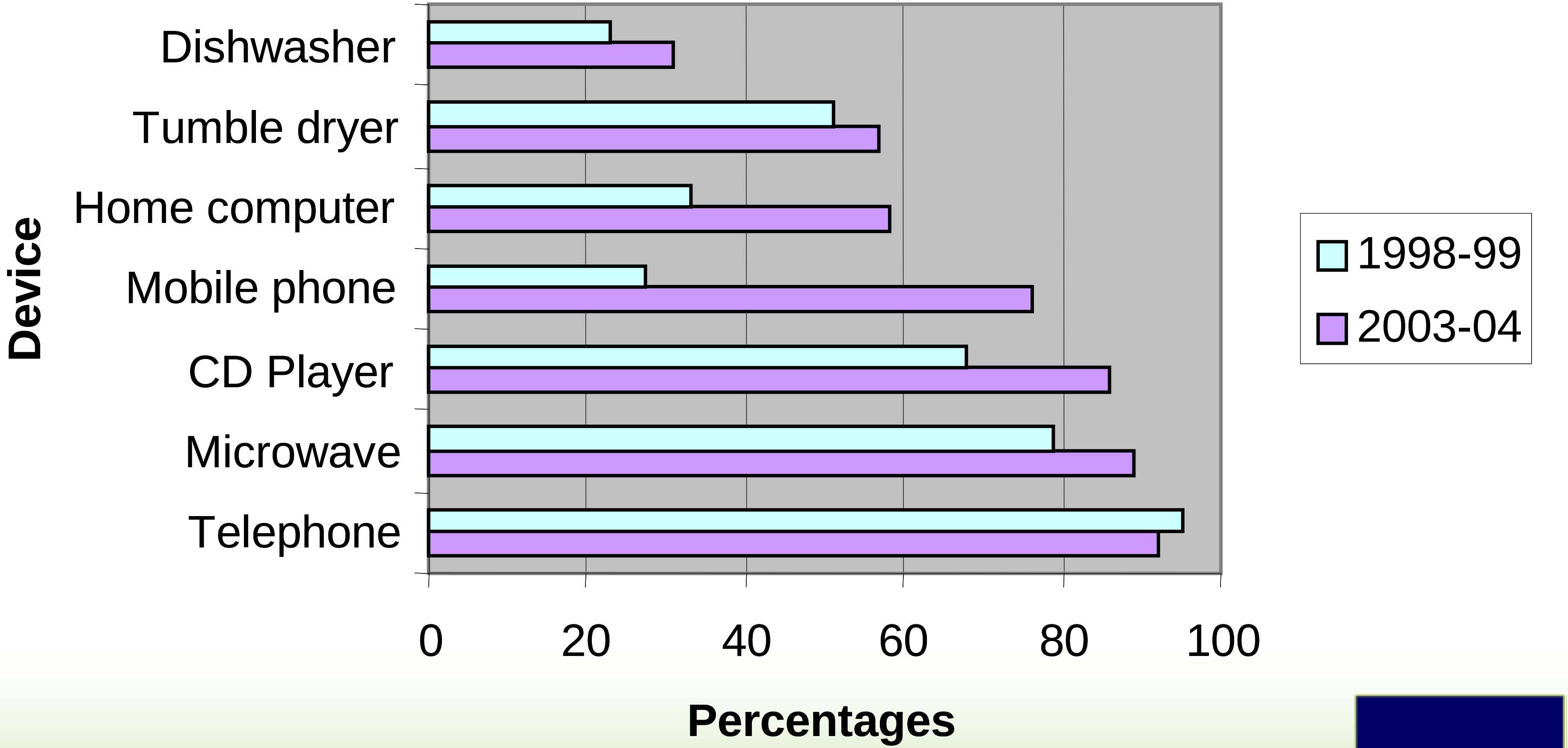
School of Computing and Mathematical Sciences
Liverpool John Moores University
Byrom Street, Liverpool L3 3AF

R.J.Askwith@ljmu.ac.uk
http://www.cms.livjm.ac.uk/PUCsec/

Overview

- Trends in computing
  - New applications
  - New environments
  - Security issues persist
- Current security approaches
  - Models for security are not coping
  - Too little flexibility
  - Too much effort required
- Making the network intelligent
  - Responsibility on nodes to become more involved
  - Responsibility on network to become more cooperative
- Example proposal
  - Distributing knowledge for DRM

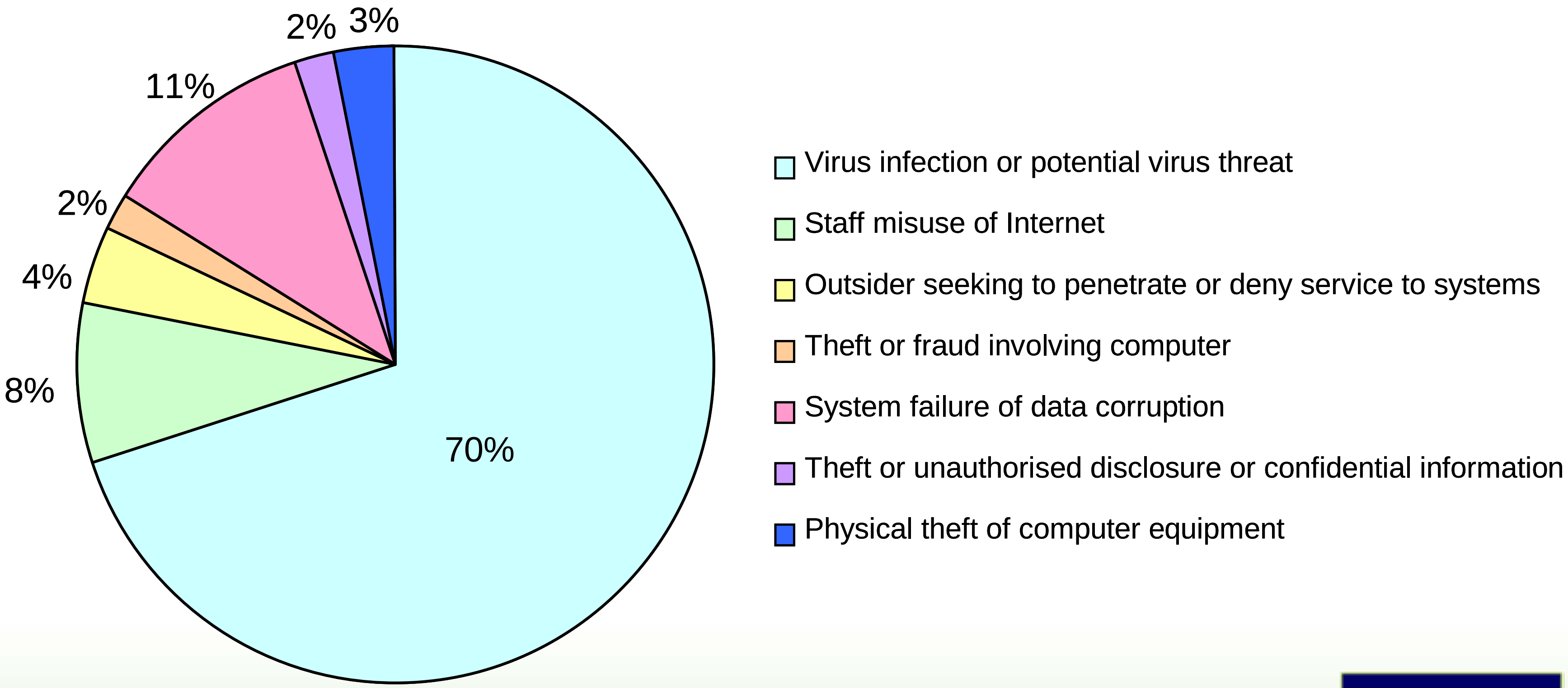
Usage of consumer durables



Changing nature of computing

- Increase in number of units
  - From one per several persons
  - To several per person
- Diversification in type of device
  - From desktop PCs and workstation terminals
  - To smart phones, PDAs, and MP3 players
  - Further ahead; all consumer devices may allow networked control
  - Even further ahead; sensor networks to enable pervasive computing
- Change in security?
  - Insider threat still the most serious
  - Viruses the most prolific
  - Patch management is increasingly time consuming
  - Requires skilled administrators to handle
  - Is any progress being made?

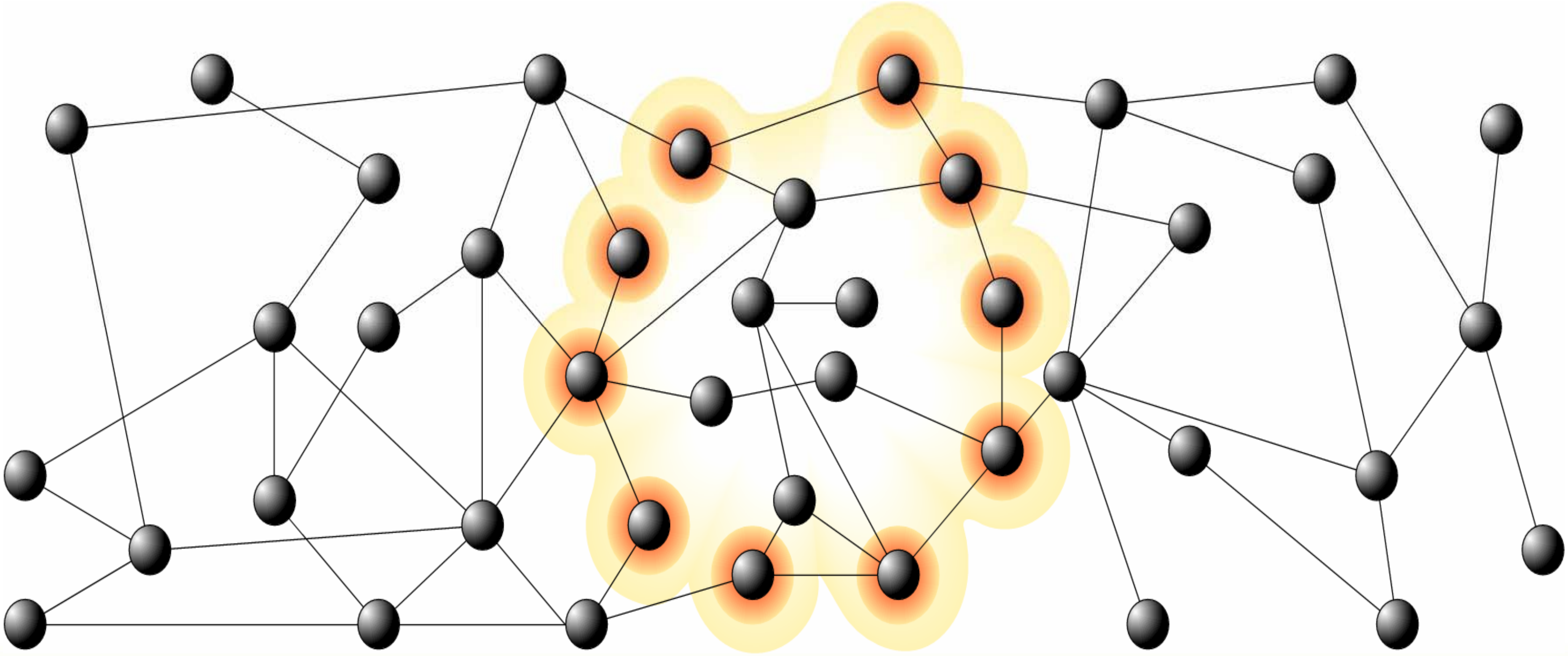
Security incidents in business



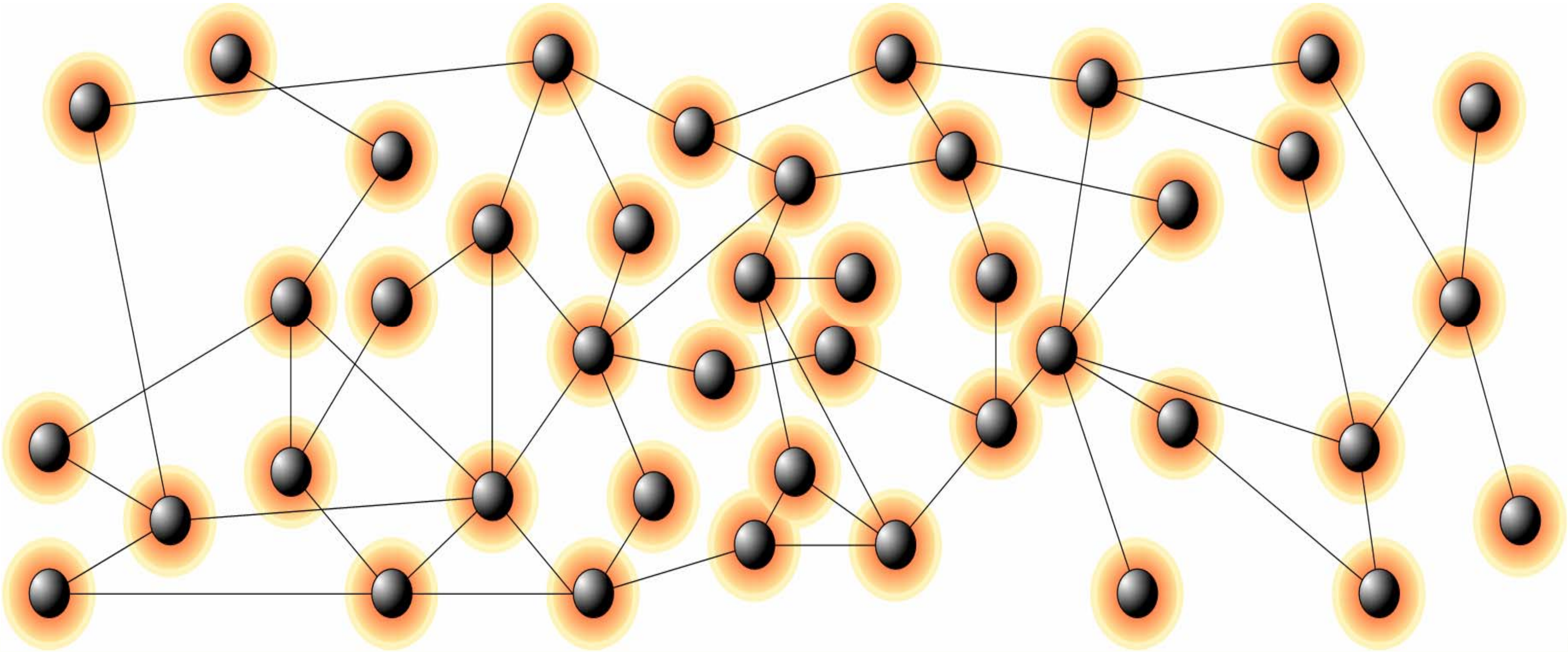
How is security tackled

- Perimeter model
  - Inside the perimeter is trusted
  - Concentrates effort into monitoring at the perimeter
  - Firewalls and Intrusion Detection Systems
  - Has not solved the network security problem
- Atomic model
  - Each node is responsible for its security, e.g. home computer
  - Blunt; all machines expend considerable effort
  - Assumption that security can be handled per node
- Bulkhead model
  - Somewhere in between the perimeter and bulkhead model
  - Security is handled on some nodes only which protect others
  - Careful distribution required to create the best balance

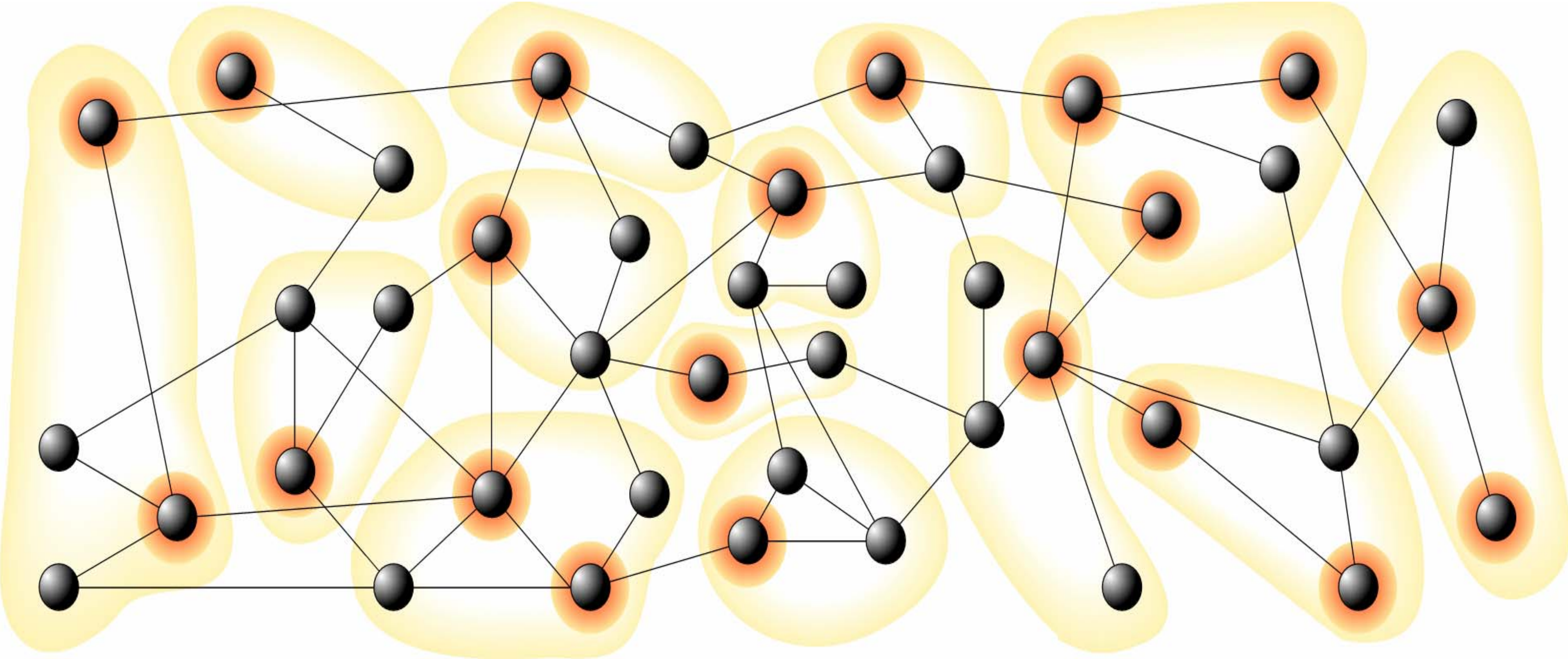
Perimeter Model



Atomic Model



Bulkhead Model

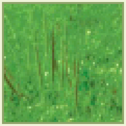
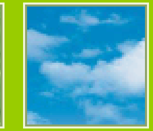


Intelligent network

- The existing models don't make the best use of the network
- This is problematic for pervasive computing
  - Many, or most, nodes cannot work in atomic model
  - Perimeter model not appropriate
  - Perimeter and bulkhead assume some level of organisation
- Challenge: can we distribute the functionality of security across the network?
- Example using cellular automata
  - Cells in a grid, each is connected in a network to direct neighbours
- Game of life
  - If less than two live neighbours, cell is lonely and dies
  - If four or more live neighbours then cell is crowded and dies
  - If cell has three alive neighbours then comes to life
  - Successive steps generate an emergent behaviour

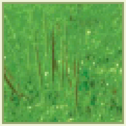
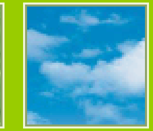
Application to networking

- Assign neighbours to each node in a network
  - Can easily be done as part of a distributed joining protocol in ad hoc or peer to peer network
- All nodes share state with neighbours
- Define rules to allow reaction to neighbours state and change own state
- Advantages
  - Each node is only performing part of the overall process
  - Simple processing can lead to complex systems
  - Sharing and cooperation can uncover network wide problems
- What sort of mechanisms could this be applied to?
  - Virus checking
  - Digital Rights Management (DRM)

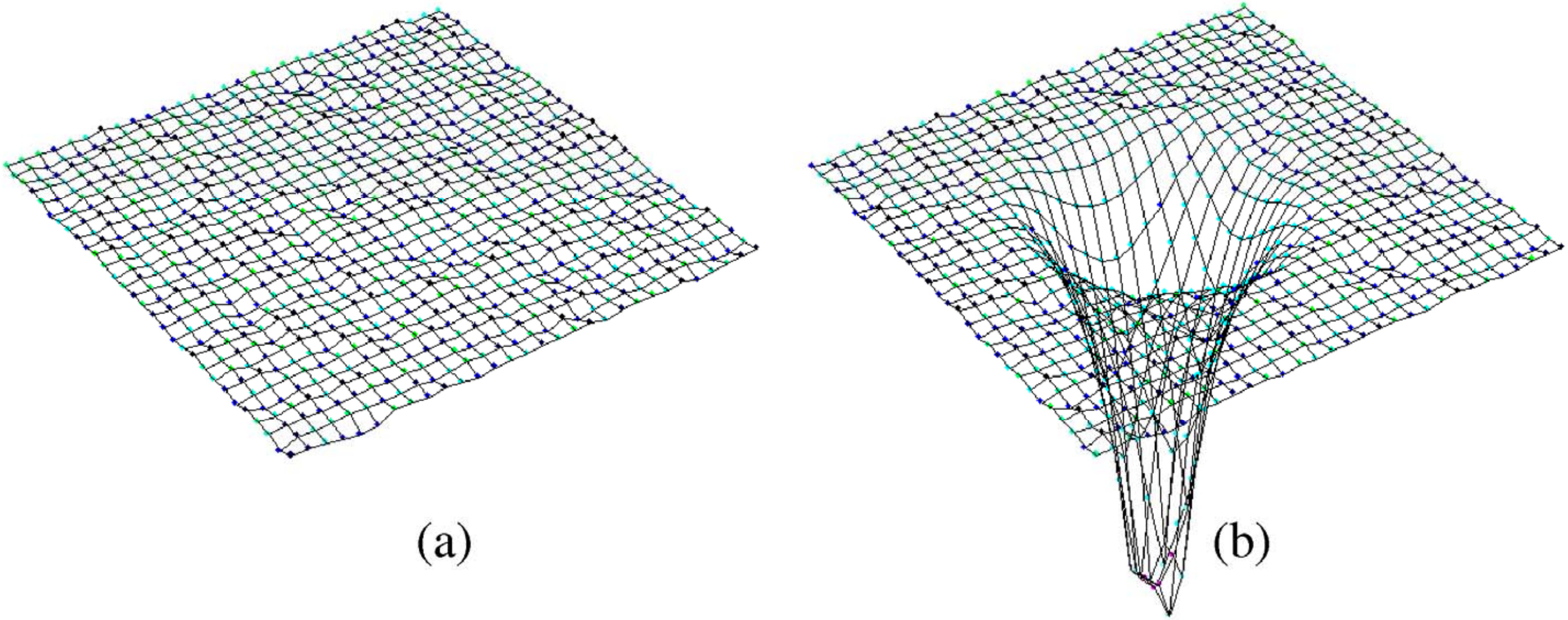



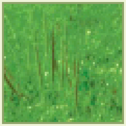
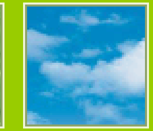
Community Security Mechanism

- Each node has a security state
- Level goes up or down depending on neighbours state
- Rate of change used to assign trust level to neighbours
- Laplace differential equation used to calculate overall position
- Security level is modelled as height
- Trust as a downward force on the node
- Network links take on ‘elastic’ property
  - If links are stretched they pull back

Effect of sharing

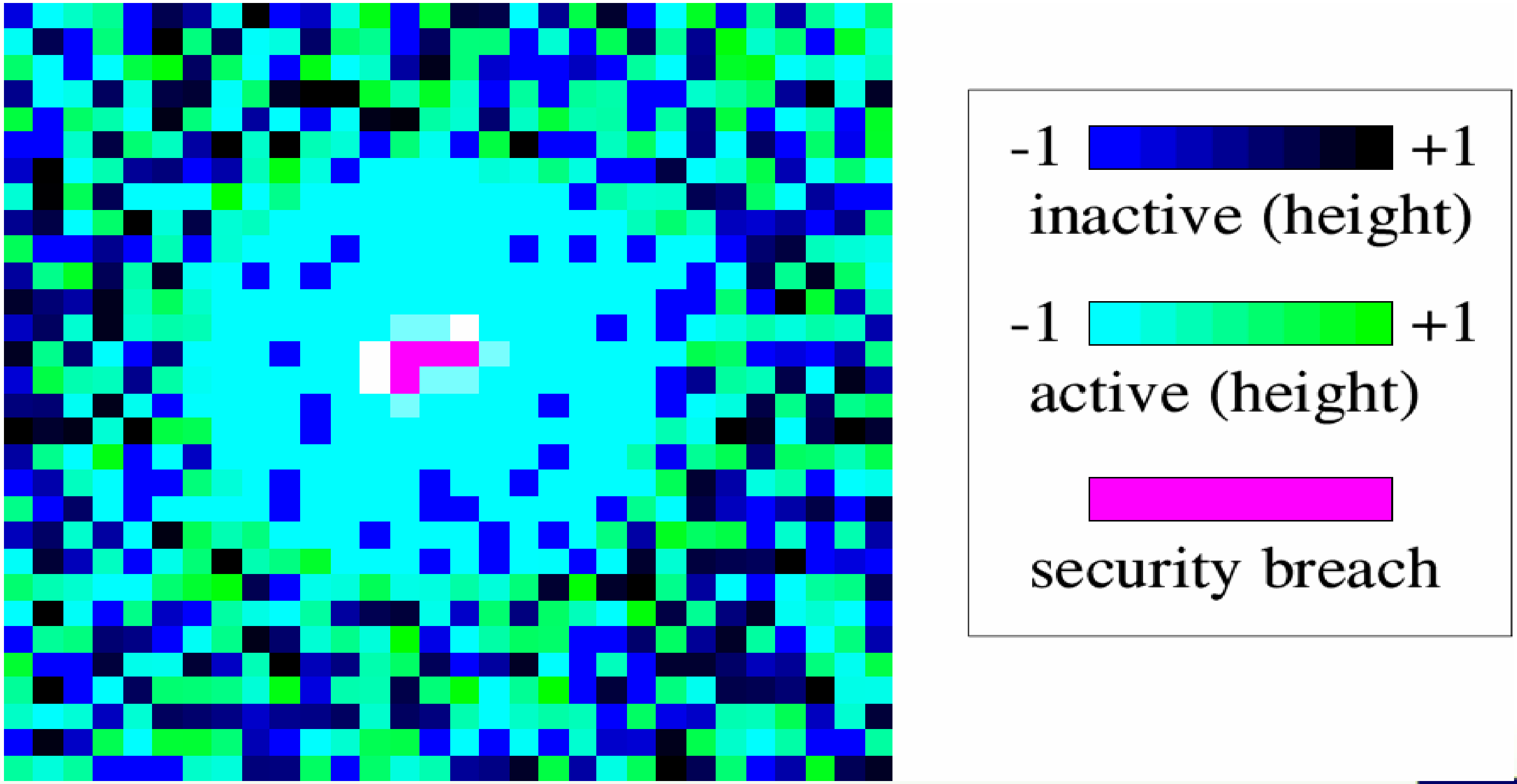


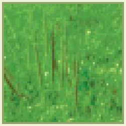
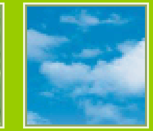



Applying mechanism to DRM

- Community of users operate a cellular automata layer
- Nodes check proportional amounts of network traffic
  - i.e. perform DRM checking on that part of the stream
- Change security and trust levels accordingly
- Neighbours propagate information locally
- Amount of checking scales locally
  - More checking if neighbours are unsafe
  - Less checking is neighbours are safe
- More checking may result in more problems being noticed
  - This is likely if a node is malicious or compromised
- The process isolates unsafe nodes

Isolation of compromised nodes

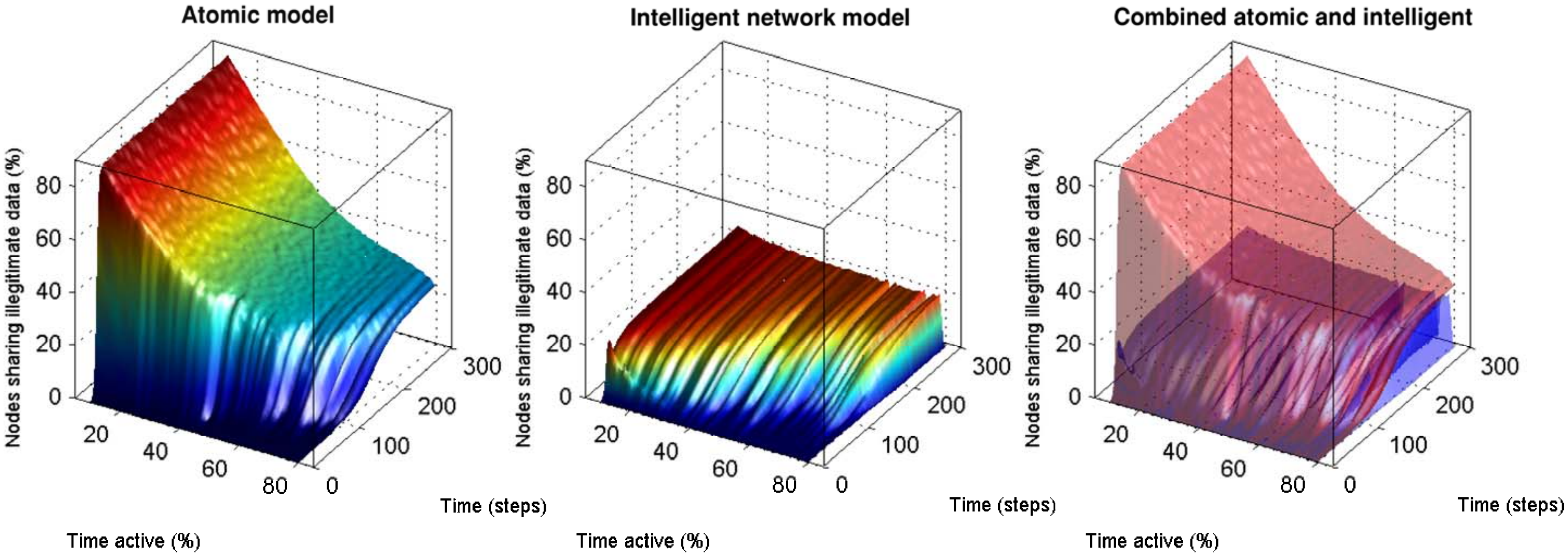


Simulation results

- Tests conducted by varying the parameters for
  - Number of nodes
  - Amount of illegitimate data
  - Amount of checking
- Using 85% checking the system is highly reliable
- Lowering the checking to 20% results become similar to atomic model
  - Saving 80% of checking!
- Self-enforcement could be better than tight controls from content providers
  - Controls are controversial
  - Acceptance of some loss may be inevitable
  - Cost to implement may be lower

Simulation results comparison



Summary

- Computing continues to change dramatically
- Internet has played a major role in the last decade
- Pervasive computing looks likely to follow…
  - Heterogeneous, resource contrained
- Security has got **worse** with increased communications
- Traditional perimeter model has been limited
- Atomic model could prove inefficient
- ‘Intelligent’ middle ground?
  - Example using cellular automata
  - DRM example isolates misbehaving nodes
  - Nodes assess neighbours and react to trust levels
  - Results suggest less processing for similar effect as atomic model
  - Potential for detection of security through ‘emergent behaviour’